Oracle® ILOM Protocol Management Reference for SNMP and IPMI Firmware Release 3.2.x

Part No: E37449-15
January 2017

Oracle ILOM Protocol Management Reference for SNMP and IPMI Firmware Release 3.2.x

Part No: E37449-15

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.

Référence: E37449-15

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Using This Documentation

- **Overview** – Provides instructions for managing remote Oracle hardware devices using the following supported management protocols: Simple Network Management Protocol (SNMP) and Intelligent Platform Management Interface (IPMI)
- **Audience** – This guide is intended for technicians, system administrators, and authorized Oracle service providers.
- **Required knowledge** – Users should have experience managing system hardware.

Product Documentation Library

Documentation and resources for this product and related products are available at `http://docs.oracle.com/cd/E37444_01/index.html`.

Feedback

Provide feedback about this documentation at `http://www.oracle.com/goto/docfeedback`.

SNMP Overview

Description	Links
Learn about Oracle ILOM support for SNMP.	■ "About Simple Network Management Protocol" on page 11
Learn about management using SNMP.	■ "SNMP Components" on page 12
Learn about the Oracle ILOM SNMP Management Information Base (MIB) files.	■ "Oracle ILOM SNMP MIBs" on page 13
Learn about the command-line syntax used in this guide.	■ "SNMP Command-Line Syntax Examples" on page 16

Related Information

- "Modifying Default Management Access Configuration Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
- "Oracle ILOM Overview" in *Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.x*

About Simple Network Management Protocol

Oracle ILOM supports Simple Network Management Protocol (SNMP), which is used to exchange data about network activity. SNMP is an open, industry-standard protocol technology that enables the management of networks and devices, or nodes, that are connected to the network. When using SNMP, data travels between a managed device (node) and a management station with network access. A managed device can be any device that runs SNMP, such as a host, router, web server, or other server on the network. SNMP messages are sent over IP using the User Datagram Protocol (UDP). Any management application that supports SNMP can manage your server.

Because SNMP is a protocol, not an application, you need an application to issue SNMP commands. Your SNMP management software might provide this functionality, or you can use an open-source tool like Net-SNMP, which is available at `http://net-snmp.sourceforge.net/`.

For a more complete description of SNMP, see the five-part, introductory SNMP tutorial available at `http://www.dpstele.com/layers/l2/snmp_l2_tut_part1.php`.

Oracle ILOM supports SNMP versions 1, 2c, and 3. Using SNMP v3 is strongly advised since SNMP v3 provides additional security, authentication, and privacy beyond SNMP v1 and v2c.

Note - Oracle ILOM users reading this document are assumed to have a working knowledge of SNMP. SNMP client-side commands are used in this text as examples of using SNMP. Users who do not have a working knowledge of SNMP should complete the tutorial at `http://net-snmp.sourceforge.net/wiki/index.php/Main_Page`. This tutorial is more advanced than the introductory tutorial referred to above.

SNMP Components

SNMP functionality requires the following two components:

- **Network management station** – A *network management station* hosts management applications, which monitor and control managed nodes.
- **Managed node** – A *managed node* is a device such as a server, router, or hub that hosts SNMP management agents that are responsible for carrying out requests from management stations, such as a service processor (SP) running Oracle ILOM. Managed nodes can also provide unsolicited status information to a management station in the form of a trap.

SNMP is the protocol used to communicate management information between management stations and SNMP agents.

The SNMP agent is preinstalled on your Oracle server and runs on Oracle ILOM, so all SNMP management occurs through Oracle ILOM. To use this feature, your operating system must have an SNMP client application.

Both management stations and agents use SNMP messages to communicate. Management stations can send and receive information. Agents can respond to requests and send unsolicited messages in the form of traps. Management stations and agents use the following functions:

- Get
- GetNext

- GetResponse
- Set
- Trap

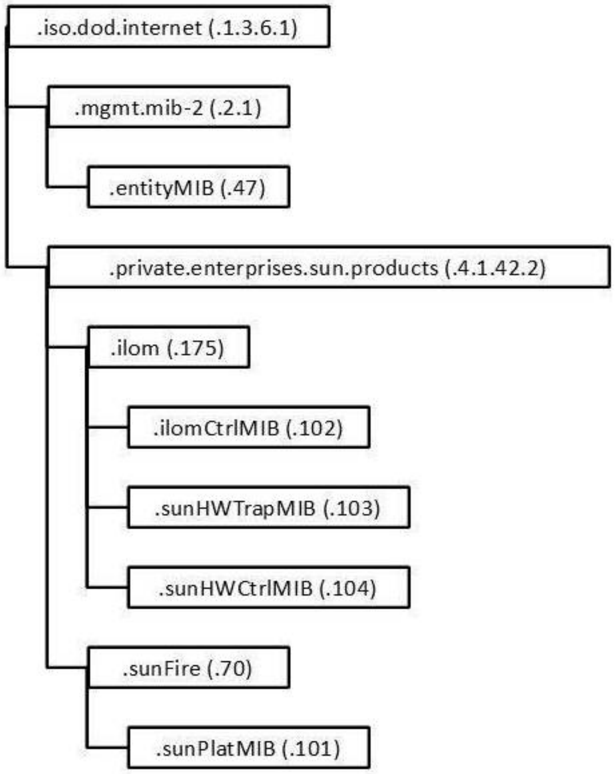
Oracle ILOM SNMP MIBs

The base component of an SNMP implementation is the Management Information Base (MIB). A MIB is a text file that describes a managed node's available information. This tree-like, hierarchical system classifies information about resources in a network as a list of data objects, each with a unique identifier, or object ID. Thus, the MIB defines the data objects, or variables, that the SNMP agent can access. When a management station requests information from a managed node, the agent receives the request and retrieves the appropriate information from the MIBs. In Oracle ILOM, the MIB makes it possible to access the server's network configuration, status, and statistics.

SNMP MIBs are a part of the Oracle ILOM firmware. You can download MIBs directly from Oracle ILOM. For more information about MIBs, and instructions for downloading MIBs from Oracle ILOM, see “Before You Begin Download SNMP MIBs” on page 41.

The following figure shows the standard MIB hierarchy and the location of the Oracle ILOM MIB modules in that hierarchy. The Oracle ILOM MIB modules are described in the table that follows.

FIGURE 1 Location of Oracle ILOM MIB Modules



The following table lists the Oracle ILOM MIB modules and the object ID for each MIB name.

TABLE 1 Description of Oracle ILOM MIB Modules, Object ID, and MIB Name

MIB Name	Description	MIB Object ID
ENTITY-MIB	The MIB module for representing multiple physical entities supported by a single SNMP agent. **Note -** The entPhysicalTable is the only part of this MIB that is implemented.	1.3.6.1.2.1.47
SUN-ILOM-CONTROL-MIB	This MIB provides objects for configuring and managing all Oracle ILOM functions. Configuration covered by this MIB includes functions such as authorization, authentication, logging, services, networking, and firmware management.	1.3.6.1.4.1.42.2.175.102

MIB Name	Description	MIB Object ID
SUN-HW-TRAP-MIB	This MIB describes the hardware-related notifications and traps that can be generated by Oracle Sun server platforms. For more information about managing SNMP traps in Oracle ILOM, see "Configuring SNMP Settings in Oracle ILOM" on page 19.	1.3.6.1.4.1.42.2.175.103
SUN-HW-CTRL-MIB	This MIB allows controls for all Oracle Sun server platform devices using Oracle ILOM. **Note -** Only the power management portions of this MIB are implemented.	1.3.6.1.4.1.42.2.175.104
SUN-PLATFORM-MIB	This MIB provides extensions to the ENTITY-MIB (RFC 2737) where each entity modeled in the system is represented by means of extensions to the entPhysicalTable.	1.3.6.1.4.1.42.2.70.101

Portions of the standard MIBs listed in the following table are implemented by Oracle ILOM.

TABLE 2 Standard MIBs Implemented by Oracle ILOM

MIB Name	Description	MIB Object ID
IF-MIB	This MIB module describes generic objects for network interface sub-layers. This MIB is an updated version of MIB-II's ifTable, and incorporates the extensions defined in RFC 1229.	1.3.6.1.2.1.31
IP-MIB	This MIB module is for managing IP and ICMP implementations, but excluding their management of IP routes.	1.3.6.1.2.1.4.
SNMP-FRAMEWORK-MIB	This is the SNMP Management Architecture MIB.	1.3.6.1.6.3.10
SNMPv2-MIB	This is the MIB module for SNMP entities. **Note -** Only the system and SNMP groups from this MIB module apply to Oracle ILOM.	1.3.6.1.6.3.1
TCP-MIB	This is the MIB module for managing TCP implementations.	1.3.6.1.2.1.49
UDP-MIB	This is the MIB module for managing UDP implementations.	1.3.6.1.2.1.50

The following table lists MIBs that are used in support of the Oracle ILOM SNMP implementation.

TABLE 3 MIBs Used in Support of the Oracle ILOM SNMP Implementation

MIB Name	Description	MIB Object ID
HOST-RESOURCES-MIB	This MIB is for use in managing host systems. The MIB supports attributes common to all Internet hosts including, for example, both personal computers and systems that run variants of UNIX.	1.3.6.1.2.1.25.1
IANAifType-MIB	This MIB module defines the IANAifType Textual Convention, and thus the enumerated values of the ifType object defined in MIB-II's ifTable.	1.3.6.1.2.1.30

MIB Name	Description	MIB Object ID
NOTIFICATION-LOG-MIB	This MIB module is used for logging SNMP notifications (traps).	1.3.6.2.1.92.1.1.3
SNMP-MPD-MIB	This MIB module is used for message processing and dispatching.	1.3.6.1.6.3.11
SNMPv2-TM	This MIB module is used for SNMP transport mappings.	1.3.6.1.6.3.19
SNMPv2-SMI	This MIB module contains definitions for the structure of management information, version 2.	1.3.6.1.6

SNMP Command-Line Syntax Examples

In some network environments, you are required to specify the SNMP version, community name, hostname, and default port when issuing SNMP commands. For example, to request the value of the object identifier (OID) `sysDescr.0` in an IPv4 environment, you might type the following:

```
%snmpget -v2c -c public 192.0.2.1:161 sysDescr.0
```

However, it is possible to configure your network environment such that most command-line arguments are not necessary. For example, for SNMP v1 or v2c, if you set default values for the SNMP version, community name, and default port, the following syntax is considered valid:

```
%snmpget SNMP_agent sysDescr.0
```

Throughout this guide, *SNMP_agent* refers to the hostname or IP address of the system you are querying.

Note - If you query a device using IPv6 addressing, you must use the following syntax: `udp6:[`*IPv6 address*`]` If you receive this message to your query: `getaddrinfo: node name or service name not known`, try adding `-YdefaultPort=<port_number>` to the SNMP command line arguments.

In addition, the examples in this guide omit most command-line arguments. To configure your network so that most command-line arguments are not necessary, see the following procedure:

- "Configure the SNMP Network Environment" on page 17

▼ Configure the SNMP Network Environment

1. **Log in the the Oracle ILOM command-line interface (CLI).**

   For instructions on logging in to Oracle ILOM, refer to the "Log In to the Oracle ILOM CLI" in *Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.x*.

2. **In Oracle ILOM, issue the `create` command to create an SNMP community with read-write access, for example:**

   ```
   -> create /SP/services/snmp/communities/community_name permission=rw
   ```

3. **Issue the `set` command to enable SNMP access and specify the SNMP agent port address, for example:**

   ```
   -> set /SP/services/snmp servicestate=enabled v2c=enabled sets=enabled port=161
   ```

4. **Download the Oracle ILOM MIBs to the `$HOME/mibs` directory.**

   For instructions on downloading the Oracle ILOM MIBs, see "Downloading SNMP MIBs Using Oracle ILOM" on page 40.

5. **In the `$HOME/.snmp/snmp.conf` file in the `$HOME/mibs` directory, specify the following:**

   ```
   defversion          2c
   defcommunity        community_name
   defaultPort         161
   mibs                ALL
   mibdirs             +$HOME/mibs
   ```

6. **Test the new configuration by issuing the following command:**

   ```
   %snmpset SNMP_agent sysName.0 s mynewname
   ```

   The command should produce similar output on your system:

   ```
   RFC1213-MIB::sysName.0 = STRING: "mynewname"
   ```

Configuring SNMP Settings in Oracle ILOM

Description	Links
Learn about Oracle ILOM CLI procedures for managing SNMP access, user accounts, and SNMP trap alerts.	■ "Managing SNMP Read and Write Access, User Accounts, and SNMP Trap Alerts (CLI)" on page 19 ■ "Managing SNMP Read and Write Access, User Accounts, and SNMP Trap Alerts (Web)" on page 30
Learn how to download SNMP MIBs directly from Oracle ILOM.	■ "Downloading SNMP MIBs Using Oracle ILOM" on page 40

Related Information

- "Modifying Default Management Access Configuration Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
- "Configuring Alert Notifications" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

Managing SNMP Read and Write Access, User Accounts, and SNMP Trap Alerts (CLI)

- "Set SNMP Access and Authorization" on page 19
- "Managing SNMP User Accounts and Communities" on page 21
- "Managing SNMP Trap Alerts Using the Oracle ILOM" on page 28

▼ Set SNMP Access and Authorization

Before You Begin

- To modify SNMP properties in Oracle ILOM, you must have the Admin role (a) enabled.
- The SNMP `servicestate` property is, by default, shipped from the factory *enabled*.

- The SNMP `sets` write access property is, by default, shipped from the factory *disabled*. To allow SNMP write access to Oracle ILOM, you must enable the SNMP `sets` property.

Note - When you are working in the Oracle ILOM CLI, if the `sets` parameter is disabled, all SNMP MIB objects are read-only and no `snmpset` commands are processed.

- Oracle ILOM provides authentication properties for each of the following SNMP protocol versions: v1, v2c, and v3.
  - For SNMP v1 and v2c, Oracle ILOM provides the `public` and `private` targets within the `communities` target for managing user authentication.
  - For SNMP v3, Oracle ILOM provides a `users` target for managing user authentication. The SNMPv3 `users` target is not shipped from the factory with pre-packaged values for users.

To set the SNMP service state, properties, follow these steps:

1. **Log in to the Oracle ILOM CLI.**

2. **To view the Oracle ILOM SNMP properties, type:**

   -> **`show /SP/services/snmp`**

   The following SNMP output appears.

```
-> show /SP/services/snmp
   /SP/services/snmp
   Targets:
     communities
     mibs
     users
   Properties:
     engineid = none
     port = 161
     servicestate = (enabled)
     sets = disabled
     v1 = disabled
     v2c = disabled
     v3 = enabled
  Commands:
     cd
     set
     show
```

3. **Use the `set` command to change any of the SNMP properties, for example:**

- To enable SNMP with read-only access, type:

  ```
  -> set /SP/services/snmp servicestate=enabled
  ```

- To enable SNMP write access, type:

  ```
  -> set /SP/services/snmp sets=enabled
  ```

- To enable the SNMP protocol version (v1, v2c, or v3) property, type:

  ```
  -> set /SP/services/snmp v#=enabled
  ```

  where # is the SNMP protocol version you want to enable.

For more information about SNMP user accounts and read and write access, see “Managing SNMP User Accounts and Communities” on page 21.

4. **Use the `create` command to create an SNMP v3 user account, for example:**

- To create a user account for authorization and provide read and write access, type:

  ```
  -> create /SP/services/snmp/users/<useraccountname> authenticationpassword=password
  permission=rw
  ```

- To create a user account for authorization and provide read-only access, type:

  ```
  -> create /SP/services/snmp/users/<useraccountname> authenticationpassword=password
  ```

For more information about SNMP user accounts and read and write access, see “Managing SNMP User Accounts and Communities” on page 21.

Managing SNMP User Accounts and Communities

- “Before You Begin SNMP User Accounts” on page 22
- “SNMP User Account Targets, Properties, and Values” on page 22
- “View and Configure SNMP Community Properties” on page 24
- “SNMPv3 User Name and Password Requirements” on page 23
- “Add an SNMP v3 User Account” on page 25
- “Edit an SNMP v3 User Account” on page 26
- “Delete an SNMP v3 User Account” on page 26
- “Set SNMP v3 User Account Privacy Protocol Value ” on page 26
- “Add or Edit an SNMP v1/v2c Community” on page 27
- “Delete an SNMP v1/v2c Community” on page 27

Before You Begin SNMP User Accounts

Before performing the procedures in this section, ensure that the following requirements are met:

- To set SNMP user account properties in Oracle ILOM, you need the User Management (`u`) role enabled.
- Verify that the proper SNMP settings are enabled in Oracle ILOM. See "Set SNMP Access and Authorization" on page 19.

Note - When you are working in the Oracle ILOM CLI, if the `sets` parameter is disabled, all SNMP MIB objects are read-only.

- To execute the `snmpset` command, you need to use an SNMP v1 or v2c community or an SNMP v3 user account with read-write (rw) privileges.

Note - The SNMP commands presented in this section are based on the Net-SNMP sample applications and, therefore, will work as presented only if you have Net-SNMP and the Net-SNMP sample applications installed.

SNMP User Account Targets, Properties, and Values

You can access the SNMP user account targets, properties, and values under the `/SP/services/snmp` target. The following table identifies the targets, properties, and values that are valid for SNMP user accounts.

TABLE 4 SNMP User Account Targets, Properties, and Values

Target	Property	Value	Default
`/SP/services/snmp/ communities/` *community_name*	`permissions`	ro|rw	ro
`/SP/services/snmp/users/` *username*	`authenticationprotocol`	MD5|SHA	MD5
	`authenticationpassword`[†]	<string>	(null string)
	`permissions`	ro|rw	ro
	`privacyprotocol`	none|DES|AES[*]	none
	`privacypassword`[‡]	<string>	(null string)

Target	Property	Value	Default
`/SP/services/snmp`	`engineid = none`	<string>	(null string)
	`port = 161`	<integer>	161
	`servicestate = enabled`	enable|disabled	enabled
	`sets = enabled`	enabled|disabled	disabled
	`v1 = disabled`	enabled|disabled	disabled
	`v2c = disabled`	enabled|disabled	disabled
	`v3 = disabled`	enabled|disabled	enabled

[†] You must provide an authentication password when you create or modify users (SNMP v3 only).

[‡] If the `privacyprotocol` property has a value other than none, then you must set a privacy password.

[*] AES (Advanced Encryption Standard) privacy protocol option is available for SNMPv 3 as of Oracle ILOM 3.0.16.

For example, to change `privacyprotocol` for user `a1` to `DES,` use the following syntax:

```
-> set /SP/services/snmp/users/al privacyprotocol=DES
privacypassword=password authenticationprotocol=SHA
authenticationpassword=password
```

Note that the changes would be invalid if the following syntax was specified:

```
-> set /SP/services/snmp/users/al privacyprotocol=DES
```

Note - You can change SNMP user permissions without resetting the `privacy` and `authentication` properties.

SNMPv3 User Name and Password Requirements

Property	Description
User Name	The SNMP user name can contain up to 32 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers).Spaces not allowed.
Authentication Password	The Authentication Password is required when authentication protocol property is set to either MD5 or SHA. Enter a case-sensitive Authentication password. The Authentication password can contain 8 to 12 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers).
Privacy Password	The Privacy Password is required when the privacy potocol property is set to DES or AES.

Property	Description
	The Privacy password must contain exactly 8 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers)

View and Configure SNMP Community Properties

1. **To go to the `/SP/services/snmp` directory, type:**

   -> **`cd /SP/services/snmp`**

2. **Within that directory, type the `show` command to view SNMP settings. The default settings are as follows:**

```
-> show
   /SP/services/snmp
   Targets:
     communities
     mibs
     users
   Properties:
     engineid = (none)
     port = 161
     servicestate = enabled
     sets = disabled
     v1 = disabled
     v2c = disabled
     v3 = enabled
  Commands:
     cd
     set
     show
```

3. **To view the communities, type:**

   -> **`show /SP/services/snmp/communities`**

   For example:

```
-> show /SP/services/snmp/communities
/SP/services/snmp/communities
Targets:
  private
  public
Properties:
Commands:
  cd
  create
  delete
  show
```

4. **To create a community with read/write privileges, type:**

   -> **`create /SP/services/snmp/communities/`***communityname* **`permission=rw`**

5. **To view the public communities, type:**

   -> **`show /SP/services/snmp/communities/public`**

   For example:

```
-> show /SP/services/snmp/communities/public
/SP/services/snmp/communities/public
Targets:
Properties:
  permission = ro
Commands:
  cd
  set
  show
```

▼ Add an SNMP v3 User Account

1. **Log in to the Oracle ILOM CLI.**

2. **To add an SNMP v3 read-only user account, type:**

   -> **`create /SP/services/snmp/users/`***username* **`authenticationpassword=`***Password* **`privacypassword=`***Password*

   Where:

   - *username* can contain up to 32 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers).
   - **`authenticationpassword=`** *Password* is required when creating or modifying an SNMP v3 user account. The Authentication password can contain 8 to 12 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers).
   - **`privacypassword=`** *Password* is only required when the Privacy Potocol property is set to DES or AES (default = None). The Privacy password must contain exactly 8 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers). To set the Privacy Protocol property, see "Set SNMP v3 User Account Privacy Protocol Value " on page 26

Edit an SNMP v3 User Account

1. **Log in to the Oracle ILOM CLI.**
2. **To edit an SNMP v3 user account, type:**

   ```
   -> set /SP/services/snmp/users/username authenticationpassword=password
   privacypassword=Password
   ```

   Note - When changing the parameters of SNMP users, you must provide a value for `authenticationpassword`, even if you are not changing the password.

   Where:

   - *username* can contain up to 32 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers).
   - **`authenticationpassword=`** *Password* is required when creating or modifying an SNMP v3 user account. The Authentication password can contain 8 to 12 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers).
   - **`privacypassword=`** *Password* is only required when the Privacy Protocol property is set to DES or AES (default = None). The Privacy password must contain exactly 8 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers). To set the Privacy Protocol property, see "Set SNMP v3 User Account Privacy Protocol Value " on page 26

Delete an SNMP v3 User Account

1. **Log in to the Oracle ILOM CLI.**
2. **To delete an SNMP v3 user account, type:**

   ```
   -> delete /SP/services/snmp/users/username
   ```

Set SNMP v3 User Account Privacy Protocol Value

Before You Begin

- By default, the Privacy Protocol property is set to None.
- If the Privacy Protocol property is set to DES or AES, a privacy password must be provided when creating or modifying an SNMP v3 User Account. For further details

about creating or editing an SNMP v3 User Account, see "Add an SNMP v3 User Account" on page 25 or "Edit an SNMP v3 User Account" on page 26.

1. **Log in to the Oracle ILOM CLI.**

2. **To modify the `privacyprotocol` property value assigned to an SNMP v3 user account, type:**

   ```
   -> set /SP/services/snmp/users/username authenticationpassword=password
   privacyprotocol=<DES|AES|None>
   ```

   Note - When changing the parameters of SNMP users, you must provide a value for `authenticationpassword`, even if you are not changing the password.

   Note - The SNMPv3 AES (Advanced Encryption Standard) option is available in Oracle ILOM as of 3.0.16.

   Where:

   - *username* can contain up to 32 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers).
   - **`authenticationpassword=`***password* is required when creating or modifying an SNMP v3 user account. The Authentication password can contain 8 to 12 characters in length and include any combination of alphanumeric characters (uppercase letters, lowercase letters, and numbers).
   - DES is the acronym for Digital Encryption Standard and AES is the acronym for Advanced Encryption Standard.

▼ Add or Edit an SNMP v1/v2c Community

1. **Log in to the Oracle ILOM CLI.**

2. **To add an SNMP v1/v2c community, type:**

   ```
   -> create /SP/services/snmp/communities/community_name
   ```

▼ Delete an SNMP v1/v2c Community

1. **Log in to the Oracle ILOM CLI.**

2. **To delete an SNMP v1/v2c community, type:**

```
-> delete /SP/services/snmp/communities/community_name
```

Managing SNMP Trap Alerts Using the Oracle ILOM

- "Configure SNMP Trap Rule Destinations and Properties " on page 28
- "CLI Commands for Managing Alert Rule Configurations" on page 30

Configure SNMP Trap Rule Destinations and Properties

Before You Begin

- To create or edit alert rules in Oracle ILOM, you need the Admin (a) role enabled.
- For you to define an SNMP v3 trap alert, the SNMPv3 user name must be defined in Oracle ILOM. If the SNMP v3 user name is not defined in Oracle ILOM, the SNMP v3 user receiving the SNMP alert will not be able to decode the SNMPv3 alert message. For more information about defining SNMPv3 authorization and SNMP v3 users in Oracle ILOM, see "Managing SNMP Read and Write Access, User Accounts, and SNMP Trap Alerts (CLI)" on page 19.
- Review "CLI Commands for Managing Alert Rule Configurations" on page 30.
- For additional information about configuring alert management settings in Oracle ILOM, refer to "Configuring Alert Notifications" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*.

To configure the destinations to which the SNMP traps are sent, follow these steps:

1. **Log in to the Oracle ILOM CLI.**

2. **To display the current settings of the alert rule, type the `show` command.**
For example:

```
-> show /SP/alertmgmt/rules/1
/SP/alertmgmt/rules/1
   Targets:

   Properties:
      type = snmptrap
      level = disable
      destination = 0.0.0.0
      destination_port = 0
      community_or_username = public
      snmp_version = 1
      testrule = (Cannot show property)

   Commands:
      cd
      set
      show
```

Note - When you test an alert notification rule, Oracle ILOM will send a test from all configured SNMP traps. Oracle ILOM does not have the ability to filter SNMP traps by destination.

3. **To show the `/SP/alertmgmt/rules` directory, type:**

   ```
   -> cd /SP/alertmgmt/rules
   ```

   ```
   -> show
   ```

   For example:

   ```
   -> cd /SP/alertmgmt/rules
   -> show
   /SP/alertmgmt/rules
     Targets:
       1
       2
       .
       .
       .
       15
     Properties:

     Commands:
         cd
         show
   ```

   Choose a rule (from targets 1 through 15) for which you would like to configure a destination for SNMP traps, and go to that directory.

   For example:

   ```
   -> cd 4
   ```

4. **To change the rule properties, within that rule directory, type the `set` command.**

   For example, to set a rule to send critical traps to a management client using SNMP v2c using a community name of “public”, enter:

```
-> set type=snmptrap level=critical destination=IPaddress_of_snmp_management_station
destination_port=port snmp_version=2c community_or_username=public
```

CLI Commands for Managing Alert Rule Configurations

The following table describes the CLI commands that you use to manage alert rule configurations in the Oracle ILOM CLI.

TABLE 5 CLI Commands for Managing Alert Rule Configurations

CLI Command	Description
`show`	The `show` command enables you to display any level of the alert management command tree by specifying either the full or relative path.
`cd`	The `cd` command enables you to set the working directory. To set alert management as a working directory on a server SP, type the following command at the command prompt: `-> cd /SP/alertmgmt`

`set`	The `set` command enables you to set values to properties from any place in the tree. You can specify either a full or relative path for the property depending on the location of the tree. For example:
	■ For full paths, type the following at the command prompt:
	`-> set /SP/alertmgmt/rules/1 type=snmptrap`
	■ For relative path (tree location is `/SP/alertmgmt`), type the following command path at the command prompt:
	`-> set rules/1 type=snmptrap`
	■ For relative path (tree location is `/SP/alertmgmt/rules/1`), type the following command path at the command prompt:
	`-> set type=snmptrap`

Managing SNMP Read and Write Access, User Accounts, and SNMP Trap Alerts (Web)

- "Set SNMP Read and Write Access and Authorization" on page 31
- "Managing SNMP User Accounts and Communities" on page 33
- "Manage SNMP Trap Alerts" on page 38

▼ Set SNMP Read and Write Access and Authorization

Before You Begin

- To modify SNMP properties in Oracle ILOM, you must have the Admin role (a) enabled.
- The SNMP `service` state is, by default, shipped from the factory *enabled*.
- The SNMP `set requests` state is, by default, shipped from the factory *disabled*. To allow SNMP write access to Oracle ILOM, enable the set requests state.

> **Note -** When the set requests state is disabled in Oracle ILOM, all SNMP objects are read-only and no `snmpset` commands are processed.

- Oracle ILOM provides authentication properties for each of the following SNMP protocol versions: v1, v2c, and v3.
  - For SNMP v1 and v2c, Oracle ILOM provides a `communities` property with values of *public* and *private* to manage user authentication. However, the property values for SNMP v1 and v2c communities are, by default, shipped from the factory *disabled*.
  - For SNMP v3, Oracle ILOM provides a `users` property to manage user authentication. The users property is, by default, shipped from the factory *enabled*. The SNMP v3 users property is not shipped from the factory with pre-packaged values for users.

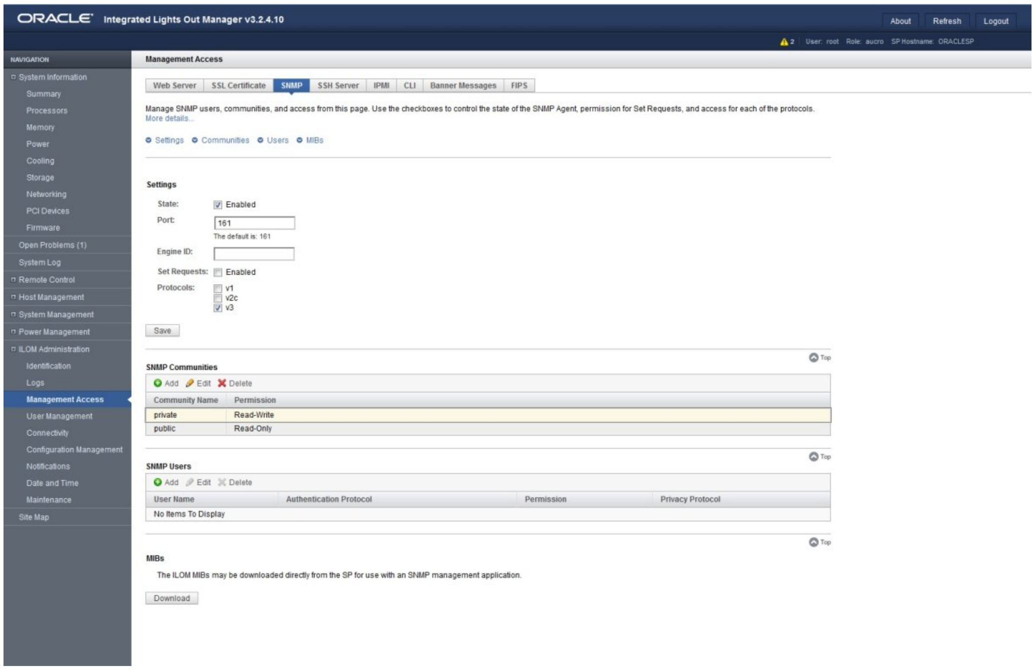
To set the SNMP service state, properties:

1. **Log in to the Oracle ILOM web interface.**

2. **On the left navigation panel, click ILOM Administration.**

3. **Click Management Access > SNMP.**

The SNMP Management page appears.



Manage SNMP users, communities, and access from this page. Use the checkboxes to control the state of the SNMP Agent, permission for Set Requests, and access for each of the protocols.
More details...

Settings

State: ☑ Enabled

Port: 161

The default is: 161

Engine ID:

Set Requests: □ Enabled

Protocols: □ v1 □ v2c ☑ v3

Save

SNMP Communities

Add Edit Delete

Community Name	Permission
private	Read-Write
public	Read-Only

SNMP Users

Add Edit Delete

User Name	Authentication Protocol	Permission	Privacy Protocol
No Items To Display			

MIBs

The ILOM MIBs may be downloaded directly from the SP for use with an SNMP management application.

Download

4. **To enable the SNMP port, click the State check box.**

   When State is disabled, the SNMP port is blocked, prohibiting all SNMP communication between Oracle ILOM and the network.

5. **In the Port text field, type the port number.**

6. **Leave the Engine ID field blank. This allows the default setting to be used.**

   The engine ID is automatically set by the SNMP agent. While you can use this field to set the engine ID, you should leave this field blank. The engine ID uniquely identifies the SNMP engine and enables users to query the SNMP agent. Use this field to set the engine ID only if you are familiar with SNMP v3 security and how this setting is used.

7. **To enable or disable the Set Requests option, select or clear the Set Requests check box.**

   If the Set Requests option is disabled, all SNMP objects are read-only and no snmpset commands will be processed.

8. **To enable SNMP v1, v2c, or v3, click a Protocols check box.**

   SNMP v3 is enabled by default. You can enable or disable v1, v2c, and v3 protocol versions.

9. **Click Save.**

   At the bottom of the SNMP Management page, you can also add, edit, or delete SNMP communities or users.

Managing SNMP User Accounts and Communities

- "Before You Begin SNMP User Accounts" on page 33
- "Add or Edit an SNMP v1/v2c Community" on page 33
- "Delete an SNMP v1/v2c Community" on page 35
- "Add or Edit an SNMP v3 User Account" on page 35
- "Delete an SNMP v3 User Account" on page 37

Before You Begin SNMP User Accounts

Before performing the procedures in this section, ensure that the following requirements are met:

- To set user account properties in Oracle ILOM, you need the User Management (`u`) role enabled.
- Verify that the proper SNMP settings are enabled in Oracle ILOM. For more details, see "Set SNMP Read and Write Access and Authorization" on page 31.
- To execute the `snmpset` command, you need to use an SNMP v1 or v2c community or an SNMP v3 user account with read-write (rw) privileges.

▼ Add or Edit an SNMP v1/v2c Community

To add or edit an SNMP v1 or v2c community, follow these steps:

1. **Log in to the Oracle ILOM web interface.**
2. **On the left navigation panel, click ILOM Administration.**
3. **Then click Management Access > SNMP.**

Scroll to the bottom half of the SNMP Management page to find the SNMP Communities dialog box.

4. **To edit a community, do the following:**

   a. **Click the appropriate community radio button.**

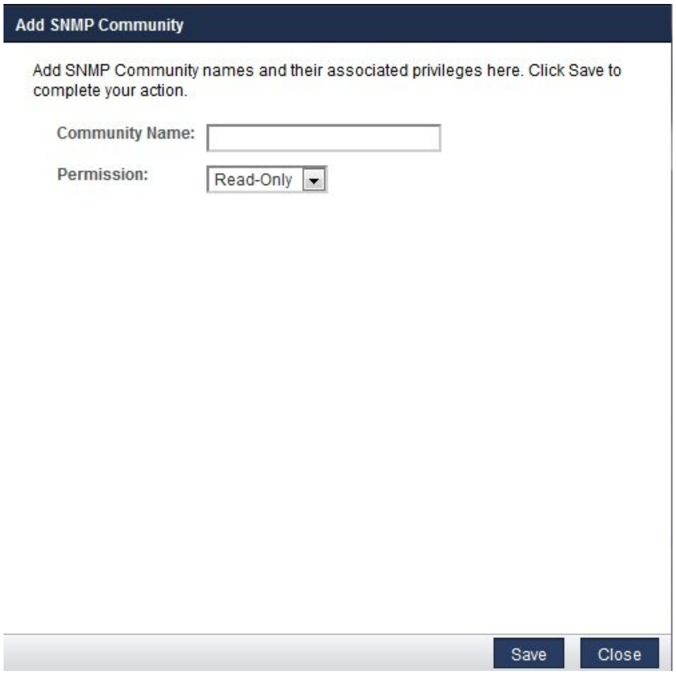
   b. **Click Edit.**
   The Edit Community dialog box appears.

   c. **Update community properties, as needed.**

   d. **Click Save.**

5. **To add a community, do the following:**

   a. **Click Add.**
   The Add Community dialog box appears.



Add SNMP Community

Add SNMP Community names and their associated privileges here. Click Save to complete your action.

Community Name:

Permission: Read-Only

b. **If you are adding a new community, type the name of the community in the Community Name field; otherwise, proceed to the next step.**

   The community name can contain up to 35 characters. It must start with an alphabetic character and cannot contain a space.

c. **In the Permissions drop-down list, select read-only (ro) or read-write (rw).**

d. **Click Save.**

▼ Delete an SNMP v1/v2c Community

To delete an SNMP v1 or v2c community, follow these steps:

1. **Log in to the Oracle ILOM web interface.**
2. **On the left navigation panel, click ILOM Administration.**
3. **Then click Management Access > SNMP.**

   The SNMP Management page appears.
4. **Click the Communities link or scroll down to the communities list.**
5. **Click the radio button of the SNMP community to delete.**
6. **Click Delete.**

   A confirmation dialog box appears.
7. **Click OK to delete the SNMP community.**

▼ Add or Edit an SNMP v3 User Account

To add or edit an SNMP v3 user account, follow these steps:

Note - User accounts are not applicable to SNMP v1 and v2c because communities are used to control access.

---

1. **Log in to the Oracle ILOM web interface.**

2. **On the left navigation panel, click ILOM Administration.**

3. **Then click Management Access > SNMP.**
   The SNMP Management page appears.

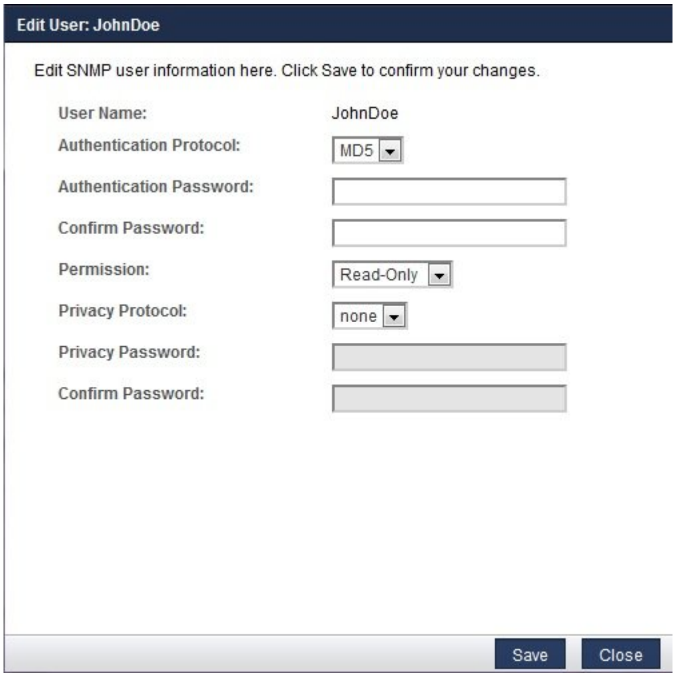
4. **Click the Users link to expand the SNMP Settings page and display SNMP Users.**

5. **To add an SNMP user, click Add.**
   The Add User dialog box appears.

6. **To edit an SNMP user, do the following:**

   a. **Click the appropriate user radio button**

   b. **Click Edit.**
   The Edit SNMP User Information dialog box appears.



Edit User: JohnDoe

Edit SNMP user information here. Click Save to confirm your changes.

User Name:	JohnDoe
Authentication Protocol:	MD5
Authentication Password:	
Confirm Password:	
Permission:	Read-Only
Privacy Protocol:	none
Privacy Password:	
Confirm Password:	

7. **If you are adding a user, type a user name in the User Name text field; otherwise proceed to the next step.**

The user name can include up to 35 characters. It must start with an alphabetic character and cannot contain spaces.

8. **In the Authentication Protocol drop-down list, select either Message Digest 5 (MD5) or Secure Hash Algorithm (SHA).**

9. **In the Authentication Password text field, type a password.**

   The authentication password is case-sensitive and must contain 8 to 16 characters, with no colons or space characters.

10. **In the Confirm Password text field, retype the authentication password.**

11. **In the Permissions drop-down list, select read-only (ro) or read-write (rw).**

12. **(Optional) To specify a privacy protocol, perform the following steps:**

    a. **In the Privacy Protocol list box, select DES (Digital Encryption Standard) or AES (Advanced Encryption Standard).**

Note - The AES privacy protocol option is available only for SNMPv3 as of ILOM 3.0.16.

    b. **In the Privacy Password text box, type a password for the privacy algorithm specified in Step 12a.**

    The privacy password is case-sensitive and must contain 8 to 16 characters, with no colons or space characters.

Note - The privacy password is only required if you selected DES or AES in Step 12a.

    c. **In the Confirm Password field, retype the privacy password to ensure that it matches the privacy password specified in Step 12b.**

13. **Click Save to apply the SNMP user account properties.**

▼ Delete an SNMP v3 User Account

To delete an SNMP v3 user account, follow these steps:

1. **Log in to the Oracle ILOM web interface.**

2. **On the left navigation panel, click ILOM Administration.**

3. **Then click Management Access > SNMP.**

   The SNMP Management page appears.

4. **Click the Users link or scroll down to the SNMP Users list.**

5. **Click the radio button of the SNMP user account to delete.**

6. **Click Delete under the SNMP User's List.**

   A confirmation dialog box opens.

7. **Click OK to delete the user account.**

▼ Manage SNMP Trap Alerts

Before You Begin

- To create or edit SNMP trap alert rules in Oracle ILOM, you need the Admin (a) role enabled.
- To define an SNMP v3 trap alert, you must define the SNMP v3 user name must be defined in Oracle ILOM. If the SNMP v3 user name is not defined in Oracle ILOM, the SNMP v3 user receiving the SNMP alert cannot decode the SNMP v3 alert message. For more information about defining SNMP v3 authorization and SNMP v3 users in Oracle ILOM, see "Managing SNMP Read and Write Access, User Accounts, and SNMP Trap Alerts (Web)" on page 30.
- For additional information about configuring alert management settings in Oracle ILOM, refer to "Configuring Alert Notifications" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*.

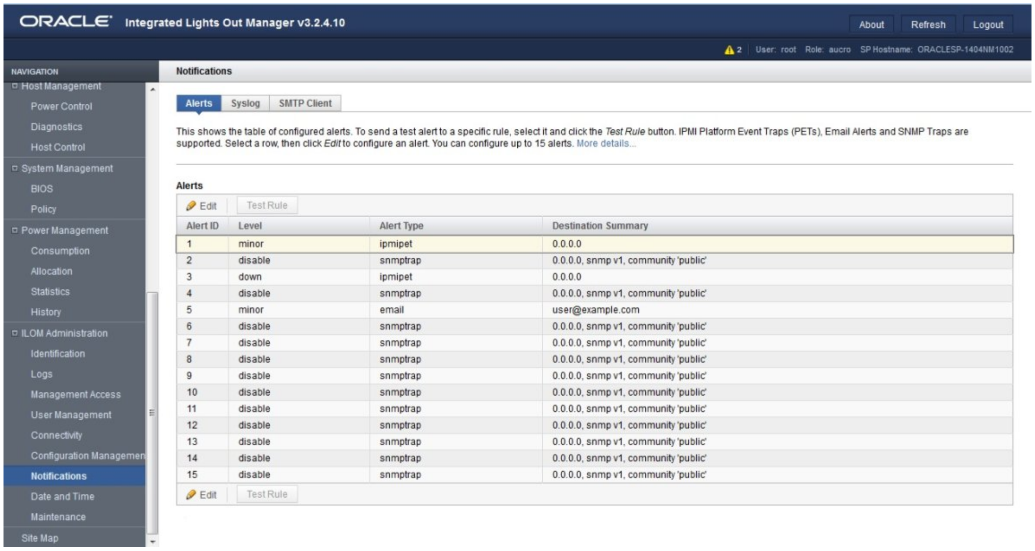
To configure SNMP Trap Alert properties, follow these steps:

1. **Log in to the Oracle ILOM web interface.**

2. **On the left navigation panel, click ILOM Administration.**

3. **Click Notifications > Alerts.**

The Alert Settings page appears. This page shows a table of the alerts that you can configure. You can configure up to 15 alerts.



This shows the table of configured alerts. To send a test alert to a specific rule, select it and click the *Test Rule* button. IPMI Platform Event Traps (PETs), Email Alerts and SNMP Traps are supported. Select a row, then click *Edit* to configure an alert. You can configure up to 15 alerts. More details...

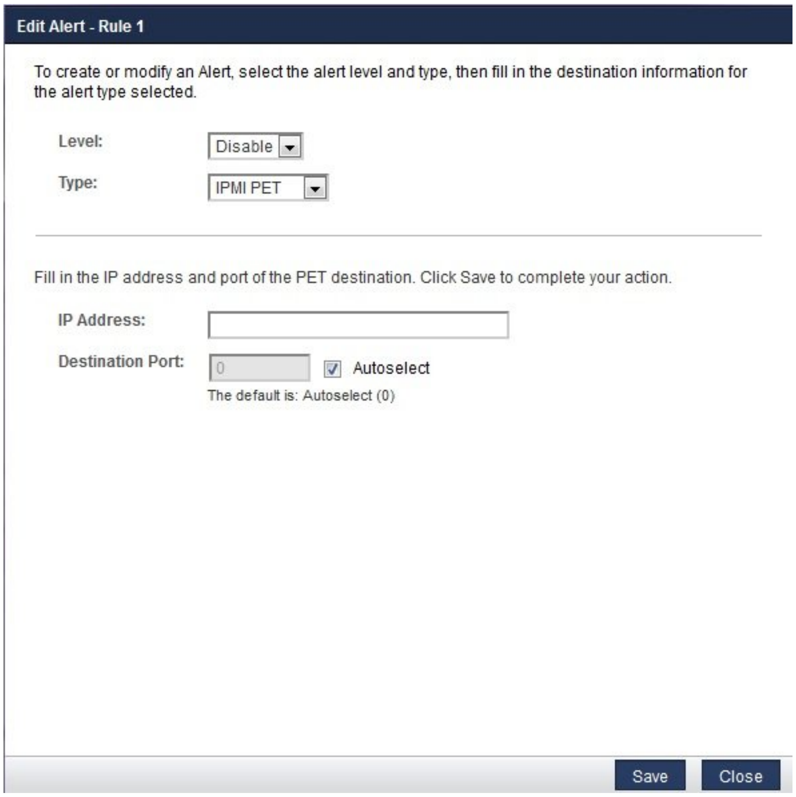
Alerts

Alert ID	Level	Alert Type	Destination Summary
1	minor	ipmipet	0.0.0.0
2	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
3	down	ipmipet	0.0.0.0
4	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
5	minor	email	user@example.com
6	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
7	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
8	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
9	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
10	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
11	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
12	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
13	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
14	disable	snmptrap	0.0.0.0, snmp v1, community 'public'
15	disable	snmptrap	0.0.0.0, snmp v1, community 'public'

4. **To create or modify an alert, click the alert radio button.**

5. **Then click Edit.**

The Create or Modify Alert dialog appears.



Edit Alert - Rule 1

To create or modify an Alert, select the alert level and type, then fill in the destination information for the alert type selected.

Level: Disable

Type: IPMI PET

Fill in the IP address and port of the PET destination. Click Save to complete your action.

IP Address:

Destination Port: 0 ☑ Autoselect

The default is: Autoselect (0)

6. **In the Level drop-down list, select the level of the alert.**

7. **In the Type drop-down list, select the alert type.**

8. **In the IP Address field, specify the alert destination IP address.**

9. **Click Save for your changes to take effect.**

Downloading SNMP MIBs Using Oracle ILOM

- “Before You Begin Download SNMP MIBs” on page 41

- “Download SNMP MIBs (CLI)” on page 41
- “Download SNMP MIBs (Web)” on page 42

Before You Begin Download SNMP MIBs

- The Reset and Host Control (`r`) role is required for you to download SNMP MIBs from Oracle ILOM.
- You must be using Oracle ILOM 3.0.4 or a later version of Oracle ILOM.

Download SNMP MIBs (CLI)

1. **Log in to the Oracle ILOM CLI.**

2. **Use the `show` command to display the SNMP MIBs.**

   For example:

```
-> show /SP/services/snmp/mibs

/SP/services/snmp/mibs
    Targets:

    Properties:
        dump_uri = (Cannot show property)

    Commands:
        cd
        dump
        set
        show
```

3. **To download the files, type either of the following commands:**

```
-> dump -destination URI /SP/services/snmp/mibs
```

   or

```
-> set /SP/services/snmp/mibs dump_uri=URI
```

   where *URI* specifies the target to which the files are downloaded.

   A zip file containing the MIBs are transferred to the destination server.

▼ Download SNMP MIBs (Web)

1. **Log in to the Oracle ILOM web interface.**

2. **On the left navigation panel, click ILOM Administration.**

3. **Click Management Access > SNMP.**

   The SNMP Management page appears.

4. **Click the MIBs jump link, or scroll down to the MIBs section.**

5. **Click Download, and then click Save and enter the destination to save the file.**

   A zip file containing the MIBs is transferred to the destination server.

Manage User Accounts Using SNMP

Description	Links
Review the access requirements for managing user accounts using SNMP.	■ "Before You Begin User Accounts (SNMP)" on page 43
Learn how to configure user accounts.	■ "Configuring Oracle ILOM User Accounts (SNMP)" on page 44
Learn how to configure Active Directory settings.	■ "Configuring Oracle ILOM for Active Directory (SNMP)" on page 47
Learn how to configure a DNS name server.	■ "Manage DNS Name Server Settings (SNMP)" on page 63
Learn how to configure LDAP settings.	■ "Configuring Oracle ILOM for LDAP (SNMP)" on page 64
Learn how to configure LDAP/SSL settings.	■ "Configuring Oracle ILOM for LDAP/SSL (SNMP)" on page 67
Learn how to configure RADIUS settings.	■ "Configuring Oracle ILOM for RADIUS (SNMP)" on page 76

Related Information

- "Managing SNMP Read and Write Access, User Accounts, and SNMP Trap Alerts (CLI)" on page 19
- "Managing SNMP Read and Write Access, User Accounts, and SNMP Trap Alerts (Web)" on page 30
- "Modifying Default Management Access Configuration Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
- "Setting Up and Maintaining User Accounts" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

Before You Begin User Accounts (SNMP)

Prior to performing the procedures in this section, you must ensure that the following requirements are met:

- To use SNMP, ensure that all the SNMP properties are correctly set. For more details, see "Configuring SNMP Settings in Oracle ILOM" on page 19.

To view user account information, you need the Read Only (o) role enabled.

- To configure user account information, you need the User Management (u) role enabled.
- To execute the `snmpset` command, you need to use an SNMP v1 or v2c community or an SNMP v3 user account with read-write (rw) privileges.

Note - For examples of SNMP commands, see “SNMP Command Examples” on page 147.

Note - The SNMP commands presented in this section are based on the Net-SNMP sample applications and, therefore, will work as presented only if you have Net-SNMP and the Net-SNMP sample applications installed.

Configuring Oracle ILOM User Accounts (SNMP)

- “Configure User Accounts” on page 44
- “Configure Single Sign On” on page 46

▼ Configure User Accounts

Note - You can use `get` and `set` commands to configure user account MIB object settings. For a description of valid MIB objects for this procedure, see the table following this procedure.

Note - The syntax in this procedure is valid for a `tcsh` shell. It might not be necessary to include the escape character (\) in your shell environment.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   `ssh` *username*`@`*snmp_manager_ipaddress*

   `Password:` *password*

2. **To create a new user account with a user role of Operator, type:**

```
% snmpset SNMP_agent ilomCtrlLocalUserRowStatus.\”user1\” i 4
ilomCtrlLocalUserRoles.\”user1\” s "operator"
ilomCtrlLocalUserPassword.\”user1\” s "password"
```

3. To delete a user account, type:

```
% snmpset SNMP_agent ilomCtrlLocalUserRowStatus.\”user1\” i 6
```

The following table describes the User Account SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default
`ilomCtrlLocalUserUsername`	A local user user name. It must start with an alphabetical letter and can contain alphabetical letters, digits, hyphens, and underscores, but cannot contain spaces. It cannot be the same as the password.	*username*	String	None
`ilomCtrlLocalUserPassword`	A local user password.	*password*	String	None

`ilomCtrlLocalUserRoles`	Specifies the role that is associated with a user. The roles can be assigned for the legacy roles of Administrator or Operator, or any of the individual role IDs of `a`, `u`, `c`, `r`, `o`, and `s`. The role IDs can be joined together. For example, `aucros`, where `a`=admin, `u`=user, `c`=console, `r`=reset, `o`=read-only, `s`=service.	`administrator,`
		`operator,`
		`admin(a),`
		`user(u),`
		`console(c),`
		`reset(r), read-only(o),`
		`service(s)`
			String	None

`ilomCtrlLocalUserRowStatus`	This object is used to create a new row or to delete an existing row in the table. This property can be set to either `createAndWait(5)` or `destroy(6)`, to create and remove a user respectively.	`active(1),`
		`notInService(2),`
		`notReady(3),`
		`createAndGo(4),`
		`createAndWait(5),`
		`destroy(6)`
			Integer	None

▼ Configure Single Sign On

Single Sign On is a convenient authentication service that reduces the number of times you need to enter a password to gain access to Oracle ILOM. Single Sign On is enabled by default. As with any authentication service, authentication credentials are passed over the network. If you do not want this, consider disabling the Single Sign On authentication service.

Note - You can use the `set` command to configure Single Sign On MIB object settings. For a description of the MIB object used in this procedure, see the table that follows the procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   ```
   ssh username@snmp_manager_ipaddress
   ```

   ```
   Password: password
   ```

2. **To enable Single Sign On, type:**

   ```
   ilomCtrlSingleSignonEnabled.0 i 1
   ```

   For example:

   ```
   % snmpset SNMP_agent ilomCtrlSingleSignonEnabled.0 i 1
   ```

   The following table describes the Single Sign On SNMP MIB object.

MIB Object	Description	Allowed Values	Type	Default

`ilomCtrlSingle`
`SignonEnabled`
	Specifies whether Single Sign On (SSO) authentication should be enabled on the device. SSO allows tokens to be passed so that it is not necessary to re-enter passwords between different applications. This allows SSO between the system controller (SC) web interface and the service processor (SP) web interface, between the SC command-line interface and the SP command-line interface, and between the SC and SP interfaces and the Java Remote Console application.	`true(1),`
		`false(2)`
			Integer	None

Configuring Oracle ILOM for Active Directory (SNMP)

▼ Manage Active Directory Settings

Note - You can use the `get` and `set` commands to view and configure Active Directory settings. For a description of the MIB objects used in this procedure, see the table that follows the procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   ```
   ssh username@snmp_manager_ipaddress
   ```

   ```
   Password: password
   ```

2. **Refer to the following SNMP command examples:**

   - **To view the Active Directory state, type:**

     ```
     % snmpget SNMP_agent ilomCtrlActiveDirectoryEnabled.0
     ```

   - **To enable the Active Directory, type:**

     ```
     % snmpset SNMP_agent ilomCtrlActiveDirectoryEnabled.0 i 1
     ```

   - **To view the Active Directory port number, type:**

     ```
     % snmpget SNMP_agent ilomCtrlActiveDirectoryPortNumber.0
     ```

- **To set the Active Directory port number, type:**

```
% snmpset SNMP_agent ilomCtrlActiveDirectoryPortNumber.0 i
portnumber
```

- **To view the Active Directory default user roles, type:**

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryDefaultRoles.0
```

- **To set the Active Directory default user roles, type:**

```
% snmpset SNMP_agent ilomCtrlActiveDirectoryDefaultRoles.0 s acro
```

- **To view the Active Directory certificate file URI, type:**

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryCertFileURI.0
```

- **To set the Active Directory certificate file URI, type:**

```
% snmpset SNMP_agent ilomCtrlActiveDirectoryCertFileURI.0 s URI
```

- **To view the Active Directory time-out, type:**

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryTimeout.0
```

- **To set the Active Directory time-out, type:**

```
% snmpset SNMP_agent ilomCtrlActiveDirectoryTimeout.0 i 6
```

- **To view the Active Directory certificate validation mode, type:**

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryStrictCertEnabled.0
```

- **To set the Active Directory certificate validation mode, type:**

```
% snmpset SNMP_agent ilomCtrlActiveDirectoryStrictCertEnabled.0 i
```

```
1
```

- **To view the Active Directory certificate file status, type:**

  ```
  % snmpget SNMP_agent ilomCtrlActiveDirectoryCertFileStatus.0
  ```

- **To view the event log setting for the number of messages sent to the event log, type:**

  ```
  % snmpget SNMP_agent ilomCtrlActiveDirectoryLogDetail.0
  ```

- **To configure the event log setting so that only the highest priority messages are sent to the event log, type:**

  ```
  % snmpset SNMP_agent ilomCtrlActiveDirectoryLogDetail.0 i 2
  ```

- **To view the role that user1 is to have when authenticated through Active Directory, type:**

  ```
  % snmpget SNMP_agent ilomCtrlActiveDirectoryDefaultRoles.'user1'
  ```

- **To specify the Admin (a) role for user1 when authenticated via Active Directory, type:**

  ```
  % snmpset SNMP_agent ilomCtrlActiveDirectoryDefaultRoles.'user1' s
  a
  ```

- **To view and clear the certificate information associated with the server when it is set to `true`, type:**

  ```
  % snmpget SNMP_agent ilomCtrlActiveDirectoryCertClear.0
  % snmpset SNMP_agent ilomCtrlActiveDirectoryCertClear.0 i 0
  ```

- **To view the version of the certificate file, type:**

  ```
  % snmpget SNMP_agent ilomCtrlActiveDirectoryCertVersion.0
  ```

- **To view the serial number of the certificate file, type:**

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryCertSerialNo.0
```

- **To view the issuer of the certificate file, type:**

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryCertIssuer.0
```

- **To view the subject of the certificate file, type:**

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryCertSubject.0
```

- **To view the valid start date of the certificate file, type:**

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryCertValidBegin.0
```

- **To view the valid end date of the certificate file, type:**

```
% snmpget SNMP_agent ilomCtrlActiveDirectoryCertValidEnd.0
```

The following table describes the Active Directory Certificates SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default

`ilomCtrlActive`
`Directory`
`Enabled`
	Specifies whether the Active Directory client is enabled.	`true(1)`,
		`false(2)`
			Integer	true

`ilomCtrlActive` `DirectoryIP`	The IP address of the Active Directory server used as a name service for user accounts.	*ipaddress*	String	None

`ilomCtrlActive`
`Directory`
`PortNumber`
	Specifies the port number for the Active Directory client. Specifying 0 as the port means autoselect, while specifying 1 to 65535 configures the actual port.	*portnumber* (range: 0 to 65535)	Integer	None

`ilomCtrl`
`Active`
`Directory`
`DefaultRoles`
	Specifies the role that a user authenticated through Active Directory should have. Setting this property to legacy roles of Administrator or Operator, or any of the individual role IDs of `a`, `u`, `c`, `r`, `o`, and `s`, will cause the	`administrator`,
		`operator`,
		`admin(a)`,
		`user(u)`,
			String	None

MIB Object	Description	Allowed Values	Type	Default

	Active Directory client to ignore the schema stored on the Active Directory server. Setting this to `none` clears the value and indicates that the native Active Directory schema should be used. The role IDs can be joined together. For example, `aucros`, where `a`=admin, `u`=user, `c`=console, `r`=reset, `o`=read-only, and `s`=service.	`console(c),`
		`reset(r),`
		`read-only(o),`
		`service(s),`
		`none`		

`ilomCtrlActiveDirectoryCertFileURI`	This is the URI of a certificate file needed when Strict Certificate Mode is enabled. Setting the URI causes the transfer of the file, making the certificate available immediately for certificate authentication.	*URI*	String	None
`ilomCtrlActiveDirectoryTimeout`	Specifies the number of seconds to wait before timing out if the Active Directory server is not responding.	Range: 1 to 20 seconds	Integer	4
`ilomCtrlActiveDirectoryStrictCertEnabled`	Specifies whether the Strict Certificate Mode is enabled for the Active Directory client. If enabled, the Active Directory certificate must be uploaded to the SP so that certificate validation can be performed when communicating with the Active Directory server.	`true(1), false(2)`	Integer	true
`ilomCtrlActiveDirectoryCertFileStatus`	A string indicating the status of the certificate file. This is useful in determining whether a certificate file is present or not.	*status*	String	None

▼ Manage Active Directory Administrator Groups

Note - If you were using the Net-SNMP sample applications, you could use the `snmpget` and `snmpset` commands to configure the Active Directory Administrator Groups settings. For a description of the MIB objects used in this procedure, see the table that follows the procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   `ssh` *username*`@`*snmp_manager_ipaddress*

```
Password: password
```

2. **To view the name of Active Directory administrator group ID number 2, type:**

```
% snmpget SNMP_agent
ilomCtrlActiveDirAdminGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAdminGroupName.2 = STRING:
CN=spAdmins,DC=spc,DC=north,DC=oracle,DC=com
```

3. **To set the name of Active Directory administrator group ID number 2 to `CN=spAdmins,DC=spc,DC=south,DC=oracle,DC=com`, type:**

```
% snmpset SNMP_agent
ilomCtrlActiveDirAdminGroupName.2 s CN=spAdmins,DC=spc,DC=
south,DC=oracle,DC=com
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAdminGroupName.2 = STRING:
CN=spAdmins,DC=spc,DC=south,DC=oracle,DC=com
% snmpget SNMP_agent
ilomCtrlActiveDirAdminGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAdminGroupName.2 = STRING:
CN=spAdmins,DC=spc,DC=south,DC=oracle,DC=com
```

The following table describes the Active Directory Administrator Groups SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default
`ilomCtrlActive` `DirAdminGroupId`	An integer identifier of the Active Directory Administrator Groups entry.	1 to 5 **Note -** This object is not accessible for reading or writing.	Integer	None

`ilomCtrlActive`
`DirAdminGroup`
`Name`
	This string should contain a Distinguished Name that exactly matches one of the group names on the Active Directory server. Any user belonging to one of these groups in this table will be assigned the Oracle ILOM role of Administrator.	*name* (maximum of 255 characters)	String	None

Manage Active Directory Operator Groups

Note - You can use the `get` and `set` commands to configure the Active Directory Operator Groups settings. For a description of the MIB objects used in this procedure, see the table that follows the procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   ```
   ssh username@snmp_manager_ipaddress
   ```

   ```
   Password: password
   ```

2. **To view the name of Active Directory operator group ID number 2, type:**

   ```
   % snmpget SNMP_agent
   ilomCtrlActiveDirOperatorGroupName.2
   SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirOperatorGroupName.2 =
   STRING: ad-oper-group-ent-2
   ```

3. **To set the name of Active Directory operator group ID number 2 to `new-name-2`, type:**

   ```
   % snmpset SNMP_agent
   ilomCtrlActiveDirOperatorGroupName.2 s new-name-2
   SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirOperatorGroupName.2 =
   STRING: new-name-2
   % snmpget SNMP_agent
   ilomCtrlActiveDirOperatorGroupName.2
   SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirOperatorGroupName.2 =
   STRING: new-name-2
   ```

The following table describes the Active Directory Operator Groups SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default
`ilomCtrlActiveDirOperatorGroupId`	An integer identifier of the Active Directory Operator Groups entry.	1 to 5 **Note -** This object is not accessible for reading or writing.	Integer	None
`ilomCtrlActiveDirOperator`	This string should contain a Distinguished Name that exactly matches one of the group names on the Active Directory server.	*name* (maximum of 255 characters)	String	None

MIB Object	Description	Allowed Values	Type	Default
`GroupName`	Any user belonging to one of these groups in this table will be assigned the Oracle ILOM role of Operator.			

Manage Active Directory Custom Groups

Note - You can use the `get` and `set` commands to configure the Active Directory Custom Groups settings. For a description of the MIB objects used in this procedure, see the table that follows the procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   `ssh` *username*`@`*snmp_manager_ipaddress*

   `Password:` *password*

2. **To view the name of Active Directory custom group ID number 2, type:**

```
% snmpget SNMP_agent
ilomCtrlActiveDirCustomGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirCustomGroupName.2 =
STRING: CN=SpSuperCust,OU=Groups,DC=johns,DC=oracle,DC=com
```

3. **To set the name of Active Directory custom group ID number 2 to `CN=SpSuperCust, OU=Groups,DC=bills,DC=oracle,DC=com`, type:**

```
% snmpset SNMP_agent
ilomCtrlActiveDirCustomGroupName.2 s CN=SpSuperCust,OU=Groups,DC=
bills,DC=oracle,DC=com
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirCustomGroupName.2 =
STRING: CN=SpSuperCust,OU=Groups,DC=bills,DC=oracle,DC=com
% snmpget SNMP_agent
 ilomCtrlActiveDirCustomGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirCustomGroupName.2 = m
STRING: CN=SpSuperCust,OU=Groups,DC=bills,DC=oracle,DC=co
```

4. **To view the roles of Active Directory custom group ID number 2, type:**

```
% snmpget SNMP_agent
```

```
 ilomCtrlActiveDirCustomGroupRoles.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirCustomGroupRoles.2 =
STRING: "aucro"
```

5. **To set the roles of Active Directory custom group ID number 2 to User Management and Read Only (`u`, `o`), type:**

```
% snmpset SNMP_agent
ilomCtrlActiveDirCustomGroupRoles.2 s “uo"
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirCustomGroupRoles.2 =
STRING: "uo"
% snmpget  SNMP_agent
ilomCtrlActiveDirCustomGroupRole.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirCustomGroupRoles.2 =
STRING: "uo"
```

The following table describes the Active Directory Custom Groups SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default
`ilomCtrlActiveDirCustomGroupId`	An integer identifier of the Active Directory Custom Groups entry.	1 to 5 This object is not accessible for reading or writing.	Integer	None
`ilomCtrlActiveDirCustomGroupName`	This string should contain a Distinguished Name that exactly matches one of the group names on the Active Directory server. Any user belonging to one of these groups in this table will be assigned the Oracle ILOM role based on the entry's configuration for roles.	*name* (maximum of 255 characters)	String	None
`ilomCtrlActiveDirCustomGroupRoles`	Specifies the role that a user authenticated through Active Directory should have. Setting this property to legacy roles of Administrator or Operator, or any of the individual role IDs of `a`, `u`, `c`, `r`, `o`, and `s`, will cause the Active Directory client to ignore the schema stored on the Active Directory server. Setting this object to `none` clears the value and indicates that the native Active Directory schema should be used. The role IDs can be joined together. For example, `aucros`, where `a`=admin, `u`=user, `c`=console, `r`=reset, `o`=read-only, and `s`=service.	`administrator`, `operator`, `admin(a)`, `user(u)`, `console(c)`, `reset(r)`, `read-only(o)`, `service(s)`, `none`	String	None

▼ Manage Active Directory User Domains

Note - You can use the `get` and `set` commands to configure the Active Directory User Domain settings. For a description of the MIB objects used in this procedure, see the table that follows the procedure.

---

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   ssh *username*@*snmp_manager_ipaddress*

   Password: *password*

2. **To view the name of Active Directory user domain ID number 2, type:**

```
% snmpget  SNMP_agent
 ilomCtrlActiveDirUserDomain.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirUserDomain.2 = STRING:
<USERNAME>@davidc.example.oracle.com
```

3. **To set the name of Active Directory user domain ID number 2 to <*USERNAME*>`@johns.example.oracle.com`, type:**

```
% snmpset  SNMP_agent
 ilomCtrlActiveDirUserDomain.2 s
“<USERNAME>@johns.example.oracle.com”
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirUserDomain.2 = STRING:
<USERNAME>@johns.example.oracle.com
% snmpget  SNMP_agent
 ilomCtrlActiveDirUserDomain.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirUserDomain.2 = STRING:
<USERNAME>@johns.example.oracle.com
```

The following table describes the Active Directory User Domains SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default

`ilomCtrlActive`
`DirUserDomain`
`Id`
	An integer identifier of the Active Directory domain.	1 to 5
		This object is not accessible for reading or writing.
			Integer	None

`ilomCtrlActive` `DirUserDomain`	This string should exactly match with an authentication domain on the Active Directory server. This	*name* (maximum of 255 characters)	String	None

MIB Object	Description	Allowed Values	Type	Default
	string should contain a substitution string (<USERNAME>), which will be replaced with the user's login name during authentication. Either the principle or Distinguished Name format is allowed.			

▼ Manage Active Directory Alternate Server

Note - You can use the `get` and `set` commands to set the values of MIB object properties to configure the Active Directory Alternate Server settings. For a description of the MIB objects used in this procedure, see the table that follows the procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   `ssh` *username*@*snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

   - **To view the IP address of Active Directory alternate server ID number 2, type:**

     ```
     % snmpget SNMP_agent
      ilomCtrlActiveDirAlternateServerIp.2
     SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerIp.2 =
     IpAddress: 10.7.143.236
     ```

   - **To set the IP address of Active Directory alternate server ID number 2 to `10.7.143.246`, type:**

     ```
     % snmpset SNMP_agent
     ilomCtrlActiveDirAlternateServerIp.2 a 10.7.143.246
     SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerIp.2 =
     IpAddress: 10.7.143.246
     % snmpget  SNMP_agent
     ilomCtrlActiveDirAlternateServerIp.2
     SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerIp.2 =
     IpAddress: 10.7.143.246
     ```

- **To view the port number of Active Directory alternate server ID number 2, type:**

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerPort.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerPort.2 =
INTEGER: 636
```

- **To set the port number of Active Directory alternate server ID number 2 to `639`, type:**

```
% snmpset SNMP_agent
ilomCtrlActiveDirAlternateServerPort.2 i 639
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerPort.2 =
INTEGER: 639
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerIp.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerPort.2 =
INTEGER: 639
```

- **To view the certificate status of Active Directory alternate server ID number 2, type:**

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerCertStatus.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerCertStatus.
2 = STRING: certificate not present
```

- **To view the certificate URI of Active Directory alternate server ID number 2, type:**

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerCertURI.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirAlternateServerCertURI.2 =
STRING: none
```

- **To clear the certificate information associated with the server when it is set to `true`, type:**

```
% snmpset SNMP_agent
```

```
ilomCtrlActiveDirAlternateServerCertClear.0 i 1
```

- **To view the certificate version of the alternate server certificate file, type:**

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerCertVersion.0
```

- **To view the serial number of the alternate server certificate file, type:**

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerCertSerialNo.0
```

- **To view the issuer of the alternate server certificate file, type:**

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerCertIssuer.0
```

- **To view the subject of the alternate server certificate file, type:**

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerCertSubject.0
```

- **To view the valid start date of the alternate server certificate file, type:**

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerCertValidBegin.0
```

- **To view the valid end date of the alternate server certificate file, type:**

```
% snmpget SNMP_agent
ilomCtrlActiveDirAlternateServerCertValidEnd.0
```

The following table describes the Active Directory Alternate Server SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default
`ilomCtrlActiveDirAlternateServerId`	An integer identifier of the Active Directory alternate server table.	1 to 5 This object is not accessible for reading or writing.	Integer	None

MIB Object	Description	Allowed Values	Type	Default
`ilomCtrlActiveDirAlternateServerIP`	The IP address of the Active Directory alternate server used as a name service for user accounts.	*ipaddress*	String	None
`ilomCtrlActiveDirAlternateServerPort`	Specifies the port number for the Active Directory alternate server. Specifying 0 as the port indicates that autoselect will use the well-known port number. Specifying 1 - 65535 explicitly sets the port number.	*portnumber* (range: 0 to 65535)	Integer	None
`ilomCtrlActiveDirAlternateServerCert Status`	A string indicating the status of the certificate file. This is useful in determining whether a certificate file is present or not.	*status* (maximum size: 255 characters)	String	None
`ilomCtrlActiveDirAlternateServerCertURI`	This is the URI of a certificate file needed when Strict Certificate Mode is enabled. Setting the URI causes the transfer of the file, making the certificate available immediately for certificate authentication. Additionally, either `remove` or `restore` is supported for direct certificate manipulation.	*URI*	String	None

▼ Manage Server Redundancy

Note - You can use the `get` and `set` commands to view and configure redundancy settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   `ssh` *username*@*snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

   - **To view the status of the server in a redundant configuration, type:**

```
% snmpget SNMP_agent ilomCtrlRedundancyStatus.0
```

- **To view the property that controls whether the server is to be promoted or demoted from active or standby status, type:**

  ```
  % snmpget SNMP_agent ilomCtrlRedundancyAction.0
  ```

- **To promote a redundant server from standby to active status, type:**

  ```
  % snmpset SNMP_agent ilomCtrlRedundancyAction.0 i 2
  ```

- **To view the FRU name of the chassis monitoring module (CMM) on which this agent is running, type:**

  ```
  % snmpget SNMP_agent ilomCtrlRedundancyFRUName.0
  ```

Manage Active Directory DNS Locator

Note - You can use the `get` and `set` commands to configure the Active Directory DNS Locator settings. For a description of the MIB objects used in this procedure, see the table that follows the procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   `ssh` *username*@*snmp_manager_ipaddress*

   `Password:` *password*

2. **To view the state of Active Directory DNS locator, type:**

   ```
   % snmpget SNMP_agent
    ilomCtrlActiveDirDnsLocatorEnabled.0
   SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorEnabled.0 =
   INTEGER: false(2)
   ```

3. **To set the state of Active Directory DNS locator ID number 2 to enabled, type:**

   ```
   % snmpset SNMP_agent
   ```

```
ilomCtrlActiveDirDnsLocatorEnabled.0 i 1
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorEnabled.0 =
INTEGER: true(1)
% snmpget SNMP_agent
ilomCtrlActiveDirDnsLocatorEnabled.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorEnabled.2 =
INTEGER: true(1)
```

4. **To view the service name of Active Directory DNS locator ID number 2, type:**

```
% snmpget SNMP_agent
ilomCtrlActiveDirDnsLocatorQueryService.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorQueryService.2 =
STRING: _ldap._tcp.dc._msdcs.<DOMAIN>.<PORT:636>
```

5. **To set the service name and port number of Active Directory DNS locator ID number 2, type:**

```
% snmpset SNMP_agent
ilomCtrlActiveDirDnsLocatorQueryService.2 s
“_ldap._tcp.pdc._msdcs.<DOMAIN>.<PORT:936>”
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorQueryService.2 =
STRING: _ldap._tcp.pdc._msdcs.<DOMAIN>.<PORT:936>
% snmpget SNMP_agent
ilomCtrlActiveDirDnsLocatorQueryService.2
SUN-ILOM-CONTROL-MIB::ilomCtrlActiveDirDnsLocatorQueryService.2 =
STRING: _ldap._tcp.pdc._msdcs.<DOMAIN>.<PORT:936>
```

The following table describes the Active Directory DNS Locator SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default
`ilomCtrlActiveDirDnsLocatorEnabled`	Specifies whether or not the Active Directory DNS locator functionality is enabled.	`true(1), false(2)`	Integer	false
`ilomCtrlActiveDirDnsLocatorQueryId`	An integer identifier of the Active Directory DNS Locator Query entry.	1 to 5 This object is not accessible for reading or writing.	Integer	None
`ilomCtrlActiveDirDnsLocatorQueryService`	The service name that is used to perform the DNS query. The name can contain <DOMAIN> as a substitution marker, being replaced by the domain information associated for the user at the time of authentication. The service name can also contain	*name* (maximum of 255 characters)	String	None

MIB Object	Description	Allowed Values	Type	Default
	<PORT:>, which can be used to override any learned port information, if necessary. For example, `<PORT: 636>` can be specified for the standard LDAP/SSL port 636.			

Manage DNS Name Server Settings (SNMP)

Note - You can use the `get` and `set` commands to view and configure DNS name server settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   ```
   ssh username@snmp_manager_ipaddress
   ```

   ```
   Password: password
   ```

2. **Refer to the following SNMP command examples:**

   - **To view and specify the name server for DNS, type:**

     ```
     % snmpget SNMP_agent
     ilomCtrlDNSNameServers.0
     % snmpset SNMP_agent
     ilomCtrlDNSNameServers.0 s ???nameservername'
     ```

   - **To view and specify the search path for DNS, type:**

     ```
     % snmpget SNMP_agent
     ilomCtrlDNSSearchPath.0
     % snmpset SNMP_agent
     ilomCtrlDNSSearchPath.0 s ???searchpath'
     ```

   - **To view state of DHCP autodns for DNS, type:**

     ```
     % snmpget SNMP_agent ilomCtrlDNSdhcpAutoDns.0
     ```

   - **To set the state of DHCP autodns for DNS to enabled, type:**

```
% snmpset SNMP_agent ilomCtrlDNSdhcpAutoDns.0 i 1
```

- **To view the number of seconds to wait before timing out if the server does not respond, type:**

  ```
  % snmpget SNMP_agent ilomCtrlDNSTimeout.0
  ```

- **To set the number of seconds to wait before timing out if the server does not respond to 5, type:**

  ```
  % snmpset SNMP_agent ilomCtrlDNSTimeout.0 i 5
  ```

- **To view the number of times a request is attempted again after a time-out, type:**

  ```
  % snmpget SNMP_agent ilomCtrlDNSRetries.0
  ```

- **To set the number of times a request is attempted again after a time-out to 5, type:**

  ```
  % snmpset SNMP_agent ilomCtrlDNSRetries.0 i 5
  ```

Configuring Oracle ILOM for LDAP (SNMP)

- "Configure LDAP Settings" on page 64

▼ Configure LDAP Settings

Note - You can use the `get` and `set` commands to configure Oracle ILOM for LDAP. For a description of the MIB objects used in this procedure, see the table that follows the procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

```
ssh username@snmp_manager_ipaddress
Password: password
```

2. **Refer to the following SNMP command examples:**

- **To view whether the LDAP server is enabled to authenticate LDAP users, type:**

```
% snmpget SNMP_agent ilomCtrlLdapEnabled.0
```

- **To set the LDAP server state to enabled to authenticate LDAP users, type:**

```
% snmpset SNMP_agent ilomCtrlLdapEnabled.0 i 1
```

- **To view the LDAP server IP address, type:**

```
% snmpget SNMP_agent ilomCtrlLdapServerIP.0
```

- **To set the LDAP server IP address, type:**

```
% snmpset SNMP_agent ilomCtrlLdapServerIP.0 a ipaddress
```

- **To view the LDAP server port number, type:**

```
% snmpget SNMP_agent ilomCtrlLdapPortNumber.0
```

- **To set the LDAP server port number, type:**

```
% snmpset SNMP_agent ilomCtrlLdapPortNumber.0 i 389
```

- **To view the LDAP server Distinguished Name, type:**

```
% snmpget SNMP_agent ilomCtrlLdapBindDn.0
```

- **To set the LDAP server Distinguished Name, type:**

```
% snmpset SNMP_agent
```

```
ilomCtrlLdapBindDn.0 s ou=people,ou=sales,dc=oracle,dc=com
```

- **To view the LDAP server password, type:**

```
% snmpget SNMP_agent ilomCtrlLdapBindPassword.0
```

- **To set the LDAP server password, type:**

```
% snmpset SNMP_agent ilomCtrlLdapBindPassword.0 s password
```

- **To view the branch of your LDAP server on which user searches are made, type:**

```
% snmpget SNMP_agent ilomCtrlLdapSearchBase.0
```

- **To set the branch of your LDAP server on which to search for users, type:**

```
% snmpset SNMP_agent ilomCtrlLdapSearchBase.0 s ldap_server_branch
```

- **To view the LDAP server default role, type:**

```
% snmpget SNMP_agent ilomCtrlLdapDefaultRoles.0
```

- **To set the LDAP server default role to Administrator, type:**

```
% snmpset SNMP_agent ilomCtrlLdapDefaultRoles.0 s administrator
```

The following table describes the LDAP Settings SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default

`ilomCtrlLdap Enabled`	Specifies whether the LDAP client is enabled.	`true(1),`
		`false(2)`
			Integer	false

`ilomCtrlLdap ServerIP`	The IP address of the LDAP server used as a name service for user accounts.	*ipaddress*	String	None
`ilomCtrlLdap PortNumber`	Specifies the port number for the LDAP client.	*portnumber* (range: 0 to 65535)	Integer	389

MIB Object	Description	Allowed Values	Type	Default
`ilomCtrlLdap BindDn`	The Distinguished Name (DN) for the read-only proxy user used to bind to the LDAP server. For example: “`cn=proxyuser,ou=people,dc=oracle,dc=com`"	*distinguished_name*	String	None
`ilomCtrlLdap BindPassword`	The password of a read-only proxy user that is used to bind to the LDAP server. This property is essentially write-only. The write-only access level is no longer supported as of SNMP v2. This property must return a null value when read.	*password*	String	None
`ilomCtrlLdap SearchBase`	A search base in the LDAP database below which to find users. For example: “`ou=people,dc=oracle,dc=com`"	The branch of your LDAP server on which to search for users	String	None

`ilomCtrlLdap DefaultRoles`	Specifies the role that a user authenticated via LDAP should have. This property supports the legacy roles of Administrator or Operator, or any of the individual role ID combinations of `a`, `u`, `c`, `r`, `o`, and `s`. For example, `aucros`, where `a`=admin, `u`=user, `c`=console, `r`=reset, `o`=read-only, and `s`=service.	`administrator,`
		`operator,`
		`admin(a),`
		`user(u),`
		`console(c),`
		`reset(r),`
		`read-only(o),`
		`service(s)`
			String	None

Configuring Oracle ILOM for LDAP/SSL (SNMP)

▼ Manage LDAP/SSL Certificate

Note - You can use the `get` and `set` commands to view and configure LDAP/SSL certificate settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   ssh *username*@*snmp_manager_ipaddress*

   Password: *password*

2. **Refer to the following SNMP command examples:**

   - **To clear the certificate information associated with the server when it is set to `true`, type:**

     ```
     % snmpset SNMP_agent ilomCtrlLdapSslCertFileClear.0 i 0
     ```

   - **To view the certificate version of the certificate file, type:**

     ```
     % snmpget SNMP_agent ilomCtrlLdapSslCertFileVersion.0
     ```

   - **To view the serial number of the certificate file, type:**

     ```
     % snmpget SNMP_agent ilomCtrlLdapSslCertFileSerialNo.0
     ```

   - **To view the issuer of the certificate file, type:**

     ```
     % snmpget SNMP_agent ilomCtrlLdapSslCertFileIssuer.0
     ```

   - **To view the subject of the certificate file, type:**

     ```
     % snmpget SNMP_agent ilomCtrlLdapSslCertFileSubject.0
     ```

   - **To view the valid start date of the certificate file, type:**

     ```
     % snmpget SNMP_agent ilomCtrlLdapSslCertFileValidBegin.0
     ```

   - **To view the valid end date of the certificate file, type:**

     ```
     % snmpget SNMP_agent ilomCtrlLdapSslCertFileValidEnd.0
     ```

▼ Manage LDAP/SSL Administrator Groups

Note - You can use the `get` and `set` commands to configure the LDAP/SSL Administrator Groups settings. For a description of the MIB objects used in this procedure, see the table that follows the procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   `ssh` *username*`@`*snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

   - **To view the name of LDAP/SSL administrator group ID number 3, type:**

     ```
     % snmpget SNMP_agent
     ilomCtrlLdapSslAdminGroupName.3
     SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAdminGroupName.3 = STRING:
     CN=SpSuperAdmin,OU=Groups,DC=davidc,DC=example,DC=oracle,DC=com
     ```

   - **To set the name of LDAP/SSL administrator group ID number 3 to `CN=SpSuperAdmin,OU=Groups,DC=tomp,DC=example,DC=oracle,DC=com`, type:**

     ```
     % snmpset SNMP_agent
     ilomCtrlLdapSslAdminGroupName.3 s CN=SpSuperAdmin,OU=Groups,DC=
     tomp,DC=example,DC=oracle,DC=com
     SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAdminGroupName.3 = STRING:
     CN=SpSuperAdmin,OU=Groups,DC=tomp,DC=example,DC=oracle,DC=com
     % snmpget SNMP_agent
     ilomCtrlLdapSslAdminGroupName.3
     SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAdminGroupName.3 = STRING:
     CN=SpSuperAdmin,OU=Groups,DC=tomp,DC=example,DC=oracle,DC=com
     ```

   The following table describes the LDAP/SSL Administrator Groups SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default
`ilomCtrlLdap`	An integer identifier of the LDAP/SSL AdminGroup entry.	1 to 5	Integer	None

MIB Object	Description	Allowed Values	Type	Default
`SslAdminGroupId`		**Note -** This object is not accessible for reading or writing.		
`ilomCtrlLdapSslAdminGroupName`	This string should contain a Distinguished Name that exactly matches one of the group names on the LDAP/SSL server. Any user belonging to one of these groups in this table will be assigned the ILOM role of Administrator.	*name* (maximum of 255 characters)	String	None

▼ Manage LDAP/SSL Operator Groups

Note - You can use the `get` and `set` commands to configure the LDAP/SSL Operator Groups settings. For a description of the MIB objects used in this procedure, see the table that follows the procedure.

---

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   `ssh` *username*`@`*snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

   - **To view the name of LDAP/SSL operator group ID number 3, type:**

     ```
     % snmpget SNMP_agent
     ilomCtrlLdapSslOperatorGroupName.3SUN-ILOM-CONTROL-MIB::ilomCtrlL
     dapSslOperatorGroupName.3 = STRING: CN=SpSuperOper,OU=Groups,DC=
     davidc,DC=example,DC=oracle,DC=com
     ```

   - **To set the name of Active Directory operator group ID number 3 to `CN=SpSuperAdmin,OU=Groups,DC=tomp,DC=example,DC=oracle,DC=com`, type:**

     ```
     % snmpset SNMP_agent
     ilomCtrlLdapSslOperatorGroupName.3 s CN=SpSuperOper,OU=Groups,DC=
     tomp,DC=example,DC=oracle,DC=com
     SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslOperatorGroupName.3 =
     STRING: CN=SpSuperOper,OU=Groups,DC=tomp,DC=example,DC=oracle,DC=com
     % snmpget SNMP_agent
     ilomCtrlLdapSslOperatorGroupName.3
     ```

```
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslOperatorGroupName.3 =
STRING: CN=SpSuperOper,OU=Groups,DC=tomp,DC=example,DC=oracle,DC=com
```

The following table describes the LDAP/SSL Operator Groups SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default
`ilomCtrlLdapSslOperatorGroupId`	An integer identifier of the LDAP/SSL Operator Group entry.	1 to 5 **Note -** This object is not accessible for reading or writing.	Integer	None
`ilomCtrlLdapSslOperatorGroupName`	This string should contain a Distinguished Name that exactly matches one of the group names on the LDAP/SSL server. Any user belonging to one of these groups in this table will be assigned the ILOM role of Operator.	*name* (maximum of 255 characters)	String	None

Manage LDAP/SSL Custom Groups

Note - You can use the `get` and `set` commands to configure the LDAP/SSL Custom Groups settings. For a description of the MIB objects used in this procedure, see the table that follows the procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   `ssh` *username*@*snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

   - **To view the name of LDAP/SSL custom group ID number 2, type:**

     ```
     % snmpget SNMP_agent
     ilomCtrlLdapSslCustomGroupName.2
     SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupName.2 = STRING:
     CN=SpSuperCust,OU=Groups,DC=johns,DC=oracle,DC=com
     ```

   - **To set the name of LDAP/SSL custom group ID number 2 to `CN=SpSuperCust,OU=Groups,DC=bills,DC=oracle,DC=com`, type:**

```
% snmpset SNMP_agent
ilomCtrlLdapSslCustomGroupName.2 s CN=SpSuperCust,OU=Groups,DC=
bills,DC=oracle,DC=com
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupName.2 = STRING:
CN=SpSuperCust,OU=Groups,DC=bills,DC=oracle,DC=com
% snmpget SNMP_agent
ilomCtrlLdapSslCustomGroupName.2
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupName.2 = STRING:
CN=SpSuperCust,OU=Groups,DC=bills,DC=oracle,DC=com
```

- **To view the roles of LDAP/SSL custom group ID number 2, type:**

```
% snmpget SNMP_agent
ilomCtrlLdapSslCustomGroupRoles.2
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupRoles.2 = STRING:
“aucro"
```

- **To set the roles of LDAP/SSL custom group ID number 2 to User Management and Read Only (`u,o`), type:**

```
% snmpset SNMP_agent
ilomCtrlLdapSslCustomGroupRoles.2 s “uo"
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupRoles.2 = STRING:
"uo"
% snmpget SNMP_agent
ilomCtrlLdapSslCustomGroupRoles.2
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslCustomGroupRoles.2 = STRING:
"uo"
```

The following table describes the LDAP/SSL Custom Groups SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default
`ilomCtrlLdapSsl CustomGroupId`	An integer identifier of the LDAP/SSL custom group entry.	1 to 5 **Note -** This object is not accessible for reading or writing.	Integer	None
`ilomCtrlLdap SslCustomGroup Name`	This string should contain a Distinguished Name that exactly matches one of the group names on the LDAP/SSL server. Any user belonging to one of these groups in this table will be assigned the ILOM role based on the entry's configuration for roles.	*name* (maximum of 255 characters)	String	None
`ilomCtrlLdap SslCustomGroup Roles`	Specifies the role that a user authenticated through LDAP/SSL should have. Setting this property to legacy roles of Administrator or Operator, or any of the individual role IDs of `a`, `u`, `c`, `r`, `o` and `s` will cause the LDAP/SSL client to ignore the	`administrator`, `operator`,	String	None

MIB Object	Description	Allowed Values	Type	Default
	schema stored on the LDAP/SSL server. Setting this object to none clears the value and indicates that the native LDAP/SSL schema should be used. The role IDs can be joined together. For example, aucros, where a=admin, u=user, c=console, r=reset, o=read-only, and s=service.	admin(a), user(u), console(c), reset(r), read-only(o), service(s), none		

Manage LDAP/SSL User Domain

Note - You can use the get and set commands to configure the LDAP/SSL User Domain settings. For a description of the MIB objects used in this procedure, see the table that follows the procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   ```
   ssh username@snmp_manager_ipaddress
   ```

   ```
   Password: password
   ```

2. **Refer to the following SNMP command examples:**

   - **To view the name of LDAP/SSL user domain ID number 3, type:**

     ```
     % snmpget SNMP_agent
     ilomCtrlLdapSslUserDomain.3
     SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslUserDomain.3 = STRING: CN=
     <USERNAME>,CN=Users,DC=davidc,DC=example,DC=oracle,DC=com
     ```

   - **To set the name of LDAP/SSL user domain ID number 3 to CN=<USERNAME>, CN=Users,DC=tomp,DC=example,DC=oracle,DC=com, type:**

     ```
     % snmpset SNMP_agent
     ilomCtrlLdapSslUserDomain.3 s CN=<USERNAME>,CN=Users,DC=tomp,DC=
     example,DC=oracle,DC=com
     ```

```
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslUserDomain.3 = STRING: CN=
<USERNAME>,CN=Users,DC=tomp,DC=example,DC=oracle,DC=com
% snmpget SNMP_agent
ilomCtrlLdapSslUserDomain.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslUserDomain.3 = STRING: CN=
<USERNAME>,CN=Users,DC=tomp,DC=example,DC=oracle,DC=com
```

The following table describes the LDAP/SSL User Domain SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default
`ilomCtrlLdapSslUserDomainId`	An integer identifier of the LDAP/SSL domain.	1 to 5 **Note -** This object is not accessible for reading or writing.	Integer	None
`ilomCtrlLdapSslUserDomain`	This string should exactly match with an authentication domain on the LDAP/SSL server. This string should contain a substitution string (<USERNAME>), which will be replaced with the user's login name during authentication. Either the principle or Distinguished Name format is allowed.	*name* (maximum of 255 characters)	String	None

▼ Manage LDAP/SSL Alternate Server

Note - You can use the `get` and `set` commands to configure the LDAP/SSL Alternate Server settings. For a description of the MIB objects used in this procedure, see the table that follows the procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   `ssh` *username*@*snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

   - **To view the IP address of LDAP/SSL alternate server ID number 3, type:**

```
% snmpget SNMP_agent
ilomCtrlLdapSslAlternateServerIp.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAlternateServerIp.3 =
IpAddress: 10.7.143.236
```

- **To set the IP address of LDAP/SSL alternate server ID number 3 to `10.7.143.246`, type:**

```
% snmpset SNMP_agent
ilomCtrlLdapSslAlternateServerIp.3 a 10.7.143.246
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAlternateServerIp.3 =
IpAddress: 10.7.143.246
% snmpget SNMP_agent
ilomCtrlLdapSslAlternateServerIp.3
SUN-ILOM-CONTROL-MIB::ilomCtrlLdapSslAlternateServerIp.3 =
IpAddress: 10.7.143.246
```

- **To view and clear the certificate information associated with the alternate server when it is set to `true`, type:**

```
% snmpget SNMP_agent
ilomCtrlLdapSslAlternateServerCertClear.0
% snmpset SNMP_agent
ilomCtrlLdapSslAlternateServerCertClear.0 i 0
```

- **To view the alternate server certificate version of the certificate file, type:**

```
% snmpget SNMP_agent ilomCtrlLdapSslAlternateServerCertVersion.0
```

- **To view the serial number of the alternate server certificate file, type:**

```
% snmpget SNMP_agent ilomCtrlLdapSslAlternateServerCertSerialNo.0
```

- **To view the issuer of the alternate server certificate file, type:**

```
% snmpget SNMP_agent ilomCtrlLdapSslAlternateServerCertIssuer.0
```

- **To view the subject of the alternate server certificate file, type:**

```
% snmpget SNMP_agent ilomCtrlLdapSslAlternateServerCertSubject.0
```

- **To view the valid start date of the alternate server certificate file, type:**

```
% snmpget SNMP_agent
ilomCtrlLdapSslAlternateServerCertValidBegin.0
```

- **To view the valid end date of the alternate server certificate file, type:**

```
% snmpget SNMP_agent ilomCtrlLdapSslAlternateServerCertValidEnd.0
```

The following table describes the LDAP/SSL Alternate Server SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default
`ilomCtrlLdapSslAlternateServerId`	An integer identifier of the LDAP/SSL alternate server table.	1 to 5 **Note -** This object is not accessible for reading or writing.	Integer	None
`ilomCtrlLdapSslAlternateServerIP`	The IP address of the LDAP/SSL alternate server used as directory server for user accounts.	*ipaddress*	String	None
`ilomCtrlLdapSslAlternateServerPort`	Specifies the port number for the LDAP/SSL alternate server. Specifying 0 as the port indicates that auto-select will use the well-known port number. Specifying 1-65535 explicitly sets the port number.	*portnumber* (range: 0 to 65535)	Integer	None
`ilomCtrlLdapSslAlternateServerCert` `Status`	A string indicating the status of the certificate file. This is useful in determining whether a certificate file is present or not.	*status* (maximum size: 255 characters)	String	None
`ilomCtrlLdapSslAlternateServerCert` `URI`	This is the URI of a certificate file needed when Strict Certificate Mode is enabled. Setting the URI causes the transfer of the file, making the certificate available immediately for certificate authentication. Additionally, either `remove` or `restore` are supported for direct certificate manipulation.	*URI*	String	None

Configuring Oracle ILOM for RADIUS (SNMP)

- "Configure RADIUS Settings" on page 77

▼ Configure RADIUS Settings

Note - Before completing this procedure, collect the appropriate information about your RADIUS environment. You can use the `get` and `set` commands to configure RADIUS. For a description of the MIB objects used in this procedure, see the table that follows the procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   `ssh` *username*`@`*snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

   - **To view whether the RADIUS server is enabled to authenticate RADIUS users, type:**

     ```
     % snmpget SNMP_agent ilomCtrlRadiusEnabled.0
     ```

   - **To set the RADIUS server state to enabled to authenticate RADIUS users, type:**

     ```
     % snmpset  SNMP_agent ilomCtrlRadiusEnabled.0 i 1
     ```

   - **To view the RADIUS server IP address, type:**

     ```
     % snmpget SNMP_agent ilomCtrlRadiusServerIP.0
     ```

   - **To set the RADIUS server IP address, type:**

     ```
     % snmpset SNMP_agent ilomCtrlRadiusServerIP.0 a ipaddress
     ```

   - **To view the RADIUS server port number, type:**

     ```
     % snmpget SNMP_agent ilomCtrlRadiusPortNumber.0
     ```

   - **To set the RADIUS server port number, type:**

```
% snmpset SNMP_agent ilomCtrlRadiusPortNumber.0 i portnumber
```

- **To view the RADIUS server shared secret, type:**

```
% snmpget SNMP_agent ilomCtrlRadiusSecret.0
```

- **To set the RADIUS server shared secret, type:**

```
% snmpset SNMP_agent ilomCtrlRadiusSecret.0 s secret
```

- **To view the RADIUS server default user roles, type:**

```
% snmpget SNMP_agent ilomCtrlRadiusDefaultRoles.0
```

- **To set the RADIUS server default user roles to console, type:**

```
% snmpset SNMP_agent ilomCtrlRadiusDefaultRoles.0 s c
```

The following table describes the RADIUS SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default

`ilomCtrlRadiusEnabled`	Specifies whether or not the RADIUS client is enabled.	`true(1),`
		`false(2)`
			Integer	false

`ilomCtrlRadiusServerIP`	The IP address of the RADIUS server used as a name service for user accounts.	*ipaddress*	String	None
`ilomCtrlRadius` `PortNumber`	Specifies the port number for the RADIUS client.	*portnumber* (range: 0 to 65535)	Integer	1812
`ilomCtrlRadius` `Secret`	The shared secret encryption key that is used to encypt traffic between the RADIUS client and server.	*secret* (maximum length: 255 characters)	Sting	None

`ilomCtrlRadius`
`DefaultRoles`
	Specifies the role that a user authenticated through RADIUS should have. This property supports the legacy roles of Administrator or Operator, or any of the individual role ID combinations of `a`, `u`, `c`, `r`, `o`, and `s`. For example, `aucros`, where `a`=admin, `u`=user, `c`=console, `r`=reset, `o`=read-only, and `s`=service.	`administrator,`
		`operator,`
		`admin(a),`
		`user(u),`
		`console(c),`
		`reset(r),`
			String	None

MIB Object	Description	Allowed Values	Type	Default

		`read-only(o),`
		`service(s)`		

Manage Component Information and Email Alerts (SNMP)

Description	Links
Review Oracle ILOM requirements for managing component information and email alerts using SNMP.	■ "Before You Begin Component Information (SNMP)" on page 81
Learn how to view component information.	■ "Viewing Component Information (SNMP)" on page 82
Learn how to manage clock settings, syslog and alert rules.	■ "Managing Clock Settings, Event Log, Syslog Receiver, and Alert Rules (SNMP)" on page 83
Learn how to configure the SMTP client for email notification alerts.	■ "Configuring SMTP Client for Email Alert Notifications (SNMP)" on page 88
Learn how to configure alerts.	■ "Configuring Email Alert Settings (SNMP)" on page 90

Related Information

- "Configuring Alert Notifications, Service Requests, or Remote Logging" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

Before You Begin Component Information (SNMP)

- Before you can use SNMP to view and configure Oracle ILOM settings, you must configure SNMP. For more information, see "Configuring SNMP Settings in Oracle ILOM" on page 19.
- When executing the `snmpset` command, you need to use a v1/v2c community or a v3 user account with read-write (rw) privileges.

Note - For examples of SNMP commands, see "SNMP Command Examples" on page 147.

Note - The SNMP commands presented in this section are based on the Net-SNMP sample applications and, therefore, will work as presented only if you have Net-SNMP and the Net-SNMP sample applications installed.

Viewing Component Information (SNMP)

- "View Component Information" on page 82

▼ View Component Information

Note - You can use `get` commands to view component information. For a description of valid MIB objects for this procedure, see the table following this procedure.

---

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   `ssh` *username*@*snmp_manager_ip_address*

   `Password:` *password*

2. **To view the firmware revision, type:**

   `%` **`snmpget`** *SNMP_agent* **`entPhysicalFirmwareRev.1`**

The following table describes the Component Information SNMP MIB objects.

MIB Object	Description	Values	Type	Default
`entPhysicalName`	The textual name of the physical entity.	Size: 0 to 255	String	Zero-length string
`entPhysicalDescr`	A textual description of the physical entity.	Size: 0 to 255	String	None
`entPhysicalContainedIn`	The value of entPhysicalIndex for the physical entity that *contains* this physical entity. A value of 0 indicates this physical entity is not contained in any other physical entity.	Range: 0 to 2147483647	Integer	None

MIB Object	Description	Values	Type	Default

`entPhysical`
`Class`
	An indication of the general hardware type of the physical entity.	`other(1),`
		`unknown(2),`
		`chassis(3),`
		`backplane(4),`
		`container(5),`
		`powerSupply(6),`
		`fan(7),`
		`sensor(8),`
		`module(9),`
		`port(10),`
		`stack(11)`
			Integer	None

`entPhysical` `FirmwareRev`	The vendor-specific firmware revision string for the physical entity.	Size: 0 to 255	String	Zero-length string

Managing Clock Settings, Event Log, Syslog Receiver, and Alert Rules (SNMP)

- "View and Set Clock Settings" on page 83
- "View and Clear the Oracle ILOM Event Log" on page 84
- "Configure Remote Syslog IP Destinations" on page 86
- "Configure Severity Level Alert Rule" on page 87

▼ View and Set Clock Settings

Note - You can use the `get` and `set` commands to view and set clock settings with respect to Network Time Protocol (NTP) synchronization. For a description of valid MIB objects for this procedure, see the table following this procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

```
ssh username@snmp_manager_ip_address
```

```
Password: password
```

2. **Refer to the following SNMP commands for examples:**

- **To view the NTP server state, type:**

```
% snmpget SNMP_agent ilomCtrlNTPEnabled.0
```

- **To set the NTP server state to enabled, type:**

```
% snmpset SNMP_agent ilomCtrlNTPEnabled.0 i 1
```

- **To view the date and time of the device, type:**

```
% snmpget SNMP_agent ilomCtrlDateAndTime.0
```

- **To set the date and time of the device, type:**

```
% snmpset SNMP_agent ilomCtrlDateAndTime.0 s 2013-3-24,4:59:47.0
```

The following table describes the valid SNMP MIB objects for Oracle ILOM clock properties.

MIB Object	Description	Allowed Values	Type	Default
`ilomCtrlDateAndTime`	The date and time of the device.	*date/time*	String	None
`ilomCtrlNTP`	Specifies whether the Network Time Protocol is enabled.	`true(1),`	Integer	false
`Enabled`		`false(2)`		
ilomCtrlTimezone	The configured time zone string.	Size: 0 to 255	String	None

▼ View and Clear the Oracle ILOM Event Log

Note - You can use the `get` command to view the Oracle ILOM event log and the `set` command to configure the event log. For a description of valid MIB objects for this procedure, see the table following this procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   ```
   ssh username@snmp_manager_ip_address
   Password: password
   ```

2. **To view the event log type for an event log with a record ID of 2, type:**

   ```
   % snmpget SNMP_agent ilomCtrlEventLogType.2
   ```

3. **To clear the event log, type:**

   ```
   % snmpset SNMP_agent ilomCtrlEventLogClear.0 i 1
   ```

   The following table describes the Oracle ILOM Event Logs SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default
ilomCtrlEventLog RecordID	The record number for a given event log entry. **Note -** This object is not accessible.	Range: 1 to 10000	Integer	None
ilomCtrlEventLog Type	An integer representing the type of event. **Note -** This object is read-only.	log(1), action(2), fault(3), state(4), repair(5), other(6)	Integer	None
ilomCtrlEvent LogTimestamp	The date and time that the event log entry was recorded. **Note -** This object is read-only.	*date/time*	String	None
ilomCtrlEvent LogClass	An integer representing the class of event. **Note -** This object is read-only.	audit(1), ipmi(2), chassis(3), fma(4), system(5) pcm(6)	Integer	None
ilomCtrlEventLog Severity	The event severity corresponding to the given log entry.	disable(1),	Integer	None

MIB Object	Description	Allowed Values	Type	Default

	Note - This object is read-only.	`critical(2),`
		`major(3),`
		`minor(4),`
		`down(5)`		

`ilomCtrlEventLogDescription`	A textual description of the event. **Note -** This object is read-only.	*description*	String	None

`ilomCtrlEventLogClear`	Setting this object to `true` clears the event log.	`true(1),`
		`false(2)`
			Integer	None

▼ Configure Remote Syslog IP Destinations

Note - You can use the `get` and `set` commands to view and set IP addresses for a remote syslog receiver. For a description of valid MIB objects for this procedure, see the table following this procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   `ssh` *username*`@`*snmp_manager_ip_address*

   `Password:` *password*

2. **To view a remote syslog destination IP address, type:**

   ```
   % snmpget SNMP_agent ilomCtrlRemoteSyslogDestAddress1.0
   ```

3. **To set a remote syslog destination IP address, type:**

   ```
   % snmpset SNMP_agent ilomCtrlRemoteSyslogDestAddress1.0 a ip_address
   ```

The following table describes the Syslog IP Destinations SNMP MIB objects.

MIB Object	Description	Values	Type	Default
`ilomCtrlRemoteSyslogDest1`	The IP address of the first remote syslog destination (log host).	*ip_address*	String	None
`ilomCtrlRemoteSyslogDest2`	The IP address of the second remote syslog destination (log host).	*ip_address*	String	None

▼ Configure Severity Level Alert Rule

Note - You can use the `get` and `set` commands to view and configure alert rule configurations. For a description of valid MIB objects for this procedure, see the table following this procedure.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   `ssh` *username*`@`*snmp_manager_ip_address*

   `Password:` *password*

2. **To view the severity level for the alert rule with an alert ID of 2, type:**

   ```
   % snmpget SNMP_agent ilomCtrlAlertSeverity.2
   ```

3. **To set the severity level to critical for the alert rule with an alert ID of 2, type:**

   ```
   % snmpset SNMP_agent ilomCtrlAlertSeverity.2 i 2
   ```

   The following table describes the Alert Rule Severity Level SNMP MIB objects.

MIB Object	Description	Allowed Values	Type	Default
`ilomCtrlAlert ID`	An integer ID associated with a given alert rule. **Note -** This object is not accessible.	Range: 0 to 65535	Integer	None

`ilomCtrlAlert Severity`	Specifies the mininum event severity that should trigger an alert for a given class.	`disable(1),`
		`critical(2),`
		`major(3),`
		`minor(4),`
		`down(5)`
			Integer	None

`ilomCtrlAlert Type`	Specifies the type of notification for a given alert. If the type is `snmptrap(2)` or `ipmipet(3)`, the `ilomCtrlAlertDestinationIP` must be specified. If the type is `email(1)`, the `ilomCtrlAlert DestinationEmail` must be specified.	`email(1)`
		`snmptrap(2)`
		`ipmipet(3)`
			Integer	None

`ilomCtrlAlert DestinationIP`	Specifies the IP address to send alert notifications to when the alert type is `snmptrap(2)` or `ipmipet(3)`.	*ip_address*	String	None

MIB Object	Description	Allowed Values	Type	Default
`ilomCtrlAlert Destination Email`	Specifies the email address to send alert notifications to when the alert type is `email(1)`.	*email address* Size: 0 to 255	String	None

`ilomCtrlAlert SNMPVersion`	Specifies the version of SNMP trap that should be used for the given alert rule.	`v1(1),`
		`v2c(2),`
		`v3(3)`
			Integer	None

`ilomCtrlAlert SNMPCommunity OrUsername`	Specifies the community string to be used when the `ilomCtrlAlertSNMPVersion` property is set to `v1(1)` or `v2c(2)`. Specifies the SNMP user name to use when the `ilomCtrlAlertSNMPVersion` is set to `v3(3)`.	Size: 0 to 255	String	None
`ilomCtrlAlert EmailEvent ClassFilter`	A class name or `all` to filter emailed alerts on.	Size: 0 to 255	String	None
`ilomCtrlAlert EmailEventTypeFilter`	A class name or `all` to filter emailed alerts on.	Size 0 to 255	String	None

Configuring SMTP Client for Email Alert Notifications (SNMP)

- "Configure SMTP Client for Alert Notification" on page 88

▼ Configure SMTP Client for Alert Notification

Before You Begin

- To generate configured email notification alerts, you must enable the Oracle ILOM client to act as an SMTP client to send the email alert messages. To enable the Oracle ILOM client as an SMTP client, you must specify the IP address and port number of an outgoing SMTP email server that will process the email notifications.
- Prior to enabling the Oracle ILOM client as an SMTP client, gather the IP address and port number of the outgoing SMTP email server.
- You can use the `get` and `set` commands to configure the SMTP client. For a description of the MIB objects used in this procedure, see Valid SMTP Client MIB Objects and the SUN-ILOM-CONTROL-MIB.

Note - For a description of valid MIB objects for this procedure, see the table following this procedure.

To configure SMTP Client properties in Oracle ILOM:

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   ```
   ssh username@snmp_manager_ip_address
   Password: password
   ```

2. **Refer to the following SNMP commands for examples:**

   - **To view an SMTP client state, type:**

     ```
     % snmpget SNMP_agent ilomCtrlSMTPEnabled.0
     ```

   - **To set an SMTP client state to `enabled`, type:**

     ```
     % snmpset SNMP_agent ilomCtrlSMTPEnabled.0 i 1
     ```

   - **To view an SMTP server IP address, type:**

     ```
     % snmpget SNMP_agent ilomCtrlSMTPServerIP.0
     ```

   - **To set an SMTP server IP address, type:**

     ```
     % snmpset SNMP_agent ilomCtrlSMTPServerIP.0 s ip_address
     ```

   - **To view an SMTP client port number, type:**

     ```
     % snmpget SNMP_agent ilomCtrlSMTPPortNumber.0
     ```

   - **To set an SMTP client port number, type:**

     ```
     % snmpset SNMP_agent ilomCtrlSMTPPortNumber.0 i 25
     ```

- **To view an optional format to identify the sender or the “from” address, type:**

```
% snmpget SNMP_agent ilomCtrlSMTPCustomSender.0
```

- **To configure an optional format to identify the sender or the “from” address, type:**

```
% snmpset SNMP_agent
 ilomCtrlSMTPCustomSender.0 s ???ilom-alert@HOSTNAME.abc.com'
```

The following table describes the SMTP Email Alert Notification SNMP MIB objects.

MIB Object	Property	Allowed Values	Type	Default
ilomCtrlSMTP Enabled	Specifies whether or not the SMTP client is enabled.	true(1), false(2)	Integer	false
ilomCtrlSMTP ServerIP	The IP address of the SMTP server used as a name service for user accounts.	*ip_address*	String	None
ilomCtrlSMTP PortNumber	Specifies the port number for the SMTP client.	Range: 0 to 65535	Integer	None

Configuring Email Alert Settings (SNMP)

- “Manage Email Alert Settings” on page 90

▼ Manage Email Alert Settings

Note - You can use the `get` and `set` commands to view and configure email alert settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   ```
   ssh username@snmp_manager_ipaddress
   ```

```
Password: password
```

2. **Refer to the following SNMP command examples:**

- **To view the optional format used to identify the sender or the “from” address, type:**

  ```
  % snmpget SNMP_agent ilomCtrlAlertEmailCustomSender.0
  ```

- **To set the optional format used to identify the sender or the “from” address, type:**

  ```
  % snmpset SNMP_agent
  ilomCtrlAlertEmailCustomSender.0 s
  ???ilom-alert@HOSTNAME.abc.com'
  ```

- **To view an optional string that can be added to the beginning of the message body, type:**

  ```
  % snmpget SNMP_agent ilomCtrlAlertEmailMessagePrefix.0
  ```

- **To define an optional string (for example: `BeginMessage`) that can be added to the beginning of the message body, type:**

  ```
  % snmpset SNMP_agent ilomCtrlAlertEmailMessagePrefix.0 s
  ???BeginMessage'
  ```

Monitor and Manage System Power (SNMP)

Description	Links
Review the SNMP requirements for managing system power properties.	■ "Before You Begin Power Management (SNMP)" on page 93
Learn how to monitor the power consumption interfaces.	■ "Monitoring the Power Consumption Interfaces (SNMP)" on page 94
Learn how to maintain the system power policy.	■ "Maintaining System Power Policy (SNMP)" on page 96
Learn how to apply power to the system.	■ "Managing System Power Properties (SNMP)" on page 98

Related Information

- "Setting Power Alert Notifications and Managing System Power Usage" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
- "Real-Time Power Monitoring Through Oracle ILOM Interfaces" in *Oracle ILOM User's Guide for System Monitoring and Diagnostics Firmware Release 3.2.x*

Before You Begin Power Management (SNMP)

Prior to performing the procedures in this section, ensure that the following requirements are met.

- Before you can use SNMP to view and configure Oracle ILOM settings, you must configure SNMP. For more information, see "Configuring SNMP Settings in Oracle ILOM" on page 19.
- To execute the `snmpset` command, you need to use an SNMP v1 or v2c community or an SNMP v3 user account with read-write (rw) privileges.

Note - For examples of SNMP commands, see "SNMP Command Examples" on page 147.

Note - The SNMP commands presented in this section are based on the Net-SNMP sample applications and, therefore, will work as presented only if you have Net-SNMP and the Net-SNMP sample applications installed.

Monitoring the Power Consumption Interfaces (SNMP)

Note - The power consumption interfaces described in this section might or might not be implemented on the platform that you are using. See the platform-specific Oracle ILOM supplement, platform administration guide, or product notes included with your system for implementation details.

▼ Monitor Actual Power Consumption

● **To view actual power consumption using SNMP, type:**

```
% snmpget SNMP_agent sunHwCtrlPowerMgmtActualPower.0
```

▼ Monitor Available Power

● **To view total available power using SNMP, type:**

```
% snmpget SNMP_agent sunHwCtrlPowerMgmtAvailablePower.0
```

Monitor Allocated Power

- **To view the total power allocated to the system using SNMP, type:**

```
% snmpget SNMP_agent sunHwCtrlPowerMgmtAllocatedPower.0
```

Monitor Permitted Power Consumption

- **To view permitted power consumption using SNMP, type:**

```
% snmpget SNMP_agent sunHwCtrlPowerMgmtPermittedPower.0
```

Monitor Power Management Properties

Note - You can use the `get` command to view power management settings. For a description of the MIB objects used in these commands, see the SUN-HW-CTRL-MIB.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   ```
   ssh username@snmp_manager_ipaddress
   Password: password
   ```

2. **To monitor various power consumption properties on a managed device, see the following SNMP command examples.**

   - **To view the name of the power management policy for `PowerMgmtTable` index number 5, type:**

     ```
     % snmpget SNMP_agent sunHwCtrlPowerMgmtName.5
     ```

   - **To view the units for the value of the power management policy for `PowerMgmtTable` index number 5, type:**

     ```
     % snmpget SNMP_agent sunHwCtrlPowerMgmtUnits.5
     ```

- **To view the value of the power management policy for `PowerMgmtTable` index number 5, type:**

```
% snmpget SNMP_agent sunHwCtrlPowerMgmtValue.5
```

Set Power Consumption Thresholds

- **To configure one or both power consumption thresholds, type:**

```
% snmpset SNMP_agent sunHwCtrlPowerMgmtConsumptionThreshold1|2.0 i
value
```

where *value* is the power consumption threshold in watts.

When the system power consumption exceeds the specified threshold, Oracle ILOM will generate an alert. If you have configured email alerts on your system, a notification will be sent to the alert destination.

Maintaining System Power Policy (SNMP)

Enable a system power policy to reduce the server power consumption. See the following procedure to manage the system power policy.

- "View and Set the Power Policy" on page 96

View and Set the Power Policy

Before You Begin Before setting a system power policy, review the power management features described in the following article:

http://www.oracle.com/technetwork/articles/servers-storage-admin/ser-howto-save-pwr-sparc-1982424.html

1. **To view the power policy on one of Oracle's SPARC servers using SNMP, type:**

```
% snmpget SNMP_agent sunHwCtrlPowerMgmtPolicy.0
```

You can view the power policy for a given domain on one of Oracle's multi-domain SPARC servers by typing:

```
% snmpget SNMP_agent sunHwCtrlDomainPowerMgmtPolicy.n
```

where *n* is the domain ID plus one.

2. **To set the power policy on one of Oracle's SPARC servers, type:**

```
% snmpset SNMP_agent
 sunHwCtrlPowerMgmtPolicy.0 i disabled|performance|elastic
```

You can set the power policy for a given domain on one of Oracle's multi-domain SPARC servers by typing:

```
% snmpset SNMP_agent
sunHwCtrlDomainPowerMgmtPolicy.n i disabled|performance|elastic
```

where *n* is the domain ID plus one.

Managing System Power Budget (SNMP)

Power budgeting allows you to set an upper limit for the system power consumption, and it enforces that limit. See the following procedure to manage the system power budget:

- "Set the System Power Budget" on page 97

▼ Set the System Power Budget

Before You Begin Before setting a system power budget, review the power management features described in the following article:

http://www.oracle.com/technetwork/articles/servers-storage-admin/ser-howto-save-pwr-sparc-1982424.html

1. **Enable power budgeting on the system:**

```
% snmpset SNMP_agent sunHWCtrlPowerMgmtBudget.0 i enabled
```

2. **Set an upper limit for the system power consumption:**

```
% snmpset SNMP_agent sunHWCtrlPowerMgmtBudgetPendingPowerlimit.0 i
 value sunHWCtrlPowerMgmtBudgetCommitPending.0 i true
```

where *value* is a power limit in watts between the installed hardware minimum and the allocated power. The default power limit is the current peak permitted power.

3. **Specify how many seconds the system power can exceed the power limit (see Step 2) before a violation action is taken:**

```
% snmpset SNMP_agent sunHwCtrlPowerMgmtBudgetTimelimit.0 i value
sunHwCtrlPowerMgmtBudgetCommitPending.0 i true
```

where *value* is an integer between -1 and 2147483647. A value of -1 instructs the system to use the factory-specified default value. A value of 0 indicates that a hard cap should be used. Some systems do not support hard capping. For more information, refer to "Setting SP Advanced Power Capping Policy to Enforce Power Limit" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*.

4. **Set a violation action to define what the system should do when the power limit has been exceeded beyond the specified time limit:**

```
% snmpset SNMP_agent sunHwCtrlPowerMgmtBudgetTimelimitActions.0 i
none|hardPowerOff sunHwCtrlPowerMgmtBudgetCommitPending.0 i true
```

Managing System Power Properties (SNMP)

- "Power On System" on page 98
- "Reset System Power" on page 99

▼ Power On System

Note - You can use the `set` command to configure the power setting. For a description of the MIB object used in this command, see the SUN-ILOM-CONTROL-MIB.

Note - The syntax in this procedure is valid for a `tcsh` shell. It might not be necessary to include the escape character (`\`) in your shell environment.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   ```
   ssh username@snmp_manager_ipaddress
   Password: password
   ```

2. **To power on the power control target named ???/SYS', type:**

   ```
   % snmpset SNMP_agent ilomCtrlPowerAction.\"/SYS\" i 1
   ```

Reset System Power

Note - You can use the `set` command to configure the reset setting. For a description of the MIB objects used in this command, see the SUN-ILOM-CONTROL-MIB.

Note - The syntax in this procedure is valid for a `tcsh` shell. It might not be necessary to include the escape character (`\`) in your shell environment.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   ```
   ssh username@snmp_manager_ipaddress
   Password: password
   ```

2. **To reset the control target named ???/SP', type:**

   ```
   % snmpset SNMP_agent ilomCtrlResetAction.\"/SP\" i 1
   ```

Manage Oracle ILOM Firmware Updates (SNMP)

Description	Links
Learn how to update Oracle ILOM firmware using SNMP.	■ "Update Oracle ILOM Firmware (SNMP)" on page 101

Related Information

- "Updating Oracle ILOM Firmware" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

▼ Update Oracle ILOM Firmware (SNMP)

Before You Begin

- Before you can use SNMP to view and update Oracle ILOM firmware, you must configure SNMP. For more information, see "Configuring SNMP Settings in Oracle ILOM" on page 19.
- To execute the `snmpset` command, you need to use an SNMP v1 or v2c community or an SNMP v3 user with read-write (rw) privileges.
- For examples of SNMP commands, see "SNMP Command Examples" on page 147.

Note - You can use the `get` and `set` commands to view and configure Oracle ILOM firmware settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

Note - The example SNMP commands presented in this section are based on the Net-SNMP sample applications and, therefore, will work as presented only if you have Net-SNMP and the Net-SNMP sample applications installed.

To update the Oracle ILOM firmware using SNMP:

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   ```
   ssh username@snmp_manager_ipaddress
   Password: password
   ```

2. **Refer to the following SNMP command examples:**

   - **To view the version of the current firmware image, type:**

     ```
     % snmpget SNMP_agent ilomCtrlFirmwareMgmtVersion.0
     ```

   - **To view the build number of the current firmware image, type:**

     ```
     % snmpget SNMP_agent ilomCtrlFirmwareBuildNumber.0
     ```

   - **To view the build date and time of the current firmware image, type:**

     ```
     % snmpget SNMP_agent ilomCtrlFirmwareBuildDate.0
     ```

   - **To view the IP address of the TFTP server that will be used to download the firmware image, type:**

     ```
     % snmpget SNMP_agent ilomCtrlFirmwareTFTPServerIP.0
     ```

   - **To set the IP address of the TFTP server that will be used to download the firmware image, type:**

     ```
     % snmpset SNMP_agent ilomCtrlFirmwareTFTPServerIP.0 a ipaddress
     ```

   - **To view the relative path of the new firmware image file on the TFTP server, type:**

     ```
     % snmpget SNMP_agent ilomCtrlFirmwareTFTPFileName.0
     ```

- **To set the relative path of the new firmware image file on the TFTP server, type:**

```
% snmpset SNMP_agent ilomCtrlFirmwareTFTPFileName.0 s ???tftpfilename'
```

- **To view the property that determines whether the previous configuration of the server should be preserved after a firmware update, type:**

```
% snmpget SNMP_agent ilomCtrlFirmwarePreserveConfig.0
```

- **To set the `PreservConfig` property to true so that the previous configuration of the server is preserved after a firmware update, type:**

```
% snmpset SNMP_agent ilomCtrlFirmwarePreserveConfig.0 i 1
```

- **To view the property that indicates the status of a firmware update, type:**

```
% snmpget SNMP_agent ilomCtrlFirmwareMgmtStatus.0
```

- **To view the property that is used to initiate a firmware update using the values of the other firmware management properties as parameters, type:**

```
% snmpget SNMP_agent ilomCtrlFirmwareMgmtAction.0
```

- **To set the property so as to initiate a firmware update using the values of the other firmware management properties as parameters, type:**

```
% snmpset SNMP_agent ilomCtrlFirmwareMgmtAction.0 i 2
```

- **To clear the values of the other firmware management properties used if and when a firmware update is initiated, type:**

```
% snmpset SNMP_agent ilomCtrlFirmwareMgmtAction.0 i 1
```

- **To view the version of the current firmware management file system, type:**

```
% snmpget SNMP_agent ilomCtrlFirmwareMgmtFilesystemVersion.0
```

- **To view the property that is used to postpone the BIOS upgrade until the next server power-off, type:**

```
% snmpget SNMP_agent ilomCtrlFirmwareDelayBIOS.0
```

- **To set the `DelayBIOS` property to postpone the BIOS upgrade until the next server power-off, type:**

```
% snmpset SNMP_agent ilomCtrlFirmwareDelayBIOS.0 i 1
```

Manage Oracle ILOM Backup and Restore Configurations (SNMP)

Note - As of **Oracle ILOM 3.2.6.x** , **SNMP support for backing up and restoring Oracle ILOM properties has been removed** and will not be supported in future Oracle ILOM firmware releases. Oracle ILOM continues to support the ability to back up and restore Oracle ILOM configuraiton properties from the Oracle ILOM CLI and web interface. For instructions on how to perfrom backup and restore functionality from the Oracle ILOM CLI or web interface, see "Backing Up, Restoring, or Resetting the Oracle ILOM Configuration" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

Description	Links
Learn how to backup and restore Oracle ILOM properties.	■ "View and Configure Backup and Restore Properties (SNMP)" on page 105

Related Information

- "Using Backup, Restore, and Reset Default Operations" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

▼ View and Configure Backup and Restore Properties (SNMP)

Note - SNMP support for Backup and Restore has been removed as of Oracle ILOM firmware 3.2.6.x. As of Oracle ILOM 3.2.6.x, refer to the following section for backing up and restoring Oracle ILOM configuration properties: "Backing Up, Restoring, or Resetting the Oracle ILOM Configuration" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

Before You Begin

- Before you can use SNMP to view and configure Oracle ILOM settings, you must configure SNMP. For more information, see “Configuring SNMP Settings in Oracle ILOM” on page 19.
- To execute the `snmpset` command, you need to use an SNMP v1 or v2c community or an SNMP v3 user with read-write (rw) privileges.

Note - You can use the `get` and `set` commands to view and configure backup and restore settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

Note - For examples of SNMP commands, see “SNMP Command Examples” on page 147.

Note - The example SNMP commands presented in this section are based on the Net-SNMP sample applications and, therefore, will work as presented only if you have Net-SNMP and the Net-SNMP sample applications installed.

Note - The syntax in this procedure is valid for a tcsh shell. It might not be necessary to include the escape character (\) in your shell environment.

To set the Oracle ILOM backup and restore properties using SNMP, follow these steps:

1. **Log in to a host that has an SNMP tool and the ILOM MIBs installed. For example, type:**

   `ssh` *username*`@`*snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

   - **To view the power policy using SNMP, type:**

     ```
     % snmpget SNMP_agent sunHwCtrlPowerMgmtPolicy.0
     ```

- **To configure the power property and apply it to the power control target named ???/SYS', type:**

  ```
  % snmpset SNMP_agent ilomCtrlPowerAction.\"/SYS\" i 1
  ```

- **To restore the configuration on the SP to the original factory default state, type:**

  ```
  % snmpset SNMP_agent ilomCtrlResetToDefaultsAction.0 i 3
  ```

- **To view the target destination of the configuration XML file during the backup and restore operation, type:**

  ```
  % snmpget SNMP_agent ilomCtrlBackupAndRestoreTargetURI.0
  ```

- **To set the target destination of the configuration XML file during the backup and restore operation using TFTP, type:**

  ```
  % snmpset SNMP_agent
   ilomCtrlBackupAndRestoreTargetURI.0 s
  ???tftp://tftp_server_ipaddress/remotedir/config_backup.xml'
  ```

- **To set the passphrase to encrypt or decrypt sensitive data during the backup and restore operation, type:**

  ```
  % snmpset SNMP_agent
   ilomCtrlBackupAndRestorePassphrase.0 s ???passphrase'
  ```

- **To view the property used to issue an action, either backup or restore, type:**

  ```
  % snmpget SNMP_agent ilomCtrlBackupAndRestoreAction.0
  ```

- **To issue a restore action using the `ilomCtrlBackupAndRestoreAction` MIB object, type:**

  ```
  % snmpset SNMP_agent ilomCtrlBackupAndRestoreAction.0 i 2
  ```

- **To monitor the current status of the backup or restore operation, type:**

```
% snmpget SNMP_agent ilomCtrlBackupAndRestoreActionStatus.0
```

- **To specify the reset action and apply it to the reset control target named ???/SP', type:**

```
% snmpset SNMP_agent ilomCtrlResetAction.\”/SP\” i 1
```

Manage SPARC Diagnostics, POST, and Boot Mode Operations (SNMP)

Description	Links
Review the requirements for managing SPARC cconfiguration management interfaces.	■ "Before You Begin Manage SPARC Hosts (SNMP)" on page 109
Learn how to manage SPARC management interface properties.	■ "Managing SPARC Diagnostic, POST, and Boot Mode Properties (SNMP)" on page 110

Related Information

- "Configuring Host Server Management Actions" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*
- "Setting Diagnostic Tests to Run" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

Before You Begin Manage SPARC Hosts (SNMP)

Prior to performing the SNMP procedures for managing SPARC diagnostics, POST, and boot mode properties, ensure that the following requirements are met.

- Before you can use SNMP to view and configure Oracle ILOM settings, you must configure SNMP. For more information, see "Configuring SNMP Settings in Oracle ILOM" on page 19.
- To execute the `snmpset` command, you need to use an SNMP v1 or v2c community or an SNMP v3 user account with read-write (rw) privileges.
- For examples of SNMP commands, see "SNMP Command Examples" on page 147.

Note - The SNMP commands presented in this section are based on the Net-SNMP sample applications and, therefore, will work as presented only if you have Net-SNMP and the Net-SNMP sample applications installed.

Managing SPARC Diagnostic, POST, and Boot Mode Properties (SNMP)

▼ Manage SPARC Host Diagnostic Properties

Note - You can use the `get` and `set` commands to view and configure SPARC diagnostic settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   `ssh` *username*@*snmp_manager_ipaddress*

   `Password:` *password*

2. **Refer to the following SNMP command examples:**

   - **To view the triggers of embedded diagnostics for the host, type:**

     ```
     % snmpget SNMP_agent ilomCtrlSPARCDiagsTrigger.0
     ```

   - **To set the triggers of embedded diagnostics for the host to power-on-reset, type:**

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsTrigger.0 i 4
```

- **To view the modes for POST, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsMode.0
```

- **To set the POST mode to `service`, type:**

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsMode.0 i 3
```

- **To view the level of embedded diagnostics that should be run on the host during a boot for the power-on-reset trigger, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsPowerOnLevel.0
```

- **To set the level of embedded diagnostics that should be run on the host during a boot for the power-on-reset trigger to `normal`, type:**

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsPowerOnLevel.0 i 3
```

- **To view the level of embedded diagnostics that should be run on the host during a boot for the user-reset trigger, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsUserResetLevel.0
```

- **To set the level of embedded diagnostics that should be run on the host during a boot for the user-reset trigger to `normal`, type:**

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsUserResetLevel.0 i 3
```

- **To view the level of embedded diagnostics that should be run on the host during a boot for the error-reset trigger, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsErrorResetLevel.0
```

- **To set the level of embedded diagnostics that should be run on the host during a boot for the error-reset trigger to `normal`, type:**

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsErrorResetLevel.0 i 3
```

- **To view the level of embedded diagnostics that should be run on the host during a boot for the hardware change trigger, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsHwChangeLevel.0
```

- **To set the level of embedded diagnostics that should be run on the host during a boot for the hardware change trigger to `maximum`, type:**

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsHwChangeLevel.0 i 4
```

- **To view the verbosity level of embedded diagnostics that should be run on the host during a boot, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsPowerOnVerbosity.0
```

- **To set the verbosity level of embedded diagnostics that should be run on the host during a boot to `maximum`, type:**

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsPowerOnVerbosity.0 i 4
```

- **To view the verbosity level of embedded diagnostics that should be run on the host during a boot for user-reset trigger, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsUserResetVerbosity.0
```

- **To set the verbosity level of embedded diagnostics that should be run on the host during a boot for user-reset trigger to `maximum`, type:**

```
% snmpset SNMP_agent ilomCtrlSPARCDiagsUserResetVerbosity.0 i 4
```

- **To view the verbosity level of embedded diagnostics that should be run on the host during a boot for error-reset trigger, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCDiagsErrorResetVerbosity.0
```

- **To set the verbosity level of embedded diagnostics that should be run on the host during a boot for error-reset trigger to `maximum`, type:**

  ```
  % snmpset SNMP_agent ilomCtrlSPARCDiagsErrorResetVerbosity.0 i 4
  ```

- **To view the verbosity level of embedded diagnostics that should be run on the host during a boot for the hardware change trigger, type:**

  ```
  % snmpget SNMP_agent ilomCtrlSPARCDiagsHwChangeVerbosity.0
  ```

- **To set the verbosity level of embedded diagnostics that should be run on the host during a boot for the hardware change trigger to `minimum`, type:**

  ```
  % snmpset SNMP_agent ilomCtrlSPARCDiagsHwChangeVerbosity.0 i 2
  ```

▼ Manage SPARC Host POST Operations

Note - You can use the `get` and `set` commands to view and configure SPARC host settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   ```
   ssh username@snmp_manager_ipaddress
   Password: password
   ```

2. **Refer to the following SNMP command examples:**

   - **To view the starting MAC address for the host, type:**

     ```
     % snmpget  SNMP_agent ilomCtrlSPARCHostMACAddress.0
     ```

   - **To view the version string for OpenBoot PROM (OBP), type:**

     ```
     % snmpget  SNMP_agent ilomCtrlSPARCHostOBPVersion.0
     ```

- **To view the version string for POST, type:**

```
% snmpget  SNMP_agent ilomCtrlSPARCHostPOSTVersion.0
```

- **To view the option that determines whether the host should continue to boot in the event of a non-fatal POST error, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCHostAutoRunOnError.0
```

- **To configure the host to continue to boot in the event of a non-fatal POST error, type:**

```
% snmpset SNMP_agent ilomCtrlSPARCHostAutoRunOnError.0 i 1
```

- **To view the option that determines what action the SP will take when it discovers that the host is hung, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCHostAutoRestartPolicy.0
```

- **To configure the SP to reset when it discovers that the host is hung, type:**

```
% snmpset SNMP_agent ilomCtrlSPARCHostAutoRestartPolicy.0 i 2
```

- **To view the string that describes the boot status of host operating system, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCHostOSBootStatus.0
```

- **To view the boot timer time-out value, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCHostBootTimeout.0
```

- **To set the boot timer time-out value to 30 seconds, type:**

```
% snmpset SNMP_agent ilomCtrlSPARCHostBootTimeout.0 i 30
```

- **To view the property that determines what action the SP will take when the boot timer expires, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCHostBootRestart.0
```

- **To configure the SP to reset when the boot timer expires, type:**

```
% snmpset SNMP_agent ilomCtrlSPARCHostBootRestart.0 i 2
```

- **To view the maximum number of boot failures allowed by the SP, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCHostMaxBootFail.0
```

- **To set the maximum number of boot failures allowed by the SP to 10, type:**

```
% snmpset SNMP_agent ilomCtrlSPARCHostMaxBootFail.0 i 10
```

- **To view the property that determines what action the SP will take when the maximum number of boot failures is reached, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCHostBootFailRecovery.0
```

- **To configure the SP to power cycle the host when the maximum number of boot failures is reached, type:**

```
% snmpset SNMP_agent ilomCtrlSPARCHostBootFailRecovery.0 i 2
```

- **To view the version string for the Hypervisor, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCHostHypervisorVersion.0
```

- **To view the version string for the system firmware (SysFw), type:**

```
% snmpget SNMP_agent ilomCtrlSPARCHostSysFwVersion.0
```

- **To view the property that determines the break action that the SP will send, type:**

  ```
  % snmpget SNMP_agent ilomCtrlSPARCHostSendBreakAction.0
  ```

- **To configure the SP to send a `dumpcore` break action, type:**

  ```
  % snmpset SNMP_agent ilomCtrlSPARCHostSendBreakAction.0 i 3
  ```

- **To view the property that determines the host I/O reconfiguration policy to apply on next host power-on, type:**

  ```
  % snmpget SNMP_agent ilomCtrlSPARCHostIoReconfigurePolicy.0
  ```

- **To configure the SP to execute the host I/O reconfiguration policy on the next power-on, type:**

  ```
  % snmpset SNMP_agent ilomCtrlSPARCHostIoReconfigurePolicy.0 i 3
  ```

▼ Manage SPARC Host Boot Mode Properties

Note - You can use the `get` and `set` commands to view and configure SPARC boot mode settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

   ```
   ssh username@snmp_manager_ipaddress
   Password: password
   ```

2. **Refer to the following SNMP command examples:**

   - **To view the boot mode state for the host, type:**

     ```
     % snmpget SNMP_agent ilomCtrlSPARCBootModeState.0
     ```

- **To configure the host to retain current NVRAM variable settings, type:**

```
% snmpset SNMP_agent ilomCtrlSPARCBootModeState.0 i 1
```

- **To view the boot script to use when the boot mode state is set to `script`, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCBootModeScript.0
```

- **To specify the boot script to use when the boot mode state is set to `??? setenv diag-switch'`, type:**

```
% snmpset SNMP_agent
 ilomCtrlSPARCBootModeScript.0 s ???setenv diag-switch'
```

- **To view date and time when the boot mode configuration will expire, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCBootModeExpires.0
```

- **To view the string that refers to the LDOM configuration name, type:**

```
% snmpget SNMP_agent ilomCtrlSPARCBootModeLDOMConfig.0
```

- **To set the LDOM configuration name to `default`, type:**

```
% snmpset SNMP_agent ilomCtrlSPARCBootModeLDOMConfig.0 s default
```

▼ Manage SPARC Host Keyswitch Property

Note - You can use the `get` and `set` commands to view and configure SPARC key switch settings. For a description of the MIB objects used in these commands, see the SUN-ILOM-CONTROL-MIB.

1. **Log in to a host that has an SNMP tool and the Oracle ILOM MIBs installed. For example, type:**

```
ssh username@snmp_manager_ipaddress
Password: password
```

2. **Refer to the following SNMP command examples:**

   - **To view the current state of the virtual key switch, type:**

     ```
     % snmpget SNMP_agent ilomCtrlSPARCKeySwitchState.0
     ```

   - **To set the state of the virtual key switch to `standby`, type:**

     ```
     % snmpset SNMP_agent ilomCtrlSPARCKeySwitchState.0 i 2
     ```

Server Management Using IPMI

Description	Links
Learn about using IPMItool to manage Oracle servers.	■ "Intelligent Platform Management Interface (IPMI)" on page 119
Learn how to configure the IPMI state and perform various management functions using the IPMItool.	■ "Managing IPMI Properties in Oracle ILOM" on page 124 ■ "Using IPMItool to Run Oracle ILOM CLI Commands" on page 126 ■ "Performing System Management Tasks (IPMItool)" on page 130
Learn about the IPMI commands.	■ "IPMItool Options and Command Summary " on page 142

Related Information

- "Modifying Default Management Access Configuration Properties" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

Intelligent Platform Management Interface (IPMI)

- "About IPMI" on page 119
- "IPMI TLS Service and Interface" on page 120
- "IPMItool" on page 122
- "IPMI Alerts" on page 123
- "IPMI Administrator and Operator Roles" on page 123

About IPMI

Oracle ILOM supports the Intelligent Platform Management Interface (IPMI), which enables you to monitor and control your server, as well as to retrieve information about your server.

IPMI is an open, industry-standard interface that was designed for the management of server systems over a number of different types of networks. IPMI functionality includes field-replaceable unit (FRU) inventory reporting, system monitoring, logging of system events, system recovery (including system resets and power-on and power-off capabilities), and alerting.

The monitoring, logging, system recovery, and alerting functions available through IPMI provide access to the management functionality that is built into the platform hardware.

IPMI Service State and Supported IPMI Sessions

By default, the IPMI service state in Oracle ILOM is enabled. The following IPMI sessions are supported as of Oracle ILOM firmware version 3.2.8:

- TLS Sessions — Enabled by default.

  Note - For increased security, always use the TLS sessions option.. For more details, see “IPMI TLS Service and Interface” on page 120.

- IPMI v2.0 Sessions — Enabled by default
- IPMI - v1.5 Sessions — Disabled by default (as of Oracle ILOM firmware 3.2.4).

The service processors (SPs) on your Oracle managed devices (servers, blade server modules, and so on) are IPMI compliant. You can access IPMI functionality through the command line using the `IPMItool` interface either in-band (using the host operating system running on the server) or out-of-band (using a remote system). Additionally, you can generate IPMI-specific traps from the Oracle ILOM web interface, or manage the SP IPMI functions from any external management solution that is IPMI compliant. For more information about the IPMItool utility, see “IPMItool” on page 122.

Note - For IPMI technical resources, including specifications, refer to the Intel and Sourceforge sites: `http://www.intel.com/design/servers/ipmi/spec.htm` or `http://openipmi.sourceforge.net`

IPMI TLS Service and Interface

IPMI TLS is an Oracle improvement to IPMI security which requires a special version of the ipmitool client that supports TLS sessions. The IPMItool command option to access the TLS interface is:

```
impitool -I orcltls
```

Note that in cases where the `-I` option is not specified, the IPMItool utility will negotiate to the most secure interface available (in the following order):

- TLS 1.2 (`orcltls` interface)
- TLS 1.1 (`orcltls` interface)
- TLS 1.0 (`orcltls` interface)
- IPMI 2.0 (`lanplus` interface)
- IPMI 1.5 (`lan` interface)

TLS Session Feature Summary

Feature	Description
Secure Communication Protocol Data Transmission	A secure TLS/TCP socket connection is used (over Ethernet and LAN over USB) to transmit and receive data between the IPMI client the server SP.
Negotiation of Highest Cipher Suite	IPMI/TLS client sessions negotiate to highest cipher suite supported on the server SP.
Authentication	Uses local SP authorization to validate user credentials and to set client session privileges. **Note -** LDAP, Active Directory, and RADIUS user authorization is currently not supported as of firmware Oracle ILOM 3.2.8.
Audit Log of IPMI Login Events	The Audit Log captures all IPMI login events (successful and failed attempts).
SSL Certificate Validation	Automatically validates the SSL client certificate against a list of trusted certificates stored in the user specified directory (`ipmitool --cert-dir` option). Note that when the IPMI TLS interface (`orcltls`) is unable to validate the client certificate, the user is prompted to cross-check the certificate's authentic fingerprint with the SSL certificate authentic fingerprints stored in the local SP directory (`/SP/services/https/ssl`). If a match is not found, the user should respond **`No`**. Otherwise, if a match is found, the user should respond **`Yes`** to proceed. For information about how to disable the check option for certificate validation when the `orcltls` interface is specified see, “Disable Default TLS Behavior for SSL Certificate Check” on page 129. For information about uploading and managing SSL certificates on the server SP, see “SSL Certificate and

Feature	Description
	Private Key Configuration Properties for HTTPS Web Server” in *Oracle ILOM Administrator’s Guide for Configuration and Maintenance Firmware Release 3.2.x*.

TLS IPMItool Interface Download Requirement

Prior to executing Oracle ILOM commands from the TLS ipmitool interface, you must download the Oracle TLS components (OS compliant driver and the `orcltls` IPMItool interface) from Oracle Hardware Management Pack. For instance, to download the Oracle TLS components from Oracle Hardware Management Pack, follow this process:

1. On the managed device, download Oracle Hardware Management Pack (v2.4 or later for Linux or v4.0 or later for Oracle Solaris) from My Oracle Support.

   Note - The Oracle TLS components (OS compliant driver and the `orcltls` IPMItool interface) are not available for download from the Oracle Hardware Management Pack for Windows.

2. Launch the installer for the Hardware Management Component GUI by following the instructions in the *Oracle Hardware Management Pack Installation Guide*.

   The Oracle Hardware Management Pack documentation is available for download at: `http://docs.oracle.com/en/servers/management.html`
3. After launching the installer for the Hardware Management Component GUI, choose the Custom Install.
4. In the Custom Install Set menu, choose IPMItool.
5. Continue to follow the instructions in the *Oracle Hardware Management Pack Installation Guide* to complete the installation.

IPMItool

IPMItool is an open-source simple command-line interface (CLI) utility for managing and configuring IPMI-enabled devices. The utility can be used to manage the IPMI functions of a local or remote system with a kernel device driver or over a LAN interface. Versions of the IPMItool utility for all Oracle ILOM supported IPMI interfaces are available for download from the Oracle Hardware Management Pack.

You can do the following with IPMItool:

- Read the sensor data record (SDR) repository.
- Print sensor values.
- Display the contents of the system event log (SEL).
- Print field-replaceable unit (FRU) inventory information.
- Read and set LAN configuration parameters.
- Perform remote chassis power control.

IPMItool features command-line help, which can be accessed by typing `ipmitool help` at the command-line prompt.

IPMItool supports a feature that enables you to enter Oracle ILOMCLI commands just as though you were using the ILOM CLI directly. CLI commands can be scripted, and then the script can be run on multiple service processor (SP) instances. For additional information, see "Using IPMItool to Run Oracle ILOM CLI Commands" on page 126.

IPMI Alerts

Oracle ILOM supports alerts in the form of IPMI Platform Event Trap (PET) alerts. Alerts provide advance warning of possible system failures. Alert configuration is available from the SP on your server. IPMI PET alerts are supported on Oracle server SPs; however, IPMI PET alerts are not supported on chassis monitoring modules (CMMs). For more information about IPMI alerts, refer to "Configuring Alert Notifications" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*.

IPMI Administrator and Operator Roles

The *IPMI Administrator role* maps to these user roles in Oracle ILOM: `aucro`. The *IPMI Operator role* maps to these user roles in Oracle ILOM: `cro.` A brief explanation of these Oracle ILOM roles appears in the following table.

TABLE 6 IPMI Administrator and Operator Roles in Oracle ILOM

IPMI Role	Enabled ILOM Role Privileges	Description
Administrator	■ Admin (`a`) ■ User Management (`u`) ■ Console (`c`) ■ Reset and Host Console (`r`) ■ Read-Only (`o`)	These user roles enable read and write privileges to these management features in Oracle ILOM: system management configuration properties, user account properties, remote console management properties, remote power management properties, and reset and host control management properties.

IPMI Role	Enabled ILOM Role Privileges	Description
Operator	■ Console (c) ■ Reset and Host Console (r) ■ Read-Only (o)	These user roles enable read and write privileges to these management features in Oracle ILOM: remote console management properties, remote power management properties, and reset and host control management properties.

Note - The Read-Only role provides read access to system management configuration properties and user management properties.

For more information about Oracle ILOM roles and privileges, refer to "Managing User Credentials" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*.

Managing IPMI Properties in Oracle ILOM

- "Set the IPMI State and Session Properties (CLI)" on page 124
- "Set the IPMI State and Session Properties (Web)" on page 125

▼ Set the IPMI State and Session Properties (CLI)

Before You Begin

- The IPMI state property in Oracle ILOM is enabled by default.
- As of Oracle ILOM firmware v3.2.8, the following IPMI properties are shipped enabled: **Service State**, **TLS Sessions**, and **v2.0 Sessions**. The session property for v1.5 is shipped disabled.
- Admin (a) role privileges are required to change the IPMI Service State or Session properties in Oracle ILOM.

  Note - The TLS Session property is always enabled and cannot be modified.

- If FIPS mode is enabled in Oracle ILOM, the IPMI v1.5 session property cannot be enabled. For additional information about FIPS mode, see "Operating Oracle ILOM in FIPS Compliance Mode" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

Follow these steps to set the IPMI state and sessions properties using the Oracle ILOM CLI:

1. **Log in to the Oracle ILOM CLI using an account with admin (a) role privileges.**
2. **To set the IPMI state property, issue the following command:**

   ```
   -> set /SP/services/ipmi state=[enabled|disabled]
   ```

   Where: `[`*enabled*`|`*disabled*`]`, type `enabled` to enable the `ipmi state` property, or type `disabled` to disable the `ipmi state` property.

   Note - If the IPMI Service State is disabled, system management information using the IPMItool utility is not accessible.

   ---

3. **To set the IPMI session properties, issue the following command:**

   ```
   -> set /SP/services/ipmi [v2_0_sessions=enabled|disabled][v1_5_sessions=enabled|disabled]
   ```

   Note - TLS sessions (`tls_sessions`) are enabled by default. To disable TLS sessions, you must disable the IPMI State property.

   Where:

   - `[v2_0_sessions=`*enabled*`|`*disabled*`]` applies only to the IPMI v2.0 session property. Type: `v_2_0_sessions=enabled` to enable the IPMI v2.0 sessions; **or** Type: `v_2_0_sessions=disabled` to disable the IPMI v2.0 sessions.
   - `[v1_5_sessions=`*enabled*`|`*disabled*`]` applies only to the IPMI v1.5 session property. Type: `v_1_5_sessions=enabled` to enable the IPMI v1.5 sessions; **or** Type: `v_1_5_sessions=disabled` to disable the IPMI v1.5 sessions.

     Note - For higher level of security, the properties for `v_2_0_sessions` and `v_1_5_sessions` should always be disabled.

     Note - If FIBS mode is enabled, the IPMI `v_1_5_sessions` property cannot be enabled.

▼ Set the IPMI State and Session Properties (Web)

Before You Begin

- The IPMI state property in Oracle ILOM is enabled by default.

- As of Oracle ILOM firmware 3.2.8, IPMI Session properties are enabled for TLS and IPMI v2.0. The property for IPMI v1.5 Sessions is disabled.
- Admin (a) role privileges are required to change the IPMI state or session properties in Oracle ILOM.
- If FIPS mode is enabled in Oracle ILOM, the IPMI v1.5 session property cannot be enabled. For additional information about FIPS mode, see "Operating Oracle ILOM in FIPS Compliance Mode" in *Oracle ILOM Administrator's Guide for Configuration and Maintenance Firmware Release 3.2.x*

Follow these steps to set the IPMI state and sessions properties using the Oracle ILOM web interface:

1. **Log in to the Oracle ILOM web interface using an account with admin (a) role privileges.**

2. **Click ILOM Administration → Management Access > IPMI.**

   The IPMI page appears.

3. **In the IPMI page, enable or disable the IPMI State check box and the applicable sessions property check boxes for TLS, IPMI v2.0 and IPMI v1.5.**

Note - If the IPMI Service State property is disabled, system management information using the IPMItool utility is not accessible.

Note - For a higher level of security, the checkboxes for IPMI 1.5 sessions and IPM 2.0 sessions should be disabled.

Note - If FIBS mode is enabled, the IPMI v1.5 session property cannot be enabled. For more details about FIPS mode, click the Details link on the Management Access > FIPS page.

Using IPMItool to Run Oracle ILOM CLI Commands

The IPMItool CLI is a convenient alternative method to executing Oracle ILOM CLI commands. It enables you to enter commands just as if you were using the Oracle ILOM CLI directly. Most Oracle ILOM CLI commands are supported.

- "IPMItool and Oracle ILOM Requirements" on page 127
- "Access the Oracle ILOM CLI From IPMItool" on page 128

- "Disable Default TLS Behavior for SSL Certificate Check" on page 129
- "Scripting Oracle ILOM CLI Commands With IPMItool" on page 129

IPMItool and Oracle ILOM Requirements

Prior to using the IPMItool to execute Oracle ILOM commands, review these requirements:

- Use the latest IPMItool that is available from the Oracle Hardware Management Pack.

  Note - IPMItool users can check the version number of the IPMItool by specifying the **`-V`** option (**`ipmitool -v`**).

- To use the IPMI TLS interface, IPMItool users must use IPMItool v1.8.15.1 or later that is available for download from Oracle Hardware Management Pack for Linux (as of v2.4 and later) and Oracle Hardware Management Pack for Solaris (as of v4.0 and later).

  Note - To access the IPMI TLS interface, IPMItool users can either specify the `-I orcltls` option or not specify an option and the IPMItool will automatically detect the most secure interface available.

- Ensure that you have the proper user roles assigned in Oracle ILOM when using the IPMItool utility to execute Oracle ILOM commands. For more information, see "IPMI Administrator and Operator Roles" on page 123.
- Unless otherwise noted, commands described in this section accept options and other arguments according to the following syntax:

  `ipmitool` `[`*option(s*`]` **`-I`** `[`*orcltls*`|`*lanplus*`]` **`-H`** `[`*hostserveraddress*`]` `[`*hostserveroptions*`]`

  `[`*command issued***`]`**
  `[`*system output***`]`**

  Where:

  - [*option(s)*] can include: **`-c [`***cipher suite level***`]`** |**`-h`** (to display help)**`|-v`** (to display verbose output) |**`-V`** (to display version number)
  - **`-I`** identifies the selected IPMI interface such as **`-I orcltls`** (IPMI TLS interface) | **`-I lanplus`** (IPMI v2.0 interface).

Note - If an IPMI interface is not specified, the IPMItool defaults to the most secure IPMI interface supported on the host server.

- `-H` [*hostserveraddress*] identifies the remote server SP hostname or IP address. The [*hostserveroption(s)*] must always specify: **-U [***username***] -P [***password***]**. The [*hostserveroption(s)*] can also include optional options such as **-p [***portnumber***]** | **-R [***retries count***]**

Note - Required host options for all IPMI interfaces include: **-H [***hostserveraddress***] -U [***username***]** and **-P [***password***]**.

- [*command issued*] can either identify a dedicated ILOM IPMItool command or a Sunoem ILOM command.
- [*system output*] displays the command results.

For more details, see the "IPMItool Options and Command Summary " on page 142.

Note - If you encounter command-syntax problems with your particular operating system, you can use the IPMItool `-h` option to determine which parameters can be passed with the IPMItool command on your operating system. Also refer to the IPMItool man page by typing: **`man ipmitool`**.

Access the Oracle ILOM CLI From IPMItool

1. **To enable the Oracle ILOM CLI using IPMItool, type:**

   $ **ipmitool -I [***orcltls*|*lanplus***] -H** *SP_hostname_or_IPaddress* **-U** *username* **-P** *password* **sunoem cli**

   The Oracle ILOM CLI prompt appears as follows:

   ```
   Connected. Use ^D to exit.
   ->
   ```

2. **To use the Oracle ILOM CLI, type CLI commands.**

   For information on how to script Oracle ILOM CLI commands, see "Scripting Oracle ILOM CLI Commands With IPMItool" on page 129.

Disable Default TLS Behavior for SSL Certificate Check

- **To disable the validation of the SSL certificate when accessing the IPMI TLS interface (orcltls), issue the `--no-check-certificate` command. For example:**

```
$ ipmitool -I orcltls  -H SP_hostname_or_IPaddress -U username -P password --no-cert-check
```

Note - For security reasons, the SSL certificate is automatically verified upon accessing the IPMI TLS interface (`orcltls`). For additional information about the SSL certificate check, see "IPMI TLS Service and Interface" on page 120.

Scripting Oracle ILOM CLI Commands With IPMItool

A key benefit of using Oracle ILOM CLI from IPMItool is that the CLI commands can be scripted and then the script can be run on multiple SP instances. Scripting is possible because the CLI commands can be included on the IPMItool command line where each argument on the command line is treated as a separate Oracle ILOM CLI command. Command separation is archived by including quotation marks at the beginning and end of each Oracle ILOM CLI command.

The following example shows how to include two CLI commands on the IPMItool command line. In the example, notice that each command begins and ends with quotation marks.

```
# ipmitool -H SP_hostname_or_IPaddress -U username -P password sunoem cli
“show /SP/services” “show /SP/logs”
Connected. Use ^D to exit.
-> show /SP/services
 /SP/services
   Targets:
      http
      https
      ipmi
      kvms
      servicetag
      snmp
      ssh
      sso
```

```
    Properties:

    Commands:
      cd
      show

-> show /SP/logs
 /SP/logs
   Targets:
      audit
      event

   Properties:

   Commands:
      cd
      show
-> Session closed
 Disconnected
```

Performing System Management Tasks (IPMItool)

- "Display Sensor List" on page 130
- "View Single Sensor Details" on page 131
- "View and Interpret Presence Sensor Type Values" on page 132
- "Manage Host Power-On, Power-Off and Shutdown Functions" on page 134
- "Manage Oracle ILOM Power Budget Interfaces" on page 135
- "Manage the System Power Policy" on page 138
- "Display FRU Manufacturing Details" on page 139
- "Display Oracle ILOM Event or Audit Log" on page 141

▼ Display Sensor List

- **To view a list of sensors on a managed device, type:**

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U username -P password
```

sdr list

Note - The IPMI TLS interface (`orcltls`) is supported as of Oracle ILOM firmware version 3.2.8 and later. For a higher level of security, you should always specify the IPMI TLS interface (`-I orcltls`) when executing Oracle ILOM commands from the IMPItool utility. For more information about using the IPMI TLS interface from Oracle, see these topics:"IPMI TLS Service and Interface" on page 120 and "Configure IPMI Management Access for Increased Security" in *Oracle ILOM Security Guide Firmware Releases 3.0, 3.1, and 3.2*.

The output might look like the following:

```
/SYS/T_AMB       | 24 degrees C       | ok
/RFM0/FAN1_SPEED | 7110 RPM          | ok
/RFM0/FAN2_SPEED | 5880 RPM          | ok
/RFM1/FAN1_SPEED | 5880 RPM          | ok
/RFM1/FAN2_SPEED | 6360 RPM          | ok
/RFM2/FAN1_SPEED | 5610 RPM          | ok
/RFM2/FAN2_SPEED | 6510 RPM          | ok
/RFM3/FAN1_SPEED | 6000 RPM          | ok
/RFM3/FAN2_SPEED | 7110 RPM          | ok
/RFM4/FAN1_SPEED | 6360 RPM          | ok
/RFM4/FAN2_SPEED | 5610 RPM          | ok
/RFM5/FAN1_SPEED | 5640 RPM          | ok
/RFM5/FAN2_SPEED | 6510 RPM          | ok
/RFM6/FAN1_SPEED | 6180 RPM          | ok
/RFM6/FAN2_SPEED | 6000 RPM          | ok
/RFM7/FAN1_SPEED | 6330 RPM          | ok
/RFM7/FAN2_SPEED | 6330 RPM          | ok
/RFM8/FAN1_SPEED | 6510 RPM          | ok
/RFM8/FAN2_SPEED | 5610 RPM          | ok
```

Note - The sensor output shown in the preceding example was shortened. The actual output will depend on the hardware platform.

▼ View Single Sensor Details

- **To view details about a single sensor on a managed device, type:**

  `sensor get` */target/sensor_name*

  For example, to view sensor details about the system temperature (`/SYS/T_AMB`), you would type:

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U username -P password

sensor get /SYS/T_AMB
```

Note - The IPMI TLS interface (`orcltls`) is supported as of Oracle ILOM firmware version 3.2.8 and later. For a higher level of security, you should always specify the IPMI TLS interface (`-I orcltls`) when executing Oracle ILOM commands from the IMPItool utility. For more information about using the IPMI TLS interface from Oracle, see these topics:“IPMI TLS Service and Interface” on page 120 and “Configure IPMI Management Access for Increased Security” in *Oracle ILOM Security Guide Firmware Releases 3.0, 3.1, and 3.2*

The output might look like the following:

```
Locating sensor record...
Sensor ID              : /SYS/T_AMB (0x8)
 Entity ID             : 41.0
 Sensor Type (Analog)  : Temperature
 Sensor Reading        : 24 (+/- 0) degrees C
 Status                : ok
 Lower Non-Recoverable : 0.000
 Lower Critical        : 4.000
 Lower Non-Critical    : 10.000
 Upper Non-Critical    : 35.000
 Upper Critical        : 40.000
 Upper Non-Recoverable : 45.000
 Assertions Enabled    : lnc- lcr- lnr- unc+ ucr+ unr+
 Deassertions Enabled  : lnc- lcr- lnr- unc+ ucr+ unr+
```

View and Interpret Presence Sensor Type Values

Before You Begin

- The IPMItool supports the output of a `States Asserted` field for each presence sensor type record. This `States Asserted` field can appear in the IPMItool output as either:
  - `States Asserted = Entity Presence`

    When the `States Asserted = Entity Presence` field appears, the sensor output for a hardware component can show one of three valid values: `Present(=1)`, `Absent(=2)`, `Disabled(=4)`.
  - `States Asserted = Availability State`

When the `States Asserted = Availability State` field appears, the sensor output for a hardware component can show one of two valid values: `Device Absent(=1)` and `Device Present(=2)`.

Note - Oracle ILOM supports the output of both `States Asserted` fields. However, some Oracle hardware platforms might support both or one of the possible `States Asserted` fields (`Entity Presence` or `Availability State`).

For additional information about how to interpret values presented for IPMI presence sensor types, refer to Section 42 - Sensor and Event Code Tables in the IPMI 2.0 Specifications. Understanding all of Section 42 is critical in understanding how to interpret a sensor value.

To view and interpret IPMItool present sensor type values, follow these steps:

1. **To view the actual sensor reading for hardware components, use the IPMItool `sdr list` command.**

   For example, after issuing the `sdr list` command the following presence sensor type readings appear for PCIe hardware components.

```
PCIE_CC/PRSNT    | 0x02              | ok
PCIE0/F20/PRSNT  | 0x01              | ok
```

2. **To determine the `States Asserted` field value for a presence sensor type, use the IPMItool `sensor get` command.**

   One of the following `States Asserted` fields appear after issuing the `sensor get` command from the IPMItool:

   - `States Asserted = Entity Presence`

     In the following example, the value shown for the `States Asserted = Entity Presence` field is *Absent*.

```
$ ipmitool sensor get  PCIE_CC/PRSNT
Locating sensor record...
Sensor ID              : PCIE_CC/PRSNT (0xad)
Entity ID             : 49.0
Sensor Type (Discrete): Entity Presence
States Asserted       : Entity Presence
[Absent]
```

   - `States Asserted = Availability State`

In the following example, the value shown for the `States Asserted = Availability State` field is *Device Absent*.

```
$ ipmitool sensor get PCIE1/PRSNT
Locating sensor record...
Sensor ID              : PCIE1/PRSNT (0xe6)
Entity ID             : 11.0
Sensor Type (Discrete): Entity Presence
States Asserted       : Availability State
[Device Absent]
```

Manage Host Power-On, Power-Off and Shutdown Functions

Note - The IPMI TLS interface (`orcltls`) is supported as of Oracle ILOM firmware version 3.2.8 and later. For a higher level of security, you should always specify the IPMI TLS interface (`-I orcltls`) when executing Oracle ILOM commands from the IMPItool utility. For more information about using the IPMI TLS interface from Oracle, see these topics:“IPMI TLS Service and Interface” on page 120 and “Configure IPMI Management Access for Increased Security” in *Oracle ILOM Security Guide Firmware Releases 3.0, 3.1, and 3.2*

1. **To power on the host on a managed device, type: `chassis power on`**

   Example:

   ```
   $ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U username -P password

   chassis power on
   ```

2. **To power off the host on a managed device, type: `chassis power off`**

   Example:

   ```
   $  ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U username -P password

    chassis power off
   ```

3. **To power cycle the host on a managed device, type: `chassis power cycle`**

   Example:

   ```
   $ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U username-P password
   ```

```
chassis power cycle
```

4. **To gracefully shut down the host power on a managed device, type: `chassis power soft`**

   Example:

   $**ipmitool -I [***orcltls***|***lanplus***]-H** *SP_hostname_or_IPaddress* **-U** *username* **-P** *password*

   ```
   chassis power soft
   ```

Manage Oracle ILOM Power Budget Interfaces

Note - The IPMI TLS interface (`orcltls`) is supported as of Oracle ILOM firmware version 3.2.8 and later. For a higher level of security, you should always specify the IPMI TLS interface (`-I orcltls`) when executing Oracle ILOM commands from the IMPItool utility. For more information about using the IPMI TLS interface from Oracle, see these topics:"IPMI TLS Service and Interface" on page 120 and "Configure IPMI Management Access for Increased Security" in *Oracle ILOM Security Guide Firmware Releases 3.0, 3.1, and 3.2*

---

1. **To set the Power Limit Activation State on a managed device, use one of the following commands:**

   - To activate, type:

     $ **ipmitool -I [***orcltls***|***lanplus***] -H** *SP_hostname_or_IPaddress* **-U** *username* **-P** *password*

     ```
     raw 0x2e 0x49 0x00 0x01 0xFF 0xFF
     ```

     Upon command completion:

     ```
     dc
     ```

   - To deactivate, type:

     $ **ipmitool -I [***orcltls***|***lanplus***] -H** *SP_hostname_or_IPaddress* **-U** *username* **-P** *password*

     ```
     raw 0x2e 0x49 0x00 0x00 0xFF 0xFF
     ```

     Upon command completion:

     ```
     dc
     ```

The following table describes the Power Limit Activation State (IPMItool) input and output fields.

Fields	Byte	Description
Input Data	1	Sunoem command group number: `0x2e`.
	2	Command code `0x49` sets the power limit activation state.
	3	Group extension identification: `0x00`. The value for this field is ignored.
	4	Sub-commands for power limit activation: `0x00` - Deactivate power limit `0x01` - Activate power limit
	5-6	Reserved fields `0xFF`. The values for these fields are ignored.
Output Data	1	Completion code consumed by IPMItool. The system does not display a status for successful completion code. However, if the result of the completion code is anything other than '`successful`', a failure message appears.
	2	Group extension identification `dc`' appears upon command completion.

2. **To get Power Limit Budget properties, type:**

Note - You should use a Get Power Limit Budget Wattage command prior to setting the Power Limit Budget Wattage property.

$ **`ipmitool -I [`***orcltls***`|`***lanplus***`] -H`** *SP_hostname_or_IPaddress* **`-U`** *username* **`-P`** *password*

`raw 0x2e 0x4A 0x00 0x00 0x00`

Upon command completion:

```
dc 00 01 b3 00 02 fa 00 00 00 00 01 e9 00 00
```

The following table describes the Get Power Limit (IPMItool) input and output fields:

Field	Byte	Description
Input Data	1	Sunoem command group number: `0x2e`.
	2	Command code `0x4A` gets Power Budget settings.
	3	Group extension identification: `0x00`. The value for this field is ignored.

Field	Byte	Description
	4-5	Reserved fields `0x00`. Values for these fields are ignored.
Output Data	1	Completion code, consumed by IPMItool. Not displayed upon command completion. However if completion code is anything other than success, then a failure message is displayed upon command completion.
	2	Group extension identification. Displayed as '`dc` in the preceding example.
	3	Activation state: `00` - Deactivated `01` - Activated
	4	Reserved field. Note that the value `b3` in the preceding example can be ignored.
	5	Exception action, taken if power limit is exceeded and cannot be controlled within the correction time limit. Return values: `00` - None `01` - Hard power-off
	6-7	Power limit in watts. `02 fa` in the preceding example.
	8-11	Correction time limit in milliseconds. `00 00 00 00` in the preceding example.
	12	Flag indicating whether the correction time limit is the system default time limit. `00` - Not default `01` - Default
	13	Reserved field. Note that the value shown (`e9`) in the preceding example can be ignored.
	14-15	Reserved fields. Note that the value shown (`00 00`) in the preceding example can be ignored.

3. **To set the Power Limit, type:**

Note - The set power limit commands sets the power budget limit for the system. Use this command to set the maximum system power usage. The power limit should always be persistent across AC and DC cycles.

```
$ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U username -P password

raw 0x2e 0x4B 0x00 0xff 0xff 0xff 0x01 0x02 0xaa 0x00 0x00 0x1b 0x58 0x00 0xff 0x00 0x00
```

Upon command completion:

```
dc 00
```

The following table describes Set Power Limit (IPMItool) input and output fields:

Fields	Byte	Description
Input Data	1	Sunoem command group number: `0x2e`.
	2	Command code `0x4B` sets power budget settings.
	3	Group extension identification: `0x00`. The value for this field is ignored.
	4-6	Reserved fields: `0xff 0xff 0xff`. The values for this field are ignored.
	7	Exception action taken: `00` - none `01` - hard power-off
	8-9	Power limit in watts. For example: `0x2a 0xaa`
	10-13	Correction time limit in milliseconds. For example: `0x00 0x00 0x1b 0x58`. This value is ignored if the time limit is set to default; see next byte.
	14	A flag indicating whether to use the system default time limit. Correction time limit in bytes 10-13 will be ignored. `0x00` - not default `0x01` - default
	15	Reserved field `0xff`. The value for this field is ignored.
	16-17	Reserved field `0x00 0x00`. The values for these fields are ignored.
Output Data	1	Completion code that is consumed by IPMItool. The system does not display a status for successful completion code. However, if the result of the completion code is anything other than successful, a failure message appears.
	2	Group extension identification '`dc`' appears upon command completion.

▼ Manage the System Power Policy

Note - The settings defined in this procedure are not applicable to all server platforms.

Note - The IPMI TLS interface (`orcltls`) is supported as of Oracle ILOM firmware version 3.2.8 and later. For a higher level of security, you should always specify the IPMI TLS interface (`-I orcltls`) when executing Oracle ILOM commands from the IMPItool utility. For more information about the IPMI TLS interface that is provided by Oracle, see “IPMI TLS Service and Interface” on page 120.

1. **To get the current system power policy, type:**

   $**ipmitool -I [***orcltls***|***lanplus***] -H** *SP_hostname_or_IPaddress* **-U** *username* **-P** *password*

```
raw 0x2e 0x43 4
```

2. **To set the power manage policy to performance, type**

   ```
   $ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U username -P password

   raw 0x2e 0x42 2 00 00 00 00
   ```

3. **To set the power manage policy to elastic, type:**

   ```
   $ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U username -P password

   raw 0x2e 0x42 2 00 00 00 01
   ```

4. **To set the power manage policy to disabled, type:**

   ```
   $ ipmitool -I [orcltls|lanplus] -H SP_hostname_or_IPaddress -U username -P password

   raw 0x2e 0x42 2 00 00 00 02
   ```

   The following table describes the Power Management Policy State (IPMItool) input fields:

Fields	Byte	Description
Input Data	1	Sunoem command group number: `0x2e`.
	2	Command code `0x42` sets the Power Policy Activation State.
	3	Group extension identification: `2`.
	4-6	Reserved fields.
	7	Sub-commands for power policy activation: `00` - Performance policy `01` - Elastic policy `02` - Disable the policy

▼ Display FRU Manufacturing Details

Note - The IPMI TLS interface (`orcltls`) is supported as of Oracle ILOM firmware version 3.2.8 and later. For a higher level of security, you should always specify the IPMI TLS interface (`-I orcltls`) when executing Oracle ILOM commands from the IMPItool utility. For more information about the IPMI TLS interface that is provided by Oracle, see “IPMI TLS Service and Interface” on page 120.

- **To display Field Replacement Unit (FRU) manufacturing details on a managed device, use the `fru print` command.**

Example:

$ **ipmitool -I [***orcltls***|***lanplus***] -H** *SP_hostname_or_IPaddress* **-U** *username* **-P** *password*

fru print

The output might look like like the following:

```
FRU Device Description : Builtin FRU Device (ID 0)
 Board Product         : ASSY,ANDY,4SKT_PCI-E,BLADE
 Board Serial          : 0000000-7001
 Board Part Number     : 501-7738-01
 Board Extra           : AXX_RevE_Blade
 Product Manufacturer  : ORACLE
 Product Name          : ILOM

FRU Device Description : /SYS (ID 4)
 Chassis Type          : Rack Mount Chassis
 Chassis Part Number   : 541-0251-05
 Chassis Serial        : 00:03:BA:CD:59:6F
 Board Product         : ASSY,ANDY,4SKT_PCI-E,BLADE
 Board Serial          : 0000000-7001
 Board Part Number     : 501-7738-01
 Board Extra           : AXX_RevE_Blade
 Product Manufacturer  : ORACLE
 Product Name          : SUN BLADE X8400 SERVER MODULE
 Product Part Number   : 602-0000-00
 Product Serial        : 0000000000
 Product Extra         : 080020ffffffffffffff0003baf15c5a

FRU Device Description : /P0 (ID 5)
 Product Manufacturer  : ADVANCED MICRO DEVICES
 Product Part Number   : 0F21
 Product Version       : 2

FRU Device Description : /P0/D0 (ID 6)
 Product Manufacturer  : MICRON TECHNOLOGY
 Product Name          : 1024MB DDR 400 (PC3200) ECC
 Product Part Number   : 18VDDF12872Y-40BD3
 Product Version       : 0300
 Product Serial        : D50209DA
 Product Extra         : 0190
 Product Extra         : 0400

FRU Device Description : /P0/D1 (ID 7)
 Product Manufacturer  : MICRON TECHNOLOGY
 Product Name          : 1024MB DDR 400 (PC3200) ECC
Product Part Number    : 18VDDF12872Y-40BD3
Product Version        : 0300
Product Serial         : D50209DE
Product Extra          : 0190
Product Extra          : 0400
```

Display Oracle ILOM Event or Audit Log

Note - The IPMI TLS interface (`orcltls`) interface is supported as of Oracle ILOM firmware version 3.2.8 and later. For a higher level of security, you should always specify the IPMI TLS interface (`-I orcltls`) when executing Oracle ILOM commands from the IMPItool utility. For more information about using the IPMI TLS interface from Oracle, see these topics:“IPMI TLS Service and Interface” on page 120 and “Configure IPMI Management Access for Increased Security” in *Oracle ILOM Security Guide Firmware Releases 3.0, 3.1, and 3.2*.

1. **To display the Oracle ILOM Audit log, type: `sunoem cli "show /SP/logs/audit/list"`**

   Example:

   $ **`ipmitool -I [`***orcltls***`|`***lanplus***`] -H`** *SP_hostname_or_IPaddress* **`-U`** *username***`-P`** *password*

   `sunoem cli "show /SP/logs/audit/list"`

   The Audit Log output might look like the following:

```
Audit
ID     Date/Time                 Class     Type      Severity
-----  ------------------------  --------  --------  --------
12050  Sat Dec 31 20:33:17 2016  Audit     UI        minor
       root : Open Session : object = "/SP/sessions/38701/type" : value =
       "shell" : success
12049  Sat Dec 31 20:31:19 2016  Audit     UI        minor
       root : Close Session : object = "/SP/sessions/38699/type" : value =
       "shell" : success
12048  Sat Dec 31 20:30:57 2016  Audit     UI        minor
       root : Open Session : object = "/SP/sessions/38699/type" : value =
       "shell" : success
12047  Sat Dec 31 20:29:16 2016  Audit     IPMI      minor
       root : Close Session : session ID = 3279888664 : success
12046  Sat Dec 31 20:29:16 2016  Audit     IPMI      minor
       root : Set Session Privilege Level: privilege level = admin : success
12045  Sat Dec 31 20:29:16 2016  Audit     IPMI      minor
       IPMI 2.0 Login Success : User = root, Client IP = #.#.#.#
12044  Sat Dec 31 19:02:28 2016  Audit     IPMI      minor
```

```
       root : Close Session : session ID = 3075033282 : success
12043  Sat Dec 31 19:02:28 2016  Audit     IPMI      minor
       root : Set Session Privilege Level: privilege level = admin : success
Paused: press any key to continue, or 'q' to quitSession closed
```

2. **To display the Oracle ILOM Event log, type: `sel list`**

   Example:

   $ **ipmitool -I [***orcltls***|***lanplus***] -H** *SP_hostname_or_IPaddress* **-U** *username* **-P** *password*

   `sel list`

   The Event Log output might look like the following:

```
 100 | Pre-Init Time-stamp   | Power Unit #0x78 | State Deasserted
 200 | Pre-Init Time-stamp   | Power Supply #0xa2 | Predictive Failure Asserted
 300 | Pre-Init Time-stamp   | Power Supply #0xba | Predictive Failure Asserted
 400 | Pre-Init Time-stamp   | Power Supply #0xc0 | Predictive Failure Asserted
 500 | Pre-Init Time-stamp   | Power Supply #0xb4 | Predictive Failure Asserted
 600 | 04/05/2007 | 12:03:24 | Power Supply #0xa3 | Predictive Failure Deasserted
 700 | 04/05/2007 | 12:03:25 | Power Supply #0xaa | Predictive Failure Deasserted
 800 | 04/05/2007 | 12:03:25 | Power Supply #0xbc | Predictive Failure Deasserted
 900 | 04/05/2007 | 12:03:26 | Power Supply #0xa2 | Predictive Failure Asserted
 a00 | 04/05/2007 | 12:03:26 | Power Supply #0xa8 | Predictive Failure Deasserted
 b00 | 04/05/2007 | 12:03:26 | Power Supply #0xb6 | Predictive Failure Deasserted
 c00 | 04/05/2007 | 12:03:26 | Power Supply #0xbb | Predictive Failure Deasserted
 d00 | 04/05/2007 | 12:03:26 | Power Supply #0xc2 | Predictive Failure Deasserted
 e00 | 04/05/2007 | 12:03:27 | Power Supply #0xb0 | Predictive Failure Deasserted
 f00 | 04/05/2007 | 12:03:27 | Power Supply #0xb5 | Predictive Failure Deasserted
1000 | 04/05/2007 | 12:03:27 | Power Supply #0xba | Predictive Failure Asserted
1100 | 04/05/2007 | 12:03:27 | Power Supply #0xc0 | Predictive Failure Asserted
1200 | 04/05/2007 | 12:03:28 | Power Supply #0xa9 | Predictive Failure Deasserted
1300 | 04/05/2007 | 12:03:28 | Power Supply #0xae | Predictive Failure Deasserted
1400 | 04/05/2007 | 12:03:28 | Power Supply #0xb4 | Predictive Failure Asserted
1500 | 04/05/2007 | 12:03:28 | Power Supply #0xbe | Predictive Failure Deasserted
```

IPMItool Options and Command Summary

The following tables summarize the supported IPMItool options and commands:

- Table 7, “Supported IPMItool Options,” on page 143
- Table 8, “Supported IPMItool Commands ,” on page 145

Note - The IPMI TLS interface (`orcltls`) is supported as of Oracle ILOM firmware version 3.2.8 and later. For a higher level of security, you should always specify the IPMI TLS interface (`-I orcltls`) when executing Oracle ILOM commands from the IMPItool utility. For more information about using the IPMI TLS interface from Oracle, see these topics:"IPMI TLS Service and Interface" on page 120 and "Configure IPMI Management Access for Increased Security" in *Oracle ILOM Security Guide Firmware Releases 3.0, 3.1, and 3.2*.

TABLE 7 Supported IPMItool Options

IPMI Option	Function
`-a`	Prompt for the remote server password.
`-A` [*authtype*]	Specify an authentication type to use during IPMI v1.5 `lan` session activation. Supported authentication types are NONE, PASSWORD, MD2, MD5, or OEM.
`-c`	Present output in CSV (comma separated variable) format. This is not available with all commands.
`-e` [*sol_escape_char*]	Use supplied character for SOL session escape character. The default is to use but this can conflict with SSH sessions.
`-K`	Read Kg key from IPMI_KGKEY environment variable.
`-k` [*key*]	Use supplied Kg key for IPMI v2 authentication. The default is not to use any Kg key.
`-y` [*hex key*]	Use supplied Kg key for IPMI v2 authentication. The key is expected in hexadecimal format and can be used to specify keys with non-printable characters. For example: '-k PASSWORD' and 'y 50415353574F5244' are equivalent. The default is not to use any Kg key.
`-Y`	Prompt for the Kg key for IPMI v2 authentication.
`-C` [*ciphersuite*]	The remote server authentication, integrity, and encryption algorithms to use for IPMI v2 `lanplus` connections. See table 22-19 in the IPMIv2 specification. The default is 3 which specifies RAKP-HMAC-SHA1 authentication, HMAC-SHA1-96 integrity, and AES-CBC-128 encryption algorithms.
`-E`	The remote server password is specified by the environment variable IPMI_PASSWORD.
`-f` [*password_file*]	Specifies a file containing the remote server password. If this option is absent, or if password_file is empty, the password will default to NULL.
`-h`	Get basic usage help from the command line.
`-H` [*address*]	Remote server address, can be IP address or hostname. This option is required for `lan` and `lanplus` interfaces.
`-i` [*interface*]	Selects the IPMI interface to use. Supported interfaces that are compiled in are visible in the usage help output. No auto-detect is attempted. See the `-I` description for more information.
`-I [interface]`	Attempt the most secure interface first (`orcltls`). If the BMC does not support the interface, attempt the next most secured interface

IPMI Option	Function
	until the specified interface. Supported interfaces that are compiled in are visible in the usage help output. If `lanplus` interface or `lan` interface is specified, certificate checking is disabled when attempting the `orcltls` interface. **Note -** If the `-I` option is not specified, auto-detect is enabled and certificate checking is enabled when attempting the `orcltls` interface.
`-m [`*local_address*`]`	Set the local IPMB address. The default is 0x20 and there should be no need to change it for normal operation.
`-N [`*sec*`]`	Specify number of seconds between retransmissions of `lan` or `lanplus` messages. Default are 2 seconds for `lan` and 1 second for `lanplus` interfaces.
`-o [`*oemtype*`]`	Select OEM type to support. This usually involves minor hacks in place in the code to work around quirks in various BMCs from various manufacturers. Use -o list to see a list of current supported OEM types.
`-O [`*sel oem*`]`	Open selected file and read OEM SEL event descriptions to be used during SEL listings.
`-p [`*port*`]`	The remote server TLS TCP connection port is 443 (default). For IPMI v2.0 and 1.5, the remote server UDP TCP connection is port 623 (default).
`-P [`*password*`]`	Remote server password is specified on the command-line. If supported it will be obscured in the process list. **Note -** Specifying the password as a command-line option is not recommended.
`-R [`*count*`]`	Set the number of retries for `lan` interface or `lanplus` interface (default=4).
`-S [`*sdr_cache_file*`]`	Use local file for remote SDR cache. Using a local SDR cache can drastically increase performance for commands that require knowledge of the entire SDR to perform their function. Local SDR cache from a remote system can be created with the `sdr dump` command.
`-t [`*target_address*`]`	Selects IPMI interface to use. Supported interfaces that are compiled in are visible in the usage help output.
`-U [`*username*`]`	Remote server username, default is NULL user.
`-d N`	Use device number N to specify the `/dev/ipmiN` (or `/dev/ipmi/N` or `/dev/ipmidev/N`) device to use for in-band BMC communication. Used to target a specific BMC on a multi-node, multi-BMC system through the IPMI device driver interface. Default is 0.
`-v`	Increase verbose output level. This option may be specified multiple times to increase the level of debug output. If given three times you will get hexdumps of all incoming and outgoing packets.
`-V`	Display version information.
`--no-cert-check`	Disables the check for validating the SSL certificate when the *orcltls* IPMI interface is specified.

IPMI Option	Function
`--cert-dir [`*path*`]`	Location of trusted SSL certificates on host server SP.

TABLE 8 Supported IPMItool Commands

IPMI Command	Function
`sunoem sshkey set`	Configure an SSH key for a remote shell user.
`ipmitool sunoem sshkey del`	Remove an SSH key from a remote shell user.
`ipmitool sunoem led get`	Read LED status.
`ipmitool sunoem led set`	Set LED status.
`ipmitool sunoem cli`	Enter Oracle ILOM CLI commands as if you were using the ILOM CLI directly. The `lan` interface or `lanplus` interface should be used.
`ipmitool sunoem CLI force`	Available as of Oracle ILOM 3.0.10, a `force` option can be invoked as an argument to the `sunoem` CLI command.
`ipmitool raw`	Execute raw IPMI commands.
`ipmitool lan print`	Print the current configuration for the given channel.
`ipmitool lan set (1) (2)`	Set the given parameter on the given channel.
`ipmitool chassis status`	Display information regarding the high-level status of the system chassis and main power subsystem.
`ipmitool chassis power`	Perform a chassis control command to view and change the power state.
`ipmitool chassis identify`	Control the front panel identify light. Default is 15. Use 0 to turn off.
`ipmitool chassis restart_cause`	Query the chassis for the cause of the last system restart.
`ipmitool chassis bootdev (1)`	Request the system to boot from an alternative boot device on next reboot.
`ipmitool chassis bootparam (1)`	Set the host boot parameters.
`ipmitool chassis selftest`	Display the BMC self-test results.
`ipmitool power`	Return the BMC self-test results.
`ipmitool event`	Send a predefined event to the system event log.
`ipmitool sdr`	Query the BMC for sensor data records (SDR) and extract sensor information of a given type, then query each sensor and print its name, reading, and status.
`ipmitool sensor`	List sensors and thresholds in a wide table format.
`ipmitool fru print`	Read all field-replaceable unit (FRU) inventory data and extract such information as serial number, part number, asset tags, and short strings describing the chassis, board, or product.
`ipmitool sel`	View the Oracle ILOM SP system event log (SEL).
`ipmitool pef info`	Query the BMC and print information about the PEF- supported features.
`ipmitool pef status`	Print the current PEF status (the last SEL entry processed by the BMC, and so on).

IPMI Command	Function
`ipmitool pef list`	Print the current PEF list (the last SEL entry processed by the BMC, and so on).
`ipmitool user`	Display a summary of user ID information, including maximum number of user IDs, the number of enabled users, and the number of fixed names defined.
`ipmitool session`	Get information about the specified sessions. You can identify sessions by their ID, by their handle number, by their active status, or by using the keyword “all” to specify all sessions.
`ipmitool firewall (1)`	Enable or disable individual command and command sub-functions; determine which commands and command sub-functions can be configured on a given implementation.
`ipmitool set (1)`	Set the runtime options including session host name, user name, password, and privilege level.
`ipmitool exec`	Execute IPMItool commands from file name. Each line is a complete command.

SNMP Command Examples

Description	Links
Example SNMP Commands	■ "snmpget Command" on page 147 ■ "snmpwalk Command" on page 148 ■ "snmpbulkwalk Command" on page 149 ■ "snmptable Command" on page 150 ■ "snmpset Command" on page 153 ■ "snmptrapd Command" on page 153

Related Information

- "SNMP Overview" on page 11
- "Configuring SNMP Settings in Oracle ILOM" on page 19

snmpget Command

snmpget *SNMP_agent* **sysName.0**

As stated in the description of the sysName.0 MIB object in the SNMPv2-MIB, this command returns an administratively assigned name for this managed node. By convention, this is the node's fully qualified domain name. If the name is unknown, the value returned is the zero-length string.

For example:

```
% snmpget SNMP_agent sysName.0 sysObjectID.0
ilomCtrlDateAndTime.0
SNMPv2-MIB::sysName.0 = STRING: SUNSPHOSTNAME
SNMPv2-MIB::sysObjectID.0 = OID: SUN-HW-TRAP-MIB::products.200.2.1.1
SUN-ILOM-CONTROL-MIB::ilomCtrlDateAndTime.0 = STRING: 2013-07-23,13:31:53.0
```

In addition to the sysName.0 object, this command displays the content of the sysObjectID.0 and the ilomCtrlDateAndTime.0 MIB objects. Notice that the MIB file name is given for each MIB object as part of the reply.

The following descriptions of the MIB objects are taken from the MIB files.

- sysName – An administratively assigned name for this managed node. By convention, this is the node's fully qualified domain name. If the name is unknown, the value is the zero-length string.
- sysObjectID – The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining ”what kind of box” is being managed.
- ilomCtrlDataAndTime – The date and time of the device.

snmpwalk Command

The snmpwalk command performs a sequence of chained GETNEXT requests automatically. It is a work-saving command. Rather than having to issue a series of snmpgetnext requests, one for each object ID, or node, in a subtree, you can issue one snmpwalk request on the root node of the subtree and the command gets the value of every node in the subtree.

For example:

```
% snmpwalk SNMP_agent system
SNMPv2-MIB::sysDescr.0 = STRING: ILOM machine custom description
SNMPv2-MIB::sysObjectID.0 = OID: SUN-HW-TRAP-MIB::products.200.2.1.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (16439826) 1 day, 21:39:58.26
SNMPv2-MIB::sysContact.0 = STRING: set via snmp test
SNMPv2-MIB::sysName.0 = STRING: SUNSPHOSTNAME
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 72
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (14) 0:00:00.14
SNMPv2-MIB::sysORID.1 = OID: IF-MIB::ifMIB
SNMPv2-MIB::sysORID.2 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.3 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.4 = OID: RFC1213-MIB::ip
SNMPv2-MIB::sysORID.5 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.6 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.7 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.8 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.9 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
```

```
SNMPv2-MIB::sysORDescr.1 = STRING: The MIB module to describe generic objects
for network interface sub-layers
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.3 = STRING: The MIB module for managing TCP
implementations
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for managing IP and ICMP
implementations
SNMPv2-MIB::sysORDescr.5 = STRING: The MIB module for managing UDP
implementations
SNMPv2-MIB::sysORDescr.6 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORDescr.7 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.8 = STRING: The MIB for Message Processing and
Dispatching.
SNMPv2-MIB::sysORDescr.9 = STRING: The management information definitions for
the SNMP User-based Security Model.
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.4 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.5 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.6 = Timeticks: (2) 0:00:00.02
SNMPv2-MIB::sysORUpTime.7 = Timeticks: (14) 0:00:00.14
SNMPv2-MIB::sysORUpTime.8 = Timeticks: (14) 0:00:00.14
SNMPv2-MIB::sysORUpTime.9 = Timeticks: (14) 0:00:00.14
```

snmpbulkwalk Command

The snmpbulkwalk command uses the GETBULK SNMP protocol feature to query for an entire tree of information about a network entity. This command can pack more objects into the packets by specifying “repeaters.” As a result, the snmpbulkwalk command is faster than the snmpwalk command.

Here is an example of the snmpwalk command with approximate start and end time stamps.

```
% date ; snmpwalk SNMP_agent entPhysicalTable >
/dev/null ; date
Sun Jun 30 18:15:38 EDT 2013
Sun Jun 30 18:16:46 EDT 2013
```

Here is an example of the snmpbulkwalk command performing the same operation. Notice that the snmpbulkwalk command is faster than the snmpwalk command.

```
% date ; snmpbulkwalk SNMP_agent entPhysicalTable >
/dev/null ; date
Sun Jun 30 18:19:19 EDT 2013
Sun Jun 30 18:19:38 EDT 2013
```

snmptable Command

The snmptable command retrieves the contents of an SNMP table and displays the contents in a tabular format, that is, one table row at a time, such that the resulting output resembles the table being retrieved. This is contrasted with the snmpwalk command, which displays the contents of the table one column at a time.

Here is an example of the snmptable command:

```
% snmptable  SNMP_agent sysORTable
SNMP table: SNMPv2-MIB::sysORTable
sysORID                  sysORDescr                  sysORUpTime
IF-MIB::ifMIB            The MIB module to           0:0:00:00.01
describe generic objects
SNMPv2-MIB::snmpMIB      The MIB module for SNMPv2   0:0:00:00.02
for network interface
entities.
TCP-MIB::tcpMIB          The MIB module for          0:0:00:00.02
sub-layers.
managing TCP
UDP implementations.
UDP-MIB::udpMIB          The MIB module for managing 0:0:00:00.02
RFC1213-MIB::ip          The MIB module for managing 0:0:00:00.02
implementations.
SNMP-VIEW-BASED-ACM-     View-based Access Control   0:0:00:00.02
SNMP-FRAMEWORK-MIB::     The SNMP Management         0:0:00:00.14
IP and ICMP implementations.
MIB::vacmBasicGroup      Model for SNMP.
snmpFrameworkMIB         Architecture MIB.
Compliance
SNMP-MPD-MIB::snmp       The MIB for Message         0:0:00:00.14
MPDCompliance            Processing and Dispatching.
SNMP-USER-BASED-SM-      The management information  0:0:00:00.14
MIB::usmMIBCompliance    definitions for the SNMP
User-based Security Model.
```

Note - While the snmpget, snmpgetnext, and snmpwalk command can be used on any type of MIB object, the snmptable command can be used only on MIB table objects. If this command is given any other type of object ID, it will be rejected. This restriction applies to a table entry object, a table column object, and any object that represents information within a table. Only a MIB table object ID can be used with the snmptable command.

In the examples of the snmptable command, the -Ci and -Cb options are used. For example, here is an snmptable command with the -Ci option:

```
% snmptable -Ci  SNMP_agent  sunPlatFanTable
SNMP table: SUN-PLATFORM-MIB::sunPlatFanTable
index sunPlatFanClass
10                        fan
11                        fan
17                        fan
23                        fan
29                        fan
30                        fan
36                        fan
42                        fan
```

Here is an example of an snmptable command without the -Ci option. Notice that the index column is not displayed:

```
% snmptable  SNMP_agent sunPlatFanTable
SNMP table: SUN-PLATFORM-MIB::sunPlatFanTable
sunPlatFanClass
fan
fan
fan
fan
fan
```

Here is an example of an snmptable command with the -Ci and -Cb options. The output is abbreviated.

```
% snmptable -Ci -Cb  SNMP_agent entPhysicalTable
index                   Descr              VendorType   ContainedIn
SNMP table: ENTITY      ?SNMPv2-           0            chassis
-MIB::entPhysical       SMI:zeroDotZero
1
Table
```

Here is an example of the same `snmptable` command with the `-Ci` option but without the `-Cb` option. Again the output is abbreviated. Notice that the name of the MIB object is repeated on each heading.

```
% snmptable -Ci  SNMP_agent entPhysicalTable
index                   entPhysicalDescr   entPhysical   entPhysical
 VendorType    ContainedIn
SNMP table: ENTITY      ?SNMPv2-           0             chassis
1
-MIB::entPhysical       SMI:zeroDotZero
```

Here is another example of an `snmptable` command with both the `-Ci` and `-Cb` options. Notice that the MIB object is not repeated on each heading.

```
% snmptable -Cb -Ci  SNMP_agent ilomCtrlAlertsTable
SNMP table: SUN-ILOM-CONTROL-MIB::ilomCtrlAlertsTable
in-    Sever-   Type   Destin-   Destin-   SNMPVer-   SNMP-Comm-   Email    Email
dex    ity             ation-    ation-    sion       unityOr-     Event    Event
1      criti-   email  ?         0.0.0.0   v1         public       none     none
 IP        Email                Username     Class    Type
cal
2-15   dis-     ipmi-  0.0.0.0   ?         v1         public       ?        ?
Filter   Filter
able     pet
```

Thus, when you used the `-Cb` option with the `snmptable` command, the table output is easier to read.

Here is an example of an `snmptable` command using version 3 of the SNMP protocol:

```
% snmptable -Cb -Ci -mALL -v3 -aMD5 -utestuser -Apassword -lauthNoPriv
SNMP_agent:port sunPlatPowerSupplyTable
SNMP table: SUN-PLATFORM-MIB::sunPlatPowerSupplyTable
index sunPlatPowerSupplyClass
90             powerSupply
92             powerSupply
96             powerSupply
```

The following `snmptable` command returns an empty table.

```
% snmptable -Cb -Ci  SNMP_agent sunPlatBatteryTable
SUN-PLATFORM-MIB::sunPlatBatteryTable: No entries
```

snmpset Command

While the syntax of the snmpset command is similar to that of the snmpget command, the commands are quite different. The snmpget command merely reads the value of the specified object ID, while the snmpset command writes the value specified to the object ID. Further, along with the value to be written to the object ID, you must also specify the data type of the object ID in the snmpset command because SNMP objects support more than one data type.

The following example shows the use of the snmpget and snmpset commands together. The sequence of steps is as follows:

1. Use the snmpget command to check the current value of the MIB object.
2. Use the snmpset command to change the value of the MIB object.
3. Use the snmpget command to verify that the MIB object was in fact changed to the requested value.

```
% snmpget  SNMP_agent ilomCtrlHttpEnabled.0
SUN-ILOM-CONTROL-MIB::ilomCtrlHttpEnabled.0 = INTEGER: false(2)
% snmpset  SNMP_agent ilomCtrlHttpEnabled.0 i 1
SUN-ILOM-CONTROL-MIB::ilomCtrlHttpEnabled.0 = INTEGER: true(1)
% snmpget  SNMP_agent ilomCtrlHttpEnabled.0
SUN-ILOM-CONTROL-MIB::ilomCtrlHttpEnabled.0 = INTEGER: true(1)
```

Note that if you try to execute this snmpset command using a public community, instead of private, it will not work. This is because the private community has write permission, but the public community does not. The reason code returned by the command does not make this clear because it simply states that the object is not writable.

Here is an example:

```
% snmpset SNMP_agent ilomCtrlHttpEnabled.0 i 1
Error in packet.
Reason: notWritable (That object does not support modification)
```

snmptrapd Command

snmptrapd is an SNMP application that receives and logs SNMP trap and inform messages. Before your system can receive such messages, you must configure the trap daemon to listen for these messages.

To configure a trap daemon:

1. Configure an SNMP trap destination.

   The following example shows how to use the `snmpset` command to configure an `snmptrapd` daemon:

```
% snmpset  SNMP_agent ilomCtrlAlertType.1 i 2 ilomCtrlAlertSeverity.1 i 2
ilomCtrlAlertDestinationIP.1 a dest_ipaddress ilomCtrlAlertDestinationPort.1 i
port_number ilomCtrlAlertSNMPCommunityOrUsername.1 s private
ilomCtrlAlertSNMPVersion.1 i 2
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertType.1 = INTEGER: snmptrap(2)
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSeverity.1 = INTEGER: critical(2)
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationIP.1 = IpAddress: dest_ipaddress
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertDestinationPort.1 = INTEGER: port_number
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSNMPCommunityOrUsername.1 = STRING: private
SUN-ILOM-CONTROL-MIB::ilomCtrlAlertSNMPVersion.1 = INTEGER: v2c(2)
```

2. Start the trap receiver application, `snmptrapd`.
3. Generate a test trap to verify that traps are being sent by the agent (on the managed node) and received by the trap receiver (the management station).

   While the daemon is running, log in to the Oracle ILOM CLI on the host that is running the SNMP agent, and type the following command:

   ```
   -> set /SP/alertmgmt/rules/n testrule=true
   ```

   Note - It is important to test the trap daemon to make sure it is configured properly.

   The following screen shows a sample output when a `testalert` trap is received at the management station:

```
SUN-ILOM-CONTROL-MIB::ilom.103.2.1.20.0 = STRING: "This is a test trap"
```

Index