Oracle® Auto Service Request

ASR Manager User's Guide

Release 5.5.1 for Linux and Solaris

E18475-39

January 2016

ORACLE®

Oracle Auto Service Request ASR Manager User's Guide, Release 5.5.1 for Linux and Solaris

E18475-39

Contents

5 ASR General Troubleshooting

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 that have purchased support 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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's Changed

This table provides a brief overview of the document changes for the latest publication of the *Oracle® Auto Service Request Installation and Operations Guide*:

Part Number	Change Summary
E18475-39	Minor correction in Setup and Overview in Appendix A, "Other ASR Manager Administration."
E18475-38	Updated the list of Features and Enhancements for Oracle ASR Release 5.5. Updated Configuring ASR Manager to Use a Proxy Server. Added a new troubleshooting item: Diagnostics Bundle Collection Fails.
E18475-37	Updated the list of Features and Enhancements for Oracle ASR Release 5.4. Added a section to address Oracle ASR Security. Added a section for ASR Manager on IPv6. Added a new ASR_INSTALL_FAILED_NOT_ENOUGH_SPACE error code, including a problem description and resolution.
E18475-36	Updated the steps in Managing SNMP Trap Destinations for Service Request Notifications to test the ASR notification trap. Added a new command to list ASR assets into a `.csv` file. See View Status from the ASR Manager for details. Added additional information about layering ASR Managers. See Enabling HTTP Receiver for ASR Manager Relay, Solaris 11, and SDP2 for details. Updated the resolutions steps for the ASR_PREP_FAILED_RPM-BUILD_MISSING and ASR_PREP_FAILED_SELINUX_ENFORCING error codes.
E18475-35	Updated to support ASR 5.2.1. Updates to the Enabling M-Series XSCF Telemetry section.
E18475-34	Updated the list of Features and Enhancements for Oracle ASR Release 5.2. Added a new Appendix B, "ASR Manager Commands" to list all ASR Manager commands. Added a new Appendix C, "ASR Auto Update Error Codes" to show the problem and resolution steps to take when encountering an Auto Update error code. Update versions of third-party software in Appendix D, "Third-Party Licenses."
E18475-33	Updated to remove support for the NTLM proxy in the Configuring ASR Manager to Use a Proxy Server section. The NTLM proxy is not supported.
E18475-32	Minor editorial changes.
E18475-31	Updated to support ASR 5.0.3. Added a new ASR Manager port (6666) to the ASR Port Usage table. Updated the ASR Diagnostics section to include information about ASR Remote Diagnostics. Replaced the e-mail examples with references to *Auto Service Request (ASR) Email Examples* (Doc ID 1963725.1) available in My Oracle Support (`https://support.oracle.com`): `https://support.oracle.com/rs?type=doc&id=1963725.1`
E18475-30	Extensive update to support ASR 5.0, including the deprecation of the OASM requirement. Added Appendix D, "Third-Party Licenses."
E18475-29	Updated the What's New chapter to clarify the Automatic updates for open service requests (SRs) feature.
E18475-28	Added a new section: ASR Audit Logging. Updated the `asr show_log_collection_status` command in ASR Diagnostics. Updated Figure 4–1, "ASR Asset Status Transition" diagram.

What's New

Oracle Auto Service Request (ASR) is designed to automatically request Oracle service when specific faults occur. This chapter identifies the features and enhancements provided by Oracle Auto Service Request Release 5.5.1.

The Oracle ASR Manager Release 5.5.1 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. See ASR Manager Auto Update for instructions on how to upgrade to the latest version of the ASR Manager.

> **Note:** Support for Oracle Auto Service Request is limited to the current release and the two previous releases. Oracle now supports ASR 5.5.1, 5.5, and 5.4. It is recommended that you upgrade to the latest version. See ASR Manager Auto Update for more information.

Features and Enhancements for Oracle ASR Release 5.5.1

The Oracle Auto Service Request Release 5.5.1 includes the following features:

- Corrects two issues with ASR Manager 5.5, where:
  - The `list_asset` command is not displaying assets if associated with an Engineered Systems product.
  - The `list_asset - c` command is incorrectly parsing values during listing export.

Features and Enhancements for Oracle ASR Release 5.5

The Oracle Auto Service Request Release 5.5 includes the following features:

- Multiple fixes to ASR Auto Update including scenarios where failures result in the ASR Manager in a non-running state.
- Corrects an issue where the SFT log shows the incorrect file transfer time for large files.
- Adds support for ASR Manager Auto Update behind an ASR Manager Relay.
- Adds support for SNMPv3 AES192 and AES256.
- Improvements to the `list_asset` command.

Features and Enhancements for Oracle ASR Release 5.4

The Oracle Auto Service Request Release 5.4 includes the following features:

- Oracle Secure File Transfer (SFT) is now part of ASR Manager. SFT is now part of the ASR Manager download and no longer has a dependency on Oracle Automated Service Manager (OASM). See the *Oracle Secure File Transport User's Guide* for details.
- ASR Manager now supports IPv6 on the customer's network. See ASR Manager on IPv6 for details.
- The `list_asset` command has been improved to show asset parent/child relationships (if appropriate and when available) as well as list last heartbeat information.
- The `test_connection` command has been updated to include HTTP listener details if it has been enabled.
- The local SNMP Service Request (SR) notification capability has been expanded to include notification for any ASR SR updates to an already open SR if desired.
- Corrects known issues where ASR auto-update and diagnostic bundle gather does not work for ASR Managers using an ASR Manager Relay.
- Adds serial number as a valid argument to the `deactivate_asset/disable_asset` commands.
- The `asr disable` command has been enhanced to allow the user to select a time period (1 - 48 hours) for auto enable of the ASR Manager assets after the selected time period. See Disabling and Enabling ASR Auto Update for details.
- Corrects a known issue with ASR Manager 5.3 where the first time the `show_version` command is run `log4j:WARN` warning messages are displayed.

Known Issues for ASR Manager

- **Warning messages for the `show_version` command:** The first time the `show_version` command is run using ASR Manager 5.3, `log4j:WARN` warning messages will be displayed. These warnings are benign and can be ignored. Running the command again resolves the issue.
- **Transport URL change required:** The following two end points are no long valid for use:
  - transport.sun.com (141.146.156.47)
  - transport.sun.co.uk (141.146.156.48)

  You may need to update your configuration to use **transport.oracle.com (141.146.1.169)**.

  Instructions for how to determine if this change is needed and how to make the change is provided in My Oracle Support (MOS) Doc ID 1954819.1:

  `https://support.oracle.com/rs?type=doc&id=1954819.1`

1

Auto Service Request (ASR) Overview

Oracle Auto Service Request (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. The ASR Manager software and system, which is an implementation of ASR for Oracle, accepts fault telemetry data sent from one or more assets.

Visit the Oracle ASR product page (http://www.oracle.com/asr) for details on the features and benefits of ASR. For a list of products supported by ASR Manager, see:

http://docs.oracle.com/cd/E37710_01/nav/products.htm

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

The following chapters provide installation, configuration, and troubleshooting information for the ASR Manager software:

- Chapter 2, "Installing and Registering ASR Manager Software."
- Chapter 3, "Configuring and Activating Oracle ASR Assets."
- Chapter 4, "Managing Your Oracle ASR Environment."
- Chapter 5, "ASR General Troubleshooting."

This overview chapter provides details about:

- Understanding ASR Architectural Components
- Verifying Oracle ASR Assets
- Verifying Operating System Requirements
- Verifying Software Requirements
- Verifying Your Network Connection
- Verifying Telemetry
- Verifying My Oracle Support Requirements

1.1 Understanding ASR Architectural Components

Understanding the architecture and the nomenclature of ASR is key to a successful installation. The following list describes the key components involved with ASR:

- ASR Manager

- ASR Assets
- Oracle/ASR Backend Infrastructure
- Oracle Support Interaction

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. For the ASR Manager, you should also know:

- 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 needed.

> **Note:** Even though an ASR Asset communicates its telemetry to one ASR Manager only, an ASR Manager can serve as a relay for other ASR Managers by sharing a common network connection to Oracle Support.

- The ASR Manager system can be installed as an ASR Asset. This way, the ASR Manager system can report its own 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.

ASR Assets

ASR Assets are qualified systems that are configured to report its hardware telemetry to an ASR Manager. For a complete list of hardware qualified for ASR, see:

http://docs.oracle.com/cd/E37710_01/nav/products.htm

Oracle/ASR Backend Infrastructure

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 ascertains 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 e-mail 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.

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)*.

Note: See the ASR Security White Paper for more information about the architectural flow.

1.2 Oracle ASR Security

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

There are several ASR implementations for various Oracle products. For details, see the *Oracle Auto Service Request Security White Paper*:

http://docs.oracle.com/cd/E37710_01/doc.41/e37468/toc.htm

1.3 Verifying Oracle ASR Assets

The ASR assets send hardware telemetry data to your selected ASR Manager. The hardware you select for ASR coverage must be qualified. Qualified ASR assets have been tested and verified to be supported by the ASR backend infrastructure.

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

To verify that your hardware is qualified for ASR (including any operating system restrictions), check the list of qualified ASR products at:

http://docs.oracle.com/cd/E37710_01/nav/products.htm

After you have verified your ASR asset system(s), record the host name(s) and hardware type of each.

1.4 Verifying Operating System Requirements

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

- Linux (ASR Manager Only)
- Solaris

1.4.1 Linux (ASR Manager Only)

ASR Manager is supported on the following versions of Linux:

- Oracle Linux 5.3 or later.
- Red Hat Enterprise Linux 6.3 or later.

To check your version of Linux, run the following command:

```
/etc/enterprise-release
```

The output of this command should look like this:

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

1.4.2 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:

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

To download any required patches, visit My Oracle Support (login required) at https://suppport.oracle.com.

1.5 Verifying Software Requirements

You can download the latest Oracle ASR package from doc ID 1185493.1 in My Oracle Support:

https://support.oracle.com/rs?type=doc&id=1185493.1

In addition to the ASR software, you may need additional software for Oracle ASR to function, depending on the asset:

- Verifying Java Requirements
- Verifying Services Tools Bundle - Solaris 10 ASR Assets Only

> **Note:** Beginning with ASR 5.0, Oracle Automated Service Manager (OASM) is no longer required. However, other applications (such as Secure File Transport (SFT)) still required OASM. When you update to ASR Manger 5.0, you may need to leave the installed version of OASM in place.

1.5.1 Verifying Java Requirements

ASR Manager systems require Oracle Java 7 - JDK 7 (JDK 1.7.0_13) or later JDK 7 updates or Oracle Java 8 (1.8.0_25 or later).

> **Note:** OpenJDK is not supported.

You can download the latest version from the Java SE Downloads page:

http://www.oracle.com/technetwork/java/javase/downloads/

To check your version of Java, run:

```
java -version
```

Note: The default Java Virtual Machine (JVM) maximum heap size is 1536 MB (1.5 GB) and meets the ASR Manager requirements. Make sure your ASR Manager system has 1 GB or more memory available for allocation.

1.5.2 Verifying Services Tools Bundle - Solaris 10 ASR Assets Only

Services Tools Bundle (STB) is a tool set (including Explorer and SNEEP) 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.

To verify that the necessary tools are installed on your system, run:

```
pkginfo -l SUNWexplo
```

To verify that your system's serial number is being reported correctly, run:

```
sneep -a
```

To verify that your system's attributes are being reported correctly, run:

```
stclient -E
```

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. See Verifying Telemetry for more information about telemetry sources.

See *Oracle Services Tools Bundle (STB) - RDA/Explorer, SNEEP, ACT* (Doc ID 1153444.1) to download the latest Oracle Service Tool Bundle (STB) software from My Oracle Support:

https://support.oracle.com/rs?type=doc&id=1153444.1

1.6 Verifying Your Network Connection

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

ASR Manager Network Connectivity

Check and make note of the ASR Manager IP address. To obtain the IP address, run the following command from the ASR Manager:

```
ifconfig -a
```

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

```
https://transport.oracle.com/v1/
```

Note: The `transport.oracle.com` IP address is **141.146.1.169**.

WARNING: ASR Auto Update will not work for ASR Managers using either of these two end points:

- **transport.sun.com (141.146.156.47)**
- **transport.sun.co.uk (141.146.156.48)**

You may need to update your configuration to use transport.oracle.com (141.146.1.169).

Instructions for how to determine if this change is needed and how to make the change is provided in My Oracle Support (MOS) Doc ID 1954819.1:

https://support.oracle.com/rs?type=doc&id=1954819.1

You can also test your connection in a terminal window:

- For Solaris:

```
telnet transport.oracle.com 443
/usr/sfw/bin/wget https://transport.oracle.com/v1/
```

- For Linux:

```
telnet transport.oracle.com 443
/usr/bin/wget https://transport.oracle.com/v1/
```

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

ASR Assets Network Connectivity

For ASR assets, 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.

   Notes:

   - If your asset is running Solaris 11 and if you are planning to use the ASR Manager Relay function, then ensure the designated HTTP(S) port is open to the ASR Manager.
   - If your asset is running Solaris 11 and if you are planning on a direct connect back to Oracle, then ensure connectivity with the following command:

     ```
     telnet transport.oracle.com 443
     ```

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 Service Tags on ASR asset, via http, using port **6481**.

Check and make note of the ASR Asset IP address. To obtain the IP address, run the following command:

```
ifconfig -a
```

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

1.7 Verifying Telemetry

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. To determine the telemetry source for your ASR Asset, see the list of qualified hardware at:

http://docs.oracle.com/cd/E37710_01/nav/products.htm

Once you find your specific hardware in the list:

1. 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.
2. Make a note of the telemetry sources on your system for later use in the installation process (for example, ILOM, FMA, XSCF, etc.).
3. 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 Verifying Operating System Requirements, if necessary.
   - In some cases, the telemetry software must be upgraded for ASR. In other cases, the telemetry source requires a dedicated network connection.
   - In some cases, multiple telemetry sources cannot run together on the same system.

1.7.1 Telemetry Sources Overview

Oracle ASR supports a variety of telemetry sources for a wide range of hardware types. The types of hardware telemetry supported by Oracle ASR include:

- Fault Management Architecture (FMA)
- Integrated Lights Out Manager (ILOM)
- M-Series Extended System Control Facility (XSCF)
- Oracle Hardware Management Pack (OHMP)

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.

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.

Note: Beginning with ASR 4.1, ILOM telemetry supports the SNMP v3 security protocol. SNMP v3 provides security (encryption and authentication) for any communication to an ASR asset.

If your environment requires SNMP v3 to use the Oracle ASR service, you will need to configure both ASR Manager and any ASR Assets. See Configuring ASR Manager for SNMP v3 and Optional ILOM Setup: SNMP v3 for ASR Assets for more information.

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.

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.

1.8 Verifying My Oracle Support Requirements

My Oracle Support (MOS) is the primary online support site for Oracle Premier Support Customers. From MOS, you can search the solutions knowledgebase, download patches and software, and create service requests (SRs). You can access MOS at:

`https://support.oracle.com`

For Oracle ASR, you will use MOS to:

- Complete the activation of ASR assets, as described in Activating ASR Assets and Approve ASR Assets in My Oracle Support.
- View and update any service request (SR) generated from Oracle ASR.

Verify that you have the following access in MOS:

- **MOS account**

  You will need a valid MOS login name to install the ASR software components. You will use your MOS account to validate key information about the systems targeted for ASR installation (for example, serial numbers).

- **Support identifier**

  All ASR assets must be associated with a *support identifier*, which includes contact information to notify you when an SR is generated. Through your MOS account, you must be able to access the support identifier before you can complete any ASR installation.

  For details about requesting access or validating your associated support identifier, see *How To Manage and Approve Pending ASR Assets In My Oracle Support* (Doc ID 1329200.1):

  https://support.oracle.com/rs?type=doc&id=1329200.1

1.8.1 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.

Note: ASR will generate a technical Service Request (not draft) if support services are provided by an Oracle Support Provider Partner for Oracle Engineered Systems (excluding Oracle Database Appliance). For more information about Oracle Engineered Systems, see:

http://www.oracle.com/us/products/engineered-systems

Contact your Oracle Support Provider Partner for details.

The Partner's My Oracle Support account *must* have access to their respective partner Customer Support Identifier (CSI) associated with the asset and must have administrator privileges. This will enable the account to manage the assets of the customer CSIs associated with the Partner CSI.

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 e-mail addresses to ASR assets. This can be used to send ASR e-mail notifications to an e-mail list maintained by the Partner.
  - Activate ASR assets.
  - Maintain ASR asset information.
- Provide a My Oracle Support username and password to register the ASR Manager, using a Partner e-mail 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.

2

Installing and Registering ASR Manager Software

This chapter explains how to install the software necessary for an ASR Manager, which must be installed first before ASR assets. Installing the ASR Manager consists of the following tasks:

1. Installing ASR Manager Software
2. Registering the 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 the ASR backend infrastructure.

> **Note:** Once you have registered the ASR Manager, many ASR features are enabled by default (such as, ASR Manager Auto Update). See Managing Your Oracle ASR Environment for information on customizing your ASR environment.

Depending on your hardware and network configuration, you may be required to complete the following optional tasks to complete your ASR Manager installation:

- Enabling HTTP Receiver for ASR Manager Relay, Solaris 11, and SDP2
- Configuring ASR Manager to Use a Proxy Server
- Configuring ASR Manager for SNMP v3
- ASR Manager and High Availability
- ASR Manager on IPv6

2.1 Installing ASR Manager Software

This section provides instructions for installing the appropriate software for the ASR Manager.

> **Note:** Beginning with ASR 5.0, Oracle Automated Service Manager (OASM) is no longer required.

Note: As part of the ASR 5.0 release, the following directories have changed:

- The `/opt/SUNWswasr` directory is replaced by the `/opt/asrmanager` directory.
- The `/var/opt/SUNWsasm` directory is replaced by the `/var/opt/asrmanager` directory.

Note: You can specify an ASR Manager to be monitored as an ASR Asset. If the ASR Manager that you want to monitor as an ASR Asset is running Solaris 10, then Services Tools Bundle must be installed. See Installing Services Tools Bundle (STB) - Solaris 10 Only for more information.

STB is not a requirement for all systems. For example:

- If your ASR Manager system is running Solaris 11, the installation of STB is not required. See Enabling HTTP Receiver for ASR Manager Relay, Solaris 11, and SDP2.
- 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.

Follow the procedure below to install the ASR package for the ***first time*** on the ASR Manager system:

Note: To upgrade an installed version of ASR Manager, see Manually Upgrading ASR Manager Software for details. The instructions outlined below are for new installations only.

1. Download and unzip the ASR software package from My Oracle Support:

   `https://support.oracle.com/rs?type=doc&id=1185493.1`

2. Open a terminal window and make sure you are logged in to the ASR Manager system as `root`.
3. From the directory where you unzipped the ASR package, install the ASR package using the following command:
   - For Solaris, run: `pkgadd -d <asrmanager-version_num-time_stamp>.pkg`
   - For Linux, run: `rpm -i <asrmanager-version_num-time_stamp>.rpm`
4. 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**.

5. To avoid need to type the full path name the ASR Manager `asr` command, you can apply one of the following options:

   - Add the `asr` command to the `PATH` environment variable. This update would be made to the root user's `.profile`, `.cshrc`, `.kshrc`, or `.bashrc` files as needed (for both Solaris and Linux):

     ```
     PATH=$PATH:/opt/asrmanager/bin
     export PATH
     ```

   - Create a symbolic link to the asr command in the /usr/bin directory:

     ```
     ln -s /opt/asrmanager/bin/asr /usr/bin
     ```

   Note: The instructions assume that you are able to run the ASR Manager command by typing `asr`.

6. Confirm proper network connectivity between the ASR Manager and Oracle, as described in Test Connectivity from the ASR Manager to Oracle. When complete, continue to Registering the ASR Manager.

2.2 Registering the ASR Manager

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

Note: If you are upgrading your ASR Manager installation, then you do not need to re-register.

1. Log in to the ASR console:

   - If you have not set your `PATH` environment variable, run:

     ```
     /opt/asrmanager/bin/asr
     ```

   Note: See Installing ASR Manager Software for instructions for setting the `PATH` environment variable.

   - If you have set your `PATH` environment variable, run:

     ```
     # asr
     ```

2. To register the ASR Manager:

   ```
   asr> register
   ```

   Enter **1** to select:

   ```
   1) transport.oracle.com
   ```

   Note: If you are registering the system with an ASR Manager Relay, see Enabling HTTP Receiver for ASR Manager Relay, Solaris 11, and SDP2.

3. Enter proxy server details:
   - If you are using a proxy server to access the internet, see the instructions in Configuring ASR Manager to Use a Proxy Server.
   - If you are not using a proxy server, enter a hyphen: -
4. Enter the username and password of your My Oracle Support (MOS) account when prompted.
5. Upon entry of your MOS credentials, ASR will validate the login. Once validated, the registration is complete.
6. Check the registration status of ASR:

   ```
   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:

   ```
   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.

Note: ASR Audit Logging is enabled by default, regardless if your ASR Manager is disabled or unregistered. See ASR Audit Logging for more details.

2.2.1 ASR Manager as an ASR Asset (Solaris Only)

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. Once you install and register the ASR Manager as described in this chapter, complete the instructions in the Configuring and Activating Oracle ASR Assets chapter.

2.2.2 ASR Manager Support for Other Platforms

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:

- Local zone: for SPARC or x86 server running Solaris 10u6 or later

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 returned:

```
Asset cannot be activated due to unknown product name or serial
number.
```

Instead, activate the global zone of the asset, for example:

```
asr> activate_asset -i <IP_address_of_the_global_zone>
```

- Logical domains: for SPARC servers running Solaris 10u6 or later
- x86 Server running Linux (see Linux (ASR Manager Only) for Linux versions supported)

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

- Virtual environments: ASR Manager is supported in virtual environments (such as Oracle VirtualBox, VMWare, and others) that meet the operating system, software, and network requirements.
- Installation on blade servers:

  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
  ```

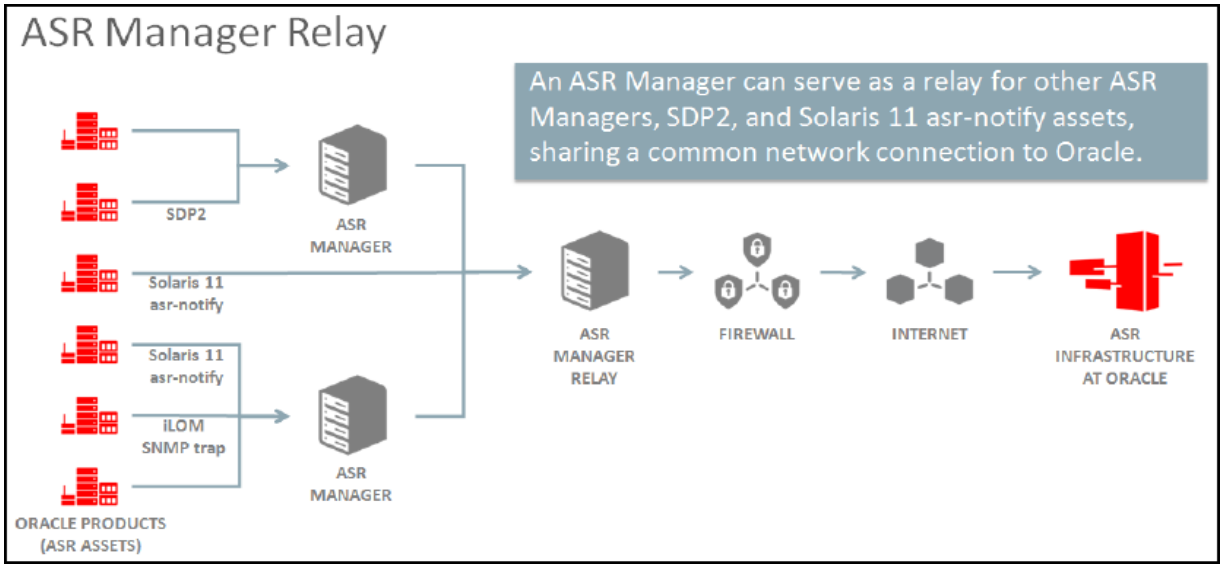
  – If the state indicates disabled, run:

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

2.3 Enabling HTTP Receiver for ASR Manager Relay, Solaris 11, and SDP2

The ASR Manager can be configured as a relay for other ASR Managers, Solaris 11 servers, and Service Delivery Platform 2 (SDP2) for tape library products (Figure 2–1):

Figure 2–1 ASR Manager Relay



Note: Beginning with ASR 5.4, the Auto Update feature has been enabled for those ASR Managers behind the relay. However, any ASR Manager behind the relay and facing DTS must be manually updated to ASR 5.4 or later before the Auto Update feature can take effect.

See Manually Upgrading ASR Manager Software for details.

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. To show the current HTTP receiver configuration port and status, run:

```
asr> show_http_receiver
```

Follow the procedure below to configure the ASR Manager as a relay for other ASR Managers and Solaris 11 ASR Assets. Make sure you are logged in to the ASR Manager system as root.

1. After installing the ASR Manager, enable the HTTP receiver:

   ```
   asr> enable_http_receiver -p <port_number>
   ```

   Note: If the following error message appears:

   ```
   Unable to determine the fully qualified domain name for this ASR
   Manager via DNS. Please refer to the Oracle ASR Installation and
   Operations Guide for troubleshooting information.
   ```

   If DNS is not available, then set up the HTTP receiver manually. Run the following commands:

   ```
   /opt/asrmanager/bin/asr set_property org.osgi.service.http.host
   <IP_address_of_ASR_manager>
   /opt/asrmanager/bin/asr set_property org.osgi.service.http.port
   <http_port>
   /opt/asrmanager/bin/asr set_property org.apache.felix.http.enable
   true
   ```

   Restart the ASR Manager and test the HTTP receiver as described in step 2.

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.

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

   ```
   asr> disable_http_receiver
   ```

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

Generate and install the SSL Certificate into the Key Store specific to the Java/JDK that the ASR Manager is pointing to:

1. Generate the Certificate Signing Request:

   a. Enter the following command:

   ```
   # keytool -genkey -alias <aliasName> -keyalg <keyAlgorithm> -keysize
   <keySize> -sigalg <signatureAlgorithm> -keystore <keyStoreFile.jks>
   ```

   Enter the valid key store password and specify the key password. Enter the Country, Locality, Organization and Common Name.

   b. Enter the following command:

   ```
   # keytool -certreq -alias <aliasName> -keystore <keyStoreFile.jks> -sigalg
   <signatureAlgorithm> -file <certRequestFile.cer>
   ```

   Enter the valid key store password and specify the key password.

   Submit the Certificate Signing Request `<certRequestFile.cer>` to the Certificate Authority, and request a Certificate.

2. Install that Certificate once you receive it from Certificate Authority:

   ```
   # keytool -import -trustcacerts -alias <aliasName> -file <certFileFromCA>
   -keystore <keyStoreFile.jks>
   ```

   Enter the valid key store password and specify the key password.

3. Once the SSL certificate from a trusted authority is loaded into keystore, run the following commands:

   ```
   # asr
   asr> set_property org.osgi.service.http.host <IP_address_of_ASR_manager>
   asr> set_property org.osgi.service.http.port.secure <https_port>
   asr> set_property org.apache.felix.https.keystore <https_keystore>
   asr> set_property org.apache.felix.https.keystore.password <https_keystore_
   password>
   asr> set_property org.apache.felix.https.keystore.key.password <https_keystore_
   key_password>
   asr> set_property org.apache.felix.https.truststore <https_truststore>
   asr> set_property org.apache.felix.https.truststore.password <https_truststore_
   password>
   asr> set_property org.apache.felix.https.enable true
   ```

   Trust Store information is same as the Key Store information.

   Passwords above can be plain text or obfuscated as follows:

   ```
   jar -xvf /opt/asrmanager/lib/com.oracle.asr.http.receiver.jar

   java -classpath org.apache.felix.http.bundle-2.2.0.jar
   org.mortbay.jetty.security.Password <plain-text-password>
   ```

   Then copy/paste the output line starting with OBF: (including the OBF: part) into the above commands..

4. Restart ASR Manager:

   - Solaris: `svcadm restart asrm`
   - Linux: `service asrm restart`

5. Verify the SSL setup by accessing the following URL from a browser:

```
https://<asr_manager_host>/asr
```

Even though an ASR Asset communicates its telemetry to one ASR Manager only, you can set up an ASR Manager to serve as a relay for other ASR Managers by sharing a common network connection to Oracle Support:

1. Verify the HTTP receiver is enabled:

   ```
   asr> show_http_receiver
   ```

   Output should look like this:

   ```
   HTTP Receiver configuration:

   HTTP Receiver Status: Enabled
   Host Name: asrmanager1.mycompany.com
   HTTP Port: 8777
   HTTPS/SSL configuration is not enabled.
   ```

2. To register an ASR Manager or Solaris 11 server with ASR Manager Relay:

   - On the ASR Manager machine, run:

     ```
     asr register -e http://asrmanager1.mycompany.com:8777/asr
     ```

   - On a Solaris 11 server, run:

     ```
     asradm register -e http://asrmanager1.mycompany.com:8777/asr
     ```

3. Test the connection:

   ```
   asr> test_connection
   ```

   Output should look like this:

   ```
   Connecting to ASR manager relay URL http://asrmanager1.mycompany.com:8777/asr
   Connectivity test to ASR manager relay completed successfully.
   ```

Note: The following layering scenarios for ASR Managers (ASRMs) are supported (all ASR Managers must be at ASR 5.3 or later):

- Any http/s client --> ASRM --> Oracle Transport
- Any http/s client --> ASRM --> ASRM Relay --> Oracle Transport

AND within a given customer network:

- Any http/s ASR client --> ASRMa --> ASRM Relay --> Oracle Transport
- Any http/s ASR client --> ASRMb --> ASRM Relay --> Oracle Transport
- Any http/s ASR client --> ASRM[n] --> ASRM Relay --> Oracle Transport

---

2.4 Configuring ASR Manager to Use a Proxy Server

As part of the registration process for ASR Manager, you can optionally set the ASR Manager to access the internet through a proxy server.

In the step for proxy server settings, enter the proxy server information as you determined in Verifying Your Network Connection. If you are not using a proxy server, enter: - (hyphen).

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>
Is this SOCKS proxy [y,n]

Note:
Is this SOCKS proxy [y,n] - enter "y" if proxy used is SOCKS otherwise enter "n"
```

Note: If you are using an NTLM-type proxy, enter the information below; otherwise, enter a hyphen (-).

Screen output should look like this:

```
NTLM Domain: ? <NTLM domain name>
NTLM Host: ? <hostname of the ASR Manager server>
```

2.5 Configuring ASR Manager for SNMP v3

ASR Manager supports two SNMP v3 telemetry sources: ILOM 3.0.16 and later (see Enabling ILOM Telemetry for details to enable ILOM telemetry for your ASR assets) and M-Series XSCF (see Enabling M-Series XSCF Telemetry for details to enable XSCF telemetry for your ASR assets).

Note: If ILOM or M-Series XSCF is not your telemetry source, then skip this section.

SNMP v3 provides security (encryption and authentication) for any communication between an ASR asset.

To configure your designated ASR Manager to allow ASR assets to use SNMP v3 through ILOM or M-Series XSCF, you must create an SNMP v3 user:

1. Create an SNMP v3 user:

```
asr> add_snmpv3_user -u userName -e engineId[,engineId2, ...] -pp
privacyProtocol
```

Notes:

- ASR Manager only supports the SHA protocol for authentication. It supports AES (ILOM) and DES (M-Series XSCF) for privacy and encryption.
- The authentication password is case-sensitive and must contain 8 to 16 characters, with no colons or space characters.
- ASR Manager supports only two SNMP v3 users at this time.
- To enable the proper telemetry for your ASR assets, see:
  - Enabling ILOM Telemetry
  - Enabling M-Series XSCF Telemetry

Note: *ILOM only:* ASR Manager supports adding multiple engine IDs (separated by comma) to the SNMP v3 user. The engine ID must match with the ILOM engine ID from ILOM Service processor. To view the ILOM engine id, run the following command from the ILOM Service Processor:

```
show /SP/services/snmp
```

For more information, see the Optional ILOM Setup: SNMP v3 for ASR Assets section.

You will be prompted to create both authentication and privacy passwords.

2. Show the SNMP v3 user:

```
asr> show_snmpv3_user
```

Running this command displays the SNMP v3 user name, engine IDs, and authentication and privacy protocols (algorithms). Passwords are not displayed.

Notes:

- ASR Manager only supports the SHA protocol for authentication and the AES (ILOM) and DES (M-Series XSCF) protocols for privacy and encryption.
- ASR Manager supports only two SNMP v3 users at this time.

Once you have created the SNMP v3 user, you must configure the ASR Assets that use ILOM for a telemetry source to use SNMP v3. See Optional ILOM Setup: SNMP v3 for ASR Assets for more information.

Other options for managing the SNMP v3 user on the ASR Manager include:

- Validate the authentication and privacy passwords of the SNMP v3 user:

```
asr> validate_snmpv3_user
```

You will be prompted to enter both authentication and privacy passwords.

- Delete the SNMP v3 user:

```
asr> delete_snmpv3_user
```

You will be prompted to continue with the deletion. Enter **Y** to delete.

- Add/delete the engine ID:

```
asr> add_engine_id -e engineId[,engineId2, ...]
asr> delete_engine_id -e engineId[,engineId2, ...]
```

- Enable/disable SNMP v1 and v2c:

```
asr> enable_snmpv1v2c : enable SNMPv1/v2c
asr> disable_snmpv1v2c : disable SNMPv1/v2c
```

2.6 ASR Manager and High Availability

Appendix A, "Other ASR Manager Administration" describes how to set up the ASR Manager in a high availability environment.

2.7 ASR Manager on IPv6

For IPv6, the ASR Manager server needs to be enabled for dual stack IPv6/IPv4. ASR Manager supports IPv6 to and from assets configured for ASR. The traffic outbound from the ASR Manager to `transport.oracle.com` currently only supports IPv4 traffic.

3

Configuring and Activating Oracle ASR Assets

ASR assets are qualified systems that are configured to report its hardware telemetry to an ASR Manager. For a complete list of hardware qualified for ASR, see:

http://docs.oracle.com/cd/E37710_01/nav/products.htm

This chapter provides the instructions to configure ASR assets running Oracle Solaris. Keep in mind that an active ASR Manager ***must*** be installed before configuring ASR assets. Configuring an ASR asset involves the following steps:

1. Verifying Assets in My Oracle Support. Your ASR Assets must be associated with a Support Identifier in My Oracle Support.
2. Installing Software - Solaris 10 Only. For ASR Assets running Solaris 10, you may need to install Services Tools Bundle.
3. Enabling Telemetry Sources.
4. Activating ASR Assets.
5. Approve ASR Assets in My Oracle Support.

Note: As part of the ASR 5.0 release, the following directories have changed:

- The `/opt/SUNWswasr` directory is replaced by the `/opt/asrmanager` directory.
- The `/var/opt/SUNWsasm` directory is replaced by the `/var/opt/asrmanager` directory.

3.1 Verifying Assets in My Oracle Support

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

1. Log in to My Oracle Support (`https://support.oracle.com`).
2. In the My Oracle Support Dashboard, select **Settings** from the More menu.
3. 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.
4. 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 Approve 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.

3.1.1 Accessing 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.***

3.2 Installing Software - Solaris 10 Only

If your ASR assets are running Solaris 10, then you will need to install Services Tools Bundle (STB) to enable ASR telemetry. Also, if your ASR Asset does not use ILOM for telemetry, you will need to use the `asrassetmenu.sh` script, which is included in the ASR Asset Bundle, to configure the asset.

- Installing Services Tools Bundle (STB) - Solaris 10 Only
- Installing the ASR Asset Bundle - Solaris 10 Only

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.

3.2.1 Installing Services Tools Bundle (STB) - Solaris 10 Only

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 STB.

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.

1. Download and untar the STB bundle that is appropriate for your platform. See *Oracle Services Tools Bundle (STB) - RDA/Explorer, SNEEP, ACT* (Doc ID 1153444.1) to download the latest Oracle Service Tool Bundle (STB) software from My Oracle Support:

   `https://support.oracle.com/rs?type=doc&id=1153444.1`

2. On the system where ASR is to be installed, open a terminal window and log in as `root`.

3. Run the `install_stb.sh` script. 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.

4. 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]**.

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

   ```
   sneep -a
   ```

   If the serial number for your system is incorrect, contact Oracle Support to resolve this problem.

6. Run the following command to be sure that STB is reporting your system attributes correctly:

   ```
   stclient -Ex
   ```

7. 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**
8. If you are not getting the correct data, re-install STB.

3.2.2 Installing the ASR Asset Bundle - Solaris 10 Only

> **Note:** If your ASR Asset does not require Solaris 10 FMA fault telemetry or uses XSCF (see Enabling M-Series XSCF Telemetry), then skip this section.

The ASR Asset Bundle includes the `asrassetmenu.sh` script used to configure an SNMP trap host for Solaris 10 FMA on assets requiring this fault telemetry. If your asset does not require this fault source, then it does not need to be installed.

To access and install 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/asrmanager/asrassetbundle` directory and copy the `ASRAssetBundle.<version_num-timestamp>.tar.gz` file to all systems that you have identified as 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. On ***each*** ASR asset, open a terminal window and log in as `root`.
4. Go to the directory where you copied the ASR Asset Bundle file and unzip and untar the file:

   ```
   tar -xvf ASRAssetBundle.<version_num-timestamp>.tar
   ```

3.3 Enabling Telemetry Sources

These procedures enable telemetry sources on your ASR assets to send hardware telemetry data to Oracle through the ASR Manager. You should have already verified what telemetry sources reside on the system, as explained in Verifying Telemetry. Depending upon what telemetry sources reside on your system, complete one or more of the following procedures:

- Enabling FMA Telemetry for Solaris 10 ASR Assets

- Enabling FMA Telemetry for Solaris 11 ASR Assets
- Enabling ILOM Telemetry
- Enabling M-Series XSCF Telemetry
- Enabling Fujitsu M10 XSCF Telemetry

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 Verifying Telemetry.

3.3.1 Enabling FMA Telemetry for Solaris 10 ASR Assets

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 ASR 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/asrmanager/asrassetbundle`
3. Launch the ASR asset menu. As root, run the following command to display the ASR asset menu:

```
# ./asrassetmenu.sh

Welcome to the ASR asset menu
---------------------------------------------
1) Add a trap-destination to FMA agent
2) Remove a trap-destination from FMA agent
3) List FMA agent trap-destinations
4) Test event to verify ASR connectivity
5) Exit

Please enter your selection [1-5]
```

4. Select **1** to enable FMA telemetry. Respond to the script's prompts as follows:
   - `Please enter Hostname or IP address of ASR Manager (q to quit)`

     Enter the information for the ASR Manager. Whether you are enabling telemetry on the ASR Manager system or on ASR asset systems, the host name or IP entered **must be for the installed ASR Manager**.
   - `Please enter SNMP port of ASR Manager (q to quit)`

     Press **[Return]** or enter another port if you have changed your port settings for ASR.
   - `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 host name of the ASR Manager).
6. Repeat for all ASR assets using Solaris 10 FMA telemetry.

3.3.1.1 Command Line Options for Setting Solaris 10 FMA Trap Destinations

You can incorporate ASR asset configuration into your automated provisioning process. The `asrassetmenu.sh` script includes command line options for setting Solaris 10 FMA trap destinations. To set a Solaris 10 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

3.3.1.2 Change Default FMA `SNMPget` Port and `community` String

FMA telemetry sources (including Solaris 10) are configured to send SNMP traps to the ASR Manager when faults occur. The ASR Manager then queries the asset for fault event details using `SNMPget` using default port and SNMP `community` string. The port and `community` string can be changed **for all assets**:

1. Change the port number:
   - To show the existing FMA enrichment port:

     ```
     asr> get_property snmp.request.port
     ```

   - To change the port:

     ```
     asr> set_property snmp.request.port <port_number>
     ```

2. Change the community string:
   - To show the `community` string:

     ```
     asr> get_property snmp.request.community
     ```

   - To change the `community` string:

     ```
     asr> set_property snmp.request.community <community_string>
     ```

3. Restart ASR for the changes to take effect:

   ```
   asr> stop
   asr> start
   ```

3.3.2 Enabling 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.

3.3.3 Enabling ILOM Telemetry

To enable ILOM telemetry, it must first be set up, configured, and confirmed. Do not continue with the installation unless you have confirmed the initial ILOM setup. You will need the ILOM service processor IP address to enable ILOM telemetry. Enabling ILOM telemetry involves the following steps:

1. Set Up ILOM

- Optional ILOM Setup: SNMP v3 for ASR Assets
- Optional ILOM Setup: ILOM Sideband Management
- Optional ILOM Setup: OHMP

2. Confirm ILOM
3. Enable ILOM: GUI Interface
4. Enable ILOM: Command Line Interface

3.3.3.1 Set Up ILOM

For complete details on configuring ILOM to send telemetry information, refer to your ILOM documentation.

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.

1. A network connection must be made from the Net Management port on the system's service processor (SP) to the network.
2. 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.
3. For some systems, ILOM can be connected using Sideband Management. ILOM Sideband Management allows the same ILOM IP address to be used, but it is routed through one of the host 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 Optional ILOM Setup: ILOM Sideband Management. When complete, return and continue with the following instructions.
4. If it is not possible to connect to the ILOM network port and your system does not support Sideband Management, OHMP telemetry can be configured on the host to generate telemetry for ILOM-diagnosed faults.

3.3.3.2 Optional ILOM Setup: SNMP v3 for ASR Assets

ILOM telemetry supports the SNMP v3 security protocol. SNMP v3 provides security (encryption and authentication) for any communication to an ASR asset.

The minimum version of ILOM that supports the AES privacy protocol for SNMP v3 is ILOM 3.0.16 and later.

1. Log in to the ILOM service processor as `root` and change to the `snmp` directory:

   ```
   cd /SP/services/snmp
   ```

2. Set a value for the engine ID:

   ```
   set engineid=<engineId>
   ```

   For example:

   ```
   set engineid=engineid1234
   ```

   Note: The value of `engineid` must be 25 characters or less.

To configure your qualified ASR assets to use SNMP v3 with ILOM telemetry:

1. Verify your ILOM service processor can support SNMP v3. Log in to the ILOM service processor IP as `root`. Run the `version` command.

   The ILOM version must be **3.0.16** or later to use SNMP v3.

2. Create an SNMP v3 user:

   ```
   cd /SP/services/snmp/users
   create <UserName> authenticationprotocol=SHA authenticationpassword=<password>
   privacyprotocol=AES privacypassword=<password>
   ```

   This user is the same created earlier in Configuring ASR Manager for SNMP v3.

3. Set SNMP v3 to send telemetry to the ASR Manager:

   ```
   cd /SP/alertmgmt/rules/<x>
   ```

   Where <x> is the alert rule slot. Refer to Enable ILOM: Command Line Interface to find the specific alert rule slot of your ILOM.

   ```
   set type=snmptrap level=minor destination=<ASR Manager IP address> destination_
   port=162 community_or_username=<SNMP v3 user name> snmp_version=3
   ```

4. See Create Test Alert - ILOM to test the configuration.

5. Verify that the test alert is received to the ASR Manager. Check for the test alert in the ASR Manager log file:

   ```
   /var/opt/asrmanager/log
   ```

   Check that you have received the test Service Request confirmation e-mail. For examples of Service Request e-mail, see *Auto Service Request (ASR) Email Examples* (Doc ID 1963725.1) available in My Oracle Support (`https://support.oracle.com`):

   ```
   https://support.oracle.com/rs?type=doc&id=1963725.1
   ```

3.3.3.3 Optional ILOM Setup: ILOM Sideband Management

ILOM Sideband Management allows ILOM telemetry to be routed through a 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 service processor 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. See the list of hardware qualified for ASR for more information:
>
> `http://www.oracle.com/technetwork/systems/asr/documentation/index.html`

1. Log in to the host and confirm the mac address:

   ```
   # ifconfig -a
   ```

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. Log in to ILOM and configure ILOM trap destination to the ASR Manager. See Enable ILOM: GUI Interface or Enable ILOM: Command Line Interface 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 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.

3.3.3.4 Optional ILOM Setup: 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.

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 Enabling FMA Telemetry for Solaris 10 ASR Assets.
2. Download and install the latest Oracle Service Hardware Management Pack. To download OHMP:
   a. Log in 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
```

3.3.3.5 Confirm ILOM

Refer to the list of qualified servers 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
  ```

> **Note:** If the product version is earlier than 2.x, upgrade it now to the latest ILOM version using your ILOM documentation for instructions.

3.3.3.6 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.

> **Note:** If using OHMP, then skip this section.

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**: Set to port **162**. For ILOM versions 2.0.4.2 or lower, the port cannot be changed from the default (162).
   - **SNMP Version:** Select **v2c** from the pull-down menu.

> **Note:** If you are using ILOM 3.0.16 or above and want to enable SNMP v3, refer to Optional ILOM Setup: SNMP v3 for ASR Assets.

   - **Community Name:** Enter **public** in the text entry field.
7. Click the **Save** button.
8. Repeat for each ASR asset required for ILOM telemetry.

If you have enabled all telemetry sources on an ASR Asset system, go to Activating ASR Assets.

3.3.3.7 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.

> **Note:** If using OHMP, then skip this section.

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:** Set to **162**. For ILOM versions 2.0.4.2 or lower, the port cannot be changed from the default (162).

   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 destination_
port=162
```

   - For the Sun Blade 6000 Chassis:

```
-> set /CMM/alertmgmt/rules/x type=snmptrap level=minor destination=[IP_of_
ASR Manager] snmp_version=2c community_or_username=public destination_
port=162
```

   Note: If you are using ILOM 3.0.16 or above and want to enable SNMP v3, refer to Optional ILOM Setup: SNMP v3 for ASR Assets.

5. Repeat for each ASR Asset using ILOM telemetry.

3.3.4 Enabling 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: Both of the M-Series XSCF service processors should be activated for ASR with their individual IP addresses used to send SNMP traps to the ASR Manager, not the failover address shared by both XSCFs.

Also, as SNMP is running only on the active XSCF, a switch of the standby XSCF to the Active role is required to activate both service processors for ASR.

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:

   - To configure an M-Series server for **SNMP v2c**, run the following command:

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

     Where:

     – **-s** = community string (default value is **public**)

     – **-p** = SNMP listener port (value should always be **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
     ```

     Where:

     – `xxx.xxx.xxx.xxx` = ASR Manager IP address

   - To configure an M-Series server for **SNMP v3**, run the following commands:

     ```
     XSCF> setsnmpusm create -a SHA <UserName>
     Enter the trap authentication passphrase:
     Enter the trap encryption passphrase:

     XSCF> setsnmp addv3traphost -u <UserName> -r SHA -n <engineId> -p 162
     xx.xxx.xxx.xxx
     Enter the trap authentication passphrase.
     Enter the trap encryption passphrase.
     ```

     Where:

     – **-n** = SNMPv3 engine ID (must be an even amount of hexidecimal digits starting with **0x**)

- **-p** = SNMPv3 listener port (value should always be **162**)
- **-r** = authentication protocol (value should always be **SHA**)
- **-u** = SNMPv3 user name
- `xxx.xxx.xxx.xxx` = ASR Manager IP address
- M-Series XSCF SNMP v3 uses the DES encryption protocol by default.

For more information, see Configuring ASR Manager for SNMP v3.

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**.

> **Note:** See M-Series Servers XSCF SNMP GET Troubleshooting for troubleshooting information.

7. Verify SNMP settings to make sure the trap destination is set, SNMP is enabled, and the FM MIB 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. Verify SNMP GET functionality. On the ASR manager, execute the following command:

```
asr> test_snmp_get -i <ip address of Active XSCF>
```

or

```
asr> test_snmp_get -h <host name of Active XSCF>
```

> **Note:** SNMP only runs on the active XSCF. The `test_snmp_get` command will fail if run against the standby XSCF.
>
> The `test_snmp_get` command does not currently support SNMPv3.

9. Repeat for each M-Series ASR asset required for XSCF telemetry.

3.3.5 Enabling Fujitsu M10 XSCF Telemetry

Follow the procedures below to enable Fujitsu M10 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.

1. Open a terminal window and initiate an `ssh` connection to the IP address of the XSCF 0 (`LAN#0`) network interface. For Building Block (BB) M10-4S configurations, this will be the IP address of `LAN#0` of the Master XSCF (that is, the XSCF installed in either `BB#00` or `XBBOX#80`, depending on the BB configuration):

   ```
   ssh -l <login name> <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.
   a. Configure Fujitsu M10 for SNMP v2c:

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

      Where:

      -s = community string (default value is **public**)

      -p = SNMP trap port (value should always be **162**)

      Note: The `-p` option can be ignored if so wished. The trap port will default to **162** on the Fujitsu M10 server.

      xx.xxx.xxx.xx = 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 xx.xxx.xxx.xx
      ```

      Where:

      xx.xxx.xxx.xx = ASR Manager IP address

      Enable the SNMP v1v2:

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

      Where:

      `<community>` = community string and should always be set to **public**

   b. Configure Fujitsu M10 for SNMP v3:
      a. Configure SNMP v3 trap:

         ```
         XSCF> setsnmp addv3traphost -u <UserName> -r SHA -n <engineId> -x AES
         xx.xxx.xxx.xxx
         ```

      b. Enter the trap authentication passphrase.
      c. Enter the trap encryption passphrase.

For more information, see Configuring ASR Manager for SNMP v3.

5. Verify SNMP settings to make sure the trap destination is set, SNMP is enabled, and the FM MIB 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
-------------  ----  ----  ----------------  --------  -------------
xx.xxx.xxx.xx  162    v2    public             n/a       n/a
SNMP V1/V2c:
Status: Enabled
Community String: public
Enabled MIB Modules:
SP MIB
```

6. Enable the SNMP agent:

```
XSCF> setsnmp enable
```

7. Once the Fujitsu M10 asset is activated/approved in My Oracle Support, send a test trap. To send a test trap from M10 XSCF, run:

```
XSCF> rastest -c test
```

8. Repeat for each Fujitsu M10 ASR Asset required for XSCF telemetry.

Note: An activation event will be sent to Oracle ASR infrastructure as soon as the trap destination is configured to an ASR Manager. You do not need to activate it on the ASR Manager.

3.4 Activating ASR Assets

Once ASR assets are activated, they will need to be enabled in My Oracle Support (see Approve ASR Assets in My Oracle Support). All assets to be activated should already have telemetry trap destinations set, as described in Enabling Telemetry Sources.

Some ASR assets are activated differently:

- Activate Blade Assets.
- Activate Exadata Assets.
- Activate Exalogic Assets.
- Activate and Register ASR Assets for Solaris 11 Systems.
- Register VOP and Activate ASR Assets for VOP.
- Activate StorageTek Virtual Storage Manager (VSM) Assets.

All other ASR asset systems are activated following the procedure below:

Note: To enter the ASR prompt as root, type `asr` on the command line. See Installing ASR Manager Software for instructions for setting the PATH environment variable.

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 rather on the ASR Manager system only.

2. Run the following activate command for each ASR asset. Be sure to use the IP or host name of the ASR asset system.

```
asr> activate_asset -i [IP address]
```

or

```
asr> activate_asset -h [host name]
```

3. Log in to My Oracle Support to complete the activation process. See Approve ASR Assets in My Oracle Support for details.

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.

3.4.1 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 Blade serial number of the Blade chassis and the Blade systems in order to complete this procedure.

3.4.1.1 ASR Activation on Blade Systems and Chassis - Solaris 10 Only

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.

Note: If activating an X627x system, see Sun Blade X627x Configuration.

2. Activate the Blade Chassis:

```
asr> activate_asset -i [Chassis_IP]
```

3. Activate the Blade System:

```
asr> activate_blade -i [Blade_IP] -c [Chassis_IP]
```

4. Repeat the `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 Qualified Sun Blade Servers:

   http://docs.oracle.com/cd/E37710_01/doc.41/e37285/ch2_sun-blade.htm#QPSVR147

5. Log in to My Oracle Support to complete the activation process. See Approve ASR Assets in My Oracle Support for details.

3.4.1.2 ASR Activation on Blade Systems and Chassis - Solaris 11 Only

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.

   Note: If activating an X627x system, see Sun Blade X627x Configuration.

2. Activate the Blade Chassis:

   ```
   asr> activate_asset -i [Chassis_IP]
   ```

3. When activating a Solaris 11 Blade host, the `asradm register` command must first be run on the Blade (see Activate and Register ASR Assets for Solaris 11 Systems). Following this, verify the Blade has a status of "Pending" by using the `list_asset` command from the ASR Manager. Copy the blade's serial number from the output of `list_asset` and paste for the `[Blade_Serial]` value. Activate the Blade System:

   ```
   asr> activate_blade -s [Blade_Serial] -c [Chassis_IP]
   ```

4. Repeat the `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 Qualified Sun Blade Servers:

   http://docs.oracle.com/cd/E37710_01/doc.41/e37285/ch2_sun-blade.htm#QPSVR147

5. Log in to My Oracle Support to complete the activation process. See Approve ASR Assets in My Oracle Support for details.

3.4.1.3 Sun Blade X627x Configuration

For the Sun X627x Blades, both the host and the service processor are ASR telemetry sources.

Note: The Sun Blade X6275 and Sun Blade X6275 M2 servers have two Service Processors that should be configured and activated for ASR using the steps described above. Also, each blade server has two Hosts than can be configured as a secondary telemetry source

- **Sun Blade X627x Service Processors**

  Activate each Sun Blade X627x Service Processor with the command:

  ```
  activate_blade -i [Service_Processor_IP] -c [Chassis_IP]
  ```

- **Sun Blade X627x Hosts**

For Sun Blade X527x hosts, see the instructions in ASR Activation on Blade Systems and Chassis - Solaris 10 Only or ASR Activation on Blade Systems and Chassis - Solaris 11 Only depending on whether the host is running Solaris 10 or Solaris 11.

3.4.2 Activate Exadata Assets

Refer to the *Quick Installation Guide for Oracle Exadata Database Machine* for complete information about activating ASR on Exadata Database Machines:

http://docs.oracle.com/cd/E37710_01/doc.41/e23333/toc.htm

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 host name 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 host name 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, refer to the Oracle Exadata documentation.

3.4.3 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 Enabling ILOM Telemetry to configure SNMP trap destinations on each of the ILOMs.

3.4.4 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. Run the following command to register the endpoint URL:
   - For the endpoint URL to be the ASR Manager:

     `asradm register -e http://[asr_manager_host]:[port_number]/asr`

     The `[port_number]` is the same port that was specified when enable HTTP receiver was done on the ASR Manager (See Enabling HTTP Receiver for ASR Manager Relay, Solaris 11, and SDP2).

- For the endpoint URL to be a direct connect back to Oracle:

  ```
  asradm register
  ```

  Notes:

  - Sun Blades does not support the direct connect back to Oracle.
  - If the same ASR Asset is using ILOM telemetry, the ILOM telemetry must go through the ASR Manager.

3. Enter your Oracle SSO user name and password.
4. 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
   #
   ```

   Note: For Sun Blade systems, see Activate Blade Assets.

5. Log in to My Oracle support to complete the activation. See Approve ASR Assets in My Oracle Support.
6. To send a test e-mail, run the following command:

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

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

   ```
   asradm unregister
   ```

3.4.5 Register VOP and Activate ASR Assets for VOP

The Virtual Operator Panel (VOP) supports Oracle ASR. Refer to the ASR section in Chapter 6, "Using the MD-VOP Interface," of the *StorageTek Virtual Operator Panel User's Guide* for instructions:

http://docs.oracle.com/cd/E37055_01/index.html

3.4.6 Activate StorageTek Virtual Storage Manager (VSM) Assets

Oracle ASR supports the StorageTek Virtual Storage Manager (VSM). VSM products supported include V2x, V2xf, VSM4, VSM5, and VSM5C.

Note: You should first install and register the ASR Manager before configuring the VSM as an ASR Asset. See Installing and Registering ASR Manager Software for more information.

Unlike other qualified ASR Assets, the setup and configuration of VSM assets requires the involvement of an Oracle Customer Support Engineer (CSE).

To set up and activate the VSM asset for Oracle ASR:

Collect VSM Information

Before configuring the VSM to use the ASR service, collect the following information:

1. Identify the VSM asset's IP address.
2. Identify the VSM asset's serial number.
3. Verify that the VSM asset and the ASR Manager are in the same subnet.

Create a Service Request (SR)

To engage an Oracle CSE to configure the VSM asset, you must submit a Service Request (SR):

1. Log in to My Oracle Support and submit an SR for an Oracle CSE to configure the VSM for ASR:

   https://support.oracle.com

   When you submit the SR, include the following information:

   - VSM asset serial number.
   - Service Identifier (SI).
   - Request the CSE reference MOS note ID 1523811.1.

2. When the Oracle CSE arrives to configure VSM for ASR, be prepared to provide the following VSM asset information:

   - IP address.
   - Subnet.
   - Netmask.

Complete ASR Activation and Verify VSM Configuration

Once the Oracle CSE has configured your VSM asset for ASR, complete ASR activation for VSM devices by running the following commands:

1. On the ASR Manager, activate the VSM asset with the `activate_storage -d` command:

   a. To activate a single VSM asset:

   ```
   asr> activate_storage -d VSM_SVA -i <IP address>
   ```

   For a successful ASR Asset activation, output should look like this:

   ```
   Successfully submitted activation for the asset
   IP Address: <IP address>
   Serial Number: <serial number>
   The e-mail address associated with the registration id for this asset's ASR
   Manager will receive an e-mail highlighting the asset activation status and
   ```

```
any additional instructions for completing activation.
Please use My Oracle Support http://support.oracle.com to complete the
activation process.
The Oracle Auto Service Request documentation can be accessed on
http://oracle.com/asr.
```

b. To activate multiple VSM_SVA assets simultaneously:

```
asr> activate_storage -d VSM_SVA -i <IP address1>, <IP address2>, <IP
address3>, <IP address4>
```

Output should look like this:

```
Please wait, discovery is in progress........

Activation process is completed
Please run "list_asset" to get the list of discovered assets
```

2. Complete the activation of the VSM asset in My Oracle Support. See Approve ASR Assets in My Oracle Support.
3. Verify the configuration by sending a test ASR message. This step verifies that the configuration of the VSM asset is correct and that connectivity to My Oracle Support is enabled.

   From the ASR Manager, run:

   ```
   asr> send_test -i <VSM's IP address>
   ```

   Output should look like this:

   ```
   Submitted test event for asset <serial number>
   Verification email will be sent to asr_contact@mycompany.com
   ```

   The e-mail is sent to the registered point of contact for the VSM asset.
4. To list all of the ASR Assets, run the following command from the ASR Manager:

   ```
   asr> list_asset
   ```

   Example 3–1 shows an example of how VSM assets appear in the output.

Example 3–1 ASR list_asset Command - Sample Output

```
Storage Assets
--------------
IP_ADDRESS   SERIAL_NUMBER  ASR      PROTOCOL  SOURCE   PRODUCT_NAME
-----------  -------------  -------- --------  ------   ------------
12.23.34.45  123456789012   Enabled  VSHELL    VSM_SVA  VSM4
13.31.13.31  123456789013   Enabled  VSHELL    VSM_SVA  VSM4
12.21.12.21  123456789014   Enabled  VSHELL    VSM_SVA  VSM5

Please use My Oracle Support 'http://support.oracle.com' to view the activation
status.
```

3.5 Approve ASR Assets in My Oracle Support

To complete the installation of ASR, you will need to log in to My Oracle Support (MOS) and approve ASR for each asset. See the "Approving ASR Activations" section of *How To Manage and Approve Pending ASR Assets In My Oracle Support* (Doc ID 1329200.1):

https://support.oracle.com/rs?type=doc&id=1329200.1

4

Managing Your Oracle ASR Environment

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

> **Note:** To enter the ASR prompt (`asr>`) as root, type `asr` on the command line. See Installing ASR Manager Software for instructions for setting the `PATH` environment variable.

The following topics are discussed.

- ASR Manager Auto Update
- Manually Upgrading ASR Manager Software
- ASR Manager Registrations
- ASR Audit Logging
- ASR Asset Management Overview
- ASR E-mails
- Add/Remove Telemetry Traps from ASR Asset(s)
- ASR Backup and Restore
- Unregister ASR
- Starting and Stopping ASR Manager
- Enable/Disable ASR Manager
- Enable/Disable ASR Assets
- Deactivate/Activate ASR Assets
- Uninstalling ASR Manager
- ASR Network Parameters Management
- ASR Integration with Enterprise Monitoring Systems
- Restore to Previous ASR Database Backup

4.1 ASR Manager Auto Update

Beginning with ASR 4.3.2, Oracle ASR, by default, checks the ASR software update server for any software updates. If there is a newer version, it will:

- Automatically download the latest Oracle ASR software bundle.

See Verifying Your Network Connection for details on how to test your connection.

- Install the new version of the software.
- Send an e-mail notification that installation is complete or if a problem was encountered.
- Store the previous version of Oracle ASR to the `/var/opt/asrmanager/backup/asrm/` directory.

Note: If using an ASR Manager Relay, starting with ASR 5.4, Auto Update will work for the ASR Manager behind the relay (see Enabling HTTP Receiver for ASR Manager Relay, Solaris 11, and SDP2). This feature does not work for ASR Managers running versions earlier than 5.4. Both ASR Managers, the one behind the relay and the one facing `transport.oracle.com`, need to be at ASR 5.4 or later.

The following topics are presented:

- Disabling and Enabling ASR Auto Update
- Using Auto Update to Manually Upgrade ASR Manager Software
- Other ASR Auto Update Commands
- ASR Auto Update `show_version` Examples

4.1.1 Disabling and Enabling ASR Auto Update

If necessary, you can disable the Auto Update feature:

```
asr> disable_autoupdate
```

To enable ASR Auto Update:

```
asr> enable_autoupdate
```

4.1.2 Using Auto Update to Manually Upgrade ASR Manager Software

Note: Using Auto Update to upgrade to ASR 5.x: Auto Update is available to upgrade to ASR 5.x, depending on your currently installed ASR version:

- If your installed version is **ASR 4.9**:

  Then Auto Update will automatically upgrade your ASR Manager software to version 5.x. If Auto Update is disabled, then you can manually run Auto Update by following the instructions in this section.

- If your installed version is **ASR 4.3.2 through ASR 4.8.1**:

  Then Auto Update must first upgrade your ASR Manager software to ASR 4.9. Once successfully upgraded to ASR 4.9, you must run Auto Update again to upgrade to ASR 5.x. Follow the instructions in this section to run Auto Update manually.

Run the following command to determine the version of your installed ASR Manager software:

```
asr> show_version
```

WARNING: ASR Auto Update will not work for ASR Managers using either of these two end points:

- **transport.sun.com (141.146.156.47)**
- **transport.sun.co.uk (141.146.156.48)**

You may need to update your configuration to use transport.oracle.com (141.146.1.169).

Instructions for how to determine if this change is needed and how to make the change is provided in My Oracle Support (MOS) Doc ID 1954819.1:

https://support.oracle.com/rs?type=doc&id=1954819.1

If Auto Update is disabled, you will need to upgrade Oracle ASR manually. You can use the Auto Update feature to download and install future versions of Oracle ASR manually:

```
asr> autoupdate
```

Output of the `autoupdate` command will look like this:

```
asr> autoupdate

This command will update the ASR Manager software with the latest bundles
available on Oracle ASR Infrastructure. Auto Update process will take up to 5
minutes to complete. During this time, assets attached to ASR Manager will not be
monitored. Do you want to proceed with Auto Update? [y/n]
```

Enter **y** to proceed. The upgrade continues with the following output:

```
New SWASR package 5.0.0.0.0 is available for update.
```

```
Started ASR Manager software Auto Update.
Autoupdate process will take approximately 5 - 10 minutes to complete. You may run
"asr show_version" to view the Auto Update status.
Please wait until you receive the Auto Update complete status email before running
any other asr commands.
An email notification will be sent to asr-contact@mycompany.com with completion
status.
```

Note: For Linux, the environment variable `SELINUX` can be set to `Enforcing` mode which will not allow the automatic update of RPM packages. If you try the Auto Update feature with this environment variable set to `Enforcing`, the following warning message will display:

```
Warning: SELINUX environment variable is set to "enforcing" mode on
this server. ASR Manager Auto Update functionality will not work
unless the SELINUX enviornment variable is set to "permissive"
```

4.1.3 Other ASR Auto Update Commands

Auto Update commands include:

- `show_version`: Shows ASR Manager and rules version information. See ASR Auto Update `show_version` Examples for sample output of the `show_version` command.
- `autoupdate`: Executes the Auto Update feature to update the ASR Manager and rules bundle software.
- `enable_autoupdate`: Enables the ASR Auto Update feature.
- `disable_autoupdate`: Disables the ASR Auto Update feature.

4.1.4 ASR Auto Update `show_version` Examples

You can run the ASR `show_version` command any time. There are several possible output examples, depending on your configuration:

Auto Update Enabled

When the ASR Auto Update feature is enabled, the output of the `show_version` command includes information about the installed ASR software versions, Auto Update statistics and status, and a history of Auto Update activity (such as, ASR Manager updates and rules definitions updates).

When you run the `show_version` command, you should expect to see output like this:

```
asr> show_version

ASR Manager version: 5.0.0

Rules definitions version: 5.0.0.0

Auto Update Statistics
==========================
Last Run Time: 2014-09-14 16:48:13.064
Last Run Status: ASR Manager software up to date and running the latest version.
Next Run Time: 2014-09-15 16:48:13.064

There are no updates available on Oracle ASR Infrastructure.

Auto Update Status
```

```
=========================
Auto Update functionality is enabled.

Auto Update History
=========================
ASR Manager Auto Update history
-----------------------------------
ASR Manager Auto Update started at: 2014-09-15 10:14:08.908
ASR Manager Auto Update completed at: 2014-09-15 10:14:08.913
ASR Manager Auto Update result: COMPLETE_SUCCESS
ASR Manager updated from version: 5.0.0
ASR Manager updated to version: 5.0.0

ASR Manager Services
--------------------
ASR Notification Trap is disabled.
Remote Request feature is enabled.
```

Auto Update Disabled

Even though the ASR Auto Update feature is disabled, you can still use the `show_version` command for information about the installed ASR software, including statistics and status.

When you run the show_version command, you should expect output like this:

```
asr> show_version

ASR Manager version: 4.4

Rules definitions version: 4.4.0

Auto Update Statistics
=========================
Last Run Time: 2013-04-03 11:21:11.283
Last Run Status: Auto Update functionality is disabled.
Next Run Time: 2013-04-03 11:23:11.283

Auto Update Status
=========================
Auto Update functionality is disabled.
Please refer to the My Oracle Support Doc Id: 1503107.1 for instructions on Auto
Update of ASR Manager software.

ASR Manager Services
--------------------
ASR Notification trap is disabled.
Remote Request feature is disabled.
```

Auto Update Enabled, ASR Manager Unregistered

For ASR to function properly, the ASR Manager must be registered. See Registering the ASR Manager for more information. You can still use the show_version command to view limited information about ASR software versions and Auto Update status.

If your ASR Manager is unregistered and you run the show_version command, the output should look like this:

```
asr> show_version

Software Versions
=================
```

```
ASR Manager version: 4.4

Rules definitions version: 4.4.0

Oracle ASR Infrastructure is not available.

Auto Update Status
==================
Auto Update functionality is enabled.
```

New Software Available

If a new software download is available (including any new rules definitions), you can use the `show_version` command to review the versions. Output should look like this:

```
asr> show_version

Software Versions
=================
ASR Manager version: 4.4

Rules definitions version: 4.4.0

New asrmanager package 4.4.0.0.0 is available for update.

Auto Update Status
==================
Auto Update functionality is enabled.
```

4.2 Manually Upgrading ASR Manager Software

Note: As part of the ASR 5.0 release, the following directories have changed:

- The `/opt/SUNWswasr` directory is replaced by the `/opt/asrmanager` directory.
- The `/var/opt/SUNWsasm` directory is replaced by the `/var/opt/asrmanager` directory.

Follow the steps below to upgrade the ASR Manager software manually:

1. Uninstall ASR. Refer to Uninstalling ASR Manager for details.
2. Obtain the new ASR package. Refer to Verifying Software Requirements for download instructions.
3. Install the new ASR package. Refer to Installing ASR Manager Software. Be sure to register and activate the ASR Manager, as explained in the referenced instructions.

4.3 ASR Manager Registrations

Beginning with ASR 4.8, the `list_registration` command provides a list of all registered ASR Manager hosts. Use this command to verify that your installed ASR Manager is registered with Oracle ASR Infrastructure or ASR Manager relay. To generate the information, run:

```
asr> list_registration
```

The following examples show a sample output of the `list_registration` command:

Sample 1

```
This ASR Manager is registered with Oracle ASR Infrastructure.
The following ASR Manager(s) are registered with this ASR Manager Relay:
ASR Manager Host : 10.12.12.11
ASR Manager Host : 10.12.12.13
```

Sample 2

```
This ASR Manager is registered with Oracle ASR Infrastructure.
```

Sample 3

```
This ASR Manager is registered with ASR Manager relay
http://host123.test.com:8928/asr
```

4.4 ASR Audit Logging

When the ASR Manager sends or attempts to send a message about an ASR Asset, that message and its corresponding status is included in an audit log in the following directory:

`/var/opt/asrmanager/log/auditlog`

Each day, a new audit log file is created to collect all unique activity from the ASR Manager. By default, a maximum of **30 days** of log files are maintained. After 30 days, the oldest log file is deleted.

You can use these logs to perform troubleshooting analysis on your qualified ASR Assets. A typical log file summarizes all ASR activity for any ASR Asset associated with the ASR Manager. Duplicate activity for a single asset is not recorded. For example, if a message from the ASR Manager fails to be sent to the Oracle ASR Infrastructure, then each retry attempt will not be recorded in the log.

By default, ASR Audit Logging is *enabled*. Use the following commands from the ASR Manager to configure and modify the ASR Audit Logging feature:

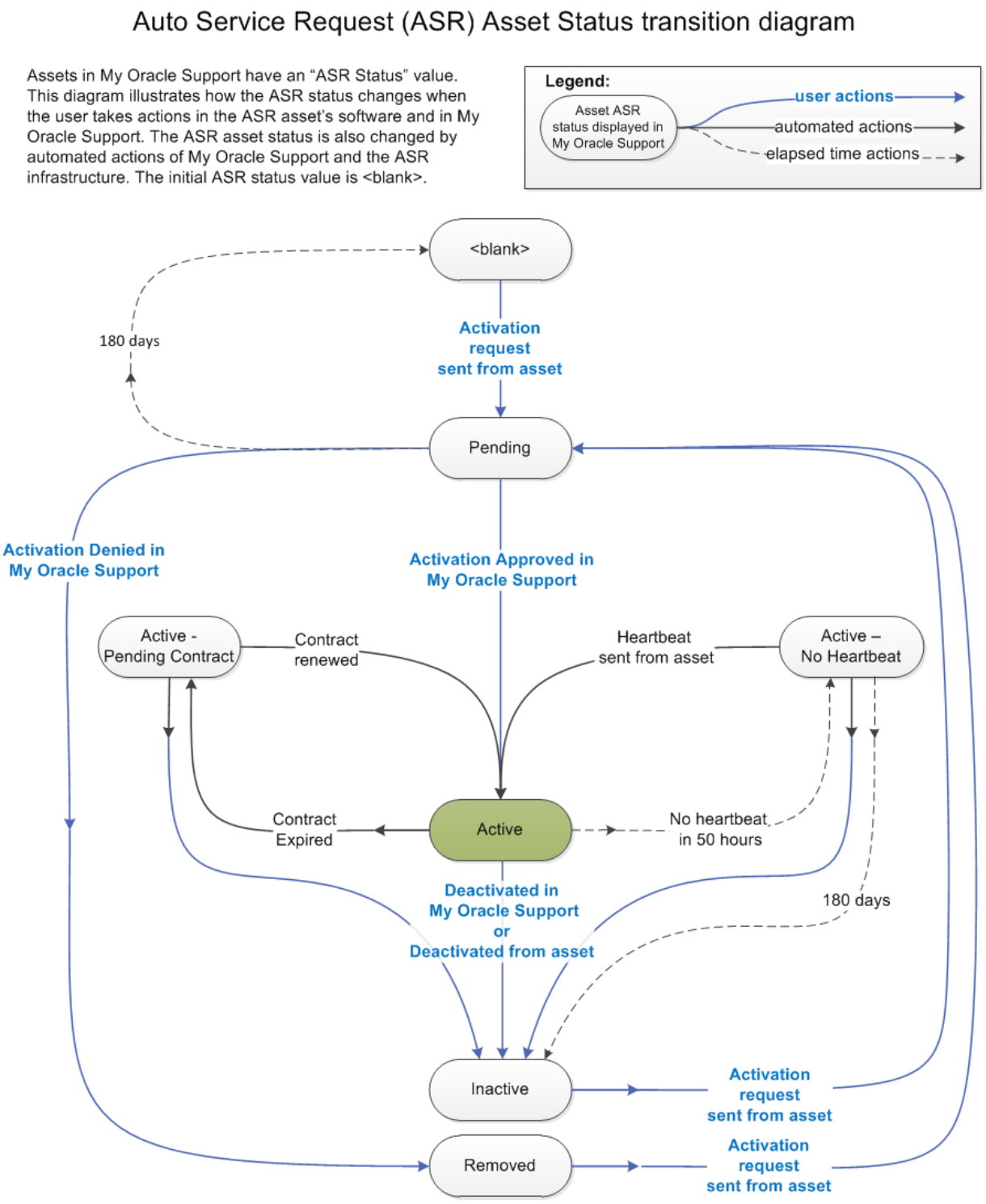
ASR Command	Description
`asr> enable_audit_log`	Enable audit logging. Messages are written to audit log in the `/var/opt/asrmanager/log/auditlog` directory.
`asr> disable_audit_log`	Disable audit logging. Messages are ***not*** written to audit log.
`asr> set_audit_log_days [1-30]`	Set how many days of audit logs to keep before rolling over (accepts any number between **1** and **30**).
`asr> get_audit_log_days`	Get how many days of audit logs are kept.
`asr> enable_asr_manager`	Enable ASR Manager. Messages are sent to the Oracle ASR Infrastructure. By default, the ASR Manager is *enabled*.
`asr> disable_asr_manager`	Disable ASR Manager. Messages are ***not*** sent to Oracle ASR Infrastructure, but are logged in the `/var/opt/asrmanager/log/auditlog` directory.

Note: ASR Audit Logging is enabled by default, regardless if your ASR Manager is disabled or unregistered.

4.5 ASR Asset Management Overview

This section provides a variety of commands and procedures for managing ASR Assets. Figure 4–1 shows the status transition of ASR Asset:

Figure 4–1 ASR Asset Status Transition



4.6 ASR E-mails

This section describes the types of e-mails generated by ASR. For examples of the e-mails generated by ASR, see *Auto Service Request (ASR) Email Examples* (Doc ID 1963725.1) available (Chinese, Japanese, and Korean versions of this document are available) in My Oracle Support (https://support.oracle.com):

https://support.oracle.com/rs?type=doc&id=1963725.1

E-mail generated by ASR 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)

Table 4–1 shows the various recipients of the typical ASR e-mail, depending on the reason for sending it, where:

- Registration user: The e-mail address used to register the asset. For the ASR Manager, this is the e-mail address entered for the `asr register` command.
- My Oracle Support Contact: The My Oracle Support (MOS) user assigned to the asset as the contact.
- MOS Dist List: a comma-separated distribution list of e-mail addresses in My Oracle Support.
- Support Identifier Administrators: The My Oracle Support users who are administrators of the Support Identifier associated with the asset.

Table 4–1 ASR E-mail Types and Recipients

	ASR E-mail Recipient				
Notification Type	**Registration User**	**Contact**	**MOS Dist List**	**Support Identifier Admins**	**Other**
Auto Update	Yes	Yes			Auto Update user SSO (typically the same as activation SSO)
Heartbeat failure	Yes	Yes	Yes		Registration SSO (if applicable)
ASR rules out of date	Yes				
ASR Manager out of date	Yes				
SR create delayed	Yes	Yes	Yes		
SR create	Yes	Yes	Yes		
SR create (partner)	No	Yes	Yes	No	
SR failed	Yes	Yes	Yes	Yes	
SR test (non-Pillar)	Yes	Yes	Yes		
SR test (Pillar)	Yes	Yes	Yes	Yes	
SR update	Yes	Yes	Yes		
Status Pending MOS	Yes	Yes	Yes	Yes	
Status Pending Contract	Yes	Yes	Yes	Yes	
Status Change	Yes				
Activation failed	Yes				

The types of e-mail generated by ASR include:

- **ASR Activation E-mail and Status of ASR Assets**

  An e-mail 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 E-mail**

  Service Request e-mails 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 e-mails indicate what issues may have prevented a Service Request from being created upon receipt of a hardware fault from ASR.

  All Service Request e-mails 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 View Status from My Oracle Support.

  Note: Any e-mail sent from Blade ASR Assets have a different e-mail format.

- **Heartbeat Failure Notification**

  If the ASR Heartbeat detects a communications error to Oracle, an e-mail is sent.

- **Fault Rules Out of Date E-mail**

  This e-mail is sent if ASR detects that its fault rules are out of date.

4.6.1 Create Test Alert

You can test the end-to-end functionality of ASR by simulating a hardware fault. The end result is an e-mail sent to the e-mail address of the My Oracle Support account associated with the ASR installation.

Note: A test alert should be run only after the asset has been enabled in My Oracle Support. See Approve ASR Assets in My Oracle Support for more information.

4.6.1.1 Create Test Alert - ILOM

Note: Only valid for ILOM 3.0 or later.

To generate a test alert from ILOM:

- **From the ILOM GUI:** 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.
- **From the ILOM CLI:** 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
```

4.6.1.2 Create Test Alert - Solaris 11

To send a test e-mail on an ASR Asset for Solaris 11, run the following command:

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

> **Note:** The ASR Asset Menu (`asrassetmenu.sh`) is not available on ASR Assets running Solaris 11.

4.6.1.3 Create Test Alert - Solaris 10

To send a test e-mail on an ASR Asset for Solaris 10:

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 "Installing the ASR Asset Bundle - Solaris 10 Only" on page 3-4 for more information.

   - If on the ASR Manager system:

     ```
     cd /opt/asrmanager/asrassetbundle/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 e-mail contact of the My Oracle Support 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 `netsnmp` library is installed on the asset.

4.7 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 "Verifying Telemetry" on page 1-7.
- An active ASR Manager should already be fully installed. Refer to Chapter 2, "Installing and Registering ASR Manager Software."

4.7.1 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 "Enabling FMA Telemetry for Solaris 10 ASR Assets" on page 3-5.
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/asrmanager/asrassetbundle/asrassetbundle`

   Note: Refer to "Installing the ASR Asset Bundle - Solaris 10 Only" on page 3-4 if you have issues locating the `asrassetbundle` directory and/or `asrassetmenu.sh` script (below).
4. Launch the ASR Asset Menu:

```
./asrassetmenu.sh

Welcome to the ASR asset menu
---------------------------------------------
1) Add a trap-destination to FMA agent
2) Remove a trap-destination from FMA agent
3) List FMA agent trap-destinations
4) Test event to verify ASR connectivity
```

```
5) Exit

Please enter your selection [1-5]
```

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.

4.7.2 Add/Remove Telemetry from Solaris 11 FMA Systems

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

1. To add Solaris FMA telemetry, see "Enabling FMA Telemetry for Solaris 11 ASR Assets" on page 3-6.
2. To delete the ASR Manager registration, run:

```
asradm unregister
```

4.7.3 Add/Remove Telemetry Traps from ILOM Systems

To add or remove an ILOM trap, refer to "Enabling ILOM Telemetry" on page 3-6. 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.

4.7.4 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 "Enabling M-Series XSCF Telemetry" on page 3-12. This referenced procedure can be used to add or remove traps.

4.8 ASR Backup and Restore

ASR Backup

1. Verify all information is in the database that is activated:

```
asr> list_asset
```

2. Stop ASR Manager so that data does not change in middle of backup:
   - For Solaris, run: `svcadm disable asrm`
   - For Linux, run: `service asrm stop`

3. Back up the database directory. Run:

   ```
   tar -cvf db.tar.bz /var/opt/asrmanager/db
   ```

4. Create a backup of the ASR configuration. Run the following commands for your installed version of ASR:

   - For ASR 5.0 and later:

     ```
     tar -cvf configuration.tar.bz /var/opt/asrmanager/configuration
     ```

   - For ASR 4.9 and earlier:

     ```
     tar -cvf 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 ASR Manager. Run:
   - For Solaris, run: `svcadm enable asrm`
   - For Linux, run: `service asrm start`

ASR Restore

1. Install the ASR Manager:
   - For Solaris, run:

     ```
     pkgadd -d <asrmanager-version-timestamp>.pkg
     ```

   - For Linux, run:

     ```
     rpm -i <asrmanager-version-timestamp>.rpm
     ```

     Note: Download and install the latest packages to upgrade to the latest version of the ASR Manager. See Verifying Software Requirements for more information.

2. Stop ASR Manager to restore files:
   - For Solaris, run: `svcadm disable asrm`
   - For Linux, run: `service asrm stop`
3. Restore the files from backup:
   a. Remove files `/var/opt/asrmanager/configuration` and `/var/opt/asrmanager/db`
   b. Copy backup data to `/var/opt/asrmanager/`
   c. Extract the tar files (both Solaris and Linux):

      ```
      tar -xvf configuration.tar.bz
      tar -xvf db.tar.bz
      ```

4. Verify the files have been correctly extracted. Run:

   ```
   ls /var/opt/asrmanager/
   ```

5. Restart ASR Manager. Run:
   - For Solaris, run: `svcadm enable asrm`

- For Linux, run: `service asrm start`

6. Register the backup configuration:

```
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:

```
asr> send_deactivations -a
```

8. Add new entries to the My Oracle Support backend:

```
asr> send_activations -a
```

9. List ASR Assets. Run:

```
asr> list_asset
```

4.9 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 e-mail contact is no longer associated with the company. The e-mail 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:

```
asr> unregister
```

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

To register ASR, refer to "Registering the ASR Manager" on page 2-3 for instructions.

4.10 Starting and Stopping ASR Manager

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.

4.10.1 Stop ASR Manager

Follow the procedure below to stop ASR Manager:

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

     ```
     svcadm disable asrm  (stops ASR Manager)
     ```

   - For Linux:

     ```
     service asrm  stop (stops ASR Manager)
     ```

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

4.10.2 Start ASR Manager

Follow the procedure below to restart ASR Manager:

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

     ```
     svcadm enable asrm (starts ASR Manager)
     ```

   - For Linux:

     ```
     service asrm start (starts ASR Manager)
     ```

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

   ```
   asr> test_connection
   ```

4.11 Enable/Disable ASR Manager

Starting with Oracle ASR 5.4, you can disable the ASR Manager for a specific amount of time. For example, if you need to perform maintenance on assets that are attached to the ASR Manager, then any faults from these systems would not be sent to Oracle.

While ASR Manager is in this disabled status, heartbeat events, fault events, and test events will not be sent to Oracle.

Run the following command to disable the ASR Manager for a specified amount of time:

```
asr> disable_asr_manager <1 to 48 hours>
```

Where `<hours>` is the number of hours that the ASR Manager is to be disabled.

Select a time between **1** and **48** to disable the ASR Manager from sending fault and heartbeat events to Oracle.

For example:

```
asr> disable_asr_manager 3
Disabling ASR for 3 hours.
```

After this period expires, the ASR Manager will be enabled automatically.

To disable ASR Manager indefinitely, run the command without specifying a time:

```
asr> disable_asr_manager
```

Note: If you run the `disable_asr_manager` command without any parameters, then the following message appears:

```
asr> disable_asr_manager

Please enter a value between 1- 48 hours to disable ASR Manager for
a specific period. After this period expires, ASR Manager will be
enabled automatically. If no value is provided then ASR Manager
will be disabled until it is enabled manually by running the asr
[y/n]:"
```

If you disable the ASR Manager without any parameters, then you must enable it manually.

To enable ASR Manager that has been disabled, run the following command:

```
asr> enable_asr_manager
ASR Manager is enabled.
```

Note: While ASR Manager is disabled, the Auto Update process will not proceed.

4.12 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.

4.12.1 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 host name 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` *host name*
   - `asr> disable_asset -s` *subnet*
     (used to disable a group of assets within the subnet)

4.12.2 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 host name 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` *host name*
- `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` *host name*

   Note: The `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 e-mail address of the My Oracle Support account associated with the ASR installation.

4.13 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.

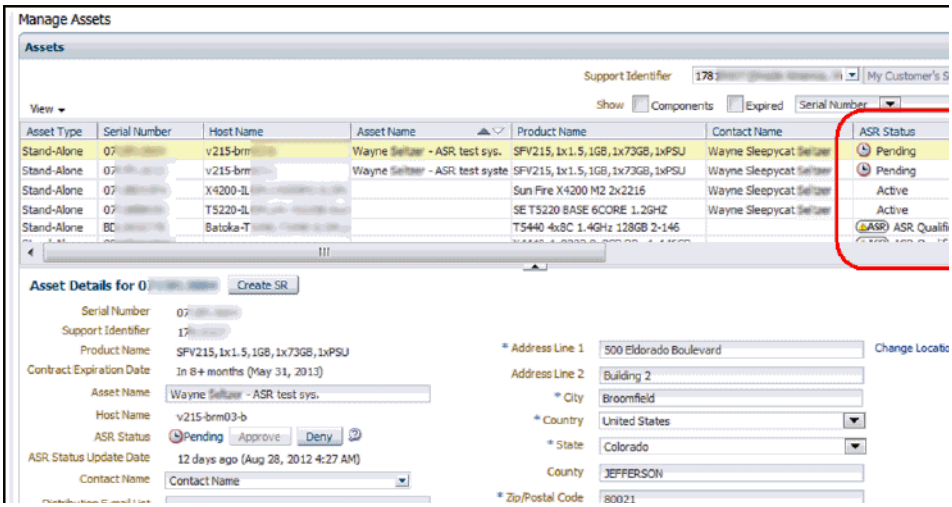
The following topics are described:

- Deactivate/Activate ASR Assets from My Oracle Support
- Deactivate/Activate ASR Assets from the ASR Manager
- Reactivate/Deactivate All ASR Assets Associated with an ASR Manager

4.13.1 Deactivate/Activate ASR Assets from My Oracle Support

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).

   Note: You must have either CUA or Asset Admin roles to update/approve ASR activation requests.



2. In the Asset's Details pane, click the "Deactive" 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).

4.13.2 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 host name of the asset you wish to deactivate.
   - `asr> deactivate_asset -i` *IP_address*
   - `asr> deactivate_asset -h` *host name*
   - `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 "Activating ASR Assets" on page 3-16.

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).

4.13.3 Reactivate/Deactivate All ASR Assets Associated with an ASR Manager

If you have multiple ASR Assets reporting to an ASR Manager, you can activate them all with one command:

```
asr> send_activations -a
```

> **Note:** Activations are resent for all the previously activated assets only.

Likewise, if you need to deactivate all of the ASR Assets associated with an ASR Manager, you can deactivate them all with one command:

```
asr> send_deactivations -a
```

4.14 Uninstalling ASR Manager

In some cases, you may need to remove or uninstall ASR Manager. For example, if you want to decommission your ASR Manager hardware or if you need to perform a manual update, then ASR Manager software must be removed. The following procedures explains how to remove ASR completely or partially for the purpose of a manual upgrade:

- ASR 5.0 and Later: Removing ASR as Part of an Upgrade
- ASR 4.9 and Earlier: Removing ASR as Part of an Upgrade
- ASR 5.0 and Later: Removing ASR Completely
- ASR 4.9 and Earlier: Removing ASR Completely

4.14.1 ASR 5.0 and Later: Removing ASR as Part of an Upgrade

1. Remove the ASR 5.0 or later package from the ASR Manager system:
   - For Solaris: `pkgrm asrmanager`

     Note: To remove the ASR package from a Solaris machine in "silent" mode, run:

     ```
     /opt/asrmanager/pkg/solaris/uninstall_silent_mode.sh
     ```

   - For Linux: `rpm -e asrmanager`
2. As part of the uninstall process, you will be asked the following question:

   ```
   Will you be upgrading to a newer version of ASR Manager [y,n,q]:
   ```

   Enter **y** to continue the process.

4.14.2 ASR 4.9 and Earlier: Removing ASR as Part of an Upgrade

1. Remove ASR 4.9 and earlier package from the ASR Manager system:
   - For Solaris: `pkgrm SUNWswasr`

     Note: To remove the ASR package from a Solaris machine in "silent" mode, run:

     ```
     /opt/SUNWswasr/pkg/uninstall_silent_mode.sh
     ```

   - For Linux: `rpm -e SUNWswasr`

   As part of the uninstall process, you will be asked the following question:

   ```
   Will you be upgrading to a newer version of ASR Manager [y,n,q]:
   ```

   Enter **y** to continue the process.

2. Remove the Oracle Automated Service Manager (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 (for example, Secure File Transport) running under OASM, then do not remove it.
   - For Solaris: `pkgrm SUNWsasm`
   - For Linux with OASM 1.5 or later: `rpm -e SUNWsasm`
   - For Linux with OASM 1.4.2 or earlier: `rpm -e --noscripts SUNWsasm`

   Note: There is a known issue when uninstalling OASM 1.4.2 (or earlier) on Linux using the `rpm -e SUNWsasm` command. Using this command to remove OASM 1.4.2 (or earlier) completely removes the `crontab` entries for OASM.

   This uninstallation issue has been resolved with OASM 1.5. To prevent losing any crontab entries, you can uninstall OASM 1.4.2 (or earlier) with the following command:

   ```
   rpm -e --noscripts SUNWsasm
   ```

4.14.3 ASR 5.0 and Later: Removing ASR Completely

1. For 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 Verifying Telemetry.
   - 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.
2. Deactivate all ASR Asset(s). Refer to Deactivate/Activate ASR Assets.
3. 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.

4. Remove the ASR package from the ASR Manager system:
   - For Solaris:

     ```
     pkgrm asrmanager
     rm -rf /var/opt/asrmanager/
     ```

   - For Linux:

     ```
     rpm -e asrmanager
     rm -rf /var/opt/asrmanager/
     ```

5. As part of the uninstall process, you will be asked the following questions (for all ASR versions):
   a. The first question is whether or not you are upgrading the ASR Manager:

      ```
      Will you be upgrading to a newer version of ASR Manager [y,n,q]:
      ```

Enter **n** to continue the process.

b. The next question is to initiates the removal of ASR Manager and the deactivation of ASR Assets:

```
Do you want to uninstall ASR Manager completely and deactivate all assets
[y,n,q]:
```

Enter **y** to continue the process. Because the removal is for a complete uninstall, you will be asked to confirm the removal:

```
You are going to deactivate all assets. Please confirm [y,n,q]
```

Enter **y** to continue the process.

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

4.14.4 ASR 4.9 and Earlier: Removing ASR Completely

1. For 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 Verifying Telemetry.
   - 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.
2. Deactivate all ASR Asset(s). Refer to Deactivate/Activate ASR Assets.
3. 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.

4. Remove the ASR package from the ASR Manager system:
   - For Solaris:

```
pkgrm SUNWswsar
pkgrm SUNWsasm
rm -rf /var/opt/SUNWsasm
```

   - For Linux:

```
rpm -e SUNWswsar
rpm -e SUNWsasm                <-- for OASM 1.5
rpm -e --noscripts SUNWswsam   <-- for OASM 1.4.2
rm -rf /var/opt/SUNWsasm
```

Note: There is a known issue when uninstalling OASM 1.4.2 (or earlier) on Linux using the `rpm -e SUNWsasm` command. Using this command to remove OASM 1.4.2 (or earlier) completely removes the `crontab` entries for OASM.

This uninstallation issue has been resolved with OASM 1.5. To prevent losing any `crontab` entries, you can uninstall OASM 1.4.2 (or earlier) with the following command:

```
rpm -e --noscripts SUNWsasm
```

5. As part of the uninstall process, you will be asked the following questions (for all ASR versions):
   a. The first question is whether or not you are upgrading the ASR Manager:

      ```
      Will you be upgrading to a newer version of ASR Manager [y,n,q]:
      ```

      Enter **n** to continue the process.

   b. The next question is to initiates the removal of ASR Manager and the deactivation of ASR Assets:

      ```
      Do you want to uninstall ASR Manager completely and deactivate all assets
      [y,n,q]:
      ```

      Enter **y** to continue the process. Because the removal is for a complete uninstall, you will be asked to confirm the removal:

      ```
      You are going to deactivate all assets. Please confirm [y,n,q]
      ```

      Enter **y** to continue the process.
6. 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 (for example, Secure File Transport) running under OASM, then do not remove it.
   - For Solaris: `pkgrm SUNWsasm`
   - For Linux: `rpm -e SUNWsasm`
7. 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
   ```
8. After completing the steps above, the uninstall of ASR is complete.

4.15 ASR Network Parameters Management

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

4.15.1 ASR Port Usage

The following table explains the network ports used by ASR:

Source	Destination	Protocol	Port	Description
ASR Asset	ASR Manager	http/https	*user defined*	For sending Solaris 11 ASR telemetry to the ASR Manager.
ASR Manager	ASR Backend (Oracle) transport.oracle.com	https	443	For sending telemetry messages to the transport.oracle.com ASR backend system 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).
ASR Manager	ASR Manager	tcp	6666	Local port used by ASR Manager Service, and it is accessible only from the ASR Manager host. ASR Manager service only listens on the local host (127.0.0.1).

WARNING: ASR Auto Update will not work for ASR Managers using either of these two end points:

- **transport.sun.com (141.146.156.47)**
- **transport.sun.co.uk (141.146.156.48)**

You may need to update your configuration to use transport.oracle.com (141.146.1.169).

Instructions for how to determine if this change is needed and how to make the change is provided in My Oracle Support (MOS) Doc ID 1954819.1:

https://support.oracle.com/rs?type=doc&id=1954819.1

4.15.2 Changing the Default SNMP Port for ASR

You can change the default SNMP port on the ASR Manager by setting or updating the following properties listed below:

1. Set the SNMP port:

   ```
   asr>  set_property snmp.receiver.port <port_number>
   ```

   For example:

   ```
   asr>  set_property snmp.receiver.port 1162
   ```

2. Verify that the SNMP port is set correctly:

   ```
   asr>  get_property snmp.receiver.port
   ```

3. Restart ASR Manager:
   - For Solaris: `svcadm restart asrm`
   - For Linux: `service asrm restart`

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

4.15.3 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 Registering the ASR Manager.

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

```
asr> set_property socksProxyHost host_name
asr> set_property socksProxyPort port_number
asr> set_property java.net.socks.password password
asr> set_property java.net.socks.username username
```

3. Restart ASR Manager:
   - For Solaris: `svcadm restart asrm`
   - For Linux: `service asrm restart`

4.15.4 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 infrastructure systems:
   - Using telnet:

     ```
     telnet transport.oracle.com 443
     ```

   - Using a web browser:

     ```
     https://transport.oracle.com/v1/
     ```

     The web page should indicate that the Data Transport Service is operating.

   - Using the `wget` utility:
     - For Solaris:

       ```
       /usr/sfw/bin/wget https://transport.oracle.com/v1/
       ```

     - For Linux:

       ```
       wget https://transport.oracle.com/v1/
       ```

Note: "Unable to locally verify the issuer's authority" is an expected error.

WARNING: ASR Auto Update will not work for ASR Managers using either of these two end points:

- **transport.sun.com (141.146.156.47)**
- **transport.sun.co.uk (141.146.156.48)**

You may need to update your configuration to use transport.oracle.com (141.146.1.169).

Instructions for how to determine if this change is needed and how to make the change is provided in My Oracle Support (MOS) Doc ID 1954819.1:

https://support.oracle.com/rs?type=doc&id=1954819.1

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:
   - Determine if your network's DNS configuration is able to resolve `transport.oracle.com`. You may need to configure your firewall to enable outbound Internet access to transport.oracle.com.

     If DNS is not available on the ASR Manager host, you may need to manually add an entry for `transport.oracle.com` and its IP address to the `/etc/hosts` file. Use any DNS lookup service on the Internet to determine the IP address for `transport.oracle.com`.
   - You may need to contact your network administrator for assistance. Refer to Verifying Your Network Connection 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. This is done by registering ASR, as discussed in the following procedure.

4.16 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 ASR Manager to enterprise monitoring systems.
- Send case creation and test alert messages to enterprise monitoring systems.
- 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

- 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 ASR Manager host to monitoring systems. Once the ASR-capable assets are activated, ASR is designed to generate a service request after specific fault events 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 "Using Auto Update to Manually Upgrade ASR Manager Software" for instructions on upgrading to the latest version of ASR.

The ASR Manager polls the ASR backend whenever a fault event or test alert occurred and updates its local database with service request or test alert information.

Note: The ASR Manager SR notification SNMP trap is sent after the Service Request is opened. If additional faults occur while the Service Request is open, then notes are added to the Service Request, but additional SR notification SNMP traps are not sent.

Once the service request/test alert information is available to the ASR Manager, it sends an SNMP v2c trap to the enterprise monitoring systems and includes the following service request/test alert data defined in the ASR MIB:

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

4.16.1 Managing SNMP Trap Destinations for Service Request Notifications

Follow the procedure below to configure SNMP trap destinations for ASR Service Request notifications. You can create up to 10 notification trap destinations.

1. Set ASR notification trap destination:

```
asr> set_notification_trap [-i ipAddress -p port -c community] [-h hostname -p
port -c community]
```

For example:

```
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 -i 127.0.0.1
   ```

4. Test the ASR notification trap:

   ```
   asr> send_test [-i ipAddress] [-h hostname]
   ```

   Check that the Enterprise Monitoring System has received the SNMP trap.

4.16.2 MIB Location and Data Elements

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

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

The MIB defines several notification types; however, only `sunAsrSrCreatedTrap` is used at this time.

Data Element	Description
`sunAsrSrHostname`	Host name 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:
	`<additional-information name=chassis_host_name>chassisHostName</additional-information>`
	`<additional-information name=chassis_serial_number>chassisSerial</additional-information>`

`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
`sunAsrSrLink`	URL for accessing the Service Request information.
`sunAsrSrSeverity`	Severity of the Service Request opened for the reported fault.

Data Element	Description
sunAsrSrName	■ 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	E-mail address of Customer Contact associated with the Serial Number of the Device for which the Service Request was created.

4.17 Restore to Previous ASR Database Backup

If you encounter a situation (such as a corrupt database issue), then you can restore your ASR database to a previous version. To restore to a previous ASR database from a backup:

1. Stop the ASR Manager so that data does not change in middle of the restore operation:
   - For Solaris, run: `svcadm disable asrm`
   - For Linux, run: `service asrm stop`
2. Back up the current database directory. Run:

   ```
   tar -cvf /var/opt/asrmanager/tmp/db_datetime.tar.bz /var/opt/asrmanager/db
   ```

3. Locate the <latest-db-backup-file-name>. Run:

   ```
   ls -t /var/opt/asrmanager/backup/db | head -1
   ```

4. Copy the latest database backup file to the ASR Manager database directory:

   ```
   cp -pr /var/opt/asrmanager/backup/db/<latest-db-backup-file-name>/sw-asr/
   /var/opt/asrmanager/db/
   ```

5. Restart ASR Manager:
   - For Solaris, run: `svcadm enable asrm`
   - For Linux, run: `service asrm start`

5 ASR General Troubleshooting

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

The instructions provided are for Solaris. When possible, corresponding Linux instructions are provided. Please see the appropriate Linux documentation for details for general administration commands.

> **Note:** To enter the ASR prompt (`asr>`) as root, type `asr` on the command line. See Installing ASR Manager Software for instructions for setting the `PATH` environment variable.

The following troubleshooting topics are presented:

- ASR Status
- ASR Diagnostics
- ASR Manager Crash Recovery
- ASR - No Heartbeat
- ASR Assets for Solaris 11 Troubleshooting
- Resolve ASR Manager Java Path Location in `asr.conf` File
- Service Tags Troubleshooting
- SMA Service Troubleshooting (Solaris 10 Only)
- Error Messages and Resolutions
- ASR Auto Update Troubleshooting
- ASR Activation Failed Troubleshooting
- Troubleshooting StorageTek Virtual Storage Manager (VSM) Assets
- Troubleshooting ILOM
- Diagnostics Bundle Collection Fails

5.1 ASR Status

You can review the status of any ASR Asset from the ASR Manager or from My Oracle Support. The following ASR Status troubleshooting topics are presented:

- View Status from the ASR Manager
- View Status from My Oracle Support

- ASR Log Files
- Check the State of ASR Bundles
- Check ASR Manager Status

5.1.1 View Status 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 Command	Description
`list_asset`	Lists all assets associated with this ASR Manager.
`list_asset -c`	Prints the ASR assets list in .csv format. Run the following command to pipe the output into a file: `list_asset -c csv_output.csv`
`list_asset -i <IP address>`	Shows the asset associated with the IP address.
`list_asset -h <host name>`	Shows the asset associated with the host name.
`list_asset -s <subnet IP address>`	Lists all assets associated with subnet IP address.

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

The results will be similar to the following example:

```
IP_ADDRESS     HOST_NAME  SERIAL_NUMBER  PARENT_SERIAL  ASR  PROTOCOL  SOURCE  LAST_HEARTBEAT_DATE  PRODUCT_NAME
-------------- ---------  -------------  -------------  ---  --------  ------  -------------------  ----------------------------
10.22.333.444  host1      SN1234567      ............   Y      SNMP      EMA       NA                 SUNW,SUN-FIRE-V490 SPARC SYSTEM
10.33.222.555  host2      SN7654321      PSN12398092    Y      SNMP      EMA       NA                 SUN FIRE X4540 X86/X64 SYSTEM

Please use My Oracle Support 'http://support.oracle.com' to view the activation status.
```

The data in `LAST_HEARTBEAT_DATE` column can show either **NA** or a date/time when the ASR Manager received the last heartbeat from the asset.

A value of **NA** indicates that the ASR Asset never sent a heartbeat to the ASR Manager.

Note: ASR assets sending individual, asset-specific heartbeats include:

- Solaris 11 `asr-notify`.
- ILOM version 3.2.2.0 and later for ASR 5.3 and earlier (ASR 5.4 and later do not have this requirement).
- M-10 XSCF.

For other assets, the ASR Manager sends heartbeats on behalf of the asset.

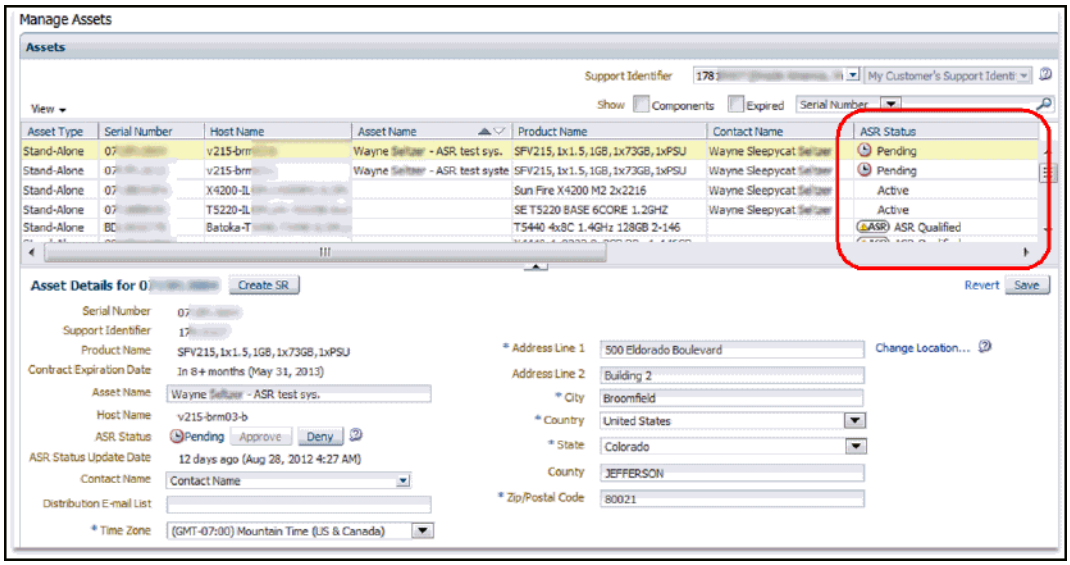
5.1.2 View Status from My Oracle Support

To view the status of all ASR Assets, log in to My Oracle Support (`https://support.oracle.com`). In the My Oracle Support Dashboard, click the

"Systems..." tab. For more information about the ASR Status value, see Figure 4–1, "ASR Asset Status Transition".

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. See the ASR Status column for the status of all ASR assets. Select an asset to view details about the asset, as shown in Figure 5–1:

Figure 5–1 Manage ASR Assets in My Oracle Support (MOS)



5.1.3 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 `asr.log` files. Log files are located on the ASR Manager system at `/var/opt/asrmanager/log`

Log File	Description
`asr-http.log`	Messages processed by the ASR Manager HTTP receiver.
`asr-snmp.log`	Activity regarding SNMP traps processing.
`asr.log`	Error messages and activity regarding the ASR Manager.
`auditlog`	Audit logs. See ASR Audit Logging.
`autoupdate.log`	Status updates for the ASR Auto Update feature.
`file-upload.log`	Activity regarding file uploads processing.
`remote-request.log`	Activity regarding remote request processing.
`service-request.log`	Oracle service request numbers created by ASR.
`trap-accepted.log`	Fault events accepted by the ASR Manager.
`trap-rejected.log`	Fault events rejected by the ASR Manager.

There are four levels of logs:

1. **Debug:** Displays the highest level of information. It contains fine, informational, warnings and severe messages.
2. **Trace:** Displays a more verbose logging than Debug.
3. **Info:** Displays not only informational data, but also both warnings and severe messages. This is the default setting.
4. **Warn:** Displays warnings and severe messages.
5. **Error:** 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.

5.1.3.1 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: **trace, debug**, **info**, **warn**, or **error**.

5.1.3.2 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]
   ```

5.1.4 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> lb

   START LEVEL 1
      ID|State |Level|Name
       0|Active | 0|System Bundle (4.4.0)
       1|Active | 1|Apache Felix Bundle Repository (1.6.6)
       2|Active | 1|Apache Felix Gogo Command (0.12.0)
       3|Active | 1|Apache Felix Gogo Runtime (0.10.0)
   ```

```
 4|Active  | 1|Apache Felix Gogo Shell (0.10.0)
 5|Active  | 1|Oracle ASR Transport (5.0.0)
 6|Active  | 1|Oracle ASR Database (5.0.0)
 7|Active  | 1|Oracle ASR Container (5.0.0)
 8|Active  | 1|Oracle ASR ServiceTags (5.0.0)
 9|Active  | 1|Oracle ASR Activation (5.0.0)
10|Active  | 1|Oracle ASR SNMP Receiver (5.0.0)
11|Active  | 1|Oracle ASR HTTP Receiver (5.0.0)
12|Active  | 1|Oracle ASR Storage (5.0.0)
13|Active  | 1|Oracle ASR Diagnostics (5.0.0)
14|Active  | 1|Oracle ASR Autoupdate (5.0.0)
15|Active  | 1|Oracle ASR TimerTask Scheduler (5.0.0)
```

3. If any of these bundles are not in an ACTIVE state, enter the following commands:

```
asr> stop
asr> start
```

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

```
asr> test_connection
asr> send_test
```

5.1.5 Check ASR Manager Status

For diagnostic purposes, it may be necessary to check the status of processes running on the ASR Manager system. For any failures, refer to Error Messages and Resolutions.

To verify the ASR Manager status, run the following script:

```
/opt/asrmanager/util/check_asr_status.sh
```

Output of a successful status check should look like this:

```
Checking ASR Manager status ..
PASS: ASR Manager bundles state is active.
PASS: ASR Manager SNMP listener is running (SNMP port 162).
PASS: ASR Manager database connectivity is working.
PASS: ASR Manager Registration SSO user name is set correctly.
PASS: ASR Manager Oracle transport connectivity is working.
PASS: ASR Manager Oracle transport endpoint is set correctly.
PASS: ASR Manager OSGI port is accessible.
PASS: ASR Manager process is running.
```

5.2 ASR Diagnostics

To assist with diagnosing issues with ASR Manager installation, configuration, and operation, ASR provides a variety of methods to collect and send the necessary details for resolving any ASR Manager issues. The following topics are provided in support of ASR diagnostics:

- ASR Diagnostic File
- ASR Remote Diagnostics
- Configure the ASR Diagnostic Utility
- ASR Diagnostic Error Messages

5.2.1 ASR Diagnostic File

ASR provides the ability to generate a diagnostic file that can be analyzed by Oracle Support as part of a Service Request, as needed. To generate and send an ASR diagnostic file for analysis with Oracle Support:

1. Create a Service Request in My Oracle Support.

   Note: If a valid SR number is not provided, then the upload to Oracle will fail.

2. Run the following command from the ASR Manager:

   ```
   asr> send_diag -sr <SR number>
   ```

   Where the `-sr <SR number>` is the newly created Service Request number.

   For example:

   ```
   asr> send_diag -sr 3-12345678

   This command will collect the diagostics file from ASR Manager and upload to
   Oracle ASR Infrastructure. Do you want to proceed with collect the diagostics
   bundle? [y/n]: y
   ```

3. Verify the diagnostic file has been successfully attached to the Service Request. Log in to My Oracle Support and view the Service Request you created earlier. The request should be updated with a new attachment.

4. (Optional) Check the status of the ASR diagnostic file:

   ```
   asr> show_log_collection_status
   ```

   This command displays the ASR diagnostics file's collection status for all collection attempts, either from the ASR command line or from the ASR portal. The collection status is displayed in ascending order.

   Output will look like this:

   ```
   asr show_log_collection_status

   Diagnostics File Upload Status
   ==========================
   File Name:
   /var/opt/asrmanager/messages/supportfile/asr-diag-bundle-98F02E0452CBB9F7961239
   17E96CEA10-140915180001.zip
   File Upload Time Stamp: 2014-09-15 18:01:16.713
   Asset Serial: Not Activated
   Service Request Number: 3-123355
   File Uploaded from Client: ASR Manager
   Client Site ID: <client site ID>
   File Upload Status Message: User asr-contact@mycompany.com is not entitled to
   upload the log files to Oracle ASR Infrastructure. Failure reason: PUT
   https://host.mycompany.com/upload/issue/3-123355/asr-diag-bundle-98F02E0452CBB9
   F796123917E96CEA10-140915180001.zip returned a response status of 403 Forbidden
   File Upload Type: Log Collection via Manual Request
   File Upload Requested By: Manual Request from ASR Commandline
   File Type: ASR Manager Diagnostics
   ==========================
   ```

You can also create a ASR diagnostic file at any time. From the ASR Manager, run the following command and follow the command-line instructions:

```
/opt/asrmanager/util/diag/asrDiagUtil.sh
```

Note: You can specify where the file is to be located. See Configure the ASR Diagnostic Utility for more information. By default, this file is stored in the following directory:

```
/var/opt/asrmanager/messages/supportfile
```

5.2.2 ASR Remote Diagnostics

Oracle Support can remotely request diagnostic files that can be analyzed as part of a Service Request, as needed. This feature is enabled by default.

To disable ASR Manager remote diagnostics, run the following command:

```
asr> disable_remote_request
```

To enable ASR Manager remote diagnostics, run the following command:

```
asr> enable_remote_request
```

5.2.3 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.

5.2.4 ASR Diagnostic Error Messages

Error Message	Resolution
`ASR Manager does not have the Minimum Java version required for the Diagnostics file upload to Oracle ASR Infrastructure. Existing Java Version: 1.6.0_26, Minimum required version: 1.6.0_43`	Upgrade the Java version to 1.6.0_43 or above (see Verifying Java Requirements for details). Then point ASR Manager to use this latest Java version. Open the `/var/opt/asrmanager/configuration/asr.conf` file and edit the `java.exec= property` to point valid Java path. For example: `java.exec=/usr/java/bin/java` Save and close the file, then restart the ASR Manager to have the updates take effect: ■ For Solaris: `svcadm restart asrm` ■ For Linux: `service asrm restart`

Error Message	Resolution
`Please enter a valid service request number.`	The Service Request (SR) number format should be valid. A valid format is `<single digit><-><multiple digits>` (for example: `3-1234566`). Check the SR number you created and run the `send_diag` command again with the valid SR number.
`Log collection was requested with an invalid SR Number.` `Cannot upload the logs to Oracle ASR Infrastructure.`	The contact registered for the ASR Manager is not authorized to upload diagnostics files to My Oracle Support for this SR. Log in to My Oracle Support to verify the upload permissions.
`ClassCastException while uploading file to Oracle ASR Infrastructure.` `A restart of the ASR Manager is required.`	Restart ASR Manager to resolve the issue. For **Solaris**: `svcadm restart asrm` For **Linux**: `service asrm restart`

5.3 ASR Manager Crash Recovery

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., host name: **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., host name: **ASRHOST02**).
4. A new ASR Manager is set up (e.g., host name: **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 4-14 for a details on creating an ASR backup).

5.4 ASR - No Heartbeat

Heartbeat is configured to run once every day via an internal timer thread. If there is no response after approximately 48 hours, the unit will be marked as a 'Heartbeat Failure' unit.

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/rs?type=doc&id=1346328.1

See the "Heartbeat Failure Notification E-mail Examples" in *Auto Service Request (ASR) Email Examples* (Doc ID 1963725.1) available in My Oracle Support (https://support.oracle.com):

https://support.oracle.com/rs?type=doc&id=1963725.1

5.5 ASR Assets for Solaris 11 Troubleshooting

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

5.6 Resolve ASR Manager Java Path Location in asr.conf File

If you have an incorrect or old version of Java installed, the ASR Manager will not start. The command to start ASR Manager will report the following message (see Start ASR Manager for Solaris and Linux command samples):

```
**************************************************************************
Warning! An old Java version ( 1.5 ) was detected (tried
'/usr/jdk/jdk1.5.0_16/bin/java').
Oracle Automated Service Manager requires a Java version of 1.6 or higher
to run correctly.

You can set 'java.exec' property in file
/var/opt/asrmanager/configuration/asr.conf
to point to JAVA 1.7 or later

Java can be downloaded from http://www.java.com
**************************************************************************
```

1. Check the Java version you have installed. From the ASR Manager, run:

   ```
   java -version
   ```

   See Verifying Java Requirements for details of the Java version requirements for ASR. ASR requires Java 7 (1.7.0_13) or later or Oracle Java 8 (1.8.0_25 or later).

2. Get the current Java path location. From the ASR Manager, run:

   ```
   cat /var/opt/asrmanager/configuration/asr.conf | grep ^java.exec
   ```

The output would look like this:

```
java.exec=/usr/bin/java
```

3. Make a backup of the `asr.conf` file. From the ASR Manager, run:

```
cp /var/opt/asrmanager/configuration/asr.conf
/var/opt/asrmanager/configuration/asr.conf_<current-timestamp>
```

4. Edit the `java.exec` property in the `asr.conf` file to point to the value of the `java.exec` output from Step 2, which should be for Java 7:

```
/usr/jdk/latest/bin/java
```

5. Stop and start ASR Manager. From the ASR Manager, run:
   - For Oracle Solaris:

     ```
     svcadm restart asrm
     ```

   - For Linux:

     ```
     service asrm restart
     ```

5.7 Service Tags Troubleshooting

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

The following Service Tags troubleshooting areas are presented:

- Check the Service Tags
- Check the Service Tags Version
- Check Service Tags Probe
- Check Service Tags Listener
- Unable to Contact Service Tags on Asset
- Unknown or Empty Service Tags on Asset
- Cannot Retrieve the ASR Manager IP Address
- Services are Disabled: stdiscover or stlisten

5.7.1 Check the Service Tags

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
```

5.7.2 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.

5.7.3 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
```

5.7.4 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
```

5.7.5 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:[ASR Manager host name]
   ```

5.7.6 Unknown or Empty Service Tags on Asset

1. View the ASR Asset's serial number using the following URL:

   ```
   http://[AgentipAddress]:6481/stv1/agent/
   ```

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

   ```
   svcs | grep sthwreg
   ```

The results should look like this:

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

3. If the serial number is incorrect, contact Oracle Support to resolve the problem.

5.7.7 Cannot Retrieve the ASR Manager IP Address

This error message indicates that the ASR Asset activation failed because the Oracle ASR Manager 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
```

5.7.8 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
   ```

5.8 SMA Service Troubleshooting (Solaris 10 Only)

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.

5.9 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.	1. Verify that the asset has 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 Enabling M-Series XSCF Telemetry for more details) 3. Review the FMA trap destination configuration file, and restart `sma` and `fmd` SMF services.

WARNING: This trap is rejected because the asset is disabled	Enable the ASR Asset using **one** of the following commands:
	`asr> enable_asset -i <ip>`
	(where *ip* is the IP address of the ASR asset)
	or
	`asr> enable_asset -h <host>`
	(where *host* is the host name of the ASR asset)

WARNING: this trap is rejected because the asset is not found	Enable the ASR Asset using **one** of the following commands: `asr> activate_asset -i` [ip] (where *ip* is the IP address of the ASR asset) or `asr> activate_asset -h` [host] (where *host* is the host name of the ASR asset)
Checking connection to /v1/ _register failed!	Run the `asr> register` command again. This time, enter **1** or the full URL: `https://transport.oracle.com` See Registering the ASR Manager.
Failure to Register Errors	The `asr.log` 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: `/var/opt/asrmanager/log/asr.log`
No Such Host Exception	This error indicates that the host running ASR Manager cannot resolve the IP address for the Data Transport Service server. Refer to Test Connectivity from the ASR Manager to Oracle to troubleshoot and resolve the problem.
Not Authorized. The My Oracle Support 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 that the socks server 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 to correct the information.

Error Message	Resolution
Activation failures: `This asset cannot be activated. Service Tags on asset abc reports: Product Name: unknown (Invalid Product Name) Serial Number: TEST 123 (Invalid Serial Number)`	Valid serial numbers contain letters, digits, period, colons, hyphens, underscores. See Activation Failed for Asset <asset name> Due to Data Error (Solaris 10 Only) for details to correct this issue.

`FAIL: Missing Registration SSO username.`
`FAIL: ASR Manager Oracle Transport end point is incorrectly set.`
`FAIL: ASR Manager Oracle Transport connectivity is not working`
	Refer to Registering the ASR Manager.
	To verify the ASR Manager status, run the following script:
	`/opt/asrmanager/util/check_asr_status.sh`

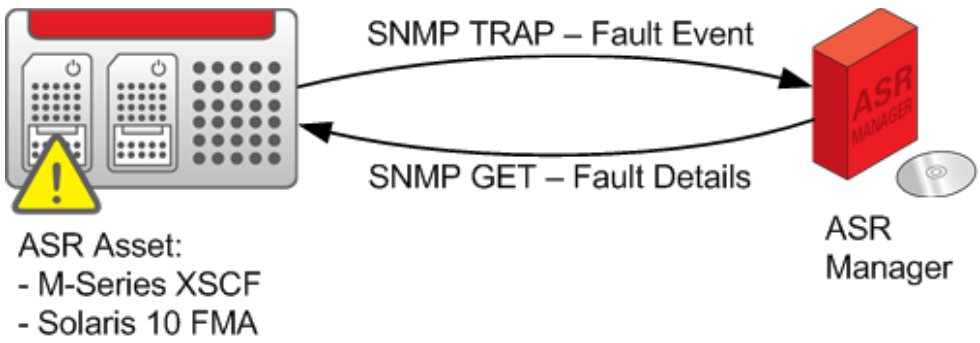
`FAIL: Multiple ASR Manager processes are running.`	1. Check the ASR Manager processes:
	`ps -eaf | grep "gosh.args=-sc" | grep java`
	Output should look like this:
	`root 3898 1 0 14:30:55 ? 0:26 /usr/bin/../java/bin/java -Dgosh.args=-sc telnetd -p6666 start -Xms512m -Xmx153`
	2. If ASR Manager is running, kill the processes with the following command:
	`kill -9 [Process_ID]`
	3. Restart ASR Manager:
	For **Solaris**: `svcadm restart asrm`
	For **Linux**: `service asrm restart`
	4. To verify the ASR Manager status, run the following script:
	`/opt/asrmanager/util/check_asr_status.sh`

`ASR Manager HTTP receiver is not running (HTTP port <http_port>)`	See Enabling HTTP Receiver for ASR Manager Relay, Solaris 11, and SDP2 To verify the ASR Manager status, run the following script: `/opt/asrmanager/util/check_asr_status.sh`

5.9.1 "SNMP GET failed" Error Message

The ASR Manager uses the `SNMP GET` protocol to query ASR assets for additional fault information (as shown in Figure 5–2).

Figure 5–2 ASR Manager SNMP GET



This is limited to the following products and fault telemetry sources:

- M-Series servers (M3000, M4000, M5000, M8000, M9000), XSCF service processor.
- Solaris 10 on ASR-qualified Oracle servers that require FMA for ASR.

These products send fault events to the ASR Manager using the SNMP TRAP protocol.

The ASR Manager uses the SNMP GET to retrieve additional fault information (such as, FRU part number, serial number, and slot location) from the product. This important information allows Oracle to streamline the service delivery process.

The ASR Manager test_snmp_get command is used to verify SNMP GET connectivity. For example:

```
asr> test_snmp_get -i <IP Address>
asr> test_snmp_get -h <host name>
```

Note: The test_snmp_get command is not supported with an SNMPv3 configuration.

Failure reasons include:

- Incorrect asset configuration.
- Network configuration on routers and firewalls that prohibit SNMP GET traffic.
- For M8000/M9000, the test_snmp_get command has been run against the *standby* XSCF. The test_snmp_get command should only be run against the *active* XSCF.

An SNMP GET error message will be returned as:

```
SNMP GET failed on: asset Hostname/IP
```

5.9.1.1 Solaris 10 FMA SNMP GET Troubleshooting

To resolve this error for ASR Assets running Solaris 10 FMA:

1. Log in to the ASR Asset.
2. Verify the fmd status:

   ```
   # svcs fmd
   ```

   Output will look like this:

   ```
   STATE STIME FMRI
   online Jan_07 svc:/system/fmd:default
   ```

3. Verify the sma status:

   ```
   # svcs sma
   ```

   Output will look like this:

   ```
   STATE STIME FMRI
   online Jan_07 svc:/application/management/sma:default
   ```

4. Enable fmd and sma:

   ```
   # svcadm enable fmd
   # svcadm enable sma
   ```

5.9.1.2 M-Series Servers XSCF SNMP GET Troubleshooting

To resolve this error for M-Series servers:

1. Log in to the M-Series XSCF.
2. Verify the following information:

- SNMP is operational with the agent running, accepting requests on port **161**.
- The Service Processor (SP) and Fault Management (FM) Management Information Base ("MIB") is enabled.
- The `community` string is set to **public** in all lower case.

To verify this information, run:

```
XSCF> showsnmp
```

The output will look like this:

```
Agent Status:       Enabled   <<-- Must be "Enabled"
Agent Port:         161       <<-- Must be "161"
System Location:    Unknown
System Contact:     Unknown
System Description: Unknown

Trap Hosts:

Hostname      Port  Type  Community String   Username   Auth Protocol
-----------   ----  ----  ----------------   --------   -------------
10.11.12.13   162    v1   public             n/a        n/a

SNMP V1/V2c:

Status:            Enabled   <<-- Must be "Enabled"
Community String:  public    <<-- Must be "public" in lower case
```

3. To enable SNMP:

```
XSCF> setsnmp enablev1v2c public
```

Note: The SNMP `community` string is case sensitive. For example, **PUBLIC** is not the same as **public**.

The default `community` string used by ASR Manager is **public**.

5.10 ASR Auto Update Troubleshooting

By default, Oracle ASR will download and install the latest version of the ASR software. ASR Auto Update includes a set of error codes to help diagnose and resolve issues you may encounter. See Appendix C, "ASR Auto Update Error Codes," for details.

5.11 ASR Activation Failed Troubleshooting

As part of the activation process (see Activating ASR Assets for details), Oracle ASR automatically checks to verify that the qualified ASR Asset has been properly configured and that telemetry information can be sent. If an ASR Asset fails this activation process, you will receive e-mail notification, depending on the following causes:

- Activation Denied
- Activation Failed for Asset <asset name> Due to Data Error (Solaris 10 Only)

For a complete list of activation-related e-mail samples, see *Auto Service Request (ASR) Email Examples* (Doc ID 1963725.1) available in My Oracle Support (https://support.oracle.com):

https://support.oracle.com/rs?type=doc&id=1963725.1

5.11.1 Activation Denied

If you receive an "activation denied" e-mail, then check to ensure that the same asset is not already activated by a different ASR Manager. If so, then you must first deactivate that asset from the previous ASR Manager or deactivate that asset in My Oracle Support before re-activating again from a different ASR Manager.

5.11.2 Activation Failed for Asset *<asset name>* Due to Data Error (Solaris 10 Only)

This message indicates that the message creation failed because of bad or missing data. For an example of the Activation Failed Bad Serial, see *Auto Service Request (ASR) Email Examples* (Doc ID 1963725.1) available in My Oracle Support (https://support.oracle.com):

https://support.oracle.com/rs?type=doc&id=1963725.1

Most of the time, this error is the result of an incorrect or incomplete serial number or product name.

To troubleshoot this message, complete the following steps:

1. View the ASR Asset's serial number using the following URL:

   ```
   http://[AgentipAddress]:6481/stv1/agent/
   ```

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

   ```
   svcs | grep sthwreg
   ```

   The results should look like this:

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

3. If the serial number is incorrect, contact Oracle Support to resolve the problem.

5.12 Troubleshooting StorageTek Virtual Storage Manager (VSM) Assets

Activate the VSM_SVA ASR Asset with the following command:

```
asr> activate_storage -d VSM_SVA -i <IP address>
```

If there are problems, common troubleshooting solutions include:

1. If the activation failed, the output should look like this:

   ```
   Failed to configure VSM_SVA device at <IP address>. Can't proceed with
   activation.
   Please refer to ASR documentation for troubleshooting steps.
   ```

   To resolve the problem, ensure the device IP address is accessible from the ASR Manager on port 9877. Run the following command:

   ```
   telnet <device IP> 9877
   ```

2. If the activation failed because the device type is unsupported, the output should look like this:

```
Cannot activate device. Unsupported Device Type. Svm-sva
Supported device Types are: VSM_SVA
```

For example, you would see this output from the following command:

```
asr> activate_storage -d Svm-sva -i <IP address>
```

To resolve the problem, use the supported device type (`-d`) **VSM_SVA**.

3. If the IP address is invalid, then output should look like this:

```
Failed to configure VSM-SVA device at <IP address> to send alerts to ASR
manager. Can't proceed with activation.
Please check if  <IP address> belongs to a VSM_SVA asset.
Ensure the asset <IP address> is accessible from ASR manager on port 9877.
Please refer to ASR documentation for troubleshooting steps.
```

To resolve the problem, verify that the setup procedures have been completely followed and implemented. Run the following command if the IP address is accessible on port 9877:

```
telnet <device IP> 9877
```

4. If the activation failed because the VSM_SVA serial number could not be determined, then the output should look like this:

```
Failed to run "status id" command to obtain serial number of VSM_SVA device at
<IP address>. Can't proceed with activation.
Please refer to ASR documentation for troubleshooting steps.
```

To resolve the problem, ensure that the VSM_SVA asset configuration is done properly. Manually run the `status id` command on the asset and ensure serial number is properly configured on the asset.

5. If the activation failed because the VSM_SVA asset configuration to send the alerts to the ASR Manager has failed, then the output should look like this:

```
Failed to configure VSM-SVA device at <IP address> to send alerts to ASR
manager. Can't proceed with activation.
Please refer to ASR documentation for troubleshooting steps to manually
configure the VSM_SVA asset.
```

To resolve the problem, you must configure the asset manually to send alerts to the ASR Manager. Run the following commands on the VSM_SVA device:

```
vshell -f "rvsadd <asr manager IP> " bye
vshell -f "rvsstem /var/opt/SUNWsasm/alerts/VSM_SVA" bye
```

5.13 Troubleshooting ILOM

The following sections provide information about troubleshooting the Integrated Lights Out Manager (ILOM):

- Check the Service Tags on ILOM

5.13.1 Check the Service Tags on ILOM

Follow the procedure below to check the Service Tags on ILOM:

1. Log in to the ILOM service processor CLI.
2. To view the ILOM Service Tags properties, enter:

   ```
   show /SP/services/servicetag
   ```

   Output should look like this:

   ```
   /SP/services/servicetag
      Targets:

      Properties:
          passphrase = none
          servicetag_urn = Q9525
          state = disabled

      Commands:
          cd
          set
          show
   ```

3. To enable Service Tags, you must enable the `state` property. Run:

   ```
   set /SP/services/servicetag state=enabled
   ```

5.14 Diagnostics Bundle Collection Fails

Problem: Diagnostics bundle collection on ASR Manager may fail with incorrect Java version or java version incompatibility issue.

Resolution: To resolve this problem:

1. Ensure the `JAVA` environment variable points to the correct Java path. You can set this variable using a symbolic link.
2. Ensure that the ASR Manager `java.exec` property is pointing to the correct Java path. This property can be set using the following command:

   ```
   /opt/asrmanager/bin/asr set_property java.exec <java path>
   ```

A

Other ASR Manager Administration

This appendix provides additional or alternative information for managing your ASR Manager environment. Sections include:

- ASR Manager and High Availability
- Allow a Non-root User to Manage an ASR Manager Service
- Asset Host Name Change

A.1 ASR Manager and High Availability

The following are steps that were used for a more recoverable ASR Manager setup than a single server. This setup shows one way without using complex cluster software but there are many other ways.

- Using Solaris 10 Local/Nonglobal Zone
- Using Linux and IP Route Package

A.1.1 Using Solaris 10 Local/Nonglobal Zone

The concept is to select 2 servers that are identical and has shared storage. A local/non-global zone path/location is setup on the shared storage where the ASR Manager software is installed. The local/non-global zone can then be moved from primary server in the event that the primary server fails and cannot be brought back on-line in a timely manner, to the secondary server where the local/non-global zone and can be brought up. ASR Manager is installed on the local/non-global zone and allows the application to be moved between primary and secondary server.

The shared storage can be direct fiber attached, SAN, iSCSI etc. In this example we use direct fiber attached storage and ZFS. The basics apply no matter what the shared storage is.

The basic concept for moving the local/non-global zone is shutdown ASR local/non-global zone on primary server, export the ZFS zpool on primary server. Then on secondary server, import zpool and boot local/nonglobal zone.

Several things to keep in mind when preparing the setup and process used for fail-over.

- It is preferred to use identical servers for primary and secondary host. This allows you to move the local/non-global zone from one server without having to run zonecfg to change network interface device or storage device.
- Both primary and secondary server must have the same Solaris 10 revision and same patches installed.

- Set zone autoboot to false. This avoids situations of the local zone/non-global zone trying to be booted on both servers.
- If using ZFS, be sure to only import the zpool to one server. ZFS does not support a zpool being imported to 2 separate hosts at the same time.
- In this example we setup the local/non-global zone manually on the secondary server. One can use the zone detach and attach within a script if preferred.

Required hardware setup:

- Two Sun Servers that are the same and support ASR Manager requirements. See Verifying Oracle ASR Assets for more details.
- Share storage that has a file system that can be moved between primary and secondary server or supports the ability to have file system mounted on both hosts at the same time such as a cluster supported file system.
- ASR Manager software.

A.1.1.1 Setup and Overview

Initial setup and overview process of primary and secondary hosts:

1. Build two Sun servers with Solaris 10 Update 6 (10u6) and later.
2. Attach shared storage to both primary and secondary host.
3. Create file system on shared storage and test the move (export/import) between primary and secondary host.
4. Create ASR local/non-global zone for ASR Manager
5. Copy the zone `cfg.xml` file and the zone index file entry from primary host to secondary host
6. Verify you can shut down ASR Manager local/non-global zone on primary host and bring up the ASR Manager on secondary host.
7. Install and verify ASR Manager (see Installing ASR Manager Software).
8. Finally configure ASR Manager to monitor systems.

The following is an example of moving zone and ZFS file system from primary host to secondary host:

In this example we will use the following labels:

- Local/non-global host name: `asrmanager`
- Primary server: `asrprd-01`
- Secondary server: `asrprd-02`
- Zpool name for ZFS: `/asr-zones`
- Path to ASR zone: `/asr-zones/asrmanager`

At this point the primary host has the ZFS zpool imported and `asrmanager` local/non-global zone is booted:

- Show running asrmanager local/non-global zone:

```
asrprd-01# zoneadm list -vc

ID NAME        STATUS     PATH                   BRAND    IP
0 global       running    /                      native   shared
1 asrmanager   running    /asr-zones/asrmanager  native   shared
```

- Show ZFS zpool:

```
asrprd-01# zpool list

NAME        SIZE  ALLOC   FREE    CAP  HEALTH  ALTROOT
asr-zones   272G  1.04G   271G     0%  ONLINE  -
```

- Show ZFS file systems:

```
asrprd-01# zfs list | grep asr

asr-zones             1.03G   267G    23K  /asr-zones
asr-zones/asrmanager  1.03G   267G  1.03G  /asr-zones/asrmanager
```

A.1.1.2 Moving from Primary Host to Secondary Host

> **Note:** This step is required in case of any issues or maintenance work with the primary server.

Steps used to move from primary host to secondary host:

1. Shut down asrmanager local/non-global zone:

```
asrprd-01# zoneadm -z asrmanager halt
```

2. Verify zone is shut down:

```
asrprd-01# zoneadm list -vc
```

Command output should look like this:

```
ID  NAME         STATUS      PATH                    BRAND    IP
0   global       running     /                       native   shared
-   asrmanager   installed   /asr-zones/asrmanager   native   shared
```

3. Export ZFS zpool:

```
asrprd-01# zpool export asr-zones
```

4. Verify ZFS zpool has been exported:

```
asrprd-01# zpool list
```

Expected command output should be:

```
no pools available
```

Now that the asrmanager local/non-global zone has been shut down and the ZFS zpool exported, log in to the secondary host and import the zpool and boot the local/non-global zone:

1. To show that ZFS zpool is not imported:

```
asrprd-02# zpool list
```

2. Import the zone ZFS zpool where asrmanager zone resides:

```
asrprd-02# zpool import asr-zones
```

3. Verify ZFS zpool has been imported:

```
asrprd-02# zpool list

NAME        SIZE  ALLOC   FREE    CAP  HEALTH  ALTROOT
asr-zones   272G  1.03G   271G     0%  ONLINE  -
```

4. Show ZFS file systems:

```
asrprd-02# zfs list | grep asr

asr-zones             1.03G   267G    23K  /asr-zones
asr-zones/asrmanager  1.03G   267G  1.03G  /asr-zones/asrmanager
```

5. Boot asrmanager local/non-global zone:

```
asrprd-02# zoneadm -z asrmanager boot
```

6. Verify `asrmanager` local/non-global zone has booted:

```
asrprd-02# zoneadm list -vc

ID  NAME         STATUS     PATH                      BRAND    IP
0   global       running    /                         native   shared
1   asrmanager   running    /asr-zones/asrmanager     native   shared
```

ASR Manager is now running in a local/non-global zone on the secondary host.

A.1.2 Using Linux and IP Route Package

The concept is to select two servers that are identical and have shared storage. A virtual IP address is set up using the IP Route utility to send ASR traffic to and from the source IP using the virtual IP. Shared storage is mounted between each host where the ASR Manager software is installed.

Using the IP Route utility, the virtual IP that ASR Manager uses can be moved from the primary server (for example, in the event that the primary server fails and cannot be brought back on-line in a timely manner) to the secondary server where the VIP/source route can be brought up. Finally, the shared storage file systems are mounted, and ASR Manager can be started.

The shared storage can be direct fiber attached, SAN, iSCSI etc. The example below uses direct fiber attached storage and ext3 file systems. The basics apply no matter what shared storage is used.

The basic concept for moving from the primary server to the secondary server is:

- On the primary server:
  1. Shut down ASR Manager on the primary host (if primary host is up).
  2. Run the `ip route` command to remove source route.
  3. Unplumb VIP.
  4. Unmount file systems that ASR Manager uses.
- On the secondary server:
  1. Plumb the VIP.
  2. Run `ip route` to add source routing.
  3. Mount file systems.
  4. Start ASR Manager.

Several things to keep in mind when preparing the setup and process used for fail-over.

- It is preferred to use identical servers for the primary and secondary host.
- Both primary and secondary servers must have the same Linux revision and same patches installed.
- Do not start ASR Manager on boot.
- If using ext3, do not mount file systems on both hosts at the same time.

Required hardware setup:

- Two servers that are the same and support ASR Manager requirements. See Verifying Oracle ASR Assets for more details.
- Shared storage that has a file system that can be moved between primary and secondary server or supports the ability to have file system mounted on both hosts at the same time (for example, a cluster supported file system).
- ASR Manager software.

A.1.2.1 Setup and Overview

Initial setup and overview process of primary and secondary hosts:

1. Build two Linux servers with versions such as Oracle Linux update7 and later.
2. Add IP Route package. The `iproute-2.6.18-11.el5.i386.rpm` file was used in the example below. This rpm file is located in the "Server" directory on the Oracle Linux DVD.
3. Attach shared storage to both primary and secondary hosts.
4. Create file systems `/opt` and `/var/opt` on shared storage and test the move of file system between primary and secondary host.
5. Plumb VIP interface and install/test IP Route source routing using the VIP's IP. (Read IP Route documentation)
6. Install and verify ASR Manager (see Installing ASR Manager Software).

The example below shows how to move the ASR Manager from a primary host to a secondary host.

In this example we will use the following labels:

- Virtual IP: `asrmanager / 10.10.0.20`
- Primary server: `asrprd-01 / 10.10.0.10`
- Secondary server: `asrprd-02 / 10.10.0.11`
- File system mounts for ASR manager: `/opt` and `/var/opt`

On the primary host, create the virtual IP, using the IP Route utility for source route and file system mount:

1. Verify file systems `/opt` and `/var/opt` are mounted:

```
[root@asrprd-01]# df | grep opt

/dev/sdc              281722700    243924 267168072   1% /opt
/dev/sdb              281722700    243776 267168220   1% /var/opt
```

2. Show the source IP:

```
[root@asrprd-01]# ip route show

10.79.208.0/24 dev eth0  scope link  src 10.10.0.20
default via 10.10.0.1 dev eth0
```

3. Plumb the virtual IP interface:

```
[root@asrprd-01]# /sbin/ifconfig eth0:0 10.10.0.20/24 broadcast 10.79.208.255
```

4. Change the source IP:

```
[root@asrprd-01]# ip route change 10.79.208.0/24 dev eth0 src 10.10.0.20
```

5. Verify the source IP is set to a virtual IP:

```
[root@asrprd-01]# ip route

10.79.208.0/24 dev eth0  scope link  src 10.10.0.20
default via 10.10.0.1 dev eth0
```

After source IP is set to the virtual IP, you can ping another host from the primary server and should see source IP of the virtual IP on that host and no longer the IP of the primary server.

At this point, install the ASR Manager software which should install in `/opt` and `/var/opt` (see Installing ASR Manager Software).

To move the ASR Manager and the virtual IP to a secondary host:

1. Log in to the primary server.
2. Shut down ASR Manager:

```
service asrm stop
```

3. Change source IP route back:

```
[root@asrprd-01]# ip route change 10.79.208.0/24 dev eth0 src 10.10.0.10
```

4. Verify the source IP is back to the primary server IP address:

```
[root@asrprd-01]# ip route show

10.79.208.0/24 dev eth0  scope link  src 10.10.0.10
default via 10.10.0.1 dev eth0
```

5. Unplumb the virtual IP interface:

```
[root@asrprd-01]# /sbin/ifconfig eth0:0 down
```

6. Unmount the `/opt` and `/var/opt` file systems from shared storage.
7. Log in into secondary server.
8. Show current source IP:

```
[root@asrprd-02]# ip route show

10.79.208.0/24 dev eth0  proto kernel  scope link  src 10.10.0.11
default via 10.10.0.1 dev eth0
```

9. Plumb virtual IP interface:

```
[root@asrprd-02]# /sbin/ifconfig eth0:0 10.10.0.20/24 broadcast 10.79.208.255
```

10. Change source IP:

```
[root@asrprd-02 ~]# ip route change 10.79.208.0/24 dev eth0 src 10.10.0.20
```

11. Verify source IP is set to the virtual IP:

```
[root@asrprd-02 ~]# ip route
 show
10.79.208.0/24 dev eth0  scope link  src 10.10.0.20
default via 10.10.0.1 dev eth0
```

12. Mount the `/opt` and `/var/opt` file system from shared storage.
13. Start ASR Manager on secondary host:

```
service asrm start
```

ASR Manager is now running on the secondary host.

A.2 Allow a Non-root User to Manage an ASR Manager Service

For Solaris, run the following command:

```
usermod -A solaris.smf.manage.asrmanager <userName>
```

Where:

- `<userName>` is the actual user name of the non-root user.

For Linux, add the following line to the `/etc/sudoers` file:

```
<userName> ALL=(root) NOPASSWD:/opt/asrmanager/bin/asr
start,/opt/asrmanager/bin/asr stop,/opt/asrmanager/bin/asr
status,/opt/asrmanager/bin/asr restart
```

Where:

- `<userName>` is the actual user name of the non-root user.

A.3 Asset Host Name Change

If there is change in the host name of an asset, then you can resend activation for that asset using the `activate_asset` command. This command will update the ASR back end with the new host name.

> **Note:** There is asset data refresh job running in ASR Manager and it is scheduled to run weekly once. The purpose of this job is to detect host name changes on the assets and resend the activation update with new hostname to the ASR back end.

B

ASR Manager Commands

This appendix shows the output for the ASR Manager `help` command. This command describes all ASR Manager commands and options available.

To add the `asr` command to the `PATH` environment variable, update the root user's `.profile`, `.cshrc`, `.kshrc`, or `.bashrc` files as needed (for both Solaris and Linux) with the following information:

```
PATH=$PATH:/opt/asrmanager/bin
export PATH
```

Once updated, you can run the ASR Manager command directly:

```
asr> help
```

If you do not update the `PATH` environment variable, you must run the ASR Manager commands as `root`:

```
# asr help
```

Table B–1 describes all of the ASR Manager commands and options:

Table B–1 ASR Manager Commands and Options

ASR Manager Command	Description

`register`
OR
`register`
`[-e asr-manager-relay-url]`
	Register the ASR Manager

`unregister`	Unregister the ASR Manager
`show_reg_status`	Show ASR registration status
`list_registration`	List ASR Manager registrations
`test_connection`	Test the ASR Manager connection to Oracle

`activate_asset`
`[-i ip]`
`[-h host name]`
`[-s subnet]`
`[-?]`
	Activates and enables the ASR asset

`activate_blade`
`[-i bladeIP -c chassisIP]`
`[-?]`
OR
`activate_blade`
`[-s bladeSN -c chassisIP]`
`[-?]`
	Activates and enables blade assets

Table B–1 (Cont.) ASR Manager Commands and Options

ASR Manager Command	Description

`activate_exadata`
`[-i exadataIP -h exadatahostname -l ilomIP]`
`[-?]`
`OR`
`activate_exadata`
`[-i exadataIP -h exadatahostname -n ilomhostname]`
`[-?]`
	Activates and enables Oracle Exadata Database Machine assets

`activate_storage`
`[-d device type]`
`[-i ip]`
`[-?]`
	Activates and enables the storage device assets

`deactivate_asset`
`[-i ip]`
`[-h host name]`
`[-s subnet]`
`[-?]`
	Deactivates and deletes the ASR asset

`enable_asset`
`[-i ip]`
`[-h host name]`
`[-s subnet]`
`[-?]`
	Enables the ASR asset

`disable_asset`
`[-i ip]`
`[-h host name]`
`[-s subnet]`
`[-?]`
	Disables the ASR asset

`list_asset`
`[-i ip]`
`[-h host name]`
`[-s subnet]`
`[-?]`
	Lists all ASR assets

`send_test`
`[-i ip]`
`[-h host name]`
`[-?]`
	Send a test alert e-mail message

`heartbeat`	Send ASR Manager heartbeat
`stop`	Stop ASR Manager
`start`	Start ASR Manager
`restart`	Restart ASR Manager
`status`	Show status of the ASR Manager

`enable_http_receiver`
`[-p port]`
`[-?]`
	Enable HTTP Receiver

`disable_http_receiver`	Disable HTTP Receiver
`show_http_receiver`	Display current configuration status of HTTP Receiver
`show_version` `[-?]`	Show ASR Manager and rules version information
`autoupdate [-?]`	Run Auto Update to update ASR Manager and rules bundle software

`set_notification_trap`
`[-i ipAddress -p port -c community]`
`[-h host name -p port -c community]`
`[-?]`
	Set ASR notification trap configuration

Table B–1 (Cont.) ASR Manager Commands and Options

ASR Manager Command	Description
`show_notification_trap`	Show ASR notification trap configuration

`delete_notification_trap`
`[-i ipAddress]`
`[-h host name]`
`[-?]`
	Delete ASR notification trap configuration

`enable_remote_request` `[-?]`	Enable Remote Request feature
`disable_remote_request` `[-?]`	Disable Remote Request feature.
`enable_autoupdate` `[-?]`	Enable ASR Manager Auto Update
`disable_autoupdate` `[-?]`	Disable ASR Manager Auto Update
`set_loglevel` `[trace, debug, info, warn, error]`	Set the logging level to trace, debug, info, warn, or error
`get_loglevel`	Get the logging level
`set_logfilecount` `[1-20]`	Set the log file count to any number between 1 and 20
`get_logfilecount`	Get the log file count
`enable_audit_log`	Enable audit logging
`disable_audit_log`	Disable audit logging
`set_audit_log_days` `[1-30]`	Set how many days of audit logs to keep before rolling over (accepts any number between 1 to 30)
`get_audit_log_days`	Get how many days of audit logs are kept
`enable_asr_manager`	Enable the ASR Manager
`disable_asr_manager`	Disable the ASR Manager

`add_snmpv3_user`
`-u userName`
`-e engineId[,engineId2, ...]`
`-pp privacyProtocol`
	Add SNMPv3 user

`show_snmpv3_user`	Show SNMPv3 user
`validate_snmpv3_user`	Validate SNMPv3 user
`delete_snmpv3_user`	Delete SNMPv3 user
`add_engine_id` `-e engineId[,engineId2, ...]`	Add SNMPv3 engine ID
`delete_engine_id` `-e engineId[,engineId2, ...]`	Delete SNMPv3 engine ID
`enable_snmpv1v2c`	Enable SNMPv1/v2c
`disable_snmpv1v2c`	Disable SNMPv1/v2c
`version`	Show ASR Manager version

`send_diag`
`-sr <SR Number>`
`[-?]`
	Collect diagnostics bundle from ASR Manager and send it to the Oracle ASR Infrastructure

`test_snmp_get`
`[-i ipAddress]`
`[-h host name]`
	Test SNMP GET access on the asset for FMA or M-series XSCF

`show_log_collection_status` `[-?]`	Show diagnostics file collection/upload status

Table B–1 (Cont.) ASR Manager Commands and Options

ASR Manager Command	Description
`exit`	Exit ASR Manager
`help`	Display a list of ASR Manager commands
`?`	Display a list of ASR Manager commands

C

ASR Auto Update Error Codes

This appendix outlines common error codes that can be triggered by the ASR Manager software.

The ASR Auto Update feature automatically updates your ASR Manager software. For this feature to function properly, you must:

- Be running ASR Manager 4.9, 5.0.3, or later.
- Have ASR Auto Update enabled (it is enabled by default).
- ASR Manager 4.9 ***only***: Be running OASM 1.4.2 or later. See Doc ID 1185493.1 in My Oracle Support to download the latest version of OASM. (OASM is not required for ASR Manager 5.x and later).

Once the ASR Auto Update process is complete, you will receive an e-mail notification of a successful upgrade of the ASR Manager software, or you will be notified that the update process failed. There are a number of reasons why the ASR Auto Update process could fail, and the e-mail notification will include an error code. A full list of the ASR Auto Update error codes is provided below.

A typical e-mail notification of an ASR Auto Update failure would look like this:

Hostname: <your host name>

Serial#: <your ASR Manager serial number, if activated>

-or-

ASR SiteID: <your ASR Manager site ID, if the ASR Manager is not activated>

Oracle Auto Service Request (ASR) Manager was unable to complete Auto Update due to a failure.

New version: 4.6.0

Current version: 4.5

Error code: ASR_INSTALL_FAILED_RESTORED_PREVIOUS_VERSION

Review Doc Id: 1503107.1.

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.

When available, a reference to a workaround or solution to the error code will be provided.

If you are unable to resolve the issue after following the troubleshooting information, please open a Service Request using My Oracle Support @ http://support.oracle.com.

Use Problem Type: "My - Auto Service Request (ASR) Installation and Configuration Issues"

The following error codes are described:

C.1 ASR_PREPARATION_FAILED_BACKEND_SERVER_CONNECTION_FAILED

Problem: The ASR Manager is unable to connect to Oracle.

Resolution: Check the connection between the ASR Manager to the Oracle ASR infrastructure. The Oracle ASR infrastructure endpoint is:

`https://transport.oracle.com`

Ensure that the ASR Manager is able to reach above URL on port 443. Also, ensure that the ASR Manager is registered to Oracle ASR infrastructure with a valid user name and password.

C.2 ASR_PREPARATION_FAILED_AUTOUPDATE_SERVER_CONNECTION_FAILED

Problem: ASR Auto Update cannot connect to the ASR software update server. The following message will be added to the `sw-asr.log` file:

```
sw-asr.log.0 contains: Oct 24, 2012 9:48:32 AM
com.sun.svc.autoupdate.AsrAutoUpdateService autoUpdatePrep SEVERE: ASR backend
server https://transport.oracle.com/em/upload is not available for auto update.
Oct 24, 2012 9:48:32 AM com.sun.svc.autoupdate.AsrAutoUpdateService autoUpdate
```

```
SEVERE: Autoupdate preparation failed. Quiting the process.
```

- When running Auto Update to update ASR Manager 4.9 to ASR Manager 5.x, then the log file to check is:

  ```
  /var/opt/SUNWsasm/log/sw-asr.log.0
  ```

- When running Auto Update to update ASR Manager 5.x to a later version of ASR Manager 5.x, then the log file to check is:

  ```
  /var/opt/asrmanager/log/asr.log
  ```

Resolution:

- Run the asr test_connection command to ensure the ASR Manager is registered properly with Oracle.
- Run the following command to check the Auto Update endpoint connection:

  ```
  asr> show_version
  ```

  Note: If using an NTLM proxy, then running Auto Update from 4.9 or 5.0.x to 5.2 is not working because of a bug that has since been fixed in ASR 5.2. Update to ASR Manager 5.2 manually.

- Verify that the ASR Manager has an internet connection and is able to reach the ASR software update server:

  https://transport.oracle.com/em/upload

C.3 ASR_PREPARATION_FAILED_DOWNLOAD_FAILED

Problem: Failed to download the package from the Oracle ASR infrastructure. It could because of slow network connection.

Resolution: Check the connection between the ASR Manager to the ASR software update server. The ASR Auto Update service endpoint is:

https://transport.oracle.com/em/upload

C.4 ASR_PREPARATION_FAILED_OCM_VERSION_CHECK_FAILED

Problem: Failed to obtain new package version from ASR Backend server. One possibility is that the ASR Manager was not able to connect to the Oracle ASR infrastructure.

Resolution: Make sure you can access the https://transport.oracle.com/em/upload URL from the ASR Manager.

C.5 ASR_INSTALL_FAILED_OASM_VERSION_CHECK_FAILED

Problem: OASM version is older than 1.4.2

Resolution: Upgrade the OASM version to 1.4.2 or above

C.6 ASR_INSTALL_FAILED_OASM_OFFLINE

Problem: ASR Auto Update failed because OASM is disabled or offline

Resolution: Enable OASM:

- For Solaris: `svcadm enable sasm`
- For Linux: `/opt/SUNWsasm/bin/sasm start-instance`

After OASM is brought online, retry ASR Auto Update manually or wait for ASR Auto Update to retry after 24 hours automatically.

C.7 ASR_INSTALL_FAILED_PACKAGE_BACKUP_FAILED

Problem: Current ASR Manager backup failed.

Resolution: As part of the ASR Auto Update process, a backup of the existing SWASR package will be attempted. If this process fails, then the ASR Auto Update process will not continue. To check the installed SWASR version, run:

- When running Auto Update to update from ASR 4.9 to ASR 5.x, check the installed ASR Manager version:
  - Solaris: `pkginfo -l SUNWswasr`
  - Linux: `rpm -qa SUNWswasr`
- When running Auto Update to update from ASR 5.x to a later version of ASR 5.x, then check the installed ASR Manager version, run:
  - Solaris: `pkginfo -l asrmanager`
  - Linux: `rpm -qa asrmanager`

If this command returns an error or if the installed version is not current, then remove the current package and install the latest ASR package manually. See Verifying Software Requirements for information on downloading the appropriate software packages.

C.8 ASR_INSTALL_FAILED_CURRENT_VERSION_CHECK_FAILED

Problem: Failed to verify existing/downloaded package versions.

Resolution: Verify the existing ASR and OASM versions.

- For ASR Manager 5.x and later:
  - Solaris: `pkginfo -l SUNWswasr`
  - Linux: `rpm -qa SUNWswasr`
- For ASR Manager 4.x:
  - Solaris:

    ```
    pkginfo -l SUNWswasr
    pkginfo -l SUNWsasm
    ```

  - Linux:

    ```
    rpm -qa SUNWswasr
    rpm -qa SUNWsasm
    ```

    Make sure both ASR 4.9 and OASM (1.4.2 or higher) are at minimum required versions required for ASR Auto Update.

C.9 ASR_INSTALL_FAILED_CURRENT_PACKAGE_REMOVAL_FAILED

Problem: Failed to remove the current Oracle ASR package (SWASR or ASRMANAGER).

Resolution: Manually remove the existing Oracle ASR package and update to latest version of the package.

C.10 ASR_INSTALL_FAILED_DEPLOYMENT_SCRIPT_FAILED

Problem: Failed to execute the deployment script.

Resolution:

- When running Auto Update to update from ASR 5.x to a later version of ASR 5.x:

  The ASR Auto Update process could not set the execute permissions for the deployment script. Check the user ID, which is set on the `/opt/asrmanager` and `/var/opt/asrmanager` directories.

  If the user ID on these folder is set to `root` or `asrm`, then try to run the `autoupdate` command manually using the asr command line:

  ```
  /opt/asrmanager/bin/asr autoupdate
  ```

- When running Auto Update to update from ASR 4.x to ASR 5.x:

  The ASR Auto Update process could not set the execute permissions for the deployment script. Check the user ID, which is set on the `/opt/SUNWswasr` and `/optSUNWsasm` directories.

  If the user ID on these folder is set to `root` or `oasm`, then try to run the `autoupdate` command manually from the `asr` command line:

  ```
  /optSUNWswasr/bin/asr autoupdate
  ```

  If ASR Auto Update fails again, then manually upgrade the ASR Manager software.

C.11 ASR_INSTALL_FAILED_RESTORED_PREVIOUS_VERSION

Problem: While a new version of the ASR software update may have been downloaded, ASR Auto Update was not able to install it. The previous version was restored. A status of `COMPLETE_FAILED` is returned in the following log file, depending on the version of ASR being updated:

- When running Auto Update to update from ASR 5.x to a later version of ASR 5.x, then the `COMPLETE_FAILED` status is returned in a `/var/opt/asrmanager/log/asr.log` log file.
- When running Auto Update to update from ASR 4.9 to ASR 5.x, then `COMPLETE_FAILED` status is returned in a `/var/opt/SUNWsasm/log/sw-asr.log.0 log` file.

Resolution: The ASR software package must be removed and then re-installed manually. To remove the current package:

- ASR Manager 5.x:
  - Solaris: `pkgrm asrmanager`
  - Linux: `rpm -e asrmanager`
- ASR Manager 4.x:

  - Solaris: `pkgrm SUNWswasr`
  - Linux: `rpm -e SUNWswasr`

See Verifying Software Requirements for information on downloading the appropriate software packages. See Installing ASR Manager Software for information on installing the ASR package.

C.12 ASR_INSTALL_FAILED_UNKNOWN_ERROR

Problem: The ASR Auto Update process failed to complete due to unknown error.

Resolution: The ASR software package must be removed and then re-installed manually. To remove the current package:

- ASR Manager 5.x:
  - Solaris: `pkgrm asrmanager`
  - Linux: `rpm -e asrmanager`
- ASR Manager 4.x:
  - Solaris: `pkgrm SUNWswasr`
  - Linux: `rpm -e SUNWswasr`

See Verifying Software Requirements for information on downloading the appropriate software packages. See Installing ASR Manager Software for information on installing the ASR package.

C.13 ASR_INSTALL_FAILED_JAR_TOOL_MISSING

Problem: If you are running JRE 1.6._04 or above (instead of JDK 1.6._04 or above), then ASR Auto Update will fail because of a missing Java jar utility. This Java jar utility that ASR Auto Update uses is not available with JRE. This issue can be corrected by using the JDK instead of the JRE.

> **Note:** If you have any issues with using the JDK instead of the JRE, you can manually download and upgrade to ASR Manager 4.5 from: http://oracle.com/asr
>
> ASR Manager Release 4.5 corrects the Java jar utility issue, which will allow ASR Auto Update to work with the JRE.

Resolution: To check for the Java jar utility, run the following command as root on the ASR Manager server:

```
# jar
```

If the Java jar utility is not available, the following output will be shown:

```
jar: command not found
```

If you receive this error message, then run the following command to check the JRE location:

```
# ls -al /usr/java
```

Output should look like this:

```
lrwxrwxrwx 1 root root 21 Dec 15 09:14 /usr/java -> /usr/j2se/jre1.6.0_xx
```

To resolve this missing Java jar utility issue:

1. Update Java to JDK (from JRE):
   a. Change the Java pointing to JDK instead of JRE:

      ```
      # rm /usr/java
      ```

   b. Add a link with the JDK version (instead of JRE). For example:

      ```
      # ln -s /usr/jdk/jdk1.6.0_xx /usr/java
      ```

   c. Test the link:

      ```
      # ls -al /usr/java
      ```

   d. Output should look like this:

      ```
      lrwxrwxrwx 1 root root 15 Apr 16 14:52 /usr/java -> /usr/ jdk/jdk1.6.0_xx
      ```

      Note: Replace _xx in the above example with the specific JDK version running on the ASR Manager server.

      Also, ensure that you are using the same Java version in the `/var/opt/SUNWsasm/configuration/config.ini` file for the `java.exec` property.

   e. Verify the Java jar utility is available. As root on the ASR Manager, run:

      ```
      # jar
      ```

      Note: You may need to manually create the symbolic link for jar. For example:

      ```
      ln -s /usr/java/bin/jar /usr/bin
      ```

2. Get the Auto Update status after fixing the Java issue. From the ASR Manager, run:

   ```
   asr> show_version
   ```

   You should now see a message that newer version of ASR Manager is available for download.

3. Run Auto Update. From the ASR Manager, run:

   ```
   asr> autoupdate
   ```

4. Once the Auto Update process is complete, run the following commands to verify the Auto Update and Connectivity status:

   ```
   asr> show_version
   asr> test_connection
   asr> heartbeat
   ```

C.14 ASR_PREP_FAILED_RPM-BUILD_MISSING

Problem: ASR Auto Update will not work on Linux, if the Linux server is missing the rpm-build package. If the rpm-build package is missing you will see the following message during ASR rpm install:

```
Warning: rpm-build package is not installed on this server. ASR Manager Auto
Update functionality will not work unless the rpm-build package is installed.

Auto Update functionality will be disabled until rpm-build package is installed.
Please install the rpm-build package and then enable Auto Update by running \"asr
enable_autoupdate\".
```

This error message will also appear in a log file if the Auto Update fails because of the missing rpm-build package. The log file is located at:

- If Auto Update is running from ASR Manager is 4.9 to 5.x, then the log file is located at:

  `/var/opt/SUNWsasm/log/sw-asr-autoupdate.log`

- If Auto Update is running from 5.x to 5.x, then the log file is located at:

  `/var/opt/asrmanager/log/autoupdate.log`

Resolution: Manually upgrade to ASR 5.3 or later. See Using Auto Update to Manually Upgrade ASR Manager Software for details.

C.15 ASR_PREP_FAILED_SELINUX_ENFORCING

Problem: ASR Auto Update will not work on Linux if the Linux server has the `seLinux` variable is not set in "permissive" mode. If the `SELinux` variable is set in *enforcing* mode, then the following message will be displayed on the command line if the `autoupdate` command is executed manually.

If the `autoupdate` command is started via timer, then the following message will be displayed in following log file:

```
SELINUX is set in \"enforcing\" mode. Cannot continue with autoupdate. Please
refer to the troubleshooting section of ASR Installation guide to resolve this
issue.
/var/opt/asrmanager/log/asr.log
```

Resolution: Manually upgrade to ASR 5.3 or later. See Using Auto Update to Manually Upgrade ASR Manager Software for details.

C.16 ASR_PREPARATION_FAILED_ASRM_VERSION_NULL

Problem: The `ASRM` package version is not available.

Resolution: Verify that the ASR Manager package installation is valid:

- Solaris: `pkginfo -l asrmanager`
- Linux: `rpm -qa asrmanager`

Remove the ASR Manager package manually and install the latest version manually:

- Solaris: pkgrm asrmanager
- Linux: rpm -e asrmanager

Download the latest ASR Manager from MOS download site and follow the instructions in Installing ASR Manager Software to install the software manually.

C.17 ASR_PREPARATION_FAILED_SSO_NULL

Problem: Oracle Single Sign-on (SSO) user name is not available.

Resolution: Ensure ASR Manager is registered with Oracle Infrastructure:

```
asr> test_connection
```

If the test connection fails, then register ASR Manager with Oracle Infrastructure:

```
asr> register
```

C.18 ASR_PREPARATION_FAILED_INVALID_OS

Problem: The Auto Update process is not able to get the operating system (OS) information from the server.

Resolution: Identify the current operating system information:

```
uname
```

Only the Oracle Solaris and Linux operating systems are supported.

- If the server is running the Solaris OS, then the result should be:

  ```
  SunOS
  ```

- If the server is running the Linux OS, then the result should be:

  ```
  Linux
  ```

C.19 ASR_PREP_FAILED_MISSING_EXECUTE_PERMS

Problem: Some of the scripts and tools required for Auto Update do not have execute permissions.

Resolution: Ensure the ASR Manager user has execute permission for the contents in the `/var/opt/asrmanager` directory.

C.20 ASR_INSTALL_FAILED_JAR_UNPACKING_FAILED

Problem: The Auto Update jar unpacking has failed on the ASR client. Most likely cause for this issue is lack of disk space on the ASR Manager server.

Resolution: Run the `df -k` command to check the disk space on the server.

If the server is running low on disk space, then try to clear the space or add more disk space on the server.

C.21 ASR_INSTALL_FAILED_SNMP_PORT_CHECK_FAILED

Problem: After Auto Update has run, the updated ASR Manager may not be able to bind the SNMP listener port. In that situation, Auto Update will fail and restore to the existing version.

The following message will appear in the `/var/opt/asrmanager/log/asr.log` log file:

```
After upgrading to $DOWNLOAD_PKG_NAME SNMP port binding failed. Restored to
```

existing version.

Resolution: The next Auto Update attempt should complete successfully. If it fails with the same error code, Manually upgrade to the latest version.

See Using Auto Update to Manually Upgrade ASR Manager Software for details.

C.22 ASR_INSTALL_FAILED_DEPLOYMENT_SCRIPT_MISSING

Problem: The Auto Update package is missing the deployment script.

Resolution: The Auto Update `jar` file could be corrupted. Download and install the ASR packages manually from My Oracle Support (`https://support.oracle.com`). See Manually Upgrading ASR Manager Software for more details.

C.23 ASR_INSTALL_FAILED_NOT_ENOUGH_SPACE

Problem: This error occurs when ASR Manager server runs our of space. This could be java heap space or physical disk space.

Resolution: The default Java Virtual Machine (JVM) maximum heap size is 1536 MB (1.5 GB) and meets the ASR Manager requirements. Make sure your ASR Manager system has 1 GB or more memory available for allocation.

Also if the ASR Manager is running low of physical disk space, then try to add more disk space to allow the Auto Update process to download the new ASR Manager package and upgrade the software.

D

Third-Party Licenses

This appendix contains licensing information about certain third-party products included with Oracle Auto Service Request (ASR).

The following sections are provided:

D.1 Open Source or Other Separately Licensed Software

Required notices for open source software products or components distributed in Oracle Auto Service Request (ASR) are identified in the following table along with the applicable licensing information. Additional notices and/or licenses may be found in the included documentation or readme files of the individual third party open source software.

Provider	Components	Version	Licensing information
Apache	Apache Derby	10.11	Copyright © 2004-2014 The Apache Software Foundation. All Rights Reserved. This license is part of the Apache Software Foundation Licenses, Version 2.0.
	Commons Codec	1.8	Copyright © 2002-2013 The Apache Software Foundation. All Rights Reserved. This license is part of the Apache Software Foundation Licenses, Version 2.0.
	Commons HttpClient	4.2.5	Copyright © 1999–2014 The Apache Software Foundation. All Rights Reserved. This license is part of the Apache Software Foundation Licenses, Version 2.0.
	Commons IO	1.4	Copyright © 2001-2008 The Apache Software Foundation. All Rights Reserved. This license is part of the Apache Software Foundation Licenses, Version 2.0.
	Felix	4.x	Copyright © 1999-2010 Apache Software Foundation. All Rights Reserved. This license is part of the Apache Software Foundation Licenses, Version 2.0.
	Felix HTTP Service	2.2.0	Copyright © 1999-2010 Apache Software Foundation. All Rights Reserved. This license is part of the Apache Software Foundation Licenses, Version 2.0.
	Felix Log	1.0.1	Copyright © 1999-2010 Apache Software Foundation. All Rights Reserved. This license is part of the Apache Software Foundation Licenses, Version 2.0.
	HttpCore	4.2.4	Copyright © 2005-2010 The Apache Software Foundation. This license is part of the Apache Software Foundation Licenses, Version 2.0.
	Jakarta Regexp	1.2	Copyright © 1999-2007 Apache Software Foundation. All Rights Reserved. This license is part of the Apache Software Foundation Licenses, Version 2.0.
	OSGi Compendium API	4.2	Copyright © 2012 Apache Software Foundation. All Rights Reserved. This license is part of the Apache Software Foundation Licenses, Version 2.0.
	snmp4j	2.2.5	Copyright © 2003-2014 Apache Software Foundation. All Rights Reserved. This license is part of the Apache Software Foundation Licenses, Version 2.0.
Apache Commons Net	Apache Commons Net FTP	1.4.1	This license is part of the Apache Software Foundation Licenses, Version 2.0.

Provider	Components	Version	Licensing information
Apache Software Foundation	Apache Commons Logging	1.1, 1.1.1	Copyright 2001-2007 The Apache Software Foundation This product includes/uses software(s) developed by 'an unknown organization': ▪ Unnamed - `avalon-framework:avalon-framework:jar:4.1.3` ▪ Unnamed - `log4j:log4j:jar:1.2.12` ▪ Unnamed - `logkit:logkit:jar:1.0.1` This license is part of the Apache Software Foundation Licenses, Version 2.0.
	Log4j	1.2.17	Copyright © 2007 Apache Software Foundation. This license is part of the Apache Software Foundation Licenses, Version 2.0.
			This license is part of the Apache Software Foundation Licenses, Version 2.0.
			This license is part of the Apache Software Foundation Licenses, Version 2.0.
JDOM	JDOM	1.1	Copyright (C) 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: 1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer. 2. 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. 3. 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. 4. 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. In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following: "This product includes software developed by the JDOM Project (http://www.jdom.org/)." Alternatively, the acknowledgment may be graphical using the logos available at http://www.jdom.org/images/logos. 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 /www.jdom.org/.

Provider	Components	Version	Licensing information
QOS.ch	SLF4J	1.7.5	Copyright © 2004-2013 QOS.ch All rights reserved. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

D.2 Apache Software Foundation Licenses, Version 2.0

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

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

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

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

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

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

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

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

   "Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions,

annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

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

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

2. Grant of Copyright License.

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

3. Grant of Patent License.

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

4. Redistribution.

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

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

   2. You must cause any modified files to carry prominent notices stating that You changed the files; and

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

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

5. Submission of Contributions.

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

6. Trademarks.

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

7. Disclaimer of Warranty.

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

8. Limitation of Liability.

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

9. Accepting Warranty or Additional Liability.

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

END OF TERMS AND CONDITIONS

Index

F

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X