# Oracle® Auto Service Request

## Quick Installation Guide for Oracle Exadata Database Machine

25.2
F29247-16
October 2025

Oracle Auto Service Request Quick Installation Guide for Oracle Exadata Database Machine, 25.2

F29247-16



Primary Author: Peter Fusek

Contributing Authors: Vira Goorah, Zheren Zhang

# Contents

# 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. Oracle ASR is designed to enable faster problem resolution by eliminating the need to initiate contact with Oracle Support Services for hardware failures.

For more information about Oracle ASR, see https://www.oracle.com/servers/technologies/auto-service-request.html.



## Audience

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

1

# Getting Started with Oracle ASR Installation

This document describes how to install and configure Oracle Auto Service Request (ASR) for Oracle Exadata.

Topics:



## About Oracle ASR

Oracle Auto Service Request (ASR) is a secure, scalable, customer-installable software feature of warranty and Oracle Support Services. Oracle ASR provides auto-case generation for common hardware component faults.

Oracle ASR simplifies support operations by automatically generating support records for common component faults. Oracle ASR auto-case generation also accelerates problem resolution by eliminating the need for you to contact Oracle Support Services for common failures. Auto-case generation reduces both the number of phone calls that you make to obtain support and the phone time required for problem resolution. Oracle ASR does not provide system management or monitoring. Oracle ASR is designed to generate Oracle service requests automatically when certain types of faults are detected on Oracle products that are qualified for Oracle ASR.

Oracle ASR works only for specific component faults. Most of the common components, such as disks, fans, and power supplies, are covered. However, some components are not covered. For example, Oracle ASR does not cover RDMA Network Fabric events; there are specific images and specific firmware for the RDMA Network Fabric switch that you must use. You cannot upgrade these components independently.

Oracle ASR is easy to install and deploy. To ensure security, you have complete control over Oracle ASR.

> **Note**
>
> Oracle recommends that you implement a system management and monitoring solution in addition to Oracle ASR, such as Oracle Enterprise Manager Cloud Control or Oracle Enterprise Manager Ops Center.

> **Caution**
>
> The commands in this document are provided for your convenience. However, the copy and paste functionality can paste different content than what is published in the guide. To ensure that the command text that you paste is identical to the text that you copy, confirm that your console session is set to receive data as UTF-8.

# Recommended Configuration for Oracle ASR

This section describes the Oracle ASR configuration.

Oracle recommends that you install Oracle ASR Manager on an external, standalone server. This server receives fault telemetry information from Oracle Exadata servers. This server must run an Oracle Solaris or Oracle Linux operating system.

> **Note**
>
> While not recommended, you can install Oracle ASR Manager on one of the Oracle Exadata servers.

# Prerequisites for Oracle ASR

This section describes the prerequisites for Oracle Auto Service Request (ASR).

Topics:

- Server and Network Requirements for Oracle ASR
  Ensure that the following conditions are met before installing Oracle Auto Service Request (ASR).
- Oracle Auto Service Request (ASR) Software Requirements
  You need `root` access to install the software and to configure Oracle ASR Manager.

## Server and Network Requirements for Oracle ASR

Ensure that the following conditions are met before installing Oracle Auto Service Request (ASR).

- Ensure that you have access to Oracle Support Services. Also ensure that your contact information is current and correct.
- Ensure that all of your assets have an assigned contact and that the contact information is current and correct.
- Identify and designate a system to serve as the Oracle ASR Manager.
- Identify and verify all of your Oracle ASR assets.
- Ensure connectivity to the Internet using HTTPS.
- Ensure the network connectivity of the operating system to the designated Oracle ASR Manager. Network connectivity is required for Oracle Exadata assets, Integrated Lights Out Manager (ILOM), and `eth0`.
- Oracle ASR Manager generally supports IPv6. However, note the following requirements and limitations:

  - Before attempting to use IPv6, ensure it is enabled on the Oracle ASR Manager server.
  - The connection between Oracle ASR Manager and the Oracle Support gateway supports only IPv4.
  - The connections between Oracle ASR Manager and each Cisco network switch in the Oracle Exadata rack support only IPv4.
- If you are using SNMP V3, you must be using Oracle ASR release 4.3 or higher.

**Related Topics**

- My Oracle Support

# Oracle Auto Service Request (ASR) Software Requirements

You need `root` access to install the software and to configure Oracle ASR Manager.

- **Oracle ASR Manager:** To install Oracle ASR Manager on a standalone server that is running either Linux or Solaris, refer to "Installing and Registering Oracle ASR Manager Software" in *Oracle Auto Service Request (ASR) Manager User's Guide*.
- **Database Server:** Oracle Exadata System Software release 11.2.1.3.1 or later.
- **Oracle Exadata System Software:**
  - Release 12.1.2.1.1 and later
  - Release 11.2.1.3.1 and later
- To configure trap destinations, use one of the following options:
  - **Oracle Exadata Deployment Assistant (OEDA):** OEDA prompts you for information used to configure Oracle ASR. OEDA configures the traps and activates the Oracle ASR assets.
  - **`dcli` Utility:** Refer to the `dcli` utility chapter in *Oracle Exadata System Software User's Guide* for instructions about enabling SSH for the `dcli` utility.
- **Port 162 Availability:** Port 162 is the SNMP port. Use the SNMP port to configure fault telemetry destinations. You can assign this port to a different port address based on your network requirements. In a managed environment, you may need to must the port from the default port assignment for Oracle ASR to work correctly.
- **The `dcli` Utility:** While not required for Oracle ASR, the `dcli` utility enables you to simultaneously configure all of the servers. You can also use `dcli` to configure the storage servers at the same time.

Refer to the topic "Setting User Equivalence" in *Oracle Exadata Database Machine Extending and Multi-Rack Cabling Guide* for instructions about enabling SSH for the `dcli` utility. Depending on your environment restrictions, it is possible that the `dcli` utility is not configured. See *Oracle Exadata System Software User's Guide* for more information about the `dcli` utility.

The `dcli` utility commands in this document run commands that require equivalency with the `root` or `celladmin` user, depending on the command. Ensure that the user account that runs the `dcli` utility command is configured with the correct equivalency.

**Related Topics**

- ASR Manager User's Guide
- *Oracle Exadata Database Machine Extending and Multi-Rack Cabling Guide*

- *Oracle Exadata System Software User's Guide*

2

# Configure Fault Notification Destinations

Use the following procedures to configure fault telemetry destinations on Oracle Exadata Storage Server and Oracle Exadata Database Server.

Topics:



## Fault Telemetry Options

You can configure the fault notification destinations using various methods.

Adding SNMP trap destinations using Oracle Exadata Deployment Assistant (OEDA) is the recommended method for new installations. After the initial configuration with OEDA, you can modify or add new fault notification destinations using the command line utilities, such as DBMCLI, CellCLI, or `dcli`.

To configure fault notification destinations, modify the SNMP subscriber attribute on the database or storage servers. The information you provide defines the SNMP trap destination.

> **Note**
>
> Oracle ASR can only use the management network. Ensure that the management network is configured to enable Oracle ASR to run on either `eth0` on the interfaces, or `net0` on the rear of the server.

### SNMP Subscriber Options

When configuring the SNMP subscriber, you set some or all of the following options:

- `host=`*`ASR Manager host name or IP address`* specifies the Oracle ASR Manager host name or IP address. The Oracle ASR Manager host name can be used when DNS is enabled for the site. If DNS is not running, then the IP address is preferred. However, you

can also use the Oracle ASR Manager host name if the entry is added to the `/etc/hosts` file.

- `type=asr` or `type=v3asr` identifies the Oracle ASR Manager as a special type of SNMP subscriber. If you want to use ASR in conjunction with SNMP v3, use `type=v3asr`. See Using Oracle ASR with SNMP v3.
- `community=`*`SNMP community`* identifies the SNMP community being used. This value is used only in conjunction with SNMP v1 (`type=asr`) and varies based on your network configuration.
- `snmpUser=`*`SNMP user`* identifies the SNMP v3 user being used. This value is used only in conjunction with SNMP v3 (`type=v3asr`) and varies based on your network configuration.
- `port=`*`SNMP port`* specifies the SNMP port number being used. You can configure the specific port number based on your network requirements. Or, you may need to use a specific port value in order for Oracle ASR to work correctly in a managed environment.
- `asrmPort=`*`ASRM port`* is an optional element that supports automatic diagnostic package uploads for Service Requests (SR). The default value is 16161. If you plan to use HTTP for upload, then the value should match the HTTP port configured on Oracle ASR Manager. If you plan to use HTTPs for upload, then the value should match the HTTPs port configured on Oracle ASR Manager. The value should be set to the same value as displayed for `HTTP Port` or `HTTPS/SSL Port` in the output of the command `asr show_http_receiver` on the Oracle ASR Manager host.
- `fromIP` enables you to specify an IP address from which the trap is sent. If this field is not specified, then it defaults to the IP address associated with `eth0`. To support automatic diagnostic package uploads, you must set `fromIP` on the database nodes to the value of the IP address of the `eth0` network interface. Otherwise, use this field if the default IP address is not registered with Oracle ASR Manager. Oracle ASR Manager only processes SNMP traps that are sent from IP addresses that Oracle ASR Manager recognizes.

  The `fromIP` attribute is allowed only for `snmpSubscribers` whose type is either `asr` or `v3asr`.

# Specifying ASR Configuration Details Using OEDA

You can specify ASR configuration details using Oracle Exadata Deployment Assistant (OEDA).

You can specify essential ASR configuration details in the Alerting section of the OEDA Web interface.

The OEDA Web interface captures ASR configuration information including:

- ASR Manager Hostname
- Contact Name and Email for the ASR technical contact
- My Oracle Support Account Name
- Optional HTTP proxy configuration information

After deployment, you can use the `ALTER CELL` or `ALTER DBSERVER` commands to customize the ASR configuration details.

**Related Topics**

- Using Oracle Exadata Deployment Assistant

# Configuring the SNMP Subscriber for Fault Notification

Use the `ALTER CELL` or `ALTER DBSERVER` commands to configure SNMP trap destinations for Exadata servers.

1. Configure the SNMP subscriber on each database server.
   a. Log in to the database server as the `root` user.
   b. Retrieve the current SNMP subscriber configuration for the server.

      ```
      # dbmcli -e list dbserver attributes snmpsubscriber
      ```

      If the SNMP subscriber has not been configured, the operating system prompt reappears without displaying any information.
   c. Modify the `snmpSubscriber` attribute for the server.

      If you want to add only a single SNMP subscriber for Oracle ASR, then enter a command similar to the following:

      ```
      # dbmcli -e alter dbserver
      snmpSubscriber="((host='asrm1.example.com',port=162,
      community=public,type=asr,fromIP='management_IP_addr',asrmPort=ASR_Mgr_h
      ttp_or_https_port))"
      ```

      If you need to add multiple fault notification destinations, then specify multiple SNMP subscribers using a comma-delimited list. For example:

      ```
      # dbmcli -e alter dbserver
      snmpSubscriber="((host='asrm1.example.com',port=162,
      community=public,type=asr,fromIP='management_IP_addr',asrmPort=ASR_Mgr_h
      ttp_or_https_port),
      (host='asrm2.example.com',port=162,community=public,type=asr,fromIP='man
      agement_IP_addr',
      asrmPort=ASR_Mgr_http_or_https_port))"
      ```

> **Note**
>
> - If you want to use ASR in conjunction with SNMP v3, modify the command to specify `type=v3asr` along with a specific SNMP user. See Using Oracle ASR with SNMP v3.
> - To support automatic diagnostic package uploads, you must set `fromIP` on the database nodes to the value of the IP address of the management network interface.
> - By default, the specified `snmpSubscriber` value replaces any previous configured value. If the `snmpSubscriber` value is already configured, and you want to add to the list of SNMP targets, then use the += operator instead of =.
>
>  For example:
>
>  ```
>  alter dbserver snmpSubscriber+="snmpSubscriber_value"
>  ```

d. Verify the SNMP subscriber attribute has been updated on the server.

```
# dbmcli -e list dbserver attributes snmpsubscriber
```

2. Configure the SNMP subscriber on each Oracle Exadata Storage Server.
   a. Log in to the storage server as `celladmin`, or an equivalent OS user.
   b. Retrieve the current SNMP subscriber configuration for the server.

```
# cellcli -e list cell attributes snmpsubscriber
```

   If the SNMP subscriber has not been configured, the operating system prompt reappears without displaying any information.

   c. Modify the `snmpSubscriber` attribute for the server.

   If you want to add only a single SNMP subscriber for Oracle ASR, then enter a command similar to the following:

```
# cellcli -e alter cell
snmpSubscriber="((host='asrm1.example.com',port=162,
community=public,type=asr,fromIP='management_IP_addr',asrmPort=ASR_Mgr_h
ttp_or_https_port))"
```

   If you need to add multiple fault notification destinations, then specify multiple SNMP subscribers using a comma-delimited list. For example:

```
# cellcli -e alter cell
snmpSubscriber="((host='asrm1.example.com',port=162,
community=public,type=asr,fromIP='management_IP_addr',asrmPort=ASR_Mgr_h
ttp_or_https_port),
(host='asrm2.example.com',port=162,community=public,type=asr,fromIP='man
agement_IP_addr',
asrmPort=ASR_Mgr_http_or_https_port))"
```

> **Note**
>
> - If you want to use ASR in conjunction with SNMP v3, modify the command to specify `type=v3asr` along with a specific SNMP user. See Using Oracle ASR with SNMP v3.
> - To support automatic diagnostic package uploads, you must set `fromIP` on the database nodes to the value of the IP address of the management network interface.
> - By default, the specified `snmpSubscriber` value replaces any previous configured value. If the `snmpSubscriber` value is already configured, and you want to add to the list of SNMP targets, then use the += operator instead of =.
>
>  For example:
>
>  ```
>  alter cell snmpSubscriber+="snmpSubscriber_value"
>  ```

d. Verify the SNMP subscriber attribute has been updated on the server.

```
# cellcli -e list cell attributes snmpsubscriber
```

Alternatively, you can use the `dcli` utility to run each command on a specified group of servers.

# Using Oracle ASR with SNMP v3

Simple Network Management Protocol (SNMP) v3 is supported on Oracle Exadata Storage Servers and Oracle Exadata Database Servers.

To use SNMP v3 you must be using Oracle ASR release 4.3 or later.

1. Choose a user or define a new user for SNMP v3.
2. Modify the user's SNMP subscriber information:
   - On a database server, use DBMCLI commands similar to the following:

     ```
     ALTER DBSERVER snmpUser=((name=v3user,authprotocol=SHA,
     authpassword=*,privprotocol=AES,privpassword=*))

     ALTER DBSERVER snmpsubscriber=((host=asrhost, port=162, SnmpUser=
     v3user, type=v3asr))
     ```

   - On a storage server, use CellCLI commands similar to the following:

     ```
     ALTER CELL snmpUser=((name=v3user,authprotocol=SHA,
     authpassword=*,privprotocol=AES,privpassword=*))

     ALTER CELL snmpsubscriber=((host=asrhost, port=162, SnmpUser=
     v3user, type=v3asr))
     ```

   DBMCLI and CellCLI prompt you for a password when adding the `snmpUser`.

The Integrated Lights Out Manager (ILOM) SNMP user for Oracle ASR and its notification rules are automatically set in the storage server or database server ILOM when `snmpSubscriber` is added with type `v3ASR`.

3. From Oracle ASR Manager, reference the same user name, protocols and passwords to add the v3 user.

```
asr> add_snmpv3_user -u v3user_name -e engineId
[,engineId2, ...] -pp AES
```

You must include both server (cell or compute) and ILOM engine IDs. By default, engine IDs are the cell name or compute node name. ILOM engine IDs are the cell name or compute node name with a `-m` suffix, for example, `mycell` and `mycell-m`.

You are prompted to create both authentication and privacy passwords for the v3 user. The passwords you specify must match the passwords set on the cells and compute nodes.

Oracle ASR Manager only supports the SHA protocol for authentication and the AES protocol for privacy and encryption with ILOM.

**Related Topics**

- ALTER CELL
- ALTER DBSERVER
- ASR Manager User's Guide

# Verifying the Server Configuration

You can verify the SNMP subscriber configuration on each individual server or on a group of servers.

For the Exadata database servers:

- You can use the `dcli` utility to verify the configuration on a group of database servers. Run the following command using a server and OS account that has SSH equivalency with the `root` user on all the database servers listed in the `dbs_group` file:

```
# dcli -g dbs_group -l root "dbmcli -e list dbserver attributes
snmpSubscriber"
```

- Alternatively, you can run the following command to individually verify the configuration on each database server:

```
# dbmcli -e list dbserver attributes snmpSubscriber
```

For the Exadata Storage Servers:

- You can use the `dcli` utility to verify the configuration on a group of storage servers. Run the following command using a server and OS account that has SSH equivalency with the `celladmin` user on all the storage servers listed in the `cell_group` file:

```
# dcli -g cell_group -l celladmin "cellcli -e list cell attributes
snmpSubscriber"
```

- Alternatively, you can run the following command to individually verify the configuration on each storage server:

  ```
  # cellcli -e list cell attributes snmpSubscriber
  ```

3

# Enabling Automatic DiagPack Upload for Oracle ASR

You can upload diagnostic packages to Oracle ASR automatically.

In Oracle Exadata System Software release 12.2.1.1.0, Management Server (MS) communicates with Oracle ASR Manager to upload a diagnostic package containing information relevant to the Oracle ASR automatically. MS provides support to automatically upload diagpacks over HTTPS starting with Oracle Exadata System Software release 19.1.0.

For Oracle ASR Manager release 5.7 or later, the `http_receiver` is enabled by default, but the HTTPS/SSL configuration might not be. If you want to use HTTP to upload the diagnostic packages, then verify that `HTTP Port` has the same value as `asrmPort` on database and storage servers. If you want to use HTTPS to upload the diagnostic packages, then verify that HTTPS/SSL configuration is enabled and that `HTTPS/SSL Port` has the same value as `asrmPort` on database and storage servers. If you are using a release earlier than Oracle ASR Manager release 5.7, then you must upgrade to release 5.7 or later to use the Automatic DiagPack Upload feature.

1. Verify the `http_receiver` is enabled and determine the port being used.

   Run the following command from Oracle ASR Manager:

   ```
   asr show_http_receiver
   ```

   The following example shows the output with HTTPS enabled:

   ```
   HTTP Receiver configuration:

   HTTP Receiver Status: Enabled
   Host Name: exa-asr.example.com
   SFB forward: true
   HTTP Port: 16161
   HTTPS/SSL Port: 8701
   HTTPS/SSL: Enabled

...
   ```

   The following example shows the output with only HTTP enabled:

   ```
   HTTP Receiver configuration:

   HTTP Receiver Status: Enabled
   Host Name: 10.65.41.141
   HTTP Port: 16161
   HTTPS/SSL configuration is not enabled.
   ```

```
...
```

2. Verify the port used by `http_receiver` for Oracle ASR is the same as the `asrmPort` set for the `snmpSubscriber` on the database servers and storage servers.

   a. Check the `asrmPort` for the `snmpSubscriber` on the database servers:

   ```
   dbmcli -e list dbserver attributes snmpSubscriber
   ```

   The output will be similar to the following:

   ```
       ((host=engsys-asr1.example.com,port=162,community=public,
   type=asr,fromIP=10.242.00.55,asrmPort=16161))
   ```

   b. Check the `asrmPort` for the `snmpSubscriber` on the storage servers:

   ```
   cellcli -e list cell attributes snmpSubscriber
   ```

   The output will be similar to the following:

   ```
       ((host=engsys-asr1.example.com,port=162,community=public,
   type=asr,fromIP=10.242.00.55,asrmPort=16161))
   ```

3. If necessary, enable the `http_receiver` or change the port to match the `asrmPort` value.

   Oracle Exadata Deployment Assistant (OEDA) automatically enables HTTPS/SSL for Oracle ASR Manager and imports the certificate on database and storage servers. However, it is still possible that you may need to manually enable HTTPS/SSL for Oracle ASR Manager under some circumstances. Refer to Enabling HTTPS/SSL on Oracle ASR Manager for instructions on how to configure HTTPS uploads for Oracle ASR Manager.

   If the `http_receiver` port is not the same, you can either disable `http_receiver` and enable it again using the same port as `asrmPort`, or you can set the `asrmPort` of `snmpSubscriber` to match that of `http_receiver`.

   To enable `http_receiver`, use a command similar to the following, where *port* is the port the `http_receiver` listens on for either HTTP or HTTPs.

   ```
   asr enable_http_receiver -p port
   ```

   > **Note**
   >
   > The port specified for the `http_receiver` has to be the same as the `asrmPort` specified for the `snmpSubscriber` on the database servers and storage servers for the automatic DiagPack upload feature to work.

4. If the `snmpSubscriber` was configured on the database or storage server before enabling HTTPS/SSL for Oracle ASR Manager, then restart MS.

   The MS on the database and storage servers need to be restarted before you can use HTTPS to upload the diagnostic packages. If HTTPS/SSL was enabled on for Oracle ASR Manager before configuring `snmpSubscriber` on the database and storage servers, then you do not need to restart MS.

- Enable HTTP Access on Oracle ASR Manager
  You can send Oracle Auto Service Request (ASR) fault events and telemetry to Oracle Support Services using XML over HTTP to the Oracle ASR Manager.
- Enabling HTTPS/SSL on Oracle ASR Manager
  You can use either a root-signed certificate or a self-signed certificate to enable HTTPS/SSL on Oracle ASR Manager.

**Related Topics**

- Automatic Diagpack Upload for Oracle ASR

# Enable HTTP Access on Oracle ASR Manager

You can send Oracle Auto Service Request (ASR) fault events and telemetry to Oracle Support Services using XML over HTTP to the Oracle ASR Manager.

Select a port for the HTTP receiver that is appropriate for your network environment and does not conflict with other network services.

1. View the current HTTP receiver configuration port and status.

   ```
   asr> show_http_receiver
   ```

2. If HTTP is not already configured, enable the HTTP receiver.

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

   If you see the following error and DNS is not available, then you will need to configure the HTTP receiver manually:

   ```
   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.
   ```

   To configure HTTP receiver manually, perform the following steps:

   a. Set the IP address of Oracle ASR Manager.

      ```
      /opt/asrmanager/bin/asr set_property org.osgi.service.http.host
      IP_address_of_ASR_manager
      ```

   b. Set the HTTP port.

      ```
      /opt/asrmanager/bin/asr set_property org.osgi.service.http.port
      http_port
      ```

   c. Enable HTTP.

      ```
      /opt/asrmanager/bin/asr set_property org.apache.felix.http.enable true
      ```

   d. Restart the Oracle ASR Manager.

3. Verify the HTTP receiver is up and running.

In a browser, enter the following address:

```
http://asr_manager_host:port_number/asr
```

You should see a message indicating that the HTTP receiver is up and running.

# Enabling HTTPS/SSL on Oracle ASR Manager

You can use either a root-signed certificate or a self-signed certificate to enable HTTPS/SSL on Oracle ASR Manager.

Generate and install the SSL Certificate into the Key Store specific to the Java/JDK used by Oracle ASR Manager.

1. Generate the Certificate Signing Request.
   a. Go to the `/java/bin` directory and create the keystore file.

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

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

      If prompted for the first and last name, enter the host name of the machine where Oracle ASR Manager is installed.
   d. Enter the following command:

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

   e. Enter the valid key store password and specify the key password.
   f. Submit the Certificate Signing Request *certRequestFile*`.cer` to the Certificate Authority, and request a Certificate.
2. Install the Certificate after you receive it from the Certificate Authority.

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

   After running the `keytool -import` command, enter the valid key store password and specify the key password.
3. When the SSL certificate from a trusted authority has been loaded into keystore, perform the following tasks on Oracle ASR Manager:

   Trust Store information is same as the Key Store information.
   a. Set the IP address.

      ```
      # asr
      asr> set_property org.osgi.service.http.host IP_address_of_ASR_manager
      ```

   b. Set the HTTPS port.

> **Note**
>
> The value of `org.osgi.service.http.port.secure` should match the HTTPs port configured on Oracle ASR Manager. The value should be set to the same value as displayed for "HTTP Port" or "HTTPS/SSL Port" in the output of the command:
>
> ```
> asr show_http_receiver
> ```

```
asr> set_property org.osgi.service.http.host set_property
org.osgi.service.http.port.secure https_port
```

c. Set the path to the keystore file.

```
asr> set_property org.apache.felix.https.keystore https_keystore
```

d. Set keystore password.

```
asr> set_property org.apache.felix.https.keystore.password
https_keystore_password
```

e. Set the key password.

```
asr> set_property org.apache.felix.https.keystore.key.password
https_keystore_key_password
```

f. Set the path of the truststore to the same as the keystore file.

```
asr> set_property org.apache.felix.https.truststore https_truststore
```

g. Set the truststore password on the same keystore password value.

```
asr> set_property org.apache.felix.https.truststore.password
https_truststore_password
```

h. Enable HTTPS for Oracle ASR Manager.

```
asr> set_property org.apache.felix.https.enable true
```

The passwords in the above commands can be plain text or obfuscated, as shown in the following example:

```
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
```

After running these Java commands, the output shows the obfuscated password. Obfuscated password values are denoted by the prefix `OBF:`. Copy and paste the output

line starting with `OBF:` (including the text 'OBF:') into the above Oracle ASR commands instead of the plain text password. The following is an example of the output.

```
2018-05-04 09:34:17.429:INFO::main: Logging initialized @118ms
password
OBF:1v2j20771x1b206z
MD5:5f4dcc9ac6b3e1a84cebb7b40329cf99
```

4. Restart Oracle ASR Manager.

   ```
   $ service asrm restart
   ```

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

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

6. On each database server and storage server, import the certificate used to enable HTTPS/SSL.

   ```
   keytool -import -trustcacerts -keystore keystore_location
   -storepass keystore_password -noprompt -alias cert_alias_name -file
   cert_file_path
   ```

   In the `keytool` command, specify the *keystore_location* value as follows:

   - On each storage server, specify `/opt/oracle/cell/cellsrv/java/lib/security/cacerts`.
   - On each database server, use `/opt/oracle/dbserver/dbms/java/lib/security/cacerts`.

7. Verify the certificate has been imported.

   ```
   keytool -list -v -keystore keystore_location
   -storepass keystore_password
   ```

# 4 Activating Nodes on Oracle ASR Manager

Use this procedure to activate nodes on Oracle ASR Manager.

> **Note**
>
> - Run the commands listed in this section only on Oracle ASR Manager hosts, not on Oracle Exadata servers.
> - Repeat these commands for each Oracle Exadata server that you attach to Oracle ASR.

1. Run the following command to validate Integrated Lights Out Manager (ILOM) auto-activation and to determine whether the network and ILOM are correctly configured:

   ```
   # asr list_asset
   ```

   The output should be similar to the following:

   ```
   IP_ADDRESS      HOST_NAME       SERIAL_NUMBER   ASR       PROTOCOL
   SOURCE          PRODUCT_NAME
   -------------   -------------   -------------   --------  ----------
   --------------  ---------------
   10.111.44.111   scac01cel08-c   12345abcde      Enabled   SNMP
   ILOM            SUN SERVER X4-2L
   10.222.33.111   scac01cel10-c   43315abcde      Enabled   SNMP
   ILOM            SUN SERVER X4-2L
   10.333.11.111   scac01cel09-c   51423abcde      Enabled   SNMP
   ILOM            SUN SERVER X4-2L
   10.133.22.111   scac01cel08     12345EDBCA      Enabled   SNMP,HTTP
   EXADATA-SQ,ADR  SUN SERVER X4-2L
   10.133.11.111   scac01cel10     12345BACDE      Enabled   SNMP,HTTP
   EXADATA-SQ,ADR  SUN SERVER X4-2L
   10.444.33.111   scac01db06      12345XXAAX      Enabled   SNMP,HTTP
   EXADATA-SQ,ADR  SUN SERVER X4-2
   ```

   - If all of the ILOMs for Oracle Exadata Database Machine servers are in the list, then skip to Step 3.
   - If some of the ILOMs are missing from the list, then proceed with Step 2.

2. Activate ILOM and run one of the following commands:

   - ILOM IP address

     ```
     # asr activate_asset -i Node ILOM IP
     ```

- ILOM host name

  ```
  # asr activate_asset -h Node ILOM host name
  ```

> **Note**
>
> If the activation did not work, then confirm that you used the IP address of the ILOM and not the server.

3. Activate the Oracle Exadata operating system side of Oracle ASR by running one of the following commands:

   - ```
     # asr activate_exadata -i Node-IP-address -h Node-host-name -l Node-ILOM-IP
     ```

   - ```
     # asr activate_exadata -i Node-IP-address -h Node-host-name -n Node-ILOM-hostname
     ```

4. Run the following command to verify that all of the Oracle Exadata servers are visible on Oracle ASR Manager:

   ```
   # asr list_asset
   ```

5. Approve and assign contacts to the Oracle Exadata servers.

**Related Topics**

- How To Manage and Approve Pending Oracle ASR Assets In My Oracle Support (My Oracle Support Doc ID 1329200.1)

5

# Validating SNMP Subscriber Configurations on Oracle Exadata

You can validate the ASR SNMP configuration on each individual server or on a group of servers.

Each time a validation command is executed, the end-to-end ASR process is tested and an email is sent indicating that the ASR service inside Oracle Support received the validation request. No service request is opened for validation requests.

For the Exadata database servers:

- You can use the `dcli` utility to validate the configuration on a group of database servers. Run the following command using a server and OS account that has SSH equivalency with the `root` user on all the database servers listed in the `dbs_group` file. If your configuration uses ASR in conjunction with SNMP v3, modify the command to specify `type=v3asr`.

  ```
  # dcli -g dbs_group -l root "dbmcli -e alter dbserver validate snmp
  type=asr"
  ```

- Alternatively, you can run the following command to individually validate the configuration on each database server. If your configuration uses ASR in conjunction with SNMP v3, modify the command to specify `type=v3asr`.

  ```
  # dbmcli -e alter dbserver validate snmp type=asr
  ```

For the Exadata Storage Servers:

- You can use the `dcli` utility to validate the configuration on a group of storage servers. Run the following command using a server and OS account that has SSH equivalency with the `celladmin` user on all the storage servers listed in the `cell_group` file. If your configuration uses ASR in conjunction with SNMP v3, modify the command to specify `type=v3asr`.

  ```
  # dcli -g cell_group -l celladmin "cellcli -e alter cell validate snmp
  type=asr"
  ```

- Alternatively, you can run the following command to individually validate the configuration on each storage server. If your configuration uses ASR in conjunction with SNMP v3, modify the command to specify `type=v3asr`.

  ```
  # cellcli -e alter cell validate snmp type=asr
  ```

After validation, Oracle sends e-mail notifications to:

- The registration user specified in the Oracle ASR Manager `asr register` command.
- The asset contact that is assigned in My Oracle Support.
- The distribution e-mail list that is assigned in My Oracle Support (optional).

6

# Configuring Switches for Oracle ASR



## Configuring Cisco Switches for Oracle ASR

This topic describes how to configure and activate Cisco switches for Oracle Auto Service Request (ASR).

Commencing with Oracle Exadata System Software release 21.2.0, when you use the Patch Manager utility (`patchmgr`) to upgrade the Cisco switch firmware, a new monitoring component is also installed on the Cisco switch. The new monitoring component propagates switch alerts to Oracle ASR, enabling automated problem detection and resolution. This capability covers the Management Network Switch and RoCE Network Fabric switches present in X8M and later systems. It also covers Management Network Switch model 9348 present in earlier X8 and some X7 systems.

After installation, the switch monitoring component must be configured to send alerts to the Oracle ASR manager. Perform the following configuration once for each switch:

1. Access the switch using SSH, and log in as the `admin` user with the administrator password.

   > **Note**
   >
   > If SSH has not been configured, then use Telnet to access the switch as the `admin` user.

2. On Management Network Switch model 9348 switches only, configure the switch to use virtual routing (`vrf`) by default.

   ```
   Switch# python bootflash:scripts/asr/bin/asr set vrf=default
   ```

   > **Warning**
   >
   > Do not run this command on any switch other than Management Network Switch model 9348.

3. If the Oracle ASR manager endpoint location uses HTTPS, copy the certificate from the Oracle ASR manager to the switch.

   The certificate must be copied to `bootflash:scripts/asr/.run/ca.pem` on the switch.

For example, you could use the following commands on a host that has SSH access to the switch and the Oracle ASR manager:

```
# openssl s_client -showcerts -servername ASR_host -connect ASR_host:port
</dev/null 2>/dev/null|openssl x509 -outform PEM > ca.pem
# scp ca.pem switch:bootflash:scripts/asr/.run/ca.pem
```

In the preceding commands:

- *ASR_host* - Specifies the Oracle ASR manager host name or IP address.
- *port* - Specifies the port number for the Oracle ASR manager endpoint. Typically, port 16161 is used.
- *switch* - Specifies the hostname or IP address of the switch.

4. Set the Oracle ASR manager endpoint location.

```
Switch# python bootflash:scripts/asr/bin/asr set endpoint="ASR_endpoint"
```

In the command, specify the URL for the Oracle ASR manager endpoint.

For example:

```
Switch# python bootflash:scripts/asr/bin/asr set endpoint="https://
192.0.2.108:16161"
```

5. Enable the Oracle ASR manager endpoint.

```
Switch# python bootflash:scripts/asr/bin/asr set state=enabled
```

6. Verify the configuration.

```
Switch# python bootflash:scripts/asr/bin/asr show
```

The following is an example of the expected command output:

```
...
ASR Properties:
       status : Registered
       state : enabled
   send-event :
       endpoint : http://192.0.2.108:16161
...
```

7. Send a test event to Oracle ASR.

```
Switch# python bootflash:scripts/asr/bin/asr set send-event=test
```

Confirm that the test event is received by Oracle ASR.

8. Exit the switch terminal session.

```
Switch# exit
```

**Related Topics**

- Upgrading RoCE Network Fabric Switch Firmware
- Patchmgr Syntax for RoCE Network Fabric Switches
- Patchmgr Syntax for the Management Network Switch

# Configuring InfiniBand Switches for Oracle ASR

This topic describes how to configure and activate InfiniBand switches for Oracle Auto Service Request (ASR).

To configure Sun Datacenter InfiniBand Switch 36 and QDR InfiniBand Gateway Switches for Oracle ASR, follow the instructions outlined in My Oracle Support Document 1902710.1.

**Related Topics**

- How to configure Datacenter InfiniBand Switch 36 & QDR InfiniBand Gateway Switches for ASR (My Oracle Support Doc ID 1902710.1)

A

# Additional Resources for Oracle Auto Service Request (ASR)

Refer to these sections for additional resources to configure and run Oracle ASR.

**Oracle ASR**

- Oracle ASR product page:

  http://www.oracle.com/asr

- Oracle ASR user documentation:

  See the Oracle ASR documentation at `http://docs.oracle.com/cd/E37710_01/nav/products.htm`

- Download Oracle ASR software (My Oracle Support login required): Oracle Auto Service Request (ASR) [My Oracle Support Note 1185493.1]

- How To Manage and Approve Pending ASR Assets In My Oracle Support [My Oracle Support Note 1329200.1]

**Oracle Exadata Database Machine Documentation**

- CellCLI command reference: *Oracle Exadata System Software User's Guide*
- dcli command reference: *Oracle Exadata System Software User's Guide*
- DBMCLI command reference: *Oracle Exadata Database Machine Maintenance Guide*

**My Oracle Support**

- https://support.oracle.com

B

# Third-Party Licenses for Oracle ASR

Oracle Auto Service Request (ASR) includes third-party products.

For a complete list of the licensed third-party products, refer to Appendix C, "Third-Party Licenses" in *Oracle Auto Service Request (ASR) Manager User's Guide*.

**Related Topics**

- ASR Manager User's Guide