

Oracle Integrated Lights Out Manager (ILOM) 3.1

構成および保守ガイド



Part No: E35732-01
2012年5月

このソフトウェアおよび関連ドキュメントの使用と開示は、ライセンス契約の制約条件に従うものとし、知的財産に関する法律により保護されています。ライセンス契約で明示的に許諾されている場合もしくは法律によって認められている場合を除き、形式、手段に関係なく、いかなる部分も使用、複写、複製、翻訳、放送、修正、ライセンス供与、送信、配布、発表、実行、公開または表示することはできません。このソフトウェアのリバース・エンジニアリング、逆アセンブル、逆コンパイルは互換性のために法律によって規定されている場合を除き、禁止されています。

ここに記載された情報は予告なしに変更される場合があります。また、誤りが無いことの保証はいたしかねます。誤りを見つけた場合は、オラクル社までご連絡ください。

このソフトウェアまたは関連ドキュメントを、米国政府機関もしくは米国政府機関に代わってこのソフトウェアまたは関連ドキュメントをライセンスされた者に提供する場合は、次の通知が適用されます。

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

このソフトウェアもしくはハードウェアは様々な情報管理アプリケーションでの一般的な使用のために開発されたものです。このソフトウェアもしくはハードウェアは、危険が伴うアプリケーション(人的傷害を発生させる可能性があるアプリケーションを含む)への用途を目的として開発されていません。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用する際、安全に使用するために、適切な安全装置、バックアップ、冗長性(redundancy)、その他の対策を講じることは使用者の責任となります。このソフトウェアもしくはハードウェアを危険が伴うアプリケーションで使用したことに起因して損害が発生しても、オラクル社およびその関連会社は一切の責任を負いかねます。

OracleおよびJavaはOracle Corporationおよびその関連企業の登録商標です。その他の名称は、それぞれの所有者の商標または登録商標です。

Intel, Intel Xeon は、Intel Corporation の商標または登録商標です。すべての SPARC の商標はライセンスをもとに使用し、SPARC International, Inc. の商標または登録商標です。AMD, Opteron, AMD ロゴ、AMD Opteron ロゴは、Advanced Micro Devices, Inc. の商標または登録商標です。UNIX は、The Open Group の登録商標です。

このソフトウェアまたはハードウェア、そしてドキュメントは、第三者のコンテンツ、製品、サービスへのアクセス、あるいはそれらに関する情報を提供することがあります。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスに関して一切の責任を負わず、いかなる保証もいたしません。オラクル社およびその関連会社は、第三者のコンテンツ、製品、サービスへのアクセスまたは使用によって損失、費用、あるいは損害が発生しても一切の責任を負いかねます。

目次

このドキュメントの使用法	7
関連ドキュメント	7
ドキュメントのフィードバック	8
製品のダウンロード	8
Oracle ILOM 3.1 ファームウェアのバージョン番号方式	9
サポートとアクセシビリティ	10
Oracle ILOM への管理接続の設定とログイン	11
関連情報	11
Oracle ILOM への管理接続の確立	11
Oracle ILOM サーバー SP または CMM へのログイン	29
セキュリティを最大化するように Oracle ILOM を構成する	36
ユーザーアカウントの設定および管理	37
関連情報	37
ユーザー資格の管理	38
ローカルユーザーアカウントの構成	46
Active Directory の構成	49
LDAP/SSL の構成	61
LDAP の構成	73
RADIUS の構成	77
ネットワークの配備および管理のデフォルト設定の変更	81
関連情報	81
ネットワーク配備の原則と考慮事項	81
デフォルトの管理アクセス構成プロパティの変更	91
デフォルトの接続構成プロパティの変更	106
動的 DNS の設定例	118
システム識別情報の割り当て	121
SP または CMM クロックのプロパティの設定	122
ネットワーク接続の問題の推奨される解決策	124

リモート KVMs コンソールを使用したホストサーバーのリダイレクション	129
関連情報	129
Oracle ILOM リモートコンソールの最初の設定	129
Oracle ILOM リモートコンソールの起動と使用	137
Oracle ILOM Storage Redirection CLI の最初の設定	142
Oracle ILOM Storage Redirection CLI の起動と使用	149
ホストシリアルリダイレクションセッションの開始と停止	157
ホストサーバー管理操作の構成	159
関連情報	160
サーバーまたはブレードシステムシャーシに対するホスト電源の制御	160
実行するホスト診断テストの設定	161
x86 ホストサーバーの次回のブートデバイスの設定	165
SPARC ホストサーバーのブート動作の設定	166
SPARC ホストブートモードのオーバーライド	170
SPARC ホストドメインの管理	172
SPARC ホストキースイッチ状態の設定	174
SPARC ホスト TPM 状態の設定	175
警告通知とイベントログ用の Syslog サーバーの設定	177
関連情報	177
警告通知の構成	177
イベントログ用の Syslog の構成	183
システム管理ポリシー構成の設定	185
関連情報	185
サーバー SP から構成できるシステム管理ポリシー	185
CMM から構成できるシステム管理ポリシー	187
電源警告通知の設定とシステムの電力使用の管理	191
関連情報	191
消費電力警告通知の設定	191
SP 電力制限および CMM 電力許可プロパティの設定	192
電力制限を実施するための SP 詳細電力上限ポリシーの設定	195
CMM 電源装置冗長性ポリシーの設定	197
Oracle ILOM の保守および構成管理タスクの実行	201
関連情報	201
ファームウェア更新の実行	201
サービスプロセッサまたはシャーシ監視モジュールの電源のリセット	210
Oracle ILOM 構成のバックアップ、復元、またはリセット	211

x86 BIOS 構成パラメータの保守	221
関連情報	221
BIOS 構成の管理	221
Oracle ILOM からの BIOS 構成タスクの実行	228
シャーシブレードストレージリソースの SAS ゾーン機能	237
シャーシレベルの SAS-2 対応リソースのゾーン管理	238
管理可能な SAS-2 ゾーン対応デバイス	239
Sun Blade Zone Manager のプロパティ	239
SAS ゾーンの割り当てに関する重要な考慮事項	248
ゾーン機能の有効化および SAS-2 ゾーンの割り当ての作成	249
既存の SAS-2 ストレージリソースの割り当ての管理	266
Sun Blade Zone Manager の割り当てを出荷時のデフォルトにリセットする	275
サードパーティーの帯域内管理でのゾーンのパスワードを出荷時のデフォルトにリセットする	276
索引	279

このドキュメントの使用法

この構成および保守ガイドは、Oracle ILOM の構成タスクと保守タスクでの Web と CLI に関する情報を提供します。

このガイドは、Oracle ILOM 3.1 ドキュメントライブラリのその他のガイドと一緒に使用してください。このガイドは、技術者、システム管理者、Oracle 認定サービスプロバイダ、およびシステムハードウェアの管理経験があるユーザーを対象としています。

- 7 ページの「関連ドキュメント」
- 8 ページの「ドキュメントのフィードバック」
- 8 ページの「製品のダウンロード」
- 9 ページの「Oracle ILOM 3.1 ファームウェアのバージョン番号方式」
- 10 ページの「サポートとアクセシビリティ」

関連ドキュメント

ドキュメント	リンク
すべての Oracle 製品	http://www.oracle.com/documentation
Oracle Integrated Lights Out Manager (ILOM) 3.1 ドキュメントライブラリ	http://www.oracle.com/ pls/topic/lookup?ctx=ilom31
システム管理、単一システム管理 (SSM) のセ キュリティー、および診断のドキュメント	http://www.oracle.com/ technetwork/documentation/ sys-mgmt-networking-190072.html
Oracle Hardware Management Pack 2.2	http://www.oracle.com/ pls/topic/lookup?ctx=ohmp

注: 使用している Sun サーバーのプラットフォームに固有の Oracle ILOM 3.1 ドキュメントを見つけるには、使用しているサーバーに付属している管理ガイドの Oracle ILOM のセクションを参照してください。

ドキュメントのフィードバック

このドキュメントについてのフィードバックをお寄せください:

<http://www.oracle.com/goto/docfeedback>

製品のダウンロード

各 Sun サーバーまたは Sun ブレードシャーシシステムの Oracle ILOM 3.1 ファームウェアの更新は、My Oracle Support (MOS) Web サイトからダウンロードできるスタンドアロンのソフトウェア更新プログラムによって入手できます。このようなソフトウェア更新プログラムを MOS Web サイトからダウンロードするには、次の手順を参照してください。

▼ 製品のソフトウェアおよびファームウェアのダウンロード

- 1 <http://support.oracle.com> にアクセスします。
- 2 **My Oracle Support** にサインインします。
- 3 ページの上部にある「パッチと更新版」タブをクリックします。
- 4 「検索」タブの上部にある「パッチ検索」パネルで、「製品またはファミリー(拡張検索)」を選択します。
- 5 「対象製品」リストボックスで、製品名の全体または一部を入力し、リストボックスに一致する製品のリストが表示されたら該当する製品名を選択します。
製品名の例: Sun Fire X4470 M2 Server または Sun Enterprise SPARC T5120。
- 6 「リリース」リストボックスで:
 - a. 「リリース」リストボックスの下向き矢印をクリックして、一致する製品のフォルダのリストを表示します。
1つまたは複数の製品フォルダのアイコンのリストが表示されます。
 - b. 製品フォルダのアイコンの横にある三角形(>)をクリックして、ソフトウェアリリースのリストを表示します。
 - c. 目的のソフトウェアリリースを選択します。
例: X4470 M2 SW 1.4 または Sun SPARC Enterprise T5120

- 7 「検索」をクリックします。
「パッチ検索結果」画面が表示され、パッチ名のリストと説明が示されます。
- 8 「パッチ検索結果」画面で、目的のパッチ名を選択します。
例: X4470 M2 Server SW 1.4.ILOM and BIOS (Patch) または Firmware SPARC Enterprise T5120 Sun System Firmware 7.1.3.2
- 9 パッチ名の選択で、次のいずれかのアクションをクリックします:
 - README - 選択したパッチの Readme ファイルを開きます。
 - 計画に追加 - 選択したパッチを新しい計画または既存の計画に追加します。
 - ダウンロード - 選択したパッチをダウンロードします。
 - コピー - 選択したパッチの詳細をメモリーにコピーします。

Oracle ILOM 3.1 ファームウェアのバージョン番号方式

Oracle ILOM 3.1 では、使用しているサーバーまたはシャーシ監視モジュール (CMM) で実行しているファームウェアバージョンを識別しやすいファームウェアバージョンの番号方式を使用しています。この番号方式では、5つのフィールドがある文字列を使用しています。たとえば、a.b.c.d.e となり、ここでは:

- a - Oracle ILOM のメジャーバージョンを示します。
- b - Oracle ILOM のマイナーバージョンを示します。
- c - Oracle ILOM の更新バージョンを示します。
- d - Oracle ILOM のマイクロバージョンを示します。マイクロバージョンは、プラットフォームまたはプラットフォームのグループ単位で管理されます。詳細は、使用しているプラットフォームの製品ノートを参照してください。
- e - Oracle ILOM のナノバージョンを示します。ナノバージョンは、マイクロバージョンの増分反復です。

たとえば、Oracle ILOM 3.1.2.1.a の意味は、次のとおりです:

- Oracle ILOM 3 はメジャーバージョンです
- Oracle ILOM 3.1 はマイナーバージョンです
- Oracle ILOM 3.1.2 は2つ目の更新バージョンです
- Oracle ILOM 3.1.2.1 はマイクロバージョンです
- Oracle ILOM 3.1.2.1.a は3.1.2.1のナノバージョンです

ヒント - 使用している Sun サーバーまたは CMM にインストールされている Oracle ILOM ファームウェアバージョンを確認するには、Web インタフェースで「System Information」 > 「Firmware」の順にクリックするか、コマンド行インタフェースで `version` と入力します。

サポートとアクセシビリティ

説明	リンク
My Oracle Support を通じた電子的なサポートへのアクセス	http://support.oracle.com 聴覚障害の方へ: http://www.oracle.com/accessibility/support.html
アクセシビリティに対する Oracle のコミットメントについて	http://www.oracle.com/us/corporate/accessibility/index.html

Oracle ILOM への管理接続の設定とログイン

説明	リンク
Oracle ILOM でサポートされる管理接続のオプションの情報については、このセクションを参照してください。	■ 11 ページの「Oracle ILOM への管理接続の確立」
Oracle ILOM へのログイン、事前構成されたユーザーアカウント、およびサポートされるオペレーティングシステムと Web ブラウザの情報については、このセクションを参照してください。	■ 29 ページの「Oracle ILOM サーバー SP または CMM へのログイン」
Oracle ILOM のセキュリティを強化するためのガイドラインを参照するには、このセクションを参照してください。	■ 36 ページの「セキュリティを最大化するように Oracle ILOM を構成する」

関連情報

- Oracle サーバーまたはブレードシステム CMM のインストールガイド
- Oracle サーバーの管理ガイド
- 『Oracle Integrated Lights Out Manager (ILOM) 3.1 セキュリティガイド』

Oracle ILOM への管理接続の確立

Oracle ILOM のファームウェアは、Oracle サーバーまたはシャーシ監視モジュール (CMM) が Oracle ILOM に対して管理接続を簡単に確立できるように事前構成された状態で出荷されます。

Oracle ILOM に対して管理接続を確立する方法については、次を参照してください:

- [12 ページの「Oracle ILOM への管理接続の選択および構成」](#)
- [27 ページの「管理サービスおよびネットワークのデフォルトのプロパティ」](#)

Oracle ILOM への管理接続の選択および構成

Oracle ILOM は次の管理接続をサポートしています:

- 12 ページの「専用ネットワーク管理接続 (デフォルト)」
- 14 ページの「サイドバンドネットワーク管理接続」
- 17 ページの「専用のローカル管理接続」
- 18 ページの「専用の相互接続 SP 管理接続」

専用ネットワーク管理接続 (デフォルト)

Oracle ILOM とともに出荷されるすべての Oracle サーバーおよび CMM には、ホストからすべての管理トラフィックをセキュアに分離する専用の帯域内管理ポートがシャーシに装備されています。

すべてのサーバーおよび CMM は、Oracle ILOM に対してセキュアな管理接続を確立する準備ができた状態で出荷されます。シャーシの物理ネットワーク管理ポート (NET MGT) にアクティブな LAN の回線を接続するだけで、ログインできるようになります。Oracle ILOM への専用の管理接続を設定する手順の詳細は、次の手順を参照してください。

▼ Oracle ILOM への専用ネットワーク管理接続の構成

始める前に

- 27 ページの「管理サービスおよびネットワークのデフォルトのプロパティ」を確認します。
- Oracle ILOM の「Management Port」プロパティは、管理対象デバイスの物理ネットワーク管理ポート (NET MGT) を使用してすべての管理トラフィックをルーティングするようにデフォルトで設定されています。

注-専用ネットワーク管理接続は、サイドバンドネットワーク管理接続から独立して実装されるように設計されています。ただし、これらのネットワーク管理接続 (専用またはサイドバンド) はいずれも、標準のローカルのシリアル管理接続および (または) 内部の高速相互接続の管理接続と共存できます。

- Oracle ILOM の「Management Port」プロパティは、Oracle ILOM の CLI および Web インタフェースから構成できます。また、x86 サーバーの場合は、BIOS ユーティリティから構成できます。

Oracle ILOM から「Management Port」プロパティを変更する場合は、デフォルトの root アカウントまたは Admin (a) 役割権限を持つユーザーアカウントを使用してログインする必要があります。ログインの手順については、[30 ページの「Oracle ILOM SP または CMM へのログイン」](#)を参照してください。

Oracle ILOM への専用ネットワーク管理接続を確認または構成するには、次の手順に従います:

- 1 物理サーバーまたは CMM で、LAN 接続が物理管理ポート (NET MGT) に対して確立されたことを確認します。

NET MGT ポートへの物理 LAN 接続が確立されていない場合は、ネットワークスイッチとデバイスの物理 NET MGT ポートを Ethernet ケーブルで接続します。詳細な手順については、Oracle サーバーまたは CMM のインストールガイドの配線のセクションを参照してください。

注 - 管理対象サーバーまたは CMM シャーシの NET MGT ポートにアクティブな LAN の回線を接続すると、Oracle ILOM は、ネットワークの IP ルーティングデバイスから、SP または CMM の IP アドレスを自動的に検出します。Oracle ILOM SP または CMM に割り当てられている IP アドレスを判別するためのガイドラインについては、32 ページの「IP ネットワーク管理アドレスを使用する際のガイドライン」を参照してください。

- 2 デフォルトの「Management Port」プロパティが Oracle ILOM SP または CMM に設定されていることを確認するには、該当するユーザーインターフェースを使用して次の手順を実行します。

ユーザーインターフェース	手順	タスク: SP または CMM のデフォルトの「Management Port」プロパティを確認またはリセットする
Oracle ILOM CLI	1:	<p>Oracle ILOM の CLI にログインし、show コマンドを使用して、管理対象デバイスのネットワークプロパティを表示します。たとえば、次のいずれかを入力します:</p> <ul style="list-style-type: none"> ■ <code>show /SP/network</code> ■ <code>show /CMM/network</code> <p>ログインの手順については、30 ページの「Oracle ILOM SP または CMM へのログイン」を参照してください。</p>
	2:	<p>/network の出力に、SP または CMM のデフォルトの「Management Port」プロパティが表示されることを確認します。例:</p> <ul style="list-style-type: none"> ■ SP の出力: <code>managementport=MGMT</code> ■ CMM の出力: <code>switchconf=port0</code>
	3:	<p>必要な場合は、SP または CMM のデフォルトの「Management Port」プロパティをリセットします。</p> <p>SP の場合、次を入力します:</p> <pre>set /SP/network pendingmanagementport=MGMT commitpending=true</pre> <p>CMM の場合、次を入力します:</p> <pre>set /CMM/network pendingswitchconf=port0 commitpending=true</pre>

ユーザーインタフェース	手順	タスク:SPまたはCMMのデフォルトの「Management Port」プロパティを確認またはリセットする
Oracle ILOM の Web インタフェース	1:	Oracle ILOM の Web インタフェースにログインして、「ILOM Administration」 > 「Connectivity」の順にクリックします。 ログインの手順については、30 ページの「Oracle ILOM SP または CMM へのログイン」を参照してください。
	2:	「Network Settings」ページで、SP の「Management Port」リストボックスに MGMT が設定されていること、または「CMM Management Network Switch」リストボックスに Port 0 が設定されていることを確認します。 必要な場合は、SP の場合は MGMT、CMM の場合は Port0 を選択してデフォルトの「Management Port」プロパティをリセットし、「Save」をクリックします。
BIOS 設定ユーティリティ (x86 サーバーの場合のみ利用可能)	1	管理対象の x86 サーバーで BIOS 設定ユーティリティにアクセスし、BIOS 設定ユーティリティのダイアログで、「Advanced」 > 「IPMI 2.0 Configuration」 > 「Set LAN Configuration」の順にクリックします。
	2	「LAN Configuration」メニューで、デフォルトの「Management Port」プロパティとして MGMT が設定されていることを確認します。 必要な場合は、デフォルトの「Management Port」プロパティを MGMT にリセットして、変更をコミットします。

参考 関連情報

- 106 ページの「デフォルトの接続構成プロパティの変更」
- 37 ページの「ユーザーアカウントの設定および管理」

サイドバンドネットワーク管理接続

サイドバンド管理がサポートされるサーバーの場合は、必要に応じて、サーバーのシャーシに装備されている標準のデータポートを使用して Oracle ILOM に接続し、サーバーをリモートから管理できます。Oracle ILOM へのサイドバンド管理接続を実装すると、ホストおよび管理トラフィックのために 2 つの別個のネットワーク接続をサポートする必要がなくなります。ただし、このアプローチは: (1) Oracle ILOM への接続のパフォーマンスが低下する可能性があり、(2) Oracle ILOM のトラフィックが信頼されていないネットワークに転送される恐れがあります。

サイドバンド管理接続を使用して管理トラフィックを転送するように Oracle ILOM を構成するには、デフォルトの「Management Port」プロパティ (MGMT|port0) をサーバー上のアクティブな物理データポート (NET0、NET1、NET2、または NET3) に変更する必要があります。

Oracle ILOM へのサイドバンド管理接続の構成の詳細は、次を参照してください:

- 15 ページの「Oracle ILOM へのサイドバンド管理接続の構成」
- 16 ページの「サイドバンド管理でのネットワーク接続に関する考慮事項」

▼ Oracle ILOM へのサイドバンド管理接続の構成

始める前に

- サイドバンド管理は、ほとんどの Oracle サーバーでサポートされています。ただし、サーバーがサイドバンド管理をサポートするかどうかを確認するには、サーバー管理ガイドまたは製品のリリースノートを参照してください。

注-サイドバンドネットワーク管理接続は、専用ネットワーク管理接続から独立して実装されるように設計されています。ただし、これらのネットワーク管理接続(専用またはサイドバンド)はいずれも、標準のローカルのシリアル管理接続および(または)内部の高速相互接続の管理接続と共存できます。

- 27 ページの「管理サービスおよびネットワークのデフォルトのプロパティ」を確認します。
- Oracle ILOM の SP の「Management Port」プロパティは、Oracle ILOM の CLI および Web インタフェースから構成できます。また、x86 サーバーの場合は、BIOS 設定ユーティリティから構成できます。

Oracle ILOM から「Management Port」プロパティを変更する場合は、次の要件が適用されます:

- Oracle ILOM への管理接続をあらかじめ確立しておくようにしてください。手順については、次のいずれかを参照してください:
 - 12 ページの「専用ネットワーク管理接続(デフォルト)」
 - 17 ページの「専用のローカル管理接続」
- Oracle ILOM にログインしておいてください。手順については、29 ページの「Oracle ILOM サーバー SP または CMM へのログイン」を参照してください。
- Oracle ILOM で「Management Port」プロパティを変更するには、デフォルトの root アカウントまたは Admin (a) 役割権限を持つユーザーアカウントが必要です。

Oracle ILOM へのサイドバンド管理接続を構成するには、次の手順に従います:

- 1 物理サーバーで、アクティブな LAN 接続が適切な Ethernet データポート (NET0、NET1、NET2、または NET3) に対して確立されていることを確認します。手順については、サーバーまたはブレードシステムのインストールガイドの配線のセクションを参照してください。

2 サイドバンド管理の SP の「Management Port」プロパティを構成するには、次のいずれかを実行します:

- Oracle ILOM の Web インタフェースから – 「ILOM Administration」 > 「Connectivity」の順にクリックして、「Management Port」リストボックスをクリックします。
「Management Port」リストボックスで、アクティブな物理データポート名 (NET0、NET1、NET2、または NET3) を選択して、「Save」をクリックします。
- Oracle ILOM の CLI から – 次を入力します:
set /SP/network pendingmanagementport=/SYS/MB/NET n commitpending=true
ここでは:
 n は、サーバー上のアクティブな物理データポート番号 (0、1、2、または 3) です。
- BIOS 設定ユーティリティーから (x86 サーバーの場合に利用可能) – 「Advanced」 > 「IPMI 2.0 Configuration」 > 「Set LAN Configuration」の順にクリックします。
「LAN Configuration」メニューで、「Management Port」設定にアクティブな物理データポート名 (NET0、NET1、NET2、または NET3) を設定し、「Commit」をクリックして、変更を反映します。

注-ホストの BIOS 設定ユーティリティーで、オプションに移動して、設定および保存を行う方法については、サーバーとともに提供されている管理ガイドを参照してください。

参考 関連情報

- 16 ページの「サイドバンド管理でのネットワーク接続に関する考慮事項」
- 32 ページの「IP ネットワーク管理アドレスを使用する際のガイドライン」
- 106 ページの「デフォルトの接続構成プロパティの変更」
- 126 ページの「スパニングツリー構成についての推奨事項」
- 37 ページの「ユーザーアカウントの設定および管理」
- 121 ページの「システム識別情報の割り当て」

サイドバンド管理でのネットワーク接続に関する考慮事項

このセクションでは、Oracle ILOM に対してサイドバンド管理接続を使用する場合に考慮すべき一般的なネットワーク接続の問題を示します:

- サーバー SP とホストオペレーティングシステム間のチップ内接続が、オンボードのホストギガビット Ethernet コントローラではサポートされないことがあります。この状況が発生した場合は、転送元ターゲットと転送先ターゲット間のトランスフィックスの転送で、L2ブリッジング/スイッチングの代わりに別のポートまたは経路を使用します。
- サーバーホストの電源を入れ直すと、サイドバンド管理用に構成されている、サーバーのギガビット Ethernet ポート (NET 0、1、2、3) で、ネットワーク接続が短時間中断することがあります。この状況が発生した場合は、隣接するスイッチ/ブリッジのポートをホストポートとして構成します。
- サーバー上の Ethernet データポートがスイッチポートとして構成されていて、Spanning Tree Protocol (STP) に参加している場合、スパニングツリーの再計算のため、機能停止が長引くことがあります。

専用のローカル管理接続

すべての Oracle サーバーおよび CMM は、Oracle ILOM へのセキュアなローカル管理接続を簡単に確立できる物理シリアルポートをシャーシに装備して出荷されます。この種類の管理接続は、システムの障害にアクセスして診断するための唯一の方法がローカルのコンソールである場合、または LAN 接続を確立する前に Oracle ILOM の事前構成されたネットワークプロパティを変更する代替の方法が必要な場合に特に便利です。

Oracle ILOM に対してローカルのシリアル管理接続を構成する場合は、次の手順を参照してください。

▼ Oracle ILOM への専用のローカル管理接続の構成

始める前に

- Oracle ILOM へのローカルなシリアル管理接続では、物理的なシリアルコンソールデバイス (テキスト端末、ワークステーション、ノートパソコン、または端末エミュレータプログラム) をサーバーまたは CMM の SER MGT ポートに接続する必要があります。

Oracle ILOM への専用のローカル管理接続を構成するには、次の手順に従います:

- 1 シリアルコンソールデバイスとサーバーまたは CMM のシリアル管理 (SER MGT) ポートをシリアルケーブルで接続します。
- 2 コンソールデバイスの通信プロパティを、9600 ボー、8 ビット、パリティなし、1 ストップビットに設定します。

注 - DTE から DTE の通信で送受信の信号が逆方向になる (転向する) 場合、null モデム構成が必要になります。システムに付属するアダプタケーブルを使用して、null モデム構成を実現します。

- 3 コンソールデバイスと **Oracle ILOM SP** または **CMM** の間に接続を作成するには、**Enter** キーを押します。

参考 関連情報

- 27 ページの「管理サービスおよびネットワークのデフォルトのプロパティ」
- 106 ページの「デフォルトの接続構成プロパティの変更」
- 40 ページの「割り当て可能な Oracle ILOM のユーザーの役割」
- 88 ページの「シリアル管理ポートの所有者」
- 121 ページの「システム識別情報の割り当て」

専用の相互接続 SP 管理接続

内部 Ethernet-over-USB インタフェースをサポートする Oracle サーバーの場合は、必要に応じて、サーバーのネットワーク管理 (NET MGT) ポートを使用せずに、ホストオペレーティングシステム (OS) のクライアントから Oracle ILOM に対して LAN 管理接続を確立できます。

この種類の管理接続を実装したときに得られる利点を次に示します:

- 配備を容易にするための事前構成されたルーティングの宛先とならない **IP** アドレス
ローカル相互接続構成は、事前構成された内部のルーティングの宛先とならない IP アドレスを使用して、各内部接続ポイント (ILOM SP およびホスト OS) を自動構成できる状態で出荷されます。
Oracle ILOM は、従来の「Ethernet」インタフェースとして管理対象サーバーにインストールされる Ethernet-over-USB インタフェースを提供しています。
- **Oracle ILOM** へのセキュアな認証されたローカル接続
ローカル相互接続を使用した Oracle ILOM への接続では、専用ネットワーク管理接続またはサイドバンドネットワーク管理接続を使用して Oracle ILOM への接続を確立するときと同様に、ユーザー認証が必要となります。
有効なユーザー名とパスワードを持つすべてのオペレーティングシステムユーザーは、Oracle ILOM へのアクセスを許可されます。
- ローカル管理を行うための高速な代替手段
内部の高速専用管理接続を使用して Oracle ILOM のすべての管理タスクを実行します。

ローカル相互接続の管理接続は、従来のローカルのシリアルコンソールまたはホストキーボードコントローラスタイル (KCS) のインタフェースを使用するよりも高速な、ローカルでサーバーの管理を行うための代替の方法です。

Oracle ILOM SP に対してローカル相互接続を確立するための詳細は、次のトピックを参照してください:

- 19 ページの「ローカル相互接続のオプションの構成」
- 19 ページの「ローカル相互接続を手動で構成する」
- 23 ページの「手動構成でのホスト OS 相互接続のガイドライン」
- 26 ページの「Oracle ILOM SP の相互接続プロパティ」

ローカル相互接続のオプションの構成

ローカル相互接続の構成オプション	説明
自動構成 (推奨)	<p>Oracle ILOM では、Oracle Hardware Management Pack 2.1.0 以降のソフトウェアをインストールすると、ローカル相互接続の管理接続の構成が自動化されます。この場合、Oracle ILOM から構成を行う必要はありません。</p> <p>注 - ローカル相互接続の接続ポイントの自動構成が行われるようにするには、Oracle ILOM のデフォルトの「Host Managed」(hostmanaged) 設定を受け入れて (True に設定)、Oracle Hardware Management Pack 2.1.0 以降のソフトウェアをサーバーにインストールする必要があります。</p> <p>Oracle Hardware Management Pack を使用した自動構成の詳細は、『Oracle Hardware Management Pack User's Guide』(E20451) を参照してください。</p>
手動構成 (上級ユーザー)	<p>上級ネットワーク管理者が Oracle Hardware Management Pack をインストールして Ethernet USB 接続を自動構成したくない場合は、内部 Ethernet USB インタフェースの接続ポイントを手動で構成することを選択できます。</p> <p>手動構成の詳細は、19 ページの「ローカル相互接続を手動で構成する」を参照してください。</p>

▼ ローカル相互接続を手動で構成する

注 - 代替の方法として、Oracle Hardware Management Pack 2.1.0 以降のソフトウェアを使用して、ローカル相互接続の接続ポイントを管理対象サーバーに自動構成できます。ローカル相互接続の自動構成の手順については、『Oracle Hardware Management Pack User's Guide』(E20451) を参照してください。

始める前に

- 19 ページの「ローカル相互接続のオプションの構成」を確認します。

- SP およびホスト OS 間のローカル相互接続を構成するこの手動の手順は、上級ユーザーのみが実行するようにしてください。
- この手動の手順は、ホスト OS の内部接続ポイントを構成するためのガイドライン、および必要に応じて Oracle ILOM SP の内部接続ポイントを構成するための詳細な手順を示します。
- Oracle ILOM のデフォルトの SP の「Local Host Interconnect」プロパティーを変更する前に、Oracle ILOM SP でネットワークまたはローカルのシリアル管理接続が確立されている必要があります。

注 - CMM では、Oracle ILOM の「Local Host Interconnect」プロパティーは利用できません。ただし、Oracle ILOM CMM の CLI または Web インタフェースを使用すると、シャーシに取り付けられているブレードサーバーの SP の「Local Host Interconnect」プロパティーに移動して構成できます。

- Oracle ILOM で SP の「Local Host Interconnect」プロパティーを変更するには、事前構成された Oracle ILOM の root アカウントまたはユーザーが構成したユーザーアカウント (Admin (a) 役割権限を持つ) が必要です。

ホスト OS および Oracle ILOM SP 間に内部 Ethernet USB 接続ポイントを手動で構成するには、次の手順に従います:

- 1 ホストオペレーティングシステムに内部 **Ethernet USB** 接続パラメータを手動で構成するには、次を実行します:
 - a. サーバーが内部 **Ethernet-over-USB** インタフェースをサポートしていることを確認します。

サーバーが Oracle ILOM に対するローカル相互接続の管理接続をサポートしているかどうかを確認するには、サーバー管理ガイドの Oracle ILOM でサポートされる機能を説明しているセクションを参照してください。
 - b. 管理対象サーバーへの OS ソフトウェア配布によって、OS 固有の **Ethernet** デバイスドライバがインストールされていることを確認します。

OS 固有の Ethernet デバイスドライバがオペレーティングシステムのインストール時に提供されなかった場合は、Oracle Hardware Management Pack 2.1.0 以降のソフトウェア配布から内部 Ethernet-over-USB インタフェース用のデバイスドライバを入手できます。このファイルを Oracle Hardware Management Pack ソフトウェア配布から抽出する方法については、『Oracle Hardware Management Pack User's Guide』を参照してください。

- c. 管理対象サーバーのホストオペレーティングシステムが、内部 **Ethernet-over-USB** インタフェースを認識することを確認します。その後、ネットワークパラメータをホスト **OS** の接続ポイントに手動で割り当てます。
- ガイドラインについては、23 ページの「**手動構成でのホスト OS 相互接続のガイドライン**」を参照してください。
- 2 **Oracle ILOM SP** の「**Local Host Interconnect**」プロパティを手動で変更するには、次の手順に従います:
- a. 26 ページの「**Oracle ILOM SP の相互接続プロパティ**」を確認します。
- b. **Web** ブラウザまたは **CLI** シェルを使用して **Oracle ILOM** にログインします。
ログインの手順については、29 ページの「**Oracle ILOM サーバー SP または CMM へのログイン**」を参照してください。
- c. **Oracle ILOM** の **SP** の「**Local Host Interconnect**」プロパティを変更するには、該当する **Oracle ILOM** インタフェースで次の手順を実行します。

Oracle ILOM インタフェース

手順:

Web ブラウザ

- a. Oracle ILOM SP の Web インタフェースで、「ILOM Administration」 > 「Connectivity」の順にクリックします。
- b. 「Local Host Interconnect」セクションまでページをスクロールダウンして、「Configure」をクリックします。
- c. 「Configure USB Ethernet Parameters」ダイアログで、「Host Managed」のチェックボックスをオフにして、「State」のチェックボックスをオンにし、必要な場合にのみ、SP に指定されているローカルのルーティングの宛先と異なる IPv4 アドレスまたはネットマスクアドレスを変更して、「Save」をクリックします。
注 - Oracle ILOM SP に割り当てられている事前構成された IP アドレスまたはネットマスクアドレスは、ネットワークでこれらのパラメータに競合が存在する場合を除き、変更する必要はありません。

Oracle ILOM インタフェース	手順:
CLI シェル	<p>a. 管理対象サーバーの /network/interconnect 作業用ディレクトリに移動します。 例: SP CLI から、次を入力します: cd /SP/network/interconnect CMM CLI から、次を入力します: cd /Servers/Blades/BLn/network/interconnect</p> <p>b. hostmanaged プロパティを無効にして、「Local Host Interconnect」の state を true に設定するには、次を入力します: set hostmanaged=disabled set state=true 注 - Oracle ILOM SP に割り当てられている事前構成されたルーティングの宛先と異なる IP アドレスおよびネットマスクアドレスは、ネットワークでこれらのパラメータに競合が存在する場合を除き、変更する必要はありません。</p> <p>c. SP に指定されている、ローカルのルーティングの宛先と異なる IPv4 アドレスまたはネットマスクアドレスを変更するには、次を入力します: set pendingipaddress=specify_new_address set pendingipnetmask=specify_new_address set commitpending=true</p>

3 ホスト OS と Oracle ILOM SP 間のローカル相互接続の管理接続をテストするには、次のいずれかを実行します:

- 管理対象サーバーのホストオペレーティングシステムで Web ブラウザまたは CLI シェルを使用し、SP の USB Ethernet 接続ポイントに割り当てられているルーティングの宛先と異なる IP アドレスを入力して、Oracle ILOM SP にログインします。

想定される結果:

Web ブラウザ接続 - Oracle ILOM のログインページが表示されます。

CLI シェル接続 - Oracle ILOM の承認プロンプトが表示されます。

- ホスト OS からローカル相互接続の SP のアドレスに対して ping を実行します。
手順については、127 ページの「IPv4 および IPv6 の接続をテストする」を参照してください。

参考 関連情報

- 23 ページの「手動構成でのホスト OS 相互接続のガイドライン」
- 26 ページの「Oracle ILOM SP の相互接続プロパティ」
- 29 ページの「Oracle ILOM サーバー SP または CMM へのログイン」
- 『Oracle Integrated Lights Out Manager (ILOM) 3.1 セキュリティーガイド』の「Oracle ILOM の LAN 相互接続インタフェースを理解する」

- Oracle Hardware Management Pack のドキュメントライブラリ:<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>

手動構成でのホスト OS 相互接続のガイドライン

次の表は、ホスト OS の内部 USB Ethernet 接続ポイントに、ローカルのネットワークパラメータを構成するための一般的なガイドラインを示しています。

注 - 管理対象サーバーにインストールされている内部 USB Ethernet は、従来の Ethernet インタフェースとしてシステムに表示されます。ホスト OS にローカル相互接続ポイントを手動で構成する場合は、ホストの MAC アドレス (hostmacaddress=) を使用して、ホスト OS のローカル相互接続ポイントに割り当てられている名前を判別する必要がある場合があります。

表1 ホスト OS の相互接続を手動構成する場合のガイドライン

オペレーティングシステム	手動でのホスト OS の相互接続のガイドライン
Windows Server 2008	<p>Microsoft Windows が管理対象サーバー上で内部 Ethernet-over-USB インタフェースを発見すると、Ethernet-over-USB インタフェースのデバイスドライバを確認するように求めるメッセージが表示されることがあります。実際にはドライバは必要ないため、Oracle Hardware Management Pack ソフトウェア配布から抽出できる .inf ファイルを指定すれば、Ethernet-over-USB インタフェースの通信スタックに対応できるはずです。</p> <p>Oracle Hardware Management Pack 2.1.0 以降のソフトウェア配布は、Oracle ソフトウェア製品のダウンロードページからダウンロードできます。</p> <p>Oracle Server Hardware Management Pack から .inf ファイルを抽出する方法については、『Oracle Server Hardware Management Pack User's Guide』(E24501)を参照してください。</p> <p>Windows Server 2008 で IP ネットワークパラメータを構成する方法については、Microsoft Windows オペレーティングシステムのドキュメントまたは次の Microsoft Tech Net サイトを参照してください:</p> <p>http://technet.microsoft.com/en-us/library/cc754203%28WS.10%29.aspx</p>

表1 ホストOSの相互接続を手動構成する場合のガイドライン (続き)

オペレーティングシステム	手動でのホストOSの相互接続のガイドライン
Linux	<p>管理対象サーバーでサポートされているほとんどのLinuxオペレーティングシステムのインストールには、Ethernet-over-USBインタフェースのデバイスドライバのインストールが含まれています。</p> <p>Ethernet-over-USBインタフェースは、通常、Linuxオペレーティングシステムによって自動的に発見され、usb0としてシステムに表示されます。ただし、このインタフェースの表示名は、各Linuxソフトウェア配布によって異なる場合があります。</p> <p>次のコマンド行の命令は、usb0に対応するホストOSの相互接続にネットワークパラメータを構成する方法を示しています：</p> <pre> \>lsusb usb0 \> ifconfig usb0 169.254.182.77 \> ifconfig usb0 netmask 255.255.255.0 \> ifconfig usb0 broadcast 169.254.182.255 \> ifconfig usb0 \> ip addr show usb0 </pre> <p>注-ネットワークパラメータの構成は、個別にifconfigコマンドを発行せずに、スクリプトに記述できます。ただし、ネットワークパラメータを構成するための実際のネットワークスクリプトは、各Linuxソフトウェア配布によって異なる場合があります。このため、各Linuxソフトウェア配布とともに通常提供されるネットワークスクリプトの例を参照するようにしてください。</p> <p>Linuxオペレーティングシステムを使用してIPネットワークパラメータを構成する方法の詳細については、Linuxオペレーティングシステムのドキュメントを参照してください。</p>

表1 ホスト OS の相互接続を手動構成する場合のガイドライン (続き)

オペレーティングシステム	手動でのホスト OS の相互接続のガイドライン
Solaris	<p>管理対象サーバーのほとんどの Oracle Solaris オペレーティングシステムのインストールには、Ethernet-over-USB インタフェースのデバイスドライバが含まれています。このインタフェースのデバイスドライバが提供されていない場合は、Oracle Hardware Management Pack 2.1.0以降のソフトウェア配布からこのドライバを抽出できます。</p> <p>Solaris 固有の OS ドライバを管理パックから抽出する方法については、『Oracle Hardware Management Pack User's Guide』(E20451)を参照してください。</p> <p>Ethernet-over-USB インタフェースは、通常、Oracle Solaris オペレーティングシステムによって自動的に発見され、<code>usbem0</code>としてシステムに表示されます。ただし、このインタフェースの表示名は、各 Oracle Solaris ソフトウェア配布によって異なる場合があります。</p> <p>次のコマンド行の命令は、<code>usbem0</code>に対応するホスト OS の相互接続にネットワークパラメータを構成する方法を示しています。</p> <ul style="list-style-type: none"> ■ IP インタフェースを <code>plumb</code> または <code>unplumb</code> するには、次のコマンドを入力します。 <pre>ifconfig usbem0 plumb ifconfig usbem0 unplumb</pre> ■ アドレス情報を設定するには、次のコマンドを入力します： <pre>ifconfig usbem0 netmask 255.255.255.0 broadcast 169.254.182.255 169.254.182.77</pre> ■ インタフェースを設定するには、次を入力します： <pre>ifconfig usbem0 up</pre> ■ インタフェースを停止するには、次を入力します： <pre>ifconfig usbem0 down</pre> ■ アクティブなインタフェースを表示するには、次を入力します： <pre>ifconfig -a</pre> ■ 接続をテストするには、Oracle Solaris ホストまたは SP 内部 USB Ethernet デバイスに対して <code>ping</code> を実行します。 <pre>ping <Oracle Solaris ホストの IPv4 アドレス> ping <SP の Ethernet-over-USB インタフェースの IPv4 アドレス></pre> <p>注-ネットワークパラメータの構成は、<code>ifconfig</code>の手順を実行せずに、スクリプトに記述できます。ただし、ネットワークパラメータを構成するための実際のネットワークスクリプトは、各 Oracle Solaris ソフトウェア配布によって異なる場合があります。このため、各 Oracle Solaris ソフトウェア配布とともに通常提供されるネットワークスクリプトの例を参照するようにしてください。</p> <p>Oracle Solaris オペレーティングシステムを使用してハードウェアデバイスの静的 IP アドレスを構成する方法については、Oracle Solaris オペレーティングシステムのドキュメントを参照してください。</p>

Oracle ILOM SPの相互接続プロパティ

次の表は、Oracle ILOMのCLI(ターゲット:/network/interconnect)およびOracle ILOMのWebインタフェース(「ILOM Administration」>「Connectivity」>「Local Host Interconnect」>「Configure」)に表示されるSPの「Local Host Interconnect」プロパティについて説明しています。

表2 Oracle ILOM SPの相互接続プロパティ

プロパティ	デフォルト値	説明
Host Managed (hostmanaged=true false)	Enabled (true)	<p>「Host Managed」プロパティは、デフォルトでは、ホスト OS と Oracle ILOM SP 間のローカル相互接続の管理接続を Oracle Hardware Management Pack ソフトウェアが自動構成できる状態で出荷されます。</p> <p>Oracle Hardware Management Pack ソフトウェアがローカル相互接続の接続を自動構成しないようにして、ホスト OS と Oracle ILOM SP 間の接続ポイントを手動で構成するには、「Host Managed」プロパティの値を無効 (false) に設定する必要があります。</p> <p>注 - Ethernet-over-USB インタフェースが使用されないようにするには、Oracle ILOM で「Host Managed」プロパティおよび「Local Host Interconnect」の state プロパティの両方を disabled (false) にする必要があります。</p>
State (state=disabled enabled)	Disabled	<p>Oracle ILOM の「Local Host Interconnect」プロパティの State は、デフォルトでは無効に設定されます。</p> <p>ホスト OS と Oracle ILOM SP 間の Ethernet-over-USB 接続ポイントを手動で構成することを選択した場合は、このプロパティの値に enabled を設定する必要があります。</p>
IP Address (pendingipaddress=)	169.254.182.7	<p>Oracle ILOM では、Oracle ILOM SP の Ethernet-over-USB 接続ポイントに対して、事前構成されたルーティングの宛先とならない IPv4 アドレスがデフォルトで用意されています。</p> <p>通常、事前構成された IP アドレス (169.254.182.76) は、ネットワークでこのアドレスに競合が存在する場合を除き、変更する必要はありません。</p>
Netmask Address (pendingipnetmask=)	255.255.255.0	<p>Oracle ILOM では、Oracle ILOM SP の Ethernet-over-USB 接続ポイントに対して、事前構成された IPv4 ネットマスクアドレスがデフォルトで用意されています。</p> <p>通常、事前構成された IPv4 ネットマスク (255.255.255.0) アドレスは、ネットワークでこのアドレスに競合が存在する場合を除き、変更する必要はありません。</p>

表 2 Oracle ILOM SP の相互接続プロパティ (続き)

プロパティ	デフォルト値	説明
Save(<code>commitpending=true false</code>)		Oracle ILOM SP の Ethernet-over-USB 接続ポイントの IP アドレスまたはネットマスクアドレスへの変更は、その変更が CLI でコミットされるか、Web インタフェースで保存されるまで、保留中とみなされます。
Service Processor MAC Address (<code>spmaddress=</code>)	読み取り専用	読み取り専用の「Service Processor MAC Address」プロパティには、Oracle ILOM SP に割り当てられている MAC アドレスが表示されます。
Host MAC Address (<code>hostmacaddress=</code>)	読み取り専用	読み取り専用の「Host MAC Address」プロパティには、管理対象サーバーに割り当てられている MAC アドレスが表示されます。また、これは、ほとんどのオペレーティングシステムが内部 Ethernet-over-USB インタフェースを認識する方法を表しています。
Connection Type	読み取り専用	この読み取り専用の「Connection Type」プロパティは、接続タイプが内部 USB Ethernet であることを示します。
CLI の help コマンド		<p><code>/network/interconnect</code> CLI ターゲットの下に表示される構成可能なプロパティまたは構成できないプロパティの追加情報を参照するには、<code>help</code> コマンドに続けてプロパティ名を入力します。</p> <p>構文: <code>help /SP CMM/network/interconnect property_name</code></p> <p>例: <code>help /SP/network/interconnect hostmanaged</code></p>

管理サービスおよびネットワークのデフォルトのプロパティ

サーバーを配備するプロセスを簡単にするために、Oracle ILOM はほとんどの管理サービスポートおよび標準のネットワーク接続プロパティが有効になるように事前構成された状態で出荷されます。ただし、セキュリティを最大化して、Oracle ILOM への承認されていないアクセスを防ぐには、必要のない管理サービスポートのプロパティを無効にしてください。

注 - Oracle ILOM のデフォルトのプロパティは、Oracle ILOM に対して管理接続を確立したあとにユーザーが構成できます。

- 表 3
- 表 4

表3 デフォルトで有効にされる管理サービス

Management Access	デフォルトのプロパティ	サービスポート	構成可能なプロパティを変更する場合の参照先
Web サーバー: モード	<ul style="list-style-type: none"> ■ HTTP 接続を HTTPS にリダイレクトする 	80	表 35
Web サーバー: 状態	<ul style="list-style-type: none"> ■ HTTPS、Enabled 	443	表 35
Web サーバー: SSL	<ul style="list-style-type: none"> ■ SSLv3 および TLSv1 を有効にする ■ デフォルトの SSL 証明書 ■ デフォルトの SSL 自己署名非公開鍵 	-	表 36
IPMI: 状態	<ul style="list-style-type: none"> ■ Enabled 	623	表 39
SNMP: 状態	<ul style="list-style-type: none"> ■ SNMPv3、Enabled 	161	表 37
WS-MAN: モード	<ul style="list-style-type: none"> ■ HTTP、Enabled 	8889	表 41
シングルサインオン	<ul style="list-style-type: none"> ■ Enabled 	11626	42 ページの「シングルサインオンサービス (デフォルトで有効)」
Secure Shell (SSH)	<ul style="list-style-type: none"> ■ Enabled ■ RSA 鍵および DSA 鍵を生成する 	22	表 38
リモート KVMs リダイレクション (ビデオ、キーボード、マウス、およびストレージ)	<ul style="list-style-type: none"> ■ Enabled 	5120-5123、5551-5556、5781-5784、5791-5794	「リモート KVMs コンソールを使用したホストサーバーのリダイレクション」
サービスタグ ¹	<ul style="list-style-type: none"> ■ Enabled 	6481	<p>「service tag」プロパティを変更するには、次を入力します:</p> <pre>set /SP/services/servicetag state=enabled disabled</pre>

¹ サーバーを識別し、Oracle サービスソリューションと統合できるようにする Oracle の発見プロトコル。

注 - Oracle ILOM によって使用されるデフォルトのネットワークポートの完全なリストについては、89 ページの「Oracle ILOM で使用するデフォルトのネットワークポート」を参照してください。

表4 デフォルトで有効にされるネットワーク接続プロパティ

ネットワーク接続プロパティ	デフォルト値	構成可能なプロパティを変更する場合の参照先:
Network: State	■ Enabled	表 43
IPv4: Mode	■ DHCP、有効	
IPv6: State	■ Enabled	表 43
IPv6: Mode	■ 自動構成、Stateless	
Management Port:	■ 専用ネットワーク管理 (MGMT)	表 43
Local Host Interconnect	■ Host Utilities Managed: Enabled ■ State: Disabled	18 ページの「専用の相互接続 SP 管理接続」
DNS	■ Auto DNS via DHCP、Enabled	表 44
Serial Port	■ Owner: Service Processor ■ Baud Rate: 9600 ■ Host Flow Control: None	表 45
ユーザー認証 ¹	■ Root のユーザーアカウント: root ■ Root のパスワード: changeme ■ 許可されるローカルアカウント: 最大 10 個のユーザーアカウントをユーザーが構成できる ■ シングルサインオン: リモート KVMS および CMM ブレードのナビゲーション (ドリルダウン) が有効になる	38 ページの「ユーザー資格の管理」

¹ LDAP、RADIUS、および Active Directory の state プロパティは、デフォルトで無効になります。

Oracle ILOM サーバー SP または CMM へのログイン

Oracle ILOM は、Oracle ILOM への初回のログインが簡単になるように、事前構成されたユーザーアカウントおよびデフォルトのネットワークパラメータが設定された状態で出荷されます。Oracle ILOM へのログインの詳細は、次のトピックを参照してください:

- 30 ページの「Oracle ILOM SP または CMM へのログイン」
- 32 ページの「IP ネットワーク管理アドレスを使用する際のガイドライン」
- 33 ページの「デフォルトで有効にされる事前構成されたユーザーアカウント」
- 35 ページの「サポートされているオペレーティングシステムの Web ブラウザ」

▼ Oracle ILOM SP または CMM へのログイン

始める前に

- Oracle ILOM に対してローカル管理接続またはネットワーク管理接続が確立されている必要があります。
手順については、12 ページの「Oracle ILOM への管理接続の選択および構成」を参照してください。
- Oracle ILOM にログインするには、事前構成された Oracle ILOM の root アカウントまたはユーザーが構成したユーザーアカウントが必要です。
事前構成された root アカウントについては、33 ページの「デフォルトで有効にされる事前構成されたユーザーアカウント」を参照してください。Oracle ILOM にユーザーアカウントを作成する方法については、38 ページの「ユーザー資格の管理」を参照してください。

ローカルのシリアル管理接続またはネットワーク管理接続から Oracle ILOM にログインするには、次の手順に従います:

- 1 Oracle ILOM にログインするには、該当する Oracle ILOM インタフェースで次の手順を実行します。

Oracle ILOM インタフェース	手順
ローカルのシリアルコンソール (SER MGT ポート)	<ul style="list-style-type: none"> ■ Enter キーを押して、コンソールと Oracle ILOM の間の接続を作成し、プロンプトが表示されたら、Oracle ILOM のユーザー名とパスワードを入力します。 例: ユーザー名に root、パスワードに changeme を入力します。
Web ブラウザ	<ol style="list-style-type: none"> a. Web ブラウザに http://ILOM_SP_or_CMM_ipaddress と入力し、Enter を押します。 Oracle ILOM のログインページが表示されます。 Oracle ILOM に割り当てられている IP アドレスを入力する際のガイドラインについては、32 ページの「IP ネットワーク管理アドレスを使用する際のガイドライン」を参照してください。 b. 有効な Oracle ILOM のユーザー名とパスワードを指定して、Oracle ILOM の Web インタフェースにログインします。 例: ユーザー名に root、パスワードに changeme を入力します。 Oracle ILOM の「Summary」ページが表示されます。

Oracle ILOM インタフェース	手順
CLI Secure Shell	<ol style="list-style-type: none"> a. Oracle ILOM CLI への SSH セッションを確立するには、端末ウィンドウを開きます。 b. デフォルト root アカウントを使用して Oracle ILOM にログインするには、次のように入力します: <pre>\$ ssh root@ILOM_SP_or_CMM_ipaddress</pre> Oracle ILOM から root パスワードを求められます。 c. パスワードプロンプトで <code>changeme</code> と入力します。 Oracle ILOM CLI プロンプト (<code>-></code>) が表示されます。

2 Oracle ILOM を終了するには、次のいずれかを実行します:

- Oracle ILOM の Web インタフェースセッションを終了するには - Web インタフェースページの右上にある「Log Out」ボタンをクリックします。
- Oracle ILOM の CLI セッションを終了するには - 次を入力します: `exit`

参考 関連情報

- [121 ページの「システム識別情報の割り当て」](#)
- [87 ページの「CLI および Web セッションのデフォルトタイムアウト」](#)
- [91 ページの「デフォルトの管理アクセス構成プロパティの変更」](#)
- [87 ページの「ログイン時のバナーメッセージの表示」](#)
- [37 ページの「ユーザーアカウントの設定および管理」](#)
- [45 ページの「root アカウントのパスワードの復旧」](#)
- [11 ページの「Oracle ILOM への管理接続の設定とログイン」](#)
- [129 ページの「リモート KVMS コンソールを使用したホストサーバーのリダイレクション」](#)
- 『ユーザーズガイド』の「システム情報の収集、健全性ステータスの監視、およびホスト管理の開始」
- 『ユーザーズガイド』の「管理タスクを CLI ネームスペースターゲットにマッピングする」
- [201 ページの「ファームウェア更新の実行」](#)

IP ネットワーク管理アドレスを使用する際のガイドライン

次の表は、次を判別するためのガイドラインを示しています:(1) デフォルトのネットワークプロパティに基づいて Oracle ILOM SP または CMM に割り当てられている IP アドレス、(2) 受け入れられる IPv6 構文、および (3) サポートされない IPv6 サーバーのリスト。

表 5 IP アドレスの識別、IPv6 で受け入れられる構文、サポートされない IPv6 サーバー

判別する内容:	ガイドライン
Oracle ILOM に割り当てられる IP アドレス	<p>割り当てられている IP アドレスを判別するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. ILOM SP または CMM に対してローカルのシリアル管理 (SER MGT) 接続を確立します。 2. Oracle ILOM にログインします。 3. <code>show</code> コマンドを使用して、次のディレクトリの下にある IP ネットワークプロパティを表示します: 現在、Oracle ILOM に割り当てられている IPv4 アドレスの場合は、<code>/SP/network</code>。 現在、Oracle ILOM に割り当てられている IPv6 アドレスの場合は、<code>/SP/networkip6</code>。 <p>ネットワーク上の IPv4 の DHCP サーバーまたは IPv6 のルーティングデバイスから IP アドレスを判別することもできます。</p>
IPv6 のネットワークアドレスとして受け入れられる構文	<ul style="list-style-type: none"> ■ Web ブラウザに URL を入力する場合、正常に動作が行われるようにするには、IPv6 アドレスを角括弧で囲む必要があります。例: <code>https://[ipv6address]</code> ■ SSH を使用して Oracle ILOM の CLI セッションを確立する場合は、IPv6 アドレスを角括弧で囲まないようにしてください。例: <code>ssh root@[ipv6address]</code> ■ CLI の <code>load -source</code> コマンドおよび <code>tftp</code> を使用してファイルを転送する場合は、IPv6 アドレスを角括弧で囲む必要があります。例: <code>load -source tftp:[ipv6address]filename.extension</code>

表 5 IP アドレスの識別、IPv6 で受け入れられる構文、サポートされない IPv6 サーバー (続き)

判別する内容:	ガイドライン
IPv6 をサポート しないレガシー Sun サーバー	<ul style="list-style-type: none"> ■ Sun SPARC サーバー <ul style="list-style-type: none"> ■ T5440 ■ T5220 ■ T5120 ■ T5140 ■ T5240 ■ T6340 ■ Sun Fire サーバー: <ul style="list-style-type: none"> ■ X4140 ■ X4150 ■ X4240 ■ X4440 ■ X4450 ■ X4600 ■ X4600 M2 ■ X4640

デフォルトで有効にされる事前構成されたユーザーアカウント

Oracle ILOM は、事前構成された管理者ユーザーアカウント (root)、およびパスワード復旧のためのユーザーアカウント (default) が設定された状態で出荷されます。これらのアカウントの使用法については、次の表を参照してください。

表6 デフォルトで有効にされるローカルユーザーアカウント

事前構成済み ユーザーアカウント	デフォルトのログインプロパティ	説明	変更する場合の参照先:
root	<ul style="list-style-type: none"> ■ ユーザー名: root ■ パスワード: changeme 	<p>Oracle ILOM の root ユーザーアカウントは、すべての Oracle ILOM インタフェース¹で利用できる永続的なローカルユーザーアカウントです (永続的な root ユーザーアカウントを削除することを選択した場合は除きます)。</p> <p>組み込みの管理権限 - root アカウントには、Oracle ILOM のすべての機能やコマンドに対して組み込みの管理権限 (読み取りおよび書き込み) があります。</p> <p>推奨されるセキュリティ対策 - 管理対象サーバーまたは CMM に対して承認されていないアクセスが行われないようにするには、次のいずれかを行うようにしてください:</p> <ul style="list-style-type: none"> ■ 各 Oracle ILOM サービスプロセッサ (SP) または シャーシ監視モジュール (CMM) に指定されている root のデフォルトのパスワード (changeme) を変更します。 または ■ Oracle ILOM SP および Oracle ILOM CMM に指定されている事前構成された root アカウントを削除します。 事前構成された root アカウントを削除する前に、root アカウントを、ユーザーが構成できるローカルユーザーアカウントまたはディレクトリサービス (LDAP、Active Directory など) に置き換える必要があります。 <p>注。root アカウントのパスワードに changeme (デフォルトのパスワード) が設定されている場合は、ログイン時に CLI に警告メッセージが表示され、Web インタフェースページの上にも警告メッセージが表示されます。</p>	38 ページの「ユーザー資格の管理」

¹ Oracle ILOM の Web インタフェース、CLI シェル、ローカルのシリアルコンソール、および IPMI。

表6 デフォルトで有効にされるローカルユーザーアカウント (続き)

事前構成済み ユーザーアカウン ト	デフォルトのログイ ンプロパティ	説明	変更する場合の参照先:
default	<ul style="list-style-type: none"> ■ ユーザー名: default ■ パスワード: default password 	<p>Oracle ILOMに指定されている事前構成された default ユーザーアカウントは、パスワードの復旧に限定されています。</p> <p>ローカルのシリアルコンソールでの使用のみ – 事前構成された default ユーザーアカウントは、ローカルのシリアル接続からのみ使用できます。また、サーバーまたは CMM のある場所に実際にいることを証明できる必要があります。</p> <p>使用シナリオ – root アカウントを、ユーザーが構成できるアカウントに置き換える前に Oracle ILOM で root アカウントを削除した場合は、default アカウントを使用して Oracle にログインし、通常の Oracle ILOM コマンドを使用して、新しいアカウントを作成できます。</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 12 ■ (サーバーのある場所にいる) 121 ページの「システム識別情報の割り当て」 	45 ページの「root アカウントのパスワードの復旧」

サポートされているオペレーティングシステムの Web ブラウザ

Oracle ILOM は、次のオペレーティングシステムの Web ブラウザをサポートしています。

注 – 管理対象サーバーでサポートされるオペレーティングシステムのリストについては、サーバー管理ガイドまたはプロダクトノートを参照してください。

表7 サポートされているオペレーティングシステムの Web ブラウザ

オペレーティングシステム	Web ブラウザ
Oracle Solaris 10	<ul style="list-style-type: none"> ■ Mozilla 1.4 および 1.7 ■ Firefox 3.6.x および 6
Linux (Oracle, Red Hat, SuSE, Ubuntu 10.10)	<ul style="list-style-type: none"> ■ Firefox 3.6.x および 6

表7 サポートされているオペレーティングシステムの Web ブラウザ (続き)

オペレーティングシステム	Web ブラウザ
Microsoft Windows (XP Service Pack 2、Windows 7)	<ul style="list-style-type: none"> ■ Internet Explorer 7.x、8.x (Windows XP Service Pack 2 の場合)、および 9 (Windows 7 の場合) ■ Firefox 3.6.x および 6
Macintosh (OSX v10.6 以降)	<ul style="list-style-type: none"> ■ Firefox 3.6.x および 6 ■ Safari すべて

セキュリティを最大化するように **Oracle ILOM** を構成する

Oracle ILOM のすべての構成可能なプロパティは、必要に応じて無効または有効にすることにより、Oracle ILOM の管理環境をよりセキュアにできます。Oracle ILOM のセキュリティを強化する方法については、『Oracle ILOM 3.1 セキュリティガイド』に記述されているセキュリティガイドラインを参照してください。

ユーザーアカウントの設定および管理

説明	リンク
認証の構成オプション、ユーザーの役割の権限、シングルサインオンサービス、許可されるユーザーセッション、SSH 鍵の構成、または事前構成された root アカウントとパスワードの復旧については、このセクションを参照してください。	■ 38 ページの「ユーザー資格の管理」
Oracle ILOM にローカルユーザーアカウントを構成するための要件および手順については、このセクションを参照してください。	■ 46 ページの「ローカルユーザーアカウントの構成」
Oracle ILOM を Active Directory クライアントとして構成するための要件および手順については、このセクションを参照してください。	■ 49 ページの「Active Directory の構成」
Oracle ILOM を LDAP/SSL クライアントまたは LDAP クライアントとして構成するための要件および手順については、これらのセクションを参照してください。	■ 61 ページの「LDAP/SSL の構成」 ■ 73 ページの「LDAP の構成」
Oracle ILOM を RADIUS クライアントとして構成するための要件および手順については、このセクションを参照してください。	■ 77 ページの「RADIUS の構成」

関連情報

- 『SNMP、IPMI、CIM、WS-MAN プロトコル管理』の「SNMP を使用したユーザーアカウントの管理」
- 『Oracle ILOM 3.1 セキュリティガイド』の「Oracle ILOM 配備時のセキュリティ」
- [33 ページの「デフォルトで有効にされる事前構成されたユーザーアカウント」](#)

ユーザー資格の管理

Oracle ILOM へのユーザーのアクセスは、認証されているユーザーアカウントによって制御されます。Oracle ILOM の個別の機能を使用するための承認は、Oracle ILOM のユーザーアカウントに割り当てられている一連のユーザーの役割によって管理されます。

Oracle ILOM にユーザー資格を最初に設定する場合、システム管理者は、最大 10 個のローカルユーザーアカウントを構成するか、集中管理認証サービスを構成して追加のユーザーアカウントを許可することを選択できます。

Oracle ILOM でサポートされているユーザー資格の構成オプションの詳細、および Oracle ILOM でのユーザー資格の管理に関する一般的な詳細については、次のトピックを参照してください:

- 38 ページの「サポートされているユーザー認証の構成オプション」
- 40 ページの「割り当て可能な Oracle ILOM のユーザーの役割」
- 42 ページの「シングルサインオンサービス (デフォルトで有効)」
- 43 ページの「サポートされるユーザーセッションの最大数」
- 43 ページの「管理対象デバイスごとに表示可能なユーザーの認証されたセッション」
- 44 ページの「ローカルユーザーの SSH 鍵を使用した CLI での認証」
- 45 ページの「root アカウントのパスワードの復旧」
- 45 ページの「サポートされるファイル転送方式」

サポートされているユーザー認証の構成オプション

Oracle ILOM にユーザー認証を実装する方法を選択および構成する前に、次の情報を考慮してください。

表8 ユーザー認証の構成オプション

オプション	機能および考慮事項
ローカルユーザーアカウントの認証	<ul style="list-style-type: none"> ■ 最大 10 個の構成可能なユーザーアカウントが Oracle ILOM にローカルに格納されます。 ■ 配備と保守を迅速に行うために、2 つの事前構成されたユーザーアカウントが用意されています: root ユーザーアカウントおよび default ユーザーアカウント (33 ページの「デフォルトで有効にされる事前構成されたユーザーアカウント」を参照)。 ■ 個別の Oracle ILOM 機能に対して読み取り専用のアクセスや読み取りおよび書き込みのアクセスを許可する構成可能なユーザーの役割権限 (40 ページの「割り当て可能な Oracle ILOM のユーザーの役割」を参照)。 ■ ローカル管理およびリモート管理のためのセキュアなユーザー認証および承認。 ■ Oracle ILOM のユーザー資格は、SP および CMM ごとに別々に管理されます。 <p>Oracle ILOM でのローカルユーザーアカウントの構成の詳細は、46 ページの「ローカルユーザーアカウントの構成」を参照してください。</p>
認証ディレクトリサービス	<ul style="list-style-type: none"> ■ 10 個を超えるローカルユーザーアカウントを使用して、Oracle ILOM にユーザーがアクセスできます。 ■ システム管理者が、すべての Oracle ILOM インスタンス (ローカルネットワーク環境にあるすべての管理対象サーバー SP および CMM) のユーザー資格を集中的に作成および管理できます。 ■ 認証された Oracle ILOM ユーザーが、すべての Oracle ILOM インスタンスにアクセスできます。 ■ システム管理者が、Oracle ILOM の機能を使用するためのユーザー認証のルールを構成できます。
サポートされている認証サービス	
Active Directory	<p>Active Directory は、Microsoft Windows Server オペレーティングシステムとともに提供される分散サービスです。Active Directory サービスはデフォルトでセキュアになっています。</p> <p>Oracle ILOM が Active Directory 認証サービスを使用するように構成する方法の詳細は、49 ページの「Active Directory の構成」を参照してください。</p>
LDAP/SSL	<p>LDAP/SSL 認証サービスはデフォルトでセキュアになっています。セキュリティ証明書の使用を要求する厳格な認証モード (省略可能) をサポートします。</p> <p>Oracle ILOM を LDAP/SSL クライアントとして構成する方法の詳細は、61 ページの「LDAP/SSL の構成」を参照してください。</p>

表 8 ユーザー認証の構成オプション (続き)

オプション	機能および考慮事項
LDAP	<p>LDAP (v2) 認証サービスは、LDAP/SSL と比べるとセキュアではありません。このサービスは、セキュリティの制限を理解して受け入れる場合にのみ構成してください。</p> <p>Oracle ILOM を LDAP クライアントとして構成する方法の詳細は、73 ページの「LDAP の構成」を参照してください。</p>
RADIUS	<p>Remote Authentication Dial In User Service (RADIUS) は、クライアントサーバーモデルを使用して、ユーザー認証および承認を提供するネットワークプロトコルです。</p> <p>Oracle ILOM が RADIUS 認証サービスを使用するように構成する方法の詳細は、77 ページの「RADIUS の構成」を参照してください。</p>

割り当て可能な Oracle ILOM のユーザーの役割

システム管理者は、Oracle ILOM のユーザーアカウントの作成時に、Oracle ILOM の個別の機能および操作のためのアクセス権をユーザーに与える一連の権限を割り当てます。Oracle ILOM のこれらの権限は、ユーザーの役割と呼ばれます。

Oracle ILOM には、最大 6 個の定義済みのユーザーの役割があります。システム管理者は、役割を割り当てることにより、ユーザーに権限を付与したり、ユーザーから権限を取り消したりできます。

ユーザーの役割のほかに、Oracle ILOM は、Administrator、Operator、および Advanced Roles と呼ばれるユーザープロファイルを提供しています。これらのユーザープロファイルを使用すると、システム管理者は、単一のユーザーに複数の権限を一度に割り当てることができます。

システム管理者は、Administrator または Operator プロファイルを使用して、一連の定義済みのユーザー役割を単一のユーザーアカウントに割り当てることができます。または、システム管理者は、Advanced Roles プロファイルを構成して、6 個の定義済みのユーザーの役割を任意に単一のアカウントに割り当てることができます。

すべてのユーザー権限は、Web インタフェースまたは CLI からユーザーアカウントに割り当てることができます。単一のプロファイルまたはユーザーの役割によって付与される権限の説明は、次の表を参照してください:

- 表 9
- 表 10

表9 ユーザープロファイルによって付与される権限

Webのプロパティ	CLIのプロパティ	プロファイルによって付与される権限
Administrator	administrator	<p>Administrator (administrator) プロファイルには、次のユーザーの役割が事前定義されています。</p> <ul style="list-style-type: none"> ■ Admin (a) ■ User Management (u) ■ Console (c) ■ Reset and Host Control (r) ■ Read-Only (o) <p>各ユーザーの役割によって付与される権限については、表 10 を参照してください。</p>
Operator	operator	<p>Operator (operator) プロファイルには、次のユーザーの役割が事前定義されています。</p> <ul style="list-style-type: none"> ■ Console (c) ■ Reset and Host Control (r) ■ Read-Only (o) <p>各ユーザーの役割によって付与される権限については、表 10 を参照してください。</p>
Advanced Roles	a u c r o s	<p>Advanced Roles プロファイルオプションは、Web インタフェースからのみユーザーが構成できます。Advanced Roles プロファイルオプションを使用すると、システム管理者は、次の 6 個のユーザーの役割を任意に単一のユーザーアカウントに割り当てることができます。</p> <ul style="list-style-type: none"> ■ Admin (a) ■ User Management (u) ■ Console (c) ■ Reset and Host Control (r) ■ Read-Only (o) ■ Service (s) <p>注 - CLI では、同じ 6 個のユーザーの役割 (a u c r o s) を個別に単一のユーザーアカウントに割り当てることができます。</p> <p>各ユーザーの役割によって付与される権限については、表 10 を参照してください。</p>

表 10 個別のユーザーの役割によって付与される権限

ユーザーの役割	付与される権限
Admin (a)	<p>Admin (a) ユーザーの役割を有効にすると、すべての Oracle ILOM システム管理機能に対する読み取りおよび書き込み権限が付与されます。ただし、Admin (a) 役割で追加のユーザーの役割 (User Management (u)、Reset and Host Control (r)、Console (c)、および Service (s)) を有効にする必要がある機能は例外です。</p>

表 10 個別のユーザーの役割によって付与される権限 (続き)

ユーザーの役割	付与される権限
User Management (u)	User Management (u) ユーザーの役割を有効にすると、Oracle ILOM のすべてのユーザー管理認証機能に対する読み取りおよび書き込みのアクセス権が付与されます。
Console (c)	Console (c) ユーザーの役割を有効にすると、リモートコンソール管理機能(リモートコンソールのロックオプション、SP コンソール履歴ログオプション、Oracle ILOM リモートコンソールの起動と使用、および Oracle ILOM Storage Redirection CLI の起動と使用) を実行するための読み取りおよび書き込みのアクセス権が付与されます。
Reset and Host Control (r)	Reset and Host Control (r) ユーザーの役割を有効にすると、ホスト管理機能(ブートデバイス制御のホスト、診断ユーティリティーの実行と構成、SP のリセット、CMM のリセット、サブコンポーネントサービス処理、障害管理処理、SPARC TPM 管理処理、および SNMP MIB のダウンロード操作) を実行するための読み取りおよび書き込みのアクセス権が付与されます。
Read-Only (o)	Read-Only (o) ユーザーの役割は、Oracle ILOM のすべての構成プロパティの状態の表示、および個別のユーザーアカウントに割り当てられているアカウントパスワードプロパティおよびセッションタイムアウトプロパティの変更を行うための読み取り専用のアクセス権を付与します。
Service (s)	Services (s) ユーザーの役割を有効にすると、オンサイトサービスが必要な場合に Oracle のサービスエンジニアを補助するための読み取りおよび書き込みのアクセス権が付与されます。
a u c r o	これらすべてのユーザー役割の組み合わせ(aucro)を有効にすると、Oracle ILOM のバックアップおよび復元の構成機能を実行するための読み取りおよび書き込みのアクセス権が付与されます。

シングルサインオンサービス(デフォルトで有効)

Oracle ILOM のシングルサインオン(SSO)機能は、次を可能にする Oracle 専用のプロトコルサービスです:

- Oracle ILOM SP の Web インタフェースで認証されたユーザーがパスワードの再入力を要求されずに KVMS アプリケーション(Oracle ILOM リモートコンソールまたは Oracle ILOM Storage CLI Redirection) を起動する。
- Oracle ILOM CMM の Web インタフェースで認証されたユーザーがパスワードの再入力を要求されずにシャーシに取り付けられている個別の管理対象ブレードサーバーにナビゲートする。

Oracle ILOM の SSO サービスのプロパティの状態は、デフォルトで有効になっています。このプロパティの状態を変更する場合は、次の表を参照してください

ユーザーインタフェースの構成可能なターゲット:

- **CLI:** `/SP|CMM/services/`
- **Web:** 「ILOM Administration」 > 「User Management」 > 「User Accounts」 > 「Single Sign On」
- ユーザーの役割: **Admin (a)** (プロパティ変更に必要な)

プロパティ	デフォルト値	説明
シングルサインオン (<code>/sso state=</code>)	Enabled	<i>Enabled Disabled</i> 「SSO State」の CLI 構文: set /SP CMM/services/sso state=enabled disabled

サポートされるユーザーセッションの最大数

Oracle ILOM は、管理対象サーバー SP または CMM ごとに、最大 10 個のアクティブなユーザーセッションをサポートします。一部の SPARC システムでは、1 つの管理対象サーバー SP でアクティブなユーザーセッションが最大 5 つに制限されています。

注 - アクティブなユーザーセッションは、Oracle ILOM への次のいずれかの接続と考えることができます: シリアルコンソール、Secure Shell (SSH)、または Web インタフェース。

管理対象デバイスごとに表示可能なユーザーの認証されたセッション

システム管理者は、CLI または Web インタフェースを使用して Oracle ILOM SP または CMM にログインしているユーザーのリストを確認できます。単一の SP または CMM インスタンスのユーザーセッションのリストを表示する場合は、次の表を参照してください。

ユーザーインタフェースの構成可能なターゲット:

- **CLI:** `/SP|CMM/services/`
- **Web:** 「ILOM Administration」 > 「User Management」 > 「Active Sessions」
- ユーザーの役割: **Administrator (administrator)** プロファイル (`aucro`)

プロパティ	説明
Active Sessions (<code>sessions</code>)	単一の SP または CMM の Active Sessions の情報は、Oracle ILOM に現在ログインしている認証されたユーザーセッションを一覧表示します。 「Active Sessions」の CLI 構文: <ul style="list-style-type: none"> ■ show /SP CMM/sessions ■ show /SP CMM/sessionsn

ローカルユーザーのSSH鍵を使用したCLIでの認証

標準のユーザーパスワードを使用する代わりに、システム管理者は、生成された公開SSH鍵ファイルをユーザーアカウントに関連付けて、Secure Shellを使用してOracle ILOM CLIにアクセスすることができます。生成された公開SSH鍵ファイルをOracle ILOMアカウントに関連付けると、Oracle ILOMで自動スクリプトがSPコマンドをセキュアに実行できます。この場合、手動の介入、または平文のパスワードの埋め込みは必要ありません。

公開SSH鍵ファイルをOracle ILOMのユーザーアカウントに追加する前に、SSH接続ツール(ssh-keygenなど)を使用して非公開鍵および公開鍵のペアを最初に生成し、生成されたSSH鍵ファイルをリモートSSHシステムに格納する必要があります。

生成されたユーザーの公開SSH鍵ファイルをアップロードしてOracle ILOMのユーザーアカウントに追加する場合、およびユーザーの公開SSH鍵ファイルをOracle ILOMのユーザーアカウントから削除する場合は、次の表を参照してください。

表 11 ローカルユーザーアカウントごとの公開SSH鍵ファイルの追加または削除

プロパティ	説明
ユーザーインタフェースの構成可能なターゲット:	
<ul style="list-style-type: none"> ■ CLI: /SP CMM/services/ ■ Web: 「ILOM Administration」 > 「User Management」 > 「User Accounts」 > 「SSH Key」 ■ ユーザーの役割: 個人のSSH鍵の場合は Read-only (o)、ほかのユーザーのSSH鍵の場合は User Management (u) 	
Key Upload - File Transfer Options (set load_uri=)	<p><i>Browser TFTP SFTP SCP HTTP HTTPS Paste</i></p> <p>各ファイル転送方法の説明は、表 13を参照してください。</p>
Add SSH Key (/ssh/keys/1)	<p>「Add SSH Key」のCLI構文:</p> <pre>set /SP/users/user_account_name/ssh/keys/1 load_uri=transfer_method://username:password@ipaddress_or_hostnamedirectorypath/filename</pre> <p>例:</p> <pre>set /SP/users/adminuser/ssh/keys/1 load_uri=scp://adminuser:userpswd@1.2.3.4/keys/sshkey_1.pub</pre>
Delete SSH Key (clear action=true)	<p>「Delete SSH Key」のCLI構文:</p> <pre>set /SP CMM/users/user_account_name/ssh/keys/1 clear_action=true</pre> <p>公開SSH鍵をクリアーする場合は y を入力し、操作を取り消す場合は n を入力します。</p>
Save	<p>Web インタフェースのみ。「SSH Key」ダイアログ内のプロパティへの変更を適用するには、「Save」をクリックする必要があります。</p>

root アカウントのパスワードの復旧

必要な場合、システム管理者は、事前構成された Oracle ILOM のデフォルトのパスワードを使用して、事前構成された Oracle ILOM のローカルの root アカウントまたはローカルの root アカウントのパスワードを回復できます。復旧の手順については、次の表を参照してください。

表 12 事前構成された root アカウントまたは root アカウントのパスワードの回復 (CLI のみ)

前提条件	手順
<ul style="list-style-type: none"> ■ Oracle ILOM へのローカルのシリアル管理接続 ■ 「Physical Presence State」が有効にされている場合 (デフォルト) は、管理対象サーバーのある場所に実際にいること 	<ol style="list-style-type: none"> 1. Oracle ILOM に対してローカルのシリアル管理接続を確立し、default ユーザーアカウントを使用して Oracle ILOM にログインします。例: SUNSP-0000000000 login: default Press and release the physical presence button.Press return when this is completed... 2. サーバーのある場所に実際にいることを証明します。 サーバーのある場所にいることを証明する方法については、サーバーハードウェアのドキュメントを参照してください。 3. シリアルコンソールに戻り、Enter キーを押します。 パスワードの入力を求めるプロンプトが表示されます。 4. default ユーザーアカウントのパスワードを入力します: defaultpassword 5. アカウントのパスワードをリセットするか、root アカウントを作成し直します。 ユーザーアカウントまたはパスワードの作成および変更のトピックについては、この表の「関連情報」セクションを参照してください。 <p>関連情報</p> <ul style="list-style-type: none"> ■ 17 ページの「Oracle ILOM への専用のローカル管理接続の構成」 ■ (サーバーのある場所にいる) 121 ページの「システム識別情報の割り当て」 ■ 表 14 ■ 表 15

サポートされるファイル転送方式

Oracle ILOM は、ファイル (SSH 鍵、セキュリティ証明書など) を Oracle ILOM にアップロードする場合に、次の転送方式をサポートしています。

表 13 ファイル転送方式

ファイル転送方式	説明
ブラウザ	Browser ファイル転送方式は、Web インタフェースでのみ使用できます。この方式では、ローカルシステム、またはリモートのネットワーク共有に格納されているファイルを選択できます。

表 13 ファイル転送方式 (続き)

ファイル転送方式	説明
TFTP	TFTP ファイル転送方式では、指定されたファイルを Oracle ILOM にアップロードするために、TFTP ホスト名およびディレクトリパスを指定する必要があります。
FTP	FTP ファイル転送方式では、FTP ホストシステム名、FTP ホストのユーザー名とパスワード、および指定されたファイルをアップロードするためのディレクトリパスを指定する必要があります。
SFTP	SFTP ファイル転送方式では、SFTP ホストシステム名、SFTP ホストのユーザー名とパスワード、および指定されたファイルへのディレクトリパスを指定する必要があります。
SCP	SCP ファイル転送方式では、SCP ホストシステム名、SCP ホストのユーザー名とパスワード、および指定されたファイルへのディレクトリパスを指定する必要があります。
ポート 8899 を介した HTTP	HTTP ファイル転送方式では、HTTP ホストシステム名、HTTP ユーザー名とパスワード、および指定されたファイルへのディレクトリパスを指定する必要があります。
HTTPS	HTTPS ファイル転送方式では、HTTPS ホストシステム名、HTTP ホストのユーザー名とパスワード、および指定されたファイルへのディレクトリパスを指定する必要があります。
Paste	Paste ファイル転送方式は、Web インタフェースでのみ使用できます。この方式では、カスタム証明書ファイルを貼り付けるためのテキストボックスを使用します。

ローカルユーザーアカウントの構成

システム管理者は、Oracle ILOM で最大 10 個のローカルユーザーアカウントを作成および管理できます。ローカルユーザーアカウントを作成および管理するために Oracle ILOM で構成できるプロパティについては、次の表を参照してください:

- 表 14
- 表 15

表 14 ユーザーアカウントの作成とユーザーの役割の割り当て

プロパティ	説明
ユーザーインターフェースの構成可能なターゲット:	
<ul style="list-style-type: none"> ■ CLI: /SP CMM/users/ ■ Web: 「ILOM Administration」 > 「User Management」 > 「User Accounts」 ■ ユーザーの役割: User Management (u) (すべてのプロパティの変更が必要) 	
「Users」 > 「Add」	<code>user_name Password= Role=administrator operator advanced (a u c r o s)</code>
(<code>user_name password= role =</code>)	<p>「Add User」プロパティにユーザー名とパスワードを設定して、パスワードを確認し、ユーザーの役割を割り当てます。</p> <p>ユーザー名は、4-16文字で英字から始まる必要があります。スペースは使用できません。パスワードは、8-16文字である必要があります。大文字と小文字が区別されます。コロンとスペース以外の文字を使用します。</p> <p>CLIでユーザーを作成する場合の構文:</p> <pre>create /SP CMM/users/user_name_for_account password= password_for_account role=administrator operator a u c r o s</pre> <p>構文例:</p> <pre>create /SP/users user5 password=administrator role=aucr</pre> <p>注 - CLIを使用してユーザーアカウントを追加する場合、役割やパスワードのプロパティ値を指定する必要はありません。役割はデフォルトでRead Only (o)に設定され、CLIはパスワードの入力と確認を要求します。</p>
Save	<p>Web インタフェース - 「Add User」ダイアログ内のプロパティへの変更を適用するには、「Save」をクリックする必要があります。</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 9 ■ 表 15 ■ 表 6 ■ 表 12 ■ 44 ページの「ローカルユーザーの SSH 鍵を使用した CLI での認証」

表 15 ユーザーアカウントの表示、変更、または削除

プロパティ	説明
ユーザーインタフェースの構成可能なターゲット:	
<ul style="list-style-type: none"> ■ CLI: <code>/SP CMM/users/</code> ■ Web: 「ILOM Administration」 > 「User Management」 > 「User Accounts」 ■ ユーザーの役割: User Management (u) (すべてのプロパティの変更が必要) 	
Users (/users)	<p>Oracle ILOM に構成されているローカルユーザーアカウントを表示します。</p> <p>「View Users」の CLI 構文:</p> <p>show /SP CMM/users Example syntax:</p> <pre>show /SP/users</pre>
「Users」 > 「Edit」 (/user_name password= role=)	<p>Password=<code>user_configurable role=administrator operator advanced (a u c r o s)</code></p> <p>パスワードおよびユーザーの役割の該当する「User」プロパティを編集します。パスワードは、8 - 16 文字である必要があり、大文字と小文字が区別されます。コロンとスペース以外の文字を使用します。事前構成された root ユーザーのユーザーの役割は変更できません。</p> <p>Web インタフェース - 「Save」をクリックして、「Edit User」ダイアログで行なった変更を適用します。</p> <p>CLI でユーザーアカウントを編集する場合の構文:</p> <pre>set /SP CMM/users user_name password=assign_new_password role=administrator operator a u c r o s</pre> <p>構文の例: <code>set /SP/users user5 password=administrator role=auco</code></p>
「Users」 > 「Delete」 (/user_name)	<p>削除するユーザーアカウントの名前を指定します。プロンプトが表示されたら、操作を確認します。</p> <p>「Delete User Account」の CLI 構文:</p> <pre>delete /SP CMM/users/user_name</pre> <p>構文の例:</p> <pre>delete /SP/users/user5</pre>
<p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 9 ■ 表 14 ■ 表 12 	

Active Directory の構成

システム管理者は、必要に応じて、Microsoft Windows Active Directory サービスを使用するように Oracle ILOM を構成し、Oracle ILOM のユーザーを認証したり、Oracle ILOM の機能を使用するためのユーザー承認のレベルを定義したりできます。このサービスは、ユーザーに割り当てられているパスワードを使用して Active Directory ユーザーを認証するクライアントサーバー型のクエリーモデルに基づいています。

Oracle ILOM の Active Directory サービスの状態プロパティは、デフォルトで無効になっています。Active Directory サービスの状態を有効にして、Oracle ILOM を Active Directory クライアントとして構成する場合は、次の表を参照してください:

- [表 16](#)
- [表 17](#)
- [表 18](#)
- [表 19](#)
- [表 20](#)
- [表 21](#)
- [表 22](#)

表 16 Active Directory 認証の有効化

ユーザーインタフェースの構成可能なターゲット:

- **CLI:** `/SP|CMM/clients/activedirectory`
- **Web:** 「ILOM Administration」 > 「User Management」 > 「Active Directory」 > 「Settings」
- ユーザーの役割: **User Management (u)** (すべてのプロパティの変更が必要)
- **前提条件:** Oracle ILOM を Active Directory クライアントとして構成する前に、Active Directory サーバーにユーザーまたはユーザーグループを構成する必要があります。

プロパティ	デフォルト値	説明
State (state=)	Disabled	<i>Disabled Enabled</i> Oracle ILOM を Active Directory クライアントとして構成するには、「State」プロパティを「Enabled」に設定します。 「State」プロパティが有効で、「Strict Certificate Mode」プロパティが無効である場合、セキュアなチャネルを使用した Oracle ILOM では、ユーザーの認証時に Active Directory サービス証明書に対していくらかの検証が行われます。 「State」プロパティおよび「Strict Certificate Mode」プロパティの両方が有効である場合、セキュアなチャネルを使用した Oracle ILOM では、ユーザーの認証時に Active Directory サービス証明書のデジタル署名が完全に検証されます。 「State」の CLI 構文: set /SP CMM/clients/activedirectory/ state=disabled enabled

表 16 Active Directory 認証の有効化 (続き)

ユーザーインターフェースの構成可能なターゲット:

- **CLI:** `/SP|CMM/clients/activedirectory`
- **Web:** 「ILOM Administration」 > 「User Management」 > 「Active Directory」 > 「Settings」
- ユーザーの役割: **User Management (u)** (すべてのプロパティの変更が必要)
- **前提条件:** Oracle ILOM を Active Directory クライアントとして構成する前に、Active Directory サーバーにユーザーまたはユーザーグループを構成する必要があります。

プロパティ	デフォルト値	説明
Roles (defaultrole=)	None (server authorization)	<p><i>Administrator Operator Advanced None (server authorization)</i></p> <p>Active Directory で認証されたユーザーがアクセスできる Oracle ILOM の機能を定義するには、デフォルトの「Role」プロパティを、受け入れられる 4 つのプロパティ値のいずれかに設定します: Administrator (a u c r o), Operator (c r o), Advanced (a u c r o s), または None (server authorization)。</p> <p>デフォルトの「Role」プロパティを Oracle ILOM のユーザーの役割に設定すると、Oracle ILOM の機能を使用するための承認レベルは、構成されている Oracle ILOM のユーザーの役割によって付与される権限で決定されます。割り当てられる権限については、下の「関連情報」セクションに示されているユーザーの役割およびユーザープロファイルのトピックを参照してください。</p> <p>「Role」プロパティが「None (server authorization)」に設定されており、Oracle ILOM が Active Directory のグループを使用するように構成されている場合、Oracle ILOM の機能を使用するための承認レベルは、Active Directory のグループによって決定されます。構成の詳細は、下の「関連情報」セクションに示されている Active Directory のグループのトピックを参照してください。</p> <p>「Roles」の CLI 構文:</p> <pre>set /SP CMM/clients/activedirectory/ defaultrole=adminstrator operator a u c r o s none</pre> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 9 ■ 表 9 ■ 表 18
アドレス (address=)	0.0.0.0	<p><i>IP address DNS host name (Active Directory Server)</i></p> <p>Active Directory サーバーのネットワークアドレスを構成するには、「Address」プロパティに Active Directory サーバーの IP アドレスまたは DNS ホスト名を設定します。DNS ホスト名を使用する場合は、Oracle ILOM の DNS 構成プロパティを適切に構成して動作可能にする必要があります。</p> <p>「Address」の CLI 構文:</p> <pre>set /SP CMM/clients/activedirectory/ address=active_directory_server ip_address active_directory_server_dns_host_name</pre> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 44

表 16 Active Directory 認証の有効化 (続き)

プロパティ	デフォルト値	説明
ポート (port=)	0、(自動選択)	<p><i>0 Auto-select Non-standard TCP port</i></p> <p>Oracle ILOM は、標準の TCP ポートを使用して Active Directory サーバーと通信します。</p> <p>「Port」の自動選択のプロパティを有効にすると、「Port」番号はデフォルトで 0 に設定されます。「Port」の自動選択のプロパティを無効にすると、Web インタフェースの「Port」番号プロパティをユーザーが構成できるようになります。</p> <p>「Port」プロパティは、Oracle ILOM で標準以外の TCP ポートを使用する必要がある例外的な場合に構成できます。</p> <p>「Port」の CLI 構文:</p> <pre>set /SP CMM/clients/activedirectory/ port=number</pre>
Timeout (timeout=)	4 秒	<p><i>4 user-specified</i></p> <p>「Timeout」プロパティは、個々のトランザクションが完了するまで待機する秒数を指定します。トランザクションの数は構成に応じて異なる場合があるため、この値は完了したすべてのトランザクションの合計時間を表すわけではありません。</p> <p>「Timeout」プロパティは、デフォルトで 4 秒に設定されます。このプロパティ値は、必要に応じて、Active Directory サーバーが通信不可能である場合または応答しない場合の応答時間を微調整するときに調整します。</p> <p>「Timeout」の CLI 構文:</p> <pre>set /SP CMM/clients/activedirectory/ timeout=number_of_seconds</pre>

表 16 Active Directory 認証の有効化 (続き)

プロパティ	デフォルト値	説明
Strict Certificate Mode (strictcertmode=)	Disabled	<p><i>Disabled Enabled</i></p> <p>「Strict Certificate Mode」プロパティを有効にすると、Oracle ILOM は、認証時に Active Directory 証明書のデジタル署名を完全に検証します。</p> <p>「Strict Certificate Mode」プロパティを無効にすると、Oracle ILOM は、セキュアなチャネルを使用した認証時にサーバー証明書に対して限定的な検証を行います。</p> <p>注意 - 「Strict Certificate Mode」プロパティを有効にする前に、Active Directory のサーバー証明書をロードする必要があります。</p> <p>「Strict Mode Certificate」の CLI 構文:</p> <pre>set /SP CMM clients/activedirectory/ strictcertmode=disabled enabled</pre> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 17
DNS Locator Mode (/dnslocatorqueries)	Disabled	<p><i>Disabled Enabled</i></p> <p>DNS Locator Queries を使用して Active Directory サーバーのリストを取得するように Oracle ILOM を構成するには、「DNS Locator Mode」プロパティを有効に設定します。</p> <p>「DNS Locator Mode」の CLI 構文:</p> <pre>set /SP CMM clients/activedirectory/ dnslocatorqueries/1=disabled enabled</pre> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 21

表 16 Active Directory 認証の有効化 (続き)

プロパティ	デフォルト値	説明
ユーザーインタフェースの構成可能なターゲット: ■ CLI: <code>/SP CMM/clients/activedirectory</code> ■ Web: 「ILOM Administration」 > 「User Management」 > 「Active Directory」 > 「Settings」 ■ ユーザーの役割: User Management (u) (すべてのプロパティの変更が必要) ■ 前提条件: Oracle ILOM を Active Directory クライアントとして構成する前に、Active Directory サーバーにユーザーまたはユーザーグループを構成する必要があります。		
Expanded Search Mode (expsearchmode=)	Disabled	<i>Enabled Enabled</i> Active Directory のユーザーエントリを検索するときに追加の検索オプションを使用するように Oracle ILOM を構成するには、「Expanded Search Mode」プロパティを Enabled に設定します。 「Expanded Search Mode」プロパティを無効にすると、Oracle ILOM は userPrincipleName を使用してユーザーエントリを検索します。この場合、userPrincipleName に完全修飾ドメイン名 (FQDN) の接尾辞が付けられている必要があります。 「Expanded Search Mode」の CLI 構文: <pre>set /SP CMM/clients/activedirectory/ expsearchmode=disabled enabled</pre>
Strict Credential Error Mode (strictcredentialerrormode=)	Disabled	<i>Disabled Enabled</i> 「Strict Credential Error Mode」プロパティが有効で、ユーザー資格エラーがサーバーから報告された場合、Oracle ILOM はこれらのユーザー資格で失敗します。 「Strict Credential Error Mode」プロパティを無効にすると、Oracle ILOM は認証のためにユーザー資格をほかの Active Directory サーバー (代替サーバーとして構成されている、または DNS Locator Queries によって見つかった) に提示します。 「Strict Certificate Mode」を構成する場合の CLI 構文: <pre>set /SP CMM/clients/activedirectory/ strictcredentialerrormode=disabled enabled</pre> 関連情報: ■ 表 17
Log Detail (logdetail=)	なし	<i>None High Medium Low Trace</i> Oracle ILOM のイベントログに記録される Active Directory イベントの診断情報の量を指定するには、「Log Detail」プロパティを、受け入れられるいずれかのプロパティ値に設定します。 「Log Detail」を構成する場合の CLI 構文: <pre>set /SP CMM/clients/activedirectory/ logdetail=none high medium low trace</pre>
Save		Web インタフェース - Active Directory の「Settings」ページ内のプロパティへの変更を適用するには、「Save」をクリックする必要があります。

表 17 Active Directory 証明書ファイルのアップロードまたは削除

プロパティ	デフォルト値	説明
ユーザーインタフェースの構成可能なターゲット:		
<ul style="list-style-type: none"> ■ CLI: <code>/SP CMM/clients/activedirectory/cert</code> ■ Web: 「ILOM Administration」 > 「User Management」 > 「Active Directory」 > 「Certificate Information」 ■ ユーザーの役割: (u) User Management (すべてのプロパティの変更が必要) 		
Certificate File Status (certstatus=)	読み取り専用	<p><code>Certificate present</code> <code>Certificate not present</code></p> <p>「Certificate File Status」プロパティは、Active Directory 証明書が Oracle ILOM にアップロードされているかどうかを示します。</p> <p>注意 - 「Strict Certificate Mode」プロパティを有効にする前に、Active Directory 証明書ファイルを Oracle ILOM にアップロードする必要があります。</p> <p>「Certificate Show」の CLI 構文:</p> <pre>show /SP CMM/clients/activedirectory/cert</pre>
ファイル転送方式	Browser (Web インタフェースのみ)	<p><code>Browser</code> <code>TFTP</code> <code>FTP</code> <code>SCP</code> <code>Paste</code></p> <p>各ファイル転送方式の詳細は、表 13 を参照してください。</p>
Load Certificate (load_uri=)		<p>Web インタフェース - 「Load Certificate」ボタンをクリックして、「File Transfer Method」プロパティに定義されている Active Directory 証明書ファイルをアップロードします。</p> <p>「Certificate Load」の CLI 構文:</p> <pre>load_uri=file_transfer_method://host_address/file_path/filename</pre>
Remove Certificate (clear_action=true)		<p>Web インタフェース - 「Remove Certificate」ボタンをクリックして、Oracle ILOM に現在格納されている Active Directory 証明書ファイルを削除します。プロンプトが表示されたら、削除する場合は <code>y</code> (はい)、または操作を取り消す場合は <code>n</code> (いいえ) を入力します。</p> <p>「Remove Certificate」の CLI 構文:</p> <pre>set /SP CMM/clients/activedirectory/cert clear_action=true</pre> <p>- または -</p> <pre>reset /SP CMM/clients/activedirectory/cert</pre> <p>確認のメッセージが表示されたら、<code>y</code> と入力して削除するか、<code>n</code> と入力して操作を取り消します。</p>

表 18 Active Directory グループの構成 (省略可能)

プロパティ	説明
ユーザーインタフェースの構成可能なターゲット:	
<ul style="list-style-type: none"> ■ CLI: /SP CMM/clients/activedirectory ■ Web: 「ILOM Administration」 > 「User Management」 > 「Active Directory」 > 「(Name) Groups」 ■ ユーザーの役割: (u) User Management (すべてのプロパティの変更が必要) ■ 前提条件: Oracle ILOM に Active Directory グループを設定する前に、Active Directory グループが Active Directory サーバー上に存在し、メンバーが割り当てられている必要があります。 	
Admin Groups (/admingroups/ 1 2 3 4 5)	<p>システム管理者は、必要に応じて、ユーザー承認のために、Oracle ILOM の「Role」プロパティの代わりに「Admin Group」プロパティを構成できます。</p> <p>Oracle ILOM は、最大 5 個の「Admin Groups」を構成することをサポートしています。Oracle ILOM で「Admin Group」プロパティを有効にすると、ユーザーのグループメンバーシップに、admin 表での定義に一致するグループがあるかどうかチェックされます。一致がある場合、そのユーザーに Administrator レベルのアクセス権が付与されます。</p> <p>注 - Oracle ILOM は、構成された各グループ表で見つかった一致するグループ (Operator, Administrator, または Custom) に基づいて、1 つ以上の承認レベルをグループのメンバーに付与します。</p> <p>次の取り得る値を使用して、Oracle ILOM の各 Active Directory Admin Group に構成プロパティを設定します:</p> <ul style="list-style-type: none"> ■ DN 形式: CN=admingroup,OU=groups,DC=domain,DC=company,DC=com ■ NT ドメイン形式: domain\admingroup ■ 完全ドメイン形式: DC=domain,DC=company,DC=com\admingroup ■ 単純な名前の形式: admingroup (最大 128 文字) <p>「Admin Groups」を構成する場合の CLI 構文:</p> <pre>set /SP CMM/clients/activedirectory/admingroups/n name=string</pre> <p>構文例:</p> <pre>set /SP/clients/activedirectory/admingroups/1/ name=CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com</pre> <p>Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle, DC=com'</p>

表 18 Active Directory グループの構成 (省略可能) (続き)

ユーザーインタフェースの構成可能なターゲット:

- **CLI:** `/SP|CMM/clients/activedirectory`
- **Web:** 「ILOM Administration」 > 「User Management」 > 「Active Directory」 > 「(Name Groups)」
- ユーザーの役割: (u) User Management (すべてのプロパティの変更が必要)
- 前提条件: Oracle ILOM に Activity Directory グループを設定する前に、Active Directory グループが Active Directory サーバー上に存在し、メンバーが割り当てられている必要があります。

プロパティ	説明
Operator Groups (/operatorgroups/ 1 2 3 4 5)	<p>システム管理者は、必要に応じて、ユーザー承認のために、Oracle ILOM の「Role」プロパティの代わりに「Operator Group」プロパティを構成できます。</p> <p>Oracle ILOM は、最大 5 個の Operator Groups を構成することをサポートしています。Oracle ILOM で「Operator Group」プロパティを有効にすると、ユーザーのグループメンバーシップに、operator 表での定義に一致するグループがあるかどうかチェックされます。一致がある場合は、そのユーザーに Operator レベルのアクセス権が付与されます。</p> <p>注 - Oracle ILOM は、構成された各グループ表で見つかった一致するグループ (Operator、Administrator、または Custom) に基づいて、1 つ以上の承認レベルをグループのメンバーに付与します。</p> <p>次の取り得る値を使用して、Oracle ILOM の各 Operator Group に構成プロパティを設定します:</p> <ul style="list-style-type: none"> ■ DN 形式: <code>CN=operatorgroup,OU=groups,DC=domain,DC=company,DC=com</code> ■ NT ドメイン形式: <code>domain\operatorgroup</code> ■ 完全ドメイン形式: <code>DC=domain,DC=company,DC=com\operatorgroup</code> ■ 単純な名前の形式: <code>operatorgroup</code> (最大 128 文字) <p>「Operator Groups」を構成する場合の CLI 構文:</p> <pre>set /SP CMM/clients/activedirectory/operatorgroups/n name=string</pre> <p>構文例:</p> <pre>set /SP/clients/activedirectory/operatorgroups/1 name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC= com'</pre>

表 18 Active Directory グループの構成 (省略可能) (続き)

プロパティ	説明
ユーザーインターフェースの構成可能なターゲット:	<ul style="list-style-type: none"> ■ CLI: <code>/SP CMM/clients/activedirectory</code> ■ Web: 「ILOM Administration」 > 「User Management」 > 「Active Directory」 > 「(Name) Groups」 ■ ユーザーの役割: (u) User Management (すべてのプロパティの変更が必要) ■ 前提条件: Oracle ILOM に Activity Directory グループを設定する前に、Active Directory グループが Active Directory サーバー上に存在し、メンバーが割り当てられている必要があります。
Custom Groups (/customgroups/ 1 2 3 4 5)	<p>システム管理者は、必要に応じて、ユーザー承認のために、Oracle ILOM に最大 5 個の「Custom Group」プロパティを構成できます。Oracle ILOM は、Custom Group のメンバーであるユーザーを認証する場合、「Custom Group」プロパティを使用して該当するユーザーの役割を判別して割り当てます。</p> <p>Oracle ILOM で「Custom Groups」を使用可能にする場合は、「Roles」プロパティおよび「Custom Groups」プロパティの両方を構成する必要があります。「Roles」の構成プロパティの詳細は、表 16 の「Roles」プロパティを参照してください。</p> <p>注 - Oracle ILOM は、構成された各グループ表で見つかった一致するグループ (Operator, Administrator, または Custom) に基づいて、1 つ以上の承認レベルをグループのメンバーに付与します。</p> <p>次の取り得る値を使用して、Oracle ILOM の各 Custom Group に構成プロパティを設定します:</p> <ul style="list-style-type: none"> ■ ユーザーの役割: <code>administrator operator advanced</code> (a u c r o s) ■ DN 形式: <code>CN=customgroup,OU=groups,DC=domain,DC=company,DC=com</code> ■ NT ドメイン形式: <code>domain\customgroup</code> ■ 完全ドメイン形式: <code>DC=domain,DC=company,DC=com\customgroup</code> ■ 単純な名前の形式: <code>customgroup</code> (最大 128 文字) <p>「Custom Groups」を構成する場合の CLI 構文:</p> <pre>set /SP CMM/clients/activedirectory/customgroups/n name=string roles=administrator operator a u c r o s</pre> <p>構文例:</p> <pre>set /SP/clients/activedirectory/customgroups/1 name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com roles=au</pre> <p>Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com' roles' to 'au'</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 40 ページの「割り当て可能な Oracle ILOM のユーザーの役割」
Save	<p>Web インタフェース - 「Admin Group」、「Operator Group」、または「Custom Group」ダイアログのプロパティへの変更を適用するには、「Save」をクリックする必要があります。</p>

表 19 Active Directory ユーザードメインの構成

プロパティ	説明
User Domains (1 2 3 4 5)	<p>システム管理者は、必要に応じて、最大 5 個のユーザードメインを構成できます。1 つ以上のユーザードメインを定義すると、Oracle ILOM は、Active Directory ユーザーを認証できるまで、これらのプロパティを順番に使用します。</p> <p>次の取り得る値を使用して、Oracle ILOM の各ユーザードメインに構成プロパティを設定します:</p> <ul style="list-style-type: none"> ■ UPN 形式: <USERNAME>@domain.company.com ■ DN 形式: CN=<USERNAME>,CN=Users,DC=domain,DC=company,DC=com <p>注 - <USERNAME> をリテラルとして使用できます。<USERNAME> をリテラルとして使用すると、Oracle ILOM はユーザー認証時に <USERNAME> を入力された現在のログイン名に置き換えます。</p> <p>「User Domains」の CLI 構文:</p> <pre>set /SP/CMM/clients/activedirectory/userdomains/n name=string</pre> <p>例 1: name=CN=<USERNAME></p> <pre>set /SP/clients/activedirectory/userdomains/1/name=CN<USERNAME>, OU=Groups, DC=sales, DC-Oracle, DC=com</pre> <p>Set 'name' to 'CN=<USERNAME>,OU=Groups,DC=sales,DC=oracle,DC=com'</p> <p>例 2: name=CN=spSuperAdmin</p> <pre>set /SP/clients/activedirectory/userdomains/1/ name=CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com</pre> <p>Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle, DC=com'</p>
Save	<p>Web インタフェース - Active Directory の「User Domains」ダイアログ内のプロパティへの変更を適用するには、「Save」をクリックする必要があります。</p>

表 20 Active Directory 代替サーバーの構成 (省略可能)

プロパティ	説明
Alternate Servers (1 2 3 4 5)	<p>Oracle ILOM では、システム管理者は、最大 5 個の Active Directory 代替サーバーを構成できます。</p> <p>代替サーバーを使用すると認証が冗長化され、ドメインを分離する必要がある場合に別の Active Directory サーバーを選択できます。</p> <p>各 Active Directory 代替サーバーは、プライマリ Active Directory サーバーと同じユーザー承認のルールおよび要件を使用します。たとえば、Oracle ILOM は「Roles」プロパティに構成されているユーザーの役割を使用してユーザーを認証します。ただし、「Roles」プロパティが構成されていない場合、Oracle ILOM は認証サーバーに対して該当する承認の役割を問い合わせます。</p> <p>各 Active Directory 代替サーバーは、プロパティ (ネットワークアドレス、ポート、証明書ステータス)、および証明書をアップロードおよび削除するためのコマンドをそれぞれ保持しています。Active Directory 証明書が提示されていないが必要な場合、Oracle ILOM は最上位のプライマリ Active Directory サーバーの証明書を使用します。</p> <p>注 - 代替サーバーが認証を冗長化するために使用されている場合は、「Strict Credential Error Mode」のプロパティを必要に応じて有効にすることができます。ただし、代替サーバーが結合されていないドメインを接続するために使用されている場合は、「Strict Credential Error Mode」のプロパティを無効にするようにしてください。「Strict Credential Error Mode」の構成プロパティについては、表 16 を参照してください。</p> <p>「Alternate Server」のアドレスとポートの CLI 構文:</p> <pre>set /SP CMM/clients/activedirectory/alternateservers/n address=string port=string</pre> <p>「Alternate Server」の証明書の CLI 構文:</p> <pre>show /SP CMM/clients/activedirectory/alternateservers/n/cert</pre> <pre>load_uri=file_transfer_method://host_address/file_path/filename</pre> <pre>set /SP CMM/clients/activedirectory/alternateservers/n/cert clear_action=true</pre>
Save	<p>Web インタフェース - Active Directory の「Alternate Servers」ダイアログ内のプロパティへの変更を適用するには、「Save」をクリックする必要があります。</p>

表 21 DNS Locator Queries の編集 (省略可能)

プロパティ	デフォルト値	説明
ユーザーインタフェースの構成可能なターゲット:		
<ul style="list-style-type: none"> ■ CLI: <code>/SP CMM/clients/activedirectory/dnslocatorqueries</code> ■ Web: 「ILOM Administration」 > 「User Management」 > 「Active Directory」 > 「DNS Locator Queries」 ■ ユーザーの役割: User Management (u) (すべてのプロパティの変更で必要) 		
DNS Locator Queries (/1)	<code>_ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269></code>	Oracle ILOM では、最大 5 個の DNS Locator Queries を構成できます。 DNS ロケータクエリーは、名前付き DNS サービスおよびそのポート ID を特定します。レコードには通常ポート ID が含まれますが、 <code><PORT:636></code> という形式でオーバーライドできます。また、 <code><DOMAIN></code> 置換マーカーを使用すると、特定のドメインの名前付き DNS サービスをオーバーライドできます。
DNS Locator Queries (/2)	<code>_ldap._tcp.dc._msdcs.<DOMAIN>.<PORT:636></code>	「DNS Locator Queries」を表示および編集する場合の CLI 構文: show /SP CMM/clients/activedirectory/dnslocatorqueries/1 set /SP CMM/clients/activedirectory/dnslocatorqueries/1 service = string DNS Locator Queries の構文の例 <code>service = string</code> <code>service =_ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:nnnn></code>
Save		Web インタフェース - Active Directory の「DNS Locator Queries」ダイアログ内のプロパティへの変更を適用するには、「Save」をクリックする必要があります。

表 22 Active Directory の認証をトラブルシューティングするためのガイドライン

Oracle ILOM での Active Directory の認証および承認の試行をトラブルシューティングする場合は、次のガイドラインを参照してください。
<ul style="list-style-type: none"> ■ Active Directory の認証をテストおよび診断するには、次の手順に従います: <ol style="list-style-type: none"> 1: Active Directory の「Log Details」プロパティを <code>trace</code> に設定します。 2: イベントを生成するために Oracle ILOM に対して認証を試行します。 3: Oracle ILOM のイベントログファイルを確認します。 ■ Active Directory サーバーに構成されているユーザーグループおよびユーザードメインが、Oracle ILOM に構成されているユーザーグループおよびユーザードメインと一致することを確認します。 ■ Oracle ILOM の Active Directory クライアントは、クロック設定を管理しません。Oracle ILOM のクロック設定は、手動で、または NTP サーバーを使用して構成できます。 注 - Oracle ILOM のクロック設定を NTP サーバーを使用して構成した場合、Oracle ILOM は、NTP デーモンを開始する前に、NTP サーバーを使用して <code>ntpdate</code> を実行します。

表 22 Active Directory の認証をトラブルシューティングするためのガイドライン (続き)

関連情報:

- [表 16](#)
 - 『ユーザーズガイド』の「Oracle ILOM のログエントリの管理」
 - [122 ページ](#)の「SP または CMM クロックのプロパティの設定」
-

LDAP/SSL の構成

システム管理者は、必要に応じて、LDAP/SSL ディレクトリサービスを使用するように Oracle ILOM を構成し、Oracle ILOM のユーザーを認証したり、Oracle ILOM の機能を使用するためのユーザー承認のレベルを定義したりできます。

Oracle ILOM の LDAP/SSL サービスの状態プロパティは、デフォルトで無効になっています。LDAP/SSL サービスの状態を有効にして、Oracle ILOM を LDAP/SSL クライアントとして構成する場合は、次の表を参照してください:

- [表 23](#)
- [表 24](#)
- [表 25](#)
- [表 26](#)
- [表 27](#)
- [表 28](#)

表 23 LDAP/SSL 認証の有効化

ユーザーインターフェースの構成可能なターゲット:

- **CLI:** `/SP|CMM/clients/ldapssl/`
- **Web:** 「ILOM Administration」 > 「User Management」 > 「LDAP/SSL」 > 「Settings」
- **ユーザーの役割:** User Management (u) (すべてのプロパティの変更が必要)
- **前提条件:** Oracle ILOM を構成する前に、LDAP/SSL サーバーにユーザーまたはユーザーグループを構成する必要があります。

プロパティ	デフォルト値	説明
State (state=)	Disabled	<p><i>Disabled Enabled</i></p> <p>LDAP/SSL 認証および承認ディレクトリサービスを使用するように Oracle ILOM を構成するには、「State」プロパティを Enabled に設定します。</p> <p>「State」プロパティを Disabled にすると、Oracle ILOM はユーザー認証および承認レベルの処理に LDAP/SSL サービスを使用しなくなります。</p> <p>「State」プロパティが有効で、「Strict Certificate Mode」プロパティが無効である場合、セキュアなチャネルを使用した Oracle ILOM では、ユーザーの認証時に LDAP/SSL サービス証明書に対して限定的な検証が行われます。</p> <p>「State」プロパティおよび「Strict Certificate Mode」プロパティが両方とも有効である場合、セキュアなチャネルを使用した Oracle ILOM では、ユーザーの認証時に LDAP/SSL サービス証明書のデジタル署名が完全に検証されます。</p> <p>「State」の CLI 構文:</p> <pre>set /SP CMM/clients/ldapssl/ state=disabled enabled</pre>

表 23 LDAP/SSL 認証の有効化 (続き)

プロパティ	デフォルト値	説明
Roles (defaultrole=)	None (server authorization)	<p><i>Administrator Operator Advanced None</i> (server authorization)</p> <p>LDAP/SSL で認証されたユーザーがアクセスできる Oracle ILOM の機能を定義するには、デフォルトの「Roles」プロパティを、受け入れられる 4 つのプロパティ値のいずれかに設定します: Administrator (a u c r o), Operator (c r o), Advanced (a u c r o s), または None (server authorization)。</p> <p>デフォルトの「Roles」プロパティを Oracle ILOM のユーザーの役割に設定すると、Oracle ILOM の機能を使用するための承認レベルは、Oracle ILOM のユーザーの役割によって付与されるユーザー権限で決定されます。割り当てられる権限については、下の「関連情報」セクションに示されているユーザーの役割およびユーザープロファイルの表を参照してください。</p> <p>デフォルトの「Roles」プロパティが「None (server authorization)」に設定されていて、Oracle ILOM が LDAP/SSL のグループを使用するように構成されている場合、Oracle ILOM の機能を使用するための承認レベルは、LDAP/SSL のグループによって決定されます。LDAP/SSL の構成の詳細は、下の「関連情報」セクションに示されている LDAP/SSL のグループを説明した表を参照してください。</p> <p>「Roles」の CLI 構文:</p> <pre>set /SP CMM clients/ldapssl/ defaultrole=adminstrator operator a u c r o s none</pre> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 9 ■ 表 10 ■ 表 25
アドレス (address=)	0.0.0.0	<p><i>IP address DNS host name</i> (Active Directory Server)</p> <p>LDAP/SSL サーバーのネットワークアドレスを構成するには、「Address」プロパティに LDAP/SSL の IP アドレスまたは DNS ホスト名を指定します。DNS ホスト名を使用する場合は、Oracle ILOM の DNS 構成プロパティを適切に構成して動作可能にする必要があります。</p> <p>「Address」の CLI 構文:</p> <pre>set /SP CMM clients/ldapssl/ address=LDAP/SSL_server ip_address active_directory_server_dns_host_name</pre> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 44

表 23 LDAP/SSL 認証の有効化 (続き)

ユーザーインターフェースの構成可能なターゲット:

- CLI: `/SP|CMM/clients/ldapssl/`
- Web: 「ILOM Administration」 > 「User Management」 > 「LDAP/SSL」 > 「Settings」
- ユーザーの役割: User Management (u) (すべてのプロパティの変更が必要)
- 前提条件: Oracle ILOM を構成する前に、LDAP/SSL サーバーにユーザーまたはユーザーグループを構成する必要があります。

プロパティ	デフォルト値	説明
ポート (port=)	0、自動選択	<p><code>0 Auto-select Non-standard TCP port</code></p> <p>Oracle ILOM は、標準の TCP ポートを使用して LDAP/SSL サーバーと通信します。</p> <p>「Port」の自動選択のプロパティを有効にすると、「Port」番号はデフォルトで 0 に設定されます。</p> <p>「Port」の自動選択のプロパティを無効にすると、Web インタフェースの「Port」番号プロパティをユーザーが構成できるようになります。</p> <p>「Port」プロパティは、Oracle ILOM で標準以外の TCP ポートを使用する必要がある例外的な場合に構成できます。</p> <p>「Port」の CLI 構文:</p> <pre>set /SP CMM/clients/ldapssl/ port=number</pre>
Timeout (timeout=)	4 秒	<p><code>4 user-specified</code></p> <p>「Timeout」プロパティは、デフォルトで 4 秒に設定されます。このプロパティ値は、必要に応じて、LDAP/SSL サーバーが通信不可能である場合または応答しない場合の応答時間を微調整するために調整します。</p> <p>「Timeout」プロパティは、個々のトランザクションが完了するまで待機する秒数を指定します。トランザクションの数は構成に応じて異なる場合がありますため、この値は完了したすべてのトランザクションの合計時間を表すわけではありません。</p> <p>「Timeout」の CLI 構文:</p> <pre>set /SP CMM/clients/ldapssl/ timeout=number_of_seconds</pre>

表 23 LDAP/SSL 認証の有効化 (続き)

ユーザーインタフェースの構成可能なターゲット:

- **CLI:** `/SP|CMM/clients/ldapssl/`
- **Web:** 「ILOM Administration」 > 「User Management」 > 「LDAP/SSL」 > 「Settings」
- ユーザーの役割: **User Management (u)** (すべてのプロパティの変更が必要)
- 前提条件: Oracle ILOM を構成する前に、LDAP/SSL サーバーにユーザーまたはユーザーグループを構成する必要があります。

プロパティ	デフォルト値	説明
Strict Certificate Mode (strictcertmode=)	Disabled	<p><i>Disabled Enabled</i></p> <p>有効にすると、Oracle ILOM は、セキュアなチャネルを使用した認証時に LDAP/SSL 証明書の署名を完全に検証します。</p> <p>無効にすると、Oracle ILOM は、セキュアなチャネルを使用した認証時にサーバー証明書に対して限定的な検証を行います。</p> <p>注意 - 「Strict Certificate Mode」プロパティを有効にする前に、LDAP/SSL サーバー証明書を Oracle ILOM にアップロードする必要があります。</p> <p>厳密な証明書モードの CLI 構文:</p> <pre>set /SP CMM/clients/ldapssl/ strictcertmode=disabled enabled</pre> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 24

表 23 LDAP/SSL 認証の有効化 (続き)

プロパティ	デフォルト値	説明
Optional User Mapping (/optionalUsermapping)	Disabled	<p><i>Disabled Enabled</i></p> <p>「Optional User Mapping」プロパティは、通常、uid がユーザードメインのログイン名の一部として使用されなかった場合に使用されます。ユーザー認証を行うために単純なユーザーログイン名をドメイン名に変換する必要がある場合は、「Optional User Mapping」プロパティを Enabled に設定します。</p> <ul style="list-style-type: none"> 「State」 - 有効にすると、ユーザー資格の認証のために代替の属性を構成できます。 「Attribute Information」 - 受け入れられる入力形式 (&(objectclass=person)(uid=<USERNAME>)) を使用してログイン情報属性を入力します。「Attribute Information」を使用すると、指定されたログイン情報属性に基づいて、LDAP/SSL クエリーがユーザードメイン名を検索できるようになります。 「Searchbase」 - 「Searchbase」プロパティは、検索ベースオブジェクトの識別名、または Oracle ILOM が LDAP ユーザーアカウントを検索する LDAP ツリーのブランチに設定します。入力形式: OU={organization},DC={company},DC={com} 「Bind DN」 - 「Bind DN」プロパティは、LDAP サーバー上の読み取り専用プロキシユーザーの識別名 (DN) に設定します。Oracle ILOM がユーザーの検索と認証を行うには、LDAP サーバーに対する読み取り専用のアクセス権が必要になります。入力形式: OU={organization},DC={company},DC={com} 「Bind Password」 - 「Bind Password」プロパティは、読み取り専用のプロキシユーザーのパスワードに設定します。 <p>オプションのユーザーマッピングの CLI 構文:</p> <pre>set /SP CMM/clients/ldapssl/optionalUsermapping/ attributeInfo=<string> searchbase=<string> binddn=cn=proxyuser, ou=organization _name, dc=company, dc=com bindpw=password</pre>
Log Detail (logdetail=)	なし	<p><i>None High Medium Low Trace</i></p> <p>Oracle ILOM のイベントログに記録される LDAP/SSL イベントの診断情報の種類を指定するには、「Log Detail」プロパティを、受け入れられる 5 個のプロパティ値 (None、High、Medium、Low、または Trace) のいずれかに設定します。</p> <p>ログの詳細の CLI 構文:</p> <pre>set /SP CMM/clients/ldapssl/ logdetail=none high medium low trace</pre>

表 23 LDAP/SSL 認証の有効化 (続き)

プロパティ	デフォルト値	説明
ユーザーインタフェースの構成可能なターゲット:		
<ul style="list-style-type: none"> ■ CLI: <code>/SP CMM/clients/ldapssl/</code> ■ Web: 「ILOM Administration」 > 「User Management」 > 「LDAP/SSL」 > 「Settings」 ■ ユーザーの役割: User Management (u) (すべてのプロパティの変更が必要) ■ 前提条件: Oracle ILOM を構成する前に、LDAP/SSL サーバーにユーザーまたはユーザーグループを構成する必要があります。 		
プロパティ	デフォルト値	説明
Save		Web インタフェース - LDAP/SSL の「Settings」ページ内のプロパティへの変更を適用するには、「Save」をクリックする必要があります。

表 24 LDAP/SSL 証明書ファイルのアップロードまたは削除

プロパティ	デフォルト値	説明
ユーザーインタフェースの構成可能なターゲット:		
<ul style="list-style-type: none"> ■ CLI: <code>/SP CMM/clients/ldapssl/cert</code> ■ Web: 「ILOM Administration」 > 「User Management」 > 「LDAP/SSL」 > 「Certificate Information」 ■ ユーザーの役割: User Management (u) (すべてのプロパティの変更が必要) 		
プロパティ	デフォルト値	説明
Certificate File Status (certstatus=)	読み取り専用	<p><i>Certificate Present</i> <i>Certificate Not Present</i></p> <p>「Certificate File Status」プロパティは、LDAP/SSL 証明書が Oracle ILOM にアップロードされているかどうかを示します。</p> <p>証明書ステータスの CLI 構文:</p> <p>show /SP CMM/clients/ldapssl/cert</p>
ファイル転送方式	Browser (Web インタフェースのみ)	<p><i>Browser</i> <i>TFTP</i> <i>FTP</i> <i>SCP</i> <i>Paste</i></p> <p>各ファイル転送方式の詳細は、表 13 を参照してください。</p>
Load Certificate (load_uri=)		<p>Web インタフェース - 「Load Certificate」ボタンをクリックして、「File Transfer Method」プロパティに指定されている LDAP/SSL 証明書ファイルをアップロードします。</p> <p>証明書のロードの CLI 構文:</p> <p>load_uri=file_transfer_method://host_address/file_path/filename</p>

表 24 LDAP/SSL 証明書ファイルのアップロードまたは削除 (続き)

プロパティ	デフォルト値	説明
Remove Certificate (clear_action=true)		<p>Web インタフェース - 「Remove Certificate」ボタンをクリックして、Oracle ILOM に現在格納されている LDAP/SSL 証明書ファイルを削除します。確認のメッセージが表示されたら、「Yes」をクリックして操作を続行するか、「No」をクリックして操作を取り消します。</p> <p>「Remove Certificate」の CLI 構文:</p> <pre>set /SP CMM/clients/ldapssl/cert clear_action=true</pre> <p>-または-</p> <pre>reset /SP CMM/clients/ldapssl/cert</pre> <p>確認のメッセージが表示されたら、y と入力して操作を続行するか、n と入力して操作を取り消します。</p>

表 25 LDAP/SSL グループの構成 (省略可能)

プロパティ	説明
Admin Groups (/admingroups/ 1 2 3 4 5)	<p>システム管理者は、必要に応じて、ユーザー承認のために、Oracle ILOM の「Role」プロパティの代わりに「Admin Group」プロパティを構成できます。</p> <p>Oracle ILOM は、最大 5 個の「Admin Groups」を構成することをサポートしています。Oracle ILOM で「Admin Group」プロパティを有効にすると、ユーザーのグループメンバーシップに、admin 表での定義に一致するグループがあるかどうかチェックされます。一致がある場合、そのユーザーに Administrator レベルのアクセス権が付与されます。</p> <p>注 - Oracle ILOM は、構成された各グループ表で見つかった一致するグループ (Operator, Administrator, または Custom) に基づいて、1 つ以上の承認レベルをグループのメンバーに付与します。</p> <p>Admin グループの CLI 構文:</p> <pre>set /SP CMM/clients/ldapssl/admingroups/n name=string</pre> <p>構文例:</p> <pre>set /SP/clients/ldapssl/admingroups/1/ name=CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com</pre> <p>Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle, DC=com'</p>
Operator Groups (/operatorgroups/ 1 2 3 4 5)	<p>システム管理者は、必要に応じて、ユーザー承認のために、Oracle ILOM の「Role」プロパティの代わりに「Operator Group」プロパティを構成できます。</p> <p>Oracle ILOM は、最大 5 個の Operator Groups を構成することをサポートしています。Oracle ILOM で「Operator Group」プロパティを有効にすると、ユーザーのグループメンバーシップに、operator 表での定義に一致するグループがあるかどうかチェックされます。一致がある場合は、そのユーザーに Operator レベルのアクセス権が付与されます。</p> <p>注 - Oracle ILOM は、構成された各グループ表で見つかった一致するグループ (Operator, Administrator, または Custom) に基づいて、1 つ以上の承認レベルをグループのメンバーに付与します。</p> <p>Operator グループの CLI 構文:</p> <pre>set /SP CMM/clients/ldapssl/operatorgroups/n name=string</pre> <p>構文例:</p> <pre>set /SP/clients/ldapssl/operatorgroups/1 name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com</pre> <p>Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC= com''</p>

表 25 LDAP/SSL グループの構成(省略可能) (続き)

プロパティ	説明
<p>ユーザーインターフェースの構成可能なターゲット:</p> <ul style="list-style-type: none"> ■ CLI: <code>/SP CMM/clients/ldapssl/</code> ■ Web: 「ILOM Administration」 > 「User Management」 > 「LDAP/SSL」 > 「(Name) Groups」 ■ ユーザーの役割: User Management (u) (すべてのプロパティの変更が必要) ■ 前提条件: Oracle ILOM に LDAP/SSL グループを設定する前に、LDAP/SSL グループが LDAP/SSL サーバー上に存在し、メンバーが割り当てられている必要があります。 	<p>システム管理者は、必要に応じて、ユーザー承認のために、Oracle ILOM に最大 5 個の「Custom Groups」プロパティを構成できます。Oracle ILOM は、Custom Group のメンバーであるユーザーを認証する場合、「Custom Group」プロパティを使用して該当するユーザーの役割を判別して割り当てます</p> <p>Oracle ILOM で「Custom Groups」を使用可能にする場合は、「Roles」プロパティおよび「Custom Groups」プロパティの両方を構成する必要があります。「Roles」の構成プロパティの詳細は、表 23 の「Roles」プロパティを参照してください。</p> <p>注 - Oracle ILOM は、構成された各グループ表で見つかった一致するグループ (Operator, Administrator, または Custom) に基づいて、1 つ以上の承認レベルをグループのメンバーに付与します。</p> <p>Custom グループの CLI 構文:</p> <pre>set /SP CMM/clients/ldapssl/customgroups/n name=string roles=administrator operator a u c r o s</pre> <p>構文例:</p> <pre>set /SP/clients/ldapssl/customgroups/1 name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com roles=au</pre> <p>Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC= com'' roles' to 'au'</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 40 ページの「割り当て可能な Oracle ILOM のユーザーの役割」
Save	<p>Web インタフェース - 「Admin Group」、「Operator Group」、または「Custom Group」ダイアログのプロパティへの変更を適用するには、「Save」をクリックする必要があります。</p>

表 26 LDAP/SSL ユーザードメインの構成

プロパティ	説明
User Domains (/1 2 3 4 5)	<p>システム管理者は、必要に応じて、最大 5 個のユーザードメインを構成できます。1 つ以上のユーザードメインを定義すると、Oracle ILOM は、LDAP/SSL ユーザーを認証できるまで、これらのプロパティを順番に使用します。</p> <p>次の取り得る値を使用して、Oracle ILOM の各ユーザードメインに構成プロパティを設定します。</p> <ul style="list-style-type: none"> ■ UID 形式: uid=<USERNAME>,ou=people,dc=company,dc=com ■ DN 形式: CN=<USERNAME>,CN=Users,DC=domain,DC=company,DC=com <p>注 - <USERNAME> をリテラルとして使用できます。<USERNAME> をリテラルとして使用すると、Oracle ILOM はユーザー認証時に <USERNAME> を入力された現在のログイン名に置き換えます。</p> <p>必要に応じて、特定の検索ベースを指定するには、ユーザードメイン構成のあとに <BASE:string> プロパティを追加します。構文の詳細は、下記の例 3 を参照してください。</p> <p>「User Domains」の CLI 構文:</p> <pre>set /SP CMM clients/ldapssl/userdomains/n domain=string</pre> <p>例 1: domain=CN=<USERNAME></p> <pre>set /SP clients/ldapssl/userdomains/1 domain=CN=<USERNAME>,OU=Groups,DC=sales,DC=oracle,DC=com</pre> <p>Set 'domain' to 'CN=<USERNAME>,OU=Groups,DC=sales,DC=oracle,DC=com'</p> <p>例 2: domain=CN=spSuperAdmin</p> <pre>set /SP clients/ldapssl/userdomains/1 domain=CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com</pre> <p>Set 'domain' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com'</p> <p>例 3: <BASE:string> を使用した検索ベースの構文</p> <pre>set /SP clients/ldapssl/userdomains/1 domain=uid=<USERNAME>,ou=people,dc=oracle,dc=com<BASE:ou=doc,dc=oracle,dc=com></pre>
Save	<p>Web インタフェース - LDAP/SSL の「User Domains」ダイアログ内のプロパティへの変更を適用するには、「Save」をクリックする必要があります。</p>

表 27 LDAP/SSL 代替サーバーの構成 (省略可能)

プロパティ	説明
ユーザーインタフェースの構成可能なターゲット: ■ CLI: <code>/SP CMM/clients/ldapssl/alternateservers/n</code> ■ Web: 「ILOM Administration」 > 「User Management」 > 「LDAP/SSL」 > 「Alternate Servers」 ■ ユーザーの役割: User Management (u) (すべてのプロパティの変更が必要)	
Alternate Servers (/1 2 3 4 5)	<p>Oracle ILOM では、最大 5 個の LDAP/SSL 代替サーバーを構成できます。</p> <p>代替サーバーを使用すると認証が冗長化され、ドメインを分離する必要がある場合に別の LDAP/SSL サーバーを選択できます。</p> <p>各 LDAP/SSL 代替サーバーは、プライマリ LDAP/SSL サーバーと同じユーザー承認のルールおよび要件を使用します。たとえば、Oracle ILOM は「Roles」プロパティに構成されているユーザーの役割を使用してユーザーを認証します。ただし、「Roles」プロパティが構成されていない場合、Oracle ILOM は認証サーバーに対して該当する承認の役割を問い合わせます。</p> <p>各代替サーバーは、プロパティ (ネットワークアドレス、ポート、証明書のステータス)、および証明書をアップロードおよび削除するためのコマンドをそれぞれ保持しています。LDAP/SSL 証明書が提示されていないが必要な場合、Oracle ILOM は最上位のプライマリ LDAP/SSL サーバーの証明書を使用します。</p> <p>代替サーバーのアドレスとポートの CLI 構文:</p> <pre>set /SP CMM/clients/ldapssl/alternateservers/n address=string port=string</pre> <p>代替サーバーの証明書の CLI 構文:</p> <pre>show /SP CMM/clients/ldapssl/alternateservers/n/cert</pre> <pre>load_uri=file_transfer_method://host_address/file_path/filename</pre> <pre>set /SP CMM/clients/ldapssl/alternateservers/n/cert clear_action=true</pre>
Save	<p>Web インタフェース - LDAP/SSL の「Alternate Servers」ダイアログ内のプロパティへの変更を適用するには、「Save」をクリックする必要があります。</p>

表 28 LDAP/SSLの認証をトラブルシューティングするためのガイドライン

Oracle ILOM での LDAP/SSL の認証および承認の試行をトラブルシューティングする場合は、次のガイドラインを参照してください。

- LDAP/SSL の認証をテストして、LDAP/SSL イベントをトレースするように Oracle ILOM のイベントログを設定するには、次の手順に従います：
 - 1: LDAP/SSL の「Log Details」プロパティを Trace に設定します。
 - 2: イベントを生成するために Oracle ILOM に対して認証を試行します。
 - 3: Oracle ILOM のイベントログファイルを確認します。
- LDAP/SSL サーバーに構成されているユーザーグループおよびユーザードメインが、Oracle ILOM に構成されているユーザーグループおよびユーザードメインと一致することを確認します。
- Oracle ILOM の LDAP/SSL クライアントは、クロック設定を管理しません。Oracle ILOM のクロック設定は、手動で、または NTP サーバーを使用して構成できます。
注。Oracle ILOM のクロック設定を NTP サーバーを使用して構成した場合、Oracle ILOM は、NTP デーモンを開始する前に、NTP サーバーを使用して ntpdate を実行します。

関連情報:

- [表 23](#)
- 『ユーザーズガイド』の「Oracle ILOM のログエントリの管理」
- [122 ページの「SP または CMM クロックのプロパティの設定」](#)

LDAP の構成

システム管理者は、Lightweight Directory Access Protocol (LDAP) サービスを使用してユーザーを認証するように Oracle ILOM を構成できます。このサービスは、ユーザーを認証するために読み取り専用のプロキシユーザーアカウントを使用して LDAP サーバーに問い合わせるクライアントサーバー型のクエリーモデルに基づいています。

Oracle ILOM の LDAP サービスの状態プロパティは、デフォルトで無効になっています。LDAP サービスの状態を有効にして、ユーザー認証に LDAP ディレクトリサービスを使用するためのプロパティを構成する場合は、これらの表を参照してください:

- [表 29](#)
- [表 30](#)

表 29 Oracle ILOM を LDAP クライアントとして有効にするための要件

Oracle ILOM を LDAP クライアントとして構成する前に、LDAP サーバーを適切に構成する必要があります。Oracle ILOM を LDAP クライアントとして認識するように LDAP サーバーを構成する場合は、次のガイドラインおよび「関連情報」セクションを参照してください。

- デフォルトのパスワード {crypt} 形式を使用するように LDAP サーバーが設定されていることを確認します。Oracle ILOM で認証を行うすべての LDAP ユーザーのパスワードは、次の 2 つの {crypt} 形式のいずれかで格納する必要があります:


```
userPassword: {CRYPT}ajCa2He4PJhNo
userPassword: {CRYPT}$1$pzKng1$du1Bf0NWBjh9t3FbUgf46
```
- `posixAccount` および `shadowAccount` にオブジェクトクラスを追加して、次の必要なプロパティ値を設定する場合は、Internet Engineering Task Force スキーマ (RFC 2307) を参照してください:
 - `uidnumber`
 - `gidnumber`
 - `uid` (Oracle ILOM ユーザー名)
- LDAP サーバーが匿名バインドを受け入れるようにするか、または LDAP サーバーにプロキシユーザーを作成して、Oracle ILOM で認証を行うすべてのユーザーアカウントに読み取り専用アクセス権を設定します。

関連情報:

- Internet Engineering Task Force スキーマ (RFC2307) (<http://www.ietf.org/rfc/rfc2307.txt>)

表 30 LDAP 認証の使用を Oracle ILOM で有効にする

ユーザーインタフェースの構成可能なターゲット:

- **CLI:** `/SP|CMM/clients/Ldap`
- **Web:** 「ILOM Administration」 > 「User Management」 > 「LDAP Settings」
- **ユーザーの役割:** User Management (u) (すべてのプロパティの変更が必要)

プロパティ	デフォルト値	説明
State (state=)	Disabled	<p><i>Disabled Enabled</i></p> <p>Oracle ILOM が LDAP ディレクトリサービスを使用してユーザーを認証するには、「State」プロパティを Enabled に設定します。</p> <p>「State」プロパティを有効にすると、Oracle ILOM は LDAP ユーザーを認証する場合に LDAP サーバーに問い合わせます。</p> <p>「State」の CLI 構文:</p> <pre>set /SP CMM/clients/ldap/ state=disabled enabled</pre>

表 30 LDAP 認証の使用を Oracle ILOM で有効にする (続き)

プロパティ	デフォルト値	説明
Roles (defaultrole=)	Operator	<p><i>Administrator Operator Advanced</i></p> <p>LDAP で認証されたユーザーがアクセスできる Oracle ILOM の機能を定義するには、デフォルトの「Roles」プロパティを、3つの Oracle ILOM ユーザーの役割のいずれかに設定します: Administrator (a u c r o)、Operator (c r o)、または Advanced (a u c r o s)</p> <p>Oracle ILOM の機能を使用するための承認レベルは、構成されている Oracle ILOM のユーザーの役割によって付与されるユーザー権限で決定されます。割り当てられる権限については、下の「関連情報」セクションに示されているユーザーの役割およびユーザープロファイルのトピックを参照してください。</p> <p>「Roles」の CLI 構文:</p> <pre>set /SP/CMM/clients/ldap/ defaultrole=adminstrator operator a u c r o s</pre> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 9 ■ 表 10
アドレス (address=)	0.0.0.0	<p><i>IP address DNS host name</i> (LDAP サーバー)</p> <p>LDAP サーバーのネットワークアドレスを構成するには、「Address」プロパティに LDAP サーバーの IP アドレスまたは DNS ホスト名を設定します。DNS ホスト名を使用する場合は、Oracle ILOM の DNS 構成プロパティを適切に構成して動作可能にする必要があります。</p> <p>「Address」の CLI 構文:</p> <pre>set /SP/CMM/clients/ldap/ address=ldap_server ip_address ldap_server_dns_host_name</pre> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 44
ポート (port=)	389	<p><i>389 User-specified TCP port</i></p> <p>Oracle ILOM は、TCP ポート 389 を使用して OpenLDAP サーバーと通信します。必要に応じて、デフォルトのポート番号 389 を変更して別のポートを使用するように Oracle ILOM を構成します。</p> <p>「Port」の CLI 構文:</p> <pre>set /SP/CMM/clients/ldap/ port=number</pre>

表 30 LDAP 認証の使用を Oracle ILOM で有効にする (続き)

プロパティ	デフォルト値	説明
Searchbase (searchbase=)	<code>ou=organization_unit dn=domain_name dc=domain </code>	<p>「Searchbase」は、ユーザー資格を検証するために Oracle ILOM が検索する LDAP ツリーの場所です。</p> <p>受け入れられる入力形式を使用して、「Searchbase」プロパティに、検索ベースオブジェクトの識別名、または Oracle ILOM が LDAP ユーザーアカウントを検索する LDAP ツリーのブランチを設定します。</p> <p>たとえば、MyCompany.com ドメインの IT コンテナを検索するには、次の検索ベースを指定します:</p> <p><code>ou=IT,dc=mycompany,dc=.com</code></p> <p>検索ベースの CLI 構文:</p> <pre>set /SP CMM clients/ldap/ searchbase= ou=organization_name, dn=domain_name,dc=domain</pre>
Bind DN (binddn=)	<code>ou=organization_unit dn=domain_name dc=domain cn=common_name</code>	<p>LDAP サーバーへの読み取り専用アクセス権を Oracle ILOM に与えるには、「Bind DN」プロパティに読み取り専用プロキシユーザーの識別名 (DN) を設定します。</p> <p>注 - Oracle ILOM が LDAP ユーザーの検索と認証を行うには、LDAP サーバーに対する読み取り専用のアクセス権が必要になります。</p> <p>バインド DN の CLI 構文:</p> <pre>set /SP CMM clients/ldap/ binddn=cn=proxyuser, ou=organization_name, dc=domain</pre>
Bind Password (bindpw=)		<p>Oracle ILOM に読み取り専用プロキシユーザーのパスワードを指定するには、「Bind Password」プロパティにパスワードを設定します。</p> <p>バインドパスワードの CLI 構文:</p> <pre>set /SP CMM clients/ldap/ bindpw=password</pre>
Save		<p>Web インタフェース - 「LDAP Settings」ページ内のプロパティへの変更を適用するには、「Save」をクリックする必要があります。</p>

RADIUSの構成

システム管理者は、Remote Authentication Dial-In User Service (RADIUS) を使用してユーザーを認証するように Oracle ILOM を構成できます。このサービスは、共有シークレットパスワードを使用してユーザーを認証するクライアントサーバー型のクエリーモデルに基づいています。Oracle ILOM の RADIUS クライアントおよび RADIUS サーバーは、共有シークレットパスワードを知っている必要があります。これは、このパスワードがネットワークを介して送信されることはないためです。

Oracle ILOM の RADIUS サービスの状態プロパティは、デフォルトで無効になっています。RADIUS サービスの状態を有効にして、Oracle ILOM のプロパティを RADIUS クライアントとして構成する場合は、次の表を参照してください。

表 31 RADIUS クライアントサーバー認証の使用を Oracle ILOM で有効にする

ユーザーインタフェースの構成可能なターゲット:

- **CLI:** `/SP|CMM/clients/radius`
- **Web:** 「ILOM Administration」 > 「User Management」 > 「RADIUS Settings」
- ユーザーの役割: **User Management (u)** (すべてのプロパティの変更が必要)
- **要件:** RADIUS サーバーにユーザーおよび共有シークレットパスワードを事前構成する必要があります。

プロパティ	デフォルト値	説明
State (state=)	Disabled	<p><i>Disabled Enabled</i></p> <p>Oracle ILOM を RADIUS クライアントとして構成するには、「State」プロパティを Enabled に設定します。</p> <p>「State」プロパティを有効にすると、Oracle ILOM は、ユーザー認証および承認のために、ユーザーのログインデータを RADIUS サーバーに送信します。</p> <p>RADIUS の状態の CLI 構文:</p> <p>set /SP CMM/clients/radius/ state=disabled enabled</p>

表 31 RADIUSクライアントサーバー認証の使用を Oracle ILOM で有効にする (続き)

プロパティ	デフォルト値	説明
ユーザーインターフェースの構成可能なターゲット: ■ CLI: <code>/SP CMM/clients/radius</code> ■ Web: 「ILOM Administration」 > 「User Management」 > 「RADIUS Settings」 ■ ユーザーの役割: User Management (u) (すべてのプロパティの変更が必要) ■ 要件: RADIUS サーバーにユーザーおよび共有シークレットパスワードを事前構成する必要があります。		
Roles (defaultrole=)	Operator	<p><i>Administrator Operator Advanced</i></p> <p>RADIUS で認証されたユーザーがアクセスできる Oracle ILOM の機能を定義するには、デフォルトの「Roles」プロパティを、3つの Oracle ILOM ユーザーの役割のいずれかに設定します: Administrator (a u c r o)、Operator (c r o)、または Advanced (a u c r o s)</p> <p>Oracle ILOM の機能を使用するための承認レベルは、構成されている Oracle ILOM のユーザーの役割によって付与される権限で決定されます。割り当てられる権限については、下の「関連情報」セクションに示されているユーザーの役割およびユーザープロファイルの表を参照してください。</p> <p>「Roles」の CLI 構文:</p> <pre>set /SP CMM/clients/radius/ defaultrole=administrator operator a u c r o s</pre> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 9 ■ 表 10
アドレス (address=)	0.0.0.0	<p><i>IP address DNS host name</i> (LDAP サーバー)</p> <p>RADIUS サーバーのネットワークアドレスを構成するには、「Address」プロパティに RADIUS サーバーの IP アドレスまたは DNS ホスト名を設定します。DNS ホスト名を指定する場合は、Oracle ILOM の DNS 構成プロパティを適切に構成して動作可能にする必要があります。</p> <p>「Address」の CLI 構文:</p> <pre>set /SP CMM/clients/radius/ address=radius_server ip_address ldap_server_dns_host_name</pre> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 44
ポート (port=)	1812	<p><i>1812 User-specified TCP port</i></p> <p>Oracle ILOM は、TCP ポート 1812 を使用して LDAP サーバーと通信します。</p> <p>必要に応じて、デフォルトのポート番号 1812 を変更して別のポートを使用するように Oracle ILOM を構成します。</p> <p>「Port」の CLI 構文:</p> <pre>set /SP CMM/clients/radius/ port=number</pre>

表 31 RADIUSクライアントサーバー認証の使用を Oracle ILOM で有効にする (続き)

プロパティ	デフォルト値	説明
Shared Secret (secret=)		<p>「Shared Secret」プロパティには、既知のRADIUSクライアントサーバーの共有パスワードを設定します。RADIUSクライアントサーバーモデルは、共有パスワードを使用して相互に認識し、機密性のあるユーザー資格データを保護します。</p> <p>共有シークレットのCLI構文:</p> <pre>set /SP CMM/clients/radius/ secret=password</pre>
Save		<p>Web インタフェース。「RADIUS Settings」ページ内のプロパティへの変更を適用するには、「Save」をクリックする必要があります。</p>

ネットワークの配備および管理のデフォルト設定の変更

説明	リンク
Oracle ILOM の配備オプションおよび管理アクセスとネットワーク接続のデフォルト設定をより深く理解するには、このセクションを参照してください。	■ 81 ページの「ネットワーク配備の原則と考慮事項」
管理アクセス要件および構成プロパティについては、このセクションを参照してください。	■ 91 ページの「デフォルトの管理アクセス構成プロパティの変更」
接続要件および構成プロパティについては、このセクションを参照してください。	■ 106 ページの「デフォルトの接続構成プロパティの変更」
Oracle ILOM でシステム識別ラベルの設定および日付と時間のプロパティの設定を行う手順については、これらのセクションを参照してください。	■ 121 ページの「システム識別情報の割り当て」 ■ 122 ページの「SP または CMM クロックのプロパティの設定」
管理アクセスおよびネットワーク接続の問題を解決するためのガイドラインについては、このセクションを参照してください。	■ 124 ページの「ネットワーク接続の問題の推奨される解決策」

関連情報

- 『Oracle ILOM 3.1 セキュリティガイド』の配備に関する考慮事項
- 『ユーザーズガイド』の「Oracle ILOM にログインする」

ネットワーク配備の原則と考慮事項

ネットワーク上で Oracle ILOM を設定する場合、Oracle ILOM に標準装備されたネットワーク初期設定に加え、ネットワーク管理者が実装を選択できるその他の構成可能なオプションを理解することが重要です。

Oracle ILOM のネットワーク配備オプション、およびネットワーク環境で Oracle ILOM を管理する場合に考慮すべき一般的な情報については、次のトピックを参照してください:

- 82 ページの「管理アクセス配備オプション」
- 85 ページの「接続配備オプション」
- 87 ページの「Web サーバー証明書およびSSH サーバー側鍵の使用」
- 87 ページの「CLI および Web セッションのデフォルトタイムアウト」
- 87 ページの「ログイン時のバナーメッセージの表示」
- 88 ページの「IPv4 および IPv6 アドレスの入力形式」
- 88 ページの「シリアル管理ポートの所有者」
- 89 ページの「Oracle ILOM で使用するデフォルトのネットワークポート」
- 90 ページの「IPv6 をサポートしないレガシー Sun サーバー」

管理アクセス配備オプション

Oracle ILOM は複数のネットワーク管理サービスの構成をサポートしています。これらのサービスのいくつかはデフォルトで有効になっていますが、その他は構成が必要です。出荷時に有効になっているのはどの管理サービスで、使用しているネットワーク環境には実際にどの管理サービスが必要なのかをより深く理解するには、次の表を参照してください。

注- 使用しているネットワーク管理環境に必要な管理サービスのみを有効にすることをお勧めします。

表 32 管理アクセス配備オプションおよびデフォルト設定

Management Access	管理サービス	デフォルト	説明
Web ブラウザクライアント	<ul style="list-style-type: none"> ■ Web サーバー 	<ul style="list-style-type: none"> ■ ポート 443 を介した HTTPS が有効 ■ TLSv1、有効 ■ SSL 証明書および自己署名鍵 ■ クライアントタイムアウトセッション、15 分 	<p>Oracle ILOM の Web サーバー管理サービスでは、Web ブラウザクライアントと Oracle ILOM SP または CMM の間のセキュアな通信チャネルがデフォルトで有効になっています。</p> <p>ネットワーク管理者は、Oracle ILOM で用意されているデフォルトの Web サーバープロパティを受け入れるか、それらを必要に応じて変更するかを選択できます。</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 87 ページの「Web サーバー証明書およびSSH サーバー側鍵の使用」 ■ 表 35 ■ 124 ページの「Web ブラウザのセキュリティー設定の解決」

表 32 管理アクセス配備オプションおよびデフォルト設定 (続き)

Management Access	管理サービス	デフォルト	説明
コマンド行 SSH クライアント	<ul style="list-style-type: none"> ■ Secure Shell (SSH) サーバー 	<ul style="list-style-type: none"> ■ ポート 22 が有効 ■ 生成済み SSH 鍵 ■ クライアントタイムアウトセッション、制限なし 	<p>Oracle ILOM の SSH サーバーサービスでは、SSH コマンド行クライアントと Oracle ILOM SP または CMM の間の管理チャンネルを暗号化するためにサーバー側鍵を使用します。</p> <p>Oracle ILOM は、出荷時のデフォルトシステムの最初のブート時にサーバー側の SSH 鍵を自動的に生成します。</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 38 ■ 87 ページの「Web サーバー証明書および SSH サーバー側鍵の使用」
SNMP アプリケーションクライアント	<ul style="list-style-type: none"> ■ Simple Network Management Protocol (SNMP) 	<ul style="list-style-type: none"> ■ ポート 161 を介した SNMPv3、有効 ■ SNMP セット disabled ■ ユーザーアカウント構成が必要 	<p>Oracle ILOM の SNMP 管理サービスは、Oracle サーバーを監視および管理するためのセキュアなプロトコルによる管理ソリューションを提供します。</p> <p>SNMP のすべての監視および管理機能は、Net-SNMP などの SNMP アプリケーションからアクセスできます。</p> <p>Oracle ILOM で SNMP 管理サービスを使用する前に、1 つまたは複数の Oracle ILOM ユーザーアカウントを作成する必要があります。また、SNMP セットを使用する前に、SNMP セットプロパティを有効にする必要があります。</p> <p>Oracle ILOM は SNMPv3 が有効の状態では出荷されていますが、管理者は SNMPv1 または SNMPv2c のプロパティを有効にするように選択することもできます。</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 37 ■ 『SNMP、IPMI、CIM、WS-MAN プロトコル管理』の「Oracle ILOM での SNMP 設定の構成」 ■ 178 ページの「警告通知の構成プロパティ」 ■ Net-SNMP (http://net-snmp.sourceforge.net/)

表 32 管理アクセス配備オプションおよびデフォルト設定 (続き)

Management Access	管理サービス	デフォルト	説明
IPMItool クライアント	■ IPMI	<ul style="list-style-type: none"> ■ ポート 623 を介した IPMPv2、有効 ■ サービス状態は有効 	<p>Oracle ILOM の IPMI 管理サービスは、Oracle サーバーを監視および管理するためのセキュアなプロトコルソリューションを提供します。</p> <p>IPMI の監視および管理機能は、IPMItool ユーティリティーを使用して Oracle ILOM CLI からアクセスできます。</p> <p>Oracle ILOM で構成可能な IPMI プロパティには、IPMI 管理サービス状態と、Oracle ILOM CLI から IPMI 管理機能を実行するために必要なユーザーの役割 (Administrator または Operator) が含まれます。</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 39 ■ 40 ページの「割り当て可能な Oracle ILOM のユーザーの役割」 ■ 『Oracle ILOM 3.1 プロトコル管理リファレンス』の「IPMI を使用したサーバー管理」 ■ 178 ページの「警告通知の構成プロパティ」 ■ IPMItool (http://ipmitool.sourceforge.net/)

表 32 管理アクセス配備オプションおよびデフォルト設定 (続き)

Management Access	管理サービス	デフォルト	説明
Web サービス管理クライアント	<ul style="list-style-type: none"> ■ WS-Management (WS-Man) 	<ul style="list-style-type: none"> ■ ポート 8899 を介した HTTP¹ が有効 ■ サービス状態は有効 	<p>Oracle ILOM の WS-Management サービスには、次のための標準 Web サービスインタフェースが用意されています:</p> <ul style="list-style-type: none"> ■ Oracle サーバーの健全性の監視 ■ インベントリスステータスの報告 ■ ホストサーバーの電源のリモート管理 ■ Oracle ILOM SP のリモートリセット <p>Oracle ILOM の構成可能な WS-Man オプションには、転送プロトコルモード (HTTP または HTTPS)、通信ポート (8899 または 8888)、およびサービス状態が含まれます。</p> <p>ネットワーク管理者は、Oracle ILOM で用意されているデフォルトの WS-Man プロパティを受け入れるか、必要に応じてそれらを変更することができます。</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 87 ページの「Web サーバー証明書および SSH サーバー側鍵の使用」 ■ 表 41 ■ 『SNMP、IPMI、CIM、WS-MAN プロトコル管理』の「WS-Management と CIM を使用したサーバー管理」

¹ セキュリティーを最大化するため、ポート 8888 を介した HTTPS が優先転送プロトコルモードとなります。

接続配備オプション

Oracle ILOM の接続オプションは事前構成された状態で出荷されるため、Oracle ILOM は物理サーバー SP または CMM のネットワークアドレスを取得できます。出荷時に有効になっているのはどの接続プロパティで、使用しているネットワーク環境にはどの接続プロパティが必要なのかをより深く理解するには、次の表を参照してください。

表 33 接続配備オプションおよびデフォルト設定

接続オプション	デフォルト	説明
ネットワーク	<ul style="list-style-type: none"> ■ IPv4、DHCP 有効 ■ IP 6、ステートレス有効 ■ 管理ポート: MGT 	<p>Oracle ILOM は、デフォルトではデュアルスタック IPv4 および IPv6 ネットワーク環境で動作するように構成された状態で出荷されます。サーバーまたは CMM に対して物理ネットワーク管理接続を設定する際、Oracle ILOM はネットワーク上で構成されている IP マッピングおよびルーティングデバイスから SP または CMM の物理アドレスを取得しようとします。</p> <p>ネットワーク管理者は、Oracle ILOM のデフォルトのデュアルスタック IP ネットワークプロパティを受け入れるか、それらを無効にして必要な IP ネットワークプロパティを構成するように選択できます。</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 43 ■ 14 ページの「サイドバンドネットワーク管理接続」 ■ 12 ページの「専用ネットワーク管理接続(デフォルト)」
DNS	<ul style="list-style-type: none"> ■ DHCP を介した自動 DNS、有効 ■ DNS タイムアウト 5 秒 ■ DNS 再試行 1 回 	<p>Oracle ILOM の「Auto DNS」プロパティは、DHCP を使用して DNS ネームサーバーおよび検索パスを自動的に割り当てます。</p> <p>ネットワーク管理者は、Oracle ILOM のデフォルトの「Auto DNS」プロパティを受け入れるか、それらを無効にして必要な DNS ネームサーバーおよび検索パスを構成するように選択できます。</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 44 ■ 118 ページの「動的 DNS の設定例」
シリアルポート	<ul style="list-style-type: none"> ■ 所有者 = SP ■ ポーレート: = 9600 ■ フロー制御 = none 	<p>サーバーの物理シリアル管理ポートのためのコンソール出力機能は、サーバー SP によって制御されます。</p> <p>ネットワーク管理者はサーバー SP をデフォルトのシリアルポート所有者として受け入れるか、ポート所有者をホストサーバーのオペレーティングシステムに切り替えることができます。</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 45 ■ 88 ページの「シリアル管理ポートの所有者」 ■ 12 ページの「専用ネットワーク管理接続(デフォルト)」

Web サーバー証明書およびSSH サーバー側鍵の使用

Oracle ILOM は、Web サーバーの自己署名証明書および生成済み SSH サーバー側鍵のセットが事前構成された状態で出荷されるため、Oracle ILOM はサーバーまたはクライアントの真正性を確保できます。

ネットワーク管理者は、出荷時構成の自己署名付き Web サーバー証明書を使用するか、署名付き Web サーバー証明書を Oracle ILOM にアップロードするかを任意に選択できます。また、生成済み SSH サーバー側鍵を必要に応じて再生成することもできます。

Web サーバー証明書の構成プロパティの詳細は、[表 36](#)を参照してください。

SSH サーバー側鍵の構成プロパティの詳細は、[表 38](#)を参照してください。

CLI および Web セッションのデフォルトタイムアウト

Oracle ILOM には、Oracle ILOM がセッションを終了する前に Web またはコマンド行クライアントが非アクティブでいられる時間(分)を制御する構成可能なプロパティがあります。

承認された Web ユーザーのデフォルトのタイムアウトセッションは 15 分に設定されており、承認されたコマンド行ユーザーに設定されているデフォルトタイムアウトセッションは 0 分です(つまり CLI のデフォルトタイムアウトは設定されていません)。無人セッションの無許可の使用を防止するために、すべての Web および CLI ユーザーに適切なタイムアウトを構成することをお勧めします。

CLI セッションのタイムアウト構成プロパティについては、[表 40](#)を参照してください。Web セッションのタイムアウト構成プロパティについては、[表 35](#)を参照してください。

ログイン時のバナーメッセージの表示

Oracle ILOM の「Banner Message」プロパティを使用すると、ネットワーク管理者は Oracle ILOM ユーザーのログイン時に重要なメッセージを表示できます。たとえば、ネットワーク管理者はユーザーへの特別なアクセス制限の警告や次のシステム保守の通知といった目的に、このメッセージ表示機能を使用できます。

Oracle ILOM の Web および CLI バナーメッセージは、ログイン前またはログイン直後に表示できます。バナーメッセージを構成して表示を有効にするには、[表 42](#)を参照してください。

IPv4 および IPv6 アドレスの入力形式

Oracle ILOM は、次の IPv4 および IPv6 アドレスの入力形式に対応しています。

アドレス	入力形式
IPv4 (32 ビット)	ドットで 4 つに区切られた 10 進数を使用します: <i>n.n.n.n</i> 例: 192.0.2.0
IPv6 (128 ビット)	IPv6 アドレスまたはリンクローカル IPv6 アドレスが正しく機能するためには、アドレスの入力時にそのアドレスを角括弧で囲む必要があります。ただし、SSH を使用して Oracle ILOM にログインするために IPv6 アドレスを指定する場合は、IPv6 アドレスを括弧で囲まないでください。 例: <ul style="list-style-type: none"> ■ IPv6 アドレス: [2001:db8:0:0:0:0:0/32] ■ SSH および root アカウントを使用する IPv6 アドレス: ssh root@2001:db8:0:0:0:0:0/32 ■ リンクローカル IPv6 アドレス: [fe80::214:4fff:feca:5f7e/64]

シリアル管理ポートの所有者

Oracle ILOM を搭載したすべての Oracle サーバーは、SER MGT ポートの出力表示がサーバー SP に設定された状態で出荷されます。ただし、一部の Oracle サーバーの Oracle ILOM には、ネットワーク管理者がサーバー SP (デフォルト) とホストサーバーのオペレーティングシステムの間でシリアルポートの所有者を切り替えられるようにするためのプロパティがあります。

シリアルポートの所有者がホストサーバーに切り替わると、ホストオペレーティングシステムがシリアルポートの機能を制御し、サーバー SP はシリアルポートを制御したりシリアルポートにアクセスしたりできなくなります。

シリアルポートの所有者をホストサーバーに切り替える前に、ネットワーク管理者はサーバー SP へのネットワーク管理接続が確立されていることを確認するようにしてください。それ以外の場合で、ネットワーク管理接続がない状態でホストサーバープロパティがシリアルポートの所有者として設定された場合、Oracle ILOM SP はローカルでもリモートでもすべてのユーザーからアクセスできなくなります。

Oracle ILOM でシリアルポート所有者のデフォルトのプロパティを変更するには、[表 45](#)を参照してください。

Oracle ILOM で使用するデフォルトのネットワークポート

Oracle ILOM がデフォルトで使用する (出荷時構成の) ネットワークポートを特定するには、次の表を参照してください:

表 34 Oracle ILOM のデフォルトのネットワークポート

ポート	プロトコル	用途
一般的なネットワークポート		
22	SSH over TCP	SSH - Secure Shell
25	SMTP over TCP	SMTP クライアント通信
69	TFTP over UDP	TFTP - Trivial File Transfer Protocol (送信)
80	HTTP over TCP	Web (ユーザー構成可能)
123	NTP over UDP	NTP - Network Time Protocol (送信)
161	SNMP over UDP	SNMP - Simple Network Management Protocol (ユーザー構成可能)
162	IPMI over UDP	IPMI - Platform Event Trap (PET) (送信)
389	LDAP over UDP/TCP	LDAP - Lightweight Directory Access Protocol (送信、ユーザー構成可能)
443	HTTPS over TCP	Web (ユーザー構成可能)
514	Syslog over UDP	Syslog - (送信)
623	IPMI over UDP	IPMI - Intelligent Platform Management Interface
546	DHCP over UDP	DHCP - 動的ホスト構成プロトコル (クライアント)
1812	RADIUS over UDP	RADIUS - Remote Authentication Dial-In User Service (送信、ユーザー構成可能)
8888	WS-Man over HTTP	WS-Man サービス
8889	WS-Man over HTTPS	WS-Man サービス
SP ネットワークポート		
5120	TCP	Oracle ILOM リモートコンソール: CD
5121	TCP	Oracle ILOM リモートコンソール: キーボードおよびマウス
5123	TCP	Oracle ILOM リモートコンソール: フロッピーディスク

表 34 Oracle ILOM のデフォルトのネットワークポート (続き)

ポート	プロトコル	用途
5555	TCP	Oracle ILOM リモートコンソール: 暗号化
5556	TCP	Oracle ILOM リモートコンソール: 認証
6481	TCP	Oracle ILOM リモートコンソール: サービススタグデーモン
7578	TCP	Oracle ILOM リモートコンソール: ビデオ
7579	TCP	Oracle ILOM リモートコンソール: シリアル
CMM ネットワークポート		
8000 - 8023	HTTP over TCP	Oracle ILOM ドリルダウン (サーバーモジュール) (ブレード)
8400 - 8423	HTTPS over TCP	Oracle ILOM ドリルダウン (サーバーモジュール) (ブレード)
8200 - 8219	HTTP over TCP	Oracle ILOM ドリルダウン (Network Express Module)。
8600 - 8619	HTTPS over TCP	Oracle ILOM ドリルダウン (Network Express Module)。

IPv6 をサポートしないレガシー Sun サーバー

現在 IPv6 がサポートされていないレガシー Sun サーバー SP のリストについては、次の表を参照してください。

Sun プラットフォーム	サーバーモデル
SPARC Enterprise	<ul style="list-style-type: none"> ■ T5440 ■ T5220 ■ T5120 ■ T5140 ■ T5240 ■ T6340

Sun プラットフォーム	サーバーモデル
x86 Sun Fire	<ul style="list-style-type: none">■ X4140■ X4150■ X4240■ X4440■ X4450■ X4600■ X4600 M2■ X4640

デフォルトの管理アクセス構成プロパティの変更

ネットワーク管理者は、Oracle ILOM に標準装備されたデフォルトの管理アクセスプロパティを必要に応じて受け入れたり変更したりできます。Oracle ILOM でデフォルトの管理アクセスプロパティを変更するには、次の表を参照してください:

- 表 35
- 表 36
- 表 37
- 表 38
- 表 39
- 表 40
- 表 41
- 表 42

表 35 Web サーバーの構成プロパティ

ユーザーインターフェースの構成可能なターゲットとユーザーの役割:

- **CLI:** `/SP|CMM/services/`
- **Web:** 「ILOM Administration」 > 「Management Access」 > 「Web Server」 > 「Web Server Settings」
- **ユーザーの役割:** `admin (a)` (すべてのプロパティ変更に必要)

プロパティ	デフォルト値	説明
HTTP Webserver (<code>http/ securedirect=enabled servicestate=disabled</code>)	Redirect Connection to HTTPS	<p><i>Redirect Connection to HTTPS</i> <i>Enabled</i> <i>Disabled</i></p> <p>「HTTP Webserver」プロパティを「Redirect Connection to HTTPS」に設定した場合、「HTTPS Webserver」のサービス状態のプロパティは自動的に有効になります。これらのデフォルトのプロパティ値は、情報を Web サーバーにセキュアに転送するために HTTPS を使用するように Oracle ILOM に指示します。</p> <p>「HTTP Webserver」プロパティを有効に設定した場合、Oracle ILOM は Web サーバーへの情報転送に非暗号化プロトコルである HTTP を使用します。</p> <p>「HTTP Webserver」プロパティを無効に設定した場合、Oracle ILOM での HTTP を使用した Web サーバーへの情報転送の使用は無効になります。</p> <p>「HTTP Web Server」の CLI 構文:</p> <pre>set /SP CMM/services/http securedirect=<i>enabled disabled</i> servicestate=<i>disabled enabled</i></pre>
HTTP Port (<code>http/ port=</code>)	80	<p><i>80</i> <i>User_defined</i></p> <p>HTTP サービスの状態が有効の場合、Oracle ILOM はデフォルトで、TCP ポート 80 を介した HTTP を使用して Web サーバーと通信します。必要に応じて、デフォルトのポート番号は変更できます。</p> <p>「HTTP Port」の CLI 構文:</p> <pre>set /SP CMM/services/http port=<i><n></i></pre>
HTTP Session Timeout (<code>http/ sessiontimeout=</code>)	15 seconds	<p><i>15 seconds</i> <i>User_defined</i></p> <p>HTTP Web セッションタイムアウトは、アクティブでない Web ブラウザクライアントが自動的にログアウトされるまでの時間 (分) を決定します。デフォルトの HTTP Web セッションタイムアウトは 15 分です。必要に応じて、デフォルトのセッションタイムアウト値は増減できます。</p> <p>「HTTP Session Timeout」の CLI 構文:</p> <pre>set /SP CMM/services/http sessiontimeout=<i><n></i></pre>

表 35 Web サーバーの構成プロパティ (続き)

プロパティ	デフォルト値	説明
ユーザーインターフェースの構成可能なターゲットとユーザーの役割: ■ CLI: <code>/SP CMM/services/</code> ■ Web: 「ILOM Administration」 > 「Management Access」 > 「Web Server」 > 「Web Server Settings」 ■ ユーザーの役割: admin (a) (すべてのプロパティ変更に必要)		
HTTPS Webservice (<code>https/ servicestate=enabled</code>)	Enabled	<i>Enabled Disabled</i> 「HTTPS Webservice」プロパティを有効に設定した場合、Oracle ILOM は Web サーバーへセキュアに情報を転送するために HTTPS を使用します。 「HTTPS Webservice」プロパティを無効に設定した場合、Oracle ILOM での HTTPS を使用した Web サーバーへの情報転送の使用は無効になります。 「HTTPS Web Server」の CLI 構文: set /SP CMM/services/https servicestate=enabled disabled
HTTPS Port (<code>https/ port=</code>)	443	<i>443 User_defined</i> HTTPS サービスの状態が有効の場合、Oracle ILOM はデフォルトで、TCP ポート 443 を介した HTTP を使用して Web サーバーと通信します。必要に応じて、デフォルトのポート番号は変更できます。 「HTTPS Port」の CLI 構文: set /SP CMM/services/https port=<n>
HTTPS Session Timeout (<code>https/sessiontimeout=</code>)	15 seconds	<i>15 seconds User_defined</i> HTTPS Web セッションタイムアウトは、アクティブでない Web ブラウザクライアントが自動的にログアウトされるまでの時間 (分) を決定します。デフォルトの HTTPS Web セッションタイムアウトは 15 分です。必要に応じて、デフォルトのセッションタイムアウト値は増減できます。 「HTTPS Session Timeout」の CLI 構文: set /SP CMM/services/https sessiontimeout=<n>
SSLv2 (<code>https/ sslv2=disabled</code>)	Disabled	<i>Disabled Enabled</i> 「SSLv2」プロパティはデフォルトで無効になっています。必要に応じて、デフォルトの「SSLv2」プロパティは有効にできます。 「SSLv2」の CLI 構文: set /SP CMM/services/https sslv2=disabled enabled

表 35 Web サーバーの構成プロパティ (続き)

プロパティ	デフォルト値	説明
SSLv3 (https/ sslv3=enabled)	Enabled	<p><i>Enabled Disabled</i></p> <p>Oracle ILOM はデフォルトで、もっとも強力な Secure Socket Layer 暗号化を有効にするために SSLv3 および TLSv1 を使用します。必要に応じて、デフォルトの「SSLv3」プロパティは無効にできます。</p> <p>「SSLv3」の CLI 構文:</p> <pre>set /SP CMM/services/https sslv3=enabled disabled</pre>
TLSv1 (https/ tlsv1=enabled)	Enabled	<p><i>Enabled Disabled</i></p> <p>Oracle ILOM はデフォルトで、もっとも強力な Secure Socket Layer 暗号化を有効にするために SSLv3 および TLSv1 を使用します。必要に応じて、デフォルトの「TLSv1」プロパティは無効にできます。</p> <p>「TLSv1」の CLI 構文:</p> <pre>set /SP CMM/services/https tlsv1=enabled disabled</pre>
Weak Ciphers (https/ weak_ciphers=disabled)	Disabled	<p><i>Disabled Enabled</i></p> <p>「Weak Ciphers」プロパティはデフォルトで無効になっています。古い Web ブラウザの使用をサポートするために、弱い暗号を有効にする必要がある場合もあります。</p> <p>「Weak Ciphers」の CLI 構文:</p> <pre>set /SP CMM/services/https weak_ciphers=disabled enabled</pre> <p>関連情報:</p> <ul style="list-style-type: none"> 124 ページの「Web ブラウザのセキュリティ設定の解決」
Save		<p>Web インタフェース - 「Web Server Settings」ページでプロパティへの変更を適用するには、「Save」をクリックする必要があります。</p>

表 36 HTTPS Web サーバーの SSL 証明書および非公開鍵の構成プロパティー

プロパティー	デフォルト値	説明
ユーザーインターフェースの構成可能ターゲット、ユーザーの役割、SSL 証明書の要件: <ul style="list-style-type: none"> ■ CLI: <code>/SP CMM/services/https/ssl</code> ■ Web: 「ILOM Administration」 > 「Management Access」 > 「SSL Certificate」 > 「SSL Certificate Upload」 ■ ユーザーの役割: <code>admin(a)</code> (すべてのプロパティー変更に必要) ■ 要件: 有効なカスタム SSL 構成には、カスタム証明書とカスタム非公開鍵の両方をアップロードする必要があります。 		
Certificate File Status (certstatus=)	Using Default (カスタムの証明書または非公開鍵はロードされません)	<p><code>Default_Certificate</code> <code>Custom_Certificate</code></p> <p>「Certificate Status」プロパティーは読み取り専用プロパティーです。このプロパティーは、現在 HTTPS Web サーバーで次のうちの種類の SSL 証明書が使用中であるかを示します:</p> <ul style="list-style-type: none"> ■ デフォルトの SSL 証明書および Oracle ILOM で用意されている非公開の自己署名鍵 または ■ カスタムの信頼できる SSL 証明書および信頼できる認証局から提供される非公開鍵 <p>注 - デフォルトの SSL 証明書を使用している場合、Oracle ILOM Web インターフェースにはじめて接続するユーザーにはデフォルトの自己署名証明書が通知され、その使用を受け入れるよう求められます。デフォルトの自己署名 SSL 証明書を使用すると、Web ブラウザクライアントと Oracle ILOM SP (または CMM) の間のすべての通信が完全に暗号化されます。</p> <p>証明書のステータスを表示する CLI 構文:</p> <pre>show /SP CMM/https/ssl</pre>
Custom Certificate Load (/custom_certificate)		<p>Web インターフェース - 「File Transfer Method」プロパティーで指定されているカスタム証明書ファイルをアップロードするには「Load Certificate」ボタンをクリックします。</p> <p>注。有効なカスタム証明書構成には、カスタム証明書とカスタム非公開鍵をアップロードする必要があります。そうすることによってはじめてカスタム SSL 証明書構成が適用され、システムのリポートおよびバックアップ操作や復元操作を実行しても持続されるようになります。</p> <p>カスタム証明書をロードする CLI 構文:</p> <pre>load_uri=file_transfer_method://host_address/file_path/custom_certificate_filename</pre> <p>ここでは、<code>file_transfer_method</code> には次を含めることができます: <code>Browser TFTP FTP SCP HTTP HTTPS Paste</code></p> <p>各ファイル転送方法 (Paste を除く) の詳細な説明は、45 ページの「サポートされるファイル転送方式」を参照してください。</p>

表 36 HTTPS Web サーバーの SSL 証明書および非公開鍵の構成プロパティー (続き)

プロパティー	デフォルト値	説明
Custom Certificate Remove (/custom_certificate_clear_action=true)		<p>Web インタフェース - Oracle ILOM に現在格納されているカスタム SSL 証明書ファイルを削除するには、「Remove Certificate」ボタンをクリックします。確認のメッセージが表示されたら、「Yes」をクリックして削除するか、「No」をクリックして操作を取り消します。</p> <p>証明書を削除する CLI 構文:</p> <pre>set /SP CMM/services/https/ssl/custom_certificate clear_action=true</pre> <p>確認のメッセージが表示されたら、y と入力して削除するか、n と入力して操作を取り消します。</p>
Custom Private Key (/custom_key)		<p>Web インタフェース - 「File Transfer Method」プロパティーで指定されているカスタム非公開鍵ファイルをアップロードするには「Load Custom Private Key」ボタンをクリックします。</p> <p>注。有効なカスタム証明書構成には、カスタム証明書とカスタム非公開鍵をアップロードする必要があります。そうすることによってはじめてカスタム SSL 証明書構成が適用され、システムのリブートおよびバックアップ操作や復元操作を実行しても持続されるようになります。</p> <p>カスタム非公開鍵をロードする CLI 構文:</p> <pre>load uri=file_transfer_method://host_address/file_path/custom_key_filename</pre> <p>ここでは、file_transfer_method には、次を含めることができます: Browser TFTP FTP SCP HTTP HTTPS Paste</p> <p>各ファイル転送方法(Paste を除く)の詳細な説明は、45 ページの「サポートされるファイル転送方式」を参照してください。</p>
Custom Private Key Remove (/custom_key_clear_action=true)		<p>Web インタフェース - Oracle ILOM に現在格納されているカスタム非公開鍵ファイルを削除するには、「Remove Custom Private Key」ボタンをクリックします。確認のメッセージが表示されたら、「Yes」をクリックして削除するか、「No」をクリックして操作を取り消します。</p> <p>証明書非公開鍵を削除する CLI 構文:</p> <pre>set /SP CMM/services/https/ssl/custom_key clear_action=true</pre> <p>確認のメッセージが表示されたら、y と入力して削除するか、n と入力して操作を取り消します。</p>

表 37 SNMP 構成プロパティ

プロパティ	デフォルト値	説明
ユーザーインターフェースの構成可能ターゲット、ユーザーの役割、および SNMP の要件: <ul style="list-style-type: none"> ■ CLI: <code>/SP CMM/services/snmp</code> ■ Web: 「ILOM Administration」 > 「Management Access」 > 「SNMP」 > 「SNMP Management」 ■ ユーザーの役割: admin (a) (すべてのプロパティ変更に必要) ■ 要件: SNMPv3 サービスにはユーザーアカウントが必要です。SNMPv1 または v2c サービスにはコミュニティが必要です。 		
State (state=)	Enabled	<p><i>Enabled Disabled</i></p> <p>「SNMP State」プロパティはデフォルトで有効になっています。このプロパティが有効で、かつ SNMP の 1 つまたは複数のユーザーアカウントまたはコミュニティのプロパティが構成されている場合に、Oracle ILOM の SNMP 管理サービスを使用できます。</p> <p>「SNMP State」プロパティが無効の場合、SNMP ポートがブロックされ、Oracle ILOM とネットワーク間の SNMP 通信はすべて禁止されます。</p> <p>「SNMP State」の CLI 構文:</p> <pre>set /SP CMM/services/snmp state=enabled disabled</pre>
ポート (port=)	161	<p><i>161 User_specified.</i></p> <p>Oracle ILOM はデフォルトで、Oracle ILOM SP (または Oracle ILOM CMM) とネットワーク間の SNMP 通信の転送に TCP ポート 161 を使用します。必要に応じて、デフォルトのポートプロパティ番号は変更できます。</p> <p>「SNMP Port」の CLI 構文:</p> <pre>set /SP CMM/services/snmp port=n</pre>
Engine ID (engineid=)	Auto-set by SNMP agent	<p>「Engine ID」プロパティは、Oracle ILOM SNMP エージェントによって自動的に設定されます。</p> <p>この ID は、Oracle ILOM SNMP が有効な各システムに固有のものです。エンジン ID は構成可能ですが、この ID は各 Oracle ILOM システムについてデータセンター全体で常に一意になるようにしてください。SNMP v3 セキュリティーに精通している経験豊富な SNMP ユーザーのみが SNMP の「Engine ID」プロパティを変更するようにしてください。</p>

表 37 SNMP 構成プロパティ (続き)

ユーザーインターフェースの構成可能ターゲット、ユーザーの役割、および SNMP の要件:

- **CLI:** `/SP|CMM/services/snmp`
- **Web:** 「ILOM Administration」 > 「Management Access」 > 「SNMP」 > 「SNMP Management」
- ユーザーの役割: **admin (a)** (すべてのプロパティ変更に必要)
- 要件: **SNMPv3** サービスにはユーザーアカウントが必要です。 **SNMPv1** または **v2c** サービスにはコミュニティが必要です。

プロパティ	デフォルト値	説明
Set Requests (sets=)	Disabled	<p><i>Disabled Enabled</i></p> <p>Oracle ILOM の「Set Requests」プロパティは、デフォルトで無効になっています。</p> <p>「Sets Requests」プロパティが無効の場合、監視を目的として次の SNMP MIB を使用できます:</p> <ul style="list-style-type: none"> ■ SUN-HW-TRAP-MIB - 障害などハードウェア関連イベントのトラップ通知を監視するにはこの MIB を使用します。 ■ SUN-PLATFORM-MIB - インベントリや健全性といったハードウェア関連情報をポーリングするにはこの MIB を使用します。 <p>「Set Requests」プロパティが有効の場合、上記の MIB を監視目的に使用でき、次の MIB を管理目的に使用できます:</p> <ul style="list-style-type: none"> ■ SUN-HW-CTRL-MIB - 電源管理などのハードウェアポリシーを構成するには、この MIB を使用します。 ■ SUN-ILOM-CONTROL-MIB - ユーザーの作成やサービスの構成といった Oracle ILOM 機能を構成するにはこの MIB を使用します。 <p>「Set Requests」の CLI 構文:</p> <pre>set /SP CMM/services/snmp sets=<i>disabled enabled</i></pre> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 『Oracle ILOM 3.1 プロトコル管理リファレンス』の SNMP を使用したサーバー管理に関する内容

表 37 SNMP 構成プロパティ (続き)

プロパティ	デフォルト値	説明
Protocols (v1 v2c v3)	v3, Enabled	<p>v1 v2c v3</p> <p>Oracle ILOM では、デフォルトで SNMP v3 の使用が有効になっており、SNMP v1 および v2c の使用が無効になっています。</p> <p>SNMPv1 と v2c は暗号化をサポートしておらず、認証の一形態としてコミュニティ文字列を使用します。SNMPv3 は暗号化を使用してセキュアなチャネルを提供し、SNMP 管理ステーションにセキュアに格納された個別のユーザー名およびパスワードを使用します。</p> <p>必要に応じて、デフォルトの「SNMP Protocol」のプロパティ値は構成可能です。</p> <p>注 - 監視目的には SNMP v2c または v3 を使用し、「Set Requests」のデフォルトプロパティは無効のままにしておきます。</p> <p>デフォルトプロトコルを変更する CLI 構文:</p> <pre>set /SP CMM/services/snmp v1 v2c v3=enabled disabled</pre>
Save		<p>Web インタフェース - 「SNMP Management」 ページでプロパティへの変更を適用するには、「Save」をクリックする必要があります。</p>
SNMP Communities (/communities)		<p>Community Name Permission= Read-only (ro) Read-write (rw)</p> <p>SNMP コミュニティは、ユーザーアクセスを制御するための SNMP v1 または v2c、および Oracle ILOM の承認レベルにのみ適用されます。SNMP v1 または v2c の「Protocols」プロパティが有効の場合、SNMP コミュニティのプロパティは Oracle ILOM で構成できます。</p> <p>コミュニティの構成時には次のルールが適用されます:</p> <ul style="list-style-type: none"> ■ コミュニティ名 - 長さは最大 35 文字まで、英字で始める必要があります、スペースは使用できません ■ 保存 (Web インタフェースのみ) - 「SNMP Add SNMP User」ダイアログで行われたすべての変更は保存する必要があります <p>SNMP コミュニティを作成する CLI 構文:</p> <pre>create /SP CMM/services/snmp/communities name=community_name permission=rw ro show /SP CMM/services/snmp/communities public private delete /SP CMM/services/snmp/communities community_name</pre>

表 37 SNMP 構成プロパティー (続き)

プロパティー	デフォルト値	説明
SNMP Users (/users)	<i>Username Authentication Password Permission Authentication Protocol Privacy Protocol</i>	<p>ユーザーインタフェースの構成可能ターゲット、ユーザーの役割、および SNMP の要件:</p> <ul style="list-style-type: none"> ■ CLI: <code>/SP CMM/services/snmp</code> ■ Web: 「ILOM Administration」 > 「Management Access」 > 「SNMP」 > 「SNMP Management」 ■ ユーザーの役割: admin (a) (すべてのプロパティー変更に必要) ■ 要件: SNMPv3 サービスにはユーザーアカウントが必要です。 SNMPv1 または v2c サービスにはコミュニティが必要です。 <p>SNMP ユーザーは、ユーザーアクセスを制御するための SNMP v3、および Oracle ILOM の承認レベルにのみ適用されます。 SNMP v3 の 「Protocol」 プロパティーが有効の場合、 SNMP ユーザーのプロパティーは Oracle ILOM で構成できます。</p> <p>SNMP ユーザーの構成時には次のルールが適用されます:</p> <ul style="list-style-type: none"> ■ ユーザー名 - 長さは最大 35 文字まで、英字で始める必要があります、スペースは使用できません ■ 認証またはプライバシーパスワード - 長さは最大 16 文字まで、大文字と小文字が区別され、コロンおよびスペースは使用できず、パスワードの確認が必要です ■ 保存 (Web インタフェースのみ) - 「SNMP Add SNMP User」 ダイアログで行われたすべての変更は保存する必要があります。 <p>SNMP ユーザーを作成する CLI 構文:</p> <pre>create /SP CMM/services/snmp/users username=value authenticationprotocol=MD5 SHA authenticationpassword=value permissions=ro rw privacyprotocol=aes des none show /SP CMM/services/snmp/users delete /SP CMM/services/snmp/username</pre>
MIBs Download (/mibs dump_uri=)		Oracle ILOM は、SUN SNMP MIB をサーバー SP または CMM から直接ダウンロードする機能を備えています。

表 38 SSH サーバーの構成プロパティ

プロパティ	デフォルト値	説明
ユーザーインタフェースの構成可能なターゲットとユーザーの役割: <ul style="list-style-type: none"> ■ CLI: <code>/SP CMM/services/ssh</code> ■ Web: 「ILOM Administration」 > 「Management Access」 > 「SSH Server」 > 「SSH Server Settings」 ■ ユーザーの役割: <code>admin (a)</code> (すべてのプロパティ変更に必要) 		
State (state=)	Enabled	<p><i>Enabled Disabled</i></p> <p>「SSH Server State」プロパティはデフォルトで有効になっています。</p> <p>「SSH Server State」プロパティが有効の場合、SSH サーバーはサーバー側鍵を使用し、リモートクライアントがコマンド行インタフェースを使用して Oracle ILOM SP (または Oracle ILOM CMM) にセキュアに接続することを許可します。</p> <p>「SSH Server State」プロパティを無効にしたり再起動したりすると、SSH を介して実行しているすべての CLI SP または CLI CMM セッションは自動的に終了します。</p> <p>注。Oracle ILOM は、出荷時のデフォルトシステムの最初のブート時に SSH サーバー側鍵を自動的に生成します。</p> <p>Web インタフェース: Web インタフェースで「SSH Server State」を変更しても、Oracle ILOM では「Save」をクリックするまで有効になりません。</p> <p>「SSH Server State」の CLI 構文:</p> <pre>set /SP CMM/services/ssh state=enabled disabled</pre>
Restart Button (restart_sshd_action=)		<p><i>True False</i></p> <p>SSH サーバーを再起動すると自動的に: (1) 接続されているすべての SP または CMM CLI セッションを終了し、(2) 新しく保留中のサーバー側鍵をアクティブ化します。</p> <p>「Restart」の CLI 構文:</p> <pre>set /SP CMM/services/ssh restart_sshd_action=true</pre>
Generate RSA Key Button (generate_new_key_type=rsa generate_new_key_action= true)		<p>新しい RSA SSH 鍵を生成する機能を提供します。</p> <p>「Generate RSA Key」の CLI 構文:</p> <pre>set /SP CMM/services/ssh generate_new_key_type=rsa generate_new_key_action=true</pre>

表 38 SSH サーバーの構成プロパティ (続き)

ユーザーインタフェースの構成可能なターゲットとユーザーの役割:

- **CLI:** `/SP|CMM/services/ssh`
- **Web:** 「ILOM Administration」 > 「Management Access」 > 「SSH Server」 > 「SSH Server Settings」
- ユーザーの役割: `admin (a)` (すべてのプロパティ変更に必要)

プロパティ	デフォルト値	説明
Generate DSA Key Button (<code>generate_new_key_type=dsa</code> <code>generate_new_key_action=</code>)		新しい DSA SSH 鍵を生成する機能を提供します。 「Generate DSA Key」の CLI 構文: set /SP CMM/services/ssh generate_new_key_type=dsa generate_new_key_action=true

表 39 IPMI サービスの構成プロパティ

ユーザーインタフェースの構成可能なターゲット:

- **CLI:** `/SP|CMM/services/ipmi`
- **Web:** 「ILOM Administration」 > 「Management Access」 > 「IPMI」 > 「IPMI Settings」

ユーザーの役割:

- `admin (a)` - IPMI 仕様の構成プロパティの変更に必要
- Administrator または Operator - Oracle ILOM CLI から IPMI サービス (IPMItool) を使用する場合に必要。

プロパティ	デフォルト値	説明
State (<code>state=</code>)	Enabled	<i>Enabled Disabled</i> IPMI v2 の「State」プロパティはデフォルトで有効になっています。 「IPMI State」プロパティを有効にすると、Oracle ILOM はリモート IPMItool クライアントがコマンド行インタフェースを使用して Oracle ILOM SP (または Oracle ILOM CMM) にセキュアに接続することを許可します。 「IPMI State」プロパティを無効にすると、Oracle ILOM CLI 経由で SP または CMM に接続されているすべての IPMItool クライアントは自動的に終了します。 Web インタフェース: Web インタフェースで「IPMI State」を変更しても、Oracle ILOM では「Save」をクリックするまで有効になりません。 「IPMI State」の CLI 構文: set /SP CMM/services/ipmi state=enabled disabled

表 40 CLIセッションタイムアウトの構成プロパティ

ユーザーインターフェースの構成可能なターゲット:

- **CLI:** `/SP|CMM/cli`
- **Web:** 「ILOM Administration」 > 「Management Access」 > 「IPMI」 > 「IPMI Settings」

ユーザーの役割:

- `admin (a)` - IPMI 仕様の構成プロパティの変更に必要
- `Administrator` または `Operator` - Oracle ILOM CLI から IPMI サービス (IPMItool) を使用する場合に必要。

プロパティ	デフォルト値	説明
Session Timeout (timeout=)	Disabled	<p><i>Disabled Enabled, minutes=n</i></p> <p>「CLI Session Timeout」プロパティは、アクティブでない CLI セッションを自動的にログアウトするまでの時間 (分) を決定します。</p> <p>デフォルトでは、CLI タイムアウトは構成されていません。Oracle ILOM CLI を共有コンソール上で使用している場合、ネットワーク管理者は CLI セッションタイムアウトの値を 15 分以下に設定することが推奨されます。</p> <p>Web インタフェース: Web インタフェースで CLI セッションタイムアウトのプロパティを変更しても、Oracle ILOM では「Save」をクリックするまで有効になりません。</p> <p>「IPMI State」の CLI 構文:</p> <pre>set /SP CMM/cli timeout=enabled disabled minutes=value</pre>

表 41 WS-Man Web サービスの構成プロパティ

プロパティ	デフォルト値	説明
ユーザーインターフェースの構成可能なターゲットとユーザーの役割: ■ CLI: <code>/SP CMM/services/wsman</code> ■ Web: 「ILOM Administration」 > 「Management Access」 > 「WS-MAN」 > 「WS-Man Settings」 ■ ユーザーの役割: admin (a) (すべてのプロパティ変更に必要)		
State (state=)	Enabled	<p><i>Enabled Disabled</i></p> <p>WS-Man Web サービスの「State」プロパティはデフォルトで有効になっています。必要に応じて、WS-Man Web サービスの状態は無効にできます。</p> <p>Web インタフェース: Web インタフェースで WS-Man の状態を変更しても、Oracle ILOM では「Save」をクリックするまで有効になりません。</p> <p>「WS-Man State」の CLI 構文:</p> <pre>set /SP CMM/services/wsman state=enabled disabled</pre> <p>関連情報: ■</p>
Mode (mode=http)	ポート 8899 を介した HTTP	<p><i>HTTP HTTPS</i></p> <p>「Mode」プロパティはデフォルトで「HTTP」に設定されています。セキュリティを強化するために、このデフォルトプロパティ値を HTTPS に設定できます。</p> <p>「WS-Man Mode」の CLI 構文:</p> <pre>set /SP CMM/services/wsman mode=http https</pre>
HTTP Port (http_port=)	8889	<p><i>8889 user_defined</i></p> <p>「State」プロパティが有効で、かつ「Mode」プロパティが「HTTP」に設定されている場合、Oracle ILOM は WS-Man Web サービスに TCP ポート 8889 を使用します。</p> <p>必要に応じて、デフォルトのポートプロパティ値は変更できません。</p> <p>「WS-MAN HTTP Port」の CLI 構文:</p> <pre>set /SP CMM/services/wsman http_port=n</pre>

表 41 WS-Man Web サービスの構成プロパティ (続き)

プロパティ	デフォルト値	説明
ユーザーインターフェースの構成可能なターゲットとユーザーの役割: <ul style="list-style-type: none"> ■ CLI: <code>/SP CMM/services/wsman</code> ■ Web: 「ILOM Administration」 > 「Management Access」 > 「WS-MAN」 > 「WS-Man Settings」 ■ ユーザーの役割: admin (a) (すべてのプロパティ変更に必要) 		
HTTPS Port (<code>https_port=</code>)	8888	8888 <i>user_defined</i> 「State」プロパティが有効で、かつ「Mode」プロパティが「HTTPS」に設定されている場合、Oracle ILOM は WS-Man Web サービスに TCP ポート 8888 を使用します。 必要に応じて、デフォルトのポートプロパティ値は変更できません。 「WS-Man HTTPS Port」の CLI 構文: set /SP CMM/services/wsman https_port=<i>n</i>

表 42 バナーメッセージの構成プロパティ

プロパティ	デフォルト値	説明
ユーザーインターフェースの構成可能なターゲットとユーザーの役割: <ul style="list-style-type: none"> ■ CLI: <code>/SP CMM/preferences/banner</code> ■ Web: 「ILOM Administration」 > 「Management Access」 > 「Banner Messages」 ■ ユーザーの役割: admin (a) (プロパティ変更に必要) 		
Connect Message (<code>connect_message=</code>)		「Connect Message」プロパティに、Oracle ILOM への接続時に Oracle ILOM インタフェースに表示する内容を入力します。 「Connect Message」を設定する CLI 構文: set /SP/preferences/banner connect_message=<content>
Login Message (<code>login_message=</code>)		「Login Message」プロパティに、Oracle ILOM へのログイン後に Oracle ILOM インタフェースに表示する内容を入力します。 「Login Message」を設定する CLI 構文: set /SP/preferences/banner login_message=<content>
Login Message Acceptance (<code>login_message_acceptance=</code>)	Disabled	Disabled Enabled バナーメッセージを表示するには「Login Banner Acceptance」プロパティを有効に設定します。 「Login Message Acceptance」の CLI 構文: set /SP/preferences/banner login_message_acceptance=disabled enabled

デフォルトの接続構成プロパティの変更

ネットワーク管理者は、Oracle ILOM に標準装備されたデフォルトの接続プロパティを必要に応じて受け入れたり変更したりできます。Oracle ILOM でデフォルトの接続プロパティを変更するには、次の表を参照してください:

- 表 43
- 表 44
- 表 45

表 43 ネットワーク接続の構成プロパティ

ユーザーインターフェースの構成可能なターゲットとユーザーの役割:

- **CLI:** `/SP|CMM/network`
- **Web:** 「ILOM Administration」 > 「Connectivity」 > 「Network」 > 「Network Settings」
- ユーザーの役割: **admin (a)** (すべてのプロパティ変更に必要な)

要件:

- CLI で保留中のネットワーク変更を Oracle ILOM で有効にするには、コミットする必要があります。
- Web の 「Network Settings」 ページで行われたネットワーク変更を Oracle ILOM で有効にするには、保存する必要があります。

プロパティ	デフォルト値	説明
State (state=)	Enabled	<p><i>Enabled Disabled</i></p> <p>「network State」プロパティはデフォルトで有効になっています。IPv4 ネットワーク環境または IPv4/IPv6 デュアルスタックネットワーク環境で Oracle ILOM を動作させるには、このプロパティを常に有効にする必要があります。</p> <p>「Network State」を設定する CLI 構文:</p> <pre>set /SP CMM/network pendingstate=enabled disabled</pre>
MAC Address	読み取り専用	<p>macaddress= outofbandaddress= sidebandmacaddress=</p> <p>サーバー SP および CMM のメディアアクセス制御 (MAC) アドレスは、出荷時に設定されます。</p> <p>SP および CMM の MAC アドレスプロパティは、どちらも Oracle ILOM の構成不可能な読み取り専用プロパティです。</p> <p>「MAC Address」プロパティを表示する CLI 構文:</p> <pre>show /SP CMM/network</pre>

表 43 ネットワーク接続の構成プロパティ (続き)

ユーザーインターフェースの構成可能なターゲットとユーザーの役割:

- **CLI:** `/SP|CMM/network`
- **Web:** 「ILOM Administration」 > 「Connectivity」 > 「Network」 > 「Network Settings」
- ユーザーの役割: **admin (a)** (すべてのプロパティ変更に必要)

要件:

- CLI で保留中のネットワーク変更を Oracle ILOM で有効にするには、コミットする必要があります。
- Web の「Network Settings」ページで行われたネットワーク変更を Oracle ILOM で有効にするには、保存する必要があります。

プロパティ	デフォルト値	説明
Management Port (managementport=)	MGMT	<p><i>MGMT NETn</i></p> <p>Oracle ILOM が標準装備されたすべてのサーバーには、ネットワークを介して Oracle ILOM に接続するために使用する物理ネットワーク管理ポート (MGT) が搭載されています。Oracle ILOM が標準装備された一部のシステムは、サイドバンド管理もサポートしています。サイドバンド管理では、サーバーの物理データポート (NETn) の使用を共有し、ホストオペレーティングシステムと Oracle ILOM 両方へのネットワークアクセスを許可します。</p> <p>このオプションをサポートしているシステムの場合、ネットワーク管理者はデフォルトの「Management Port」プロパティ (MGMT) を受け入れるか、「Management Port」プロパティを変更してサイドバンド管理を使用 (NETn) するかを選択できます。</p> <p>「SP Management Port」の CLI 構文:</p> <pre>set /SP/network pendingmanagementport=MGMT NETn</pre> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 14 ページの「サイドバンドネットワーク管理接続」 ■ 12 ページの「専用ネットワーク管理接続 (デフォルト)」

表 43 ネットワーク接続の構成プロパティー (続き)

ユーザーインターフェースの構成可能なターゲットとユーザーの役割:

- CLI: `/SP|CMM/network`
- Web: 「ILOM Administration」 > 「Connectivity」 > 「Network」 > 「Network Settings」
- ユーザーの役割: `admin (a)` (すべてのプロパティー変更に必要)

要件:

- CLI で保留中のネットワーク変更を Oracle ILOM で有効にするには、コミットする必要があります。
- Web の 「Network Settings」 ページで行われたネットワーク変更を Oracle ILOM で有効にするには、保存する必要があります。

プロパティー	デフォルト値	説明
IPv4 IP Discovery Mode (<code>ipdiscovery=</code>)	DHCP	<p><i>DHCP Static</i></p> <p>Oracle ILOM の 「IPv4 Discovery Mode」 プロパティーはデフォルトで 「DHCP」 に設定されています。このプロパティーが 「DHCP」 に設定されている場合、Oracle ILOM はサーバー SP または CMM の物理ネットワークアドレスの判定に DHCP を使用します。</p> <p>また、ネットワーク管理者は 「DHCP」 プロパティーを無効にして、サーバー SP または CMM に静的 IPv4 ネットワークアドレス、ネットマスクアドレス、およびゲートウェイアドレスを構成するように選択することもできます。</p> <p>注。 「DHCP」 が設定されている場合、Oracle ILOM は DNS ネームサーバーおよび検索パスの割り当てにデフォルトの 「Auto DNS」 プロパティーを使用します。デュアルスタック DHCP 構成の場合、Oracle ILOM の DNS 設定では、DNS 情報を IPv4 または IPv6 DHCP サーバーのどちらかから受信するように設定できます。</p> <p>「IPv4 IP Discovery Mode」 の CLI 構文:</p> <pre>set /SP CMM/network pendingipdiscoverymode=<i>dhcp static</i></pre> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 表 44
IPv4 DHCP Client ID (<code>dhcp_clientid=</code>)	なし	<p><i>None SysID</i></p> <p>「DHCP Client ID」 のプロパティーはデフォルトで 「None」 に設定されています。ネットワーク管理者は、DHCP クライアントに 「SysID」 (システム識別子) を設定することもできます。</p> <p>「IPv4 DHCP Client ID」 の CLI 構文:</p> <pre>set /SP CMM/network pendingdhcip_clientid=<i>none sysid</i></pre> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 121 ページの 「システム識別情報の割り当て」

表 43 ネットワーク接続の構成プロパティ (続き)

プロパティ	デフォルト値	説明
IPv4 Network Address Netmask Address Gateway Address	Static IP Discovery Mode、Disabled	<p>ipaddress= ipnetmask= ipgateway=</p> <p>Oracle ILOM のネットワーク、ネットマスク、およびゲートウェイのユーザー構成可能な IPv4 アドレスプロパティは、デフォルトで無効になっています。</p> <p>ネットワーク管理者は任意で「IP Discovery Mode」プロパティの「Static」の値を設定し、ネットワーク、ネットマスク、およびゲートウェイの静的 IPv4 アドレスを手動で入力できます。</p> <p>「IPv4 Static Addresses」の CLI 構文:</p> <pre>set /SP CMM/network pendingipaddress=value pendingipnetmask=value pendingipgateway=value</pre> <p>関連情報:</p> <ul style="list-style-type: none"> 88 ページの「IPv4 および IPv6 アドレスの入力形式」
IPv6 State (/ipv6/ state=)	Enabled	<p>Enabled Disabled</p> <p>Oracle ILOM の「IPv6 State」プロパティは、デフォルトで有効になっています。ネットワーク管理者は、デュアルスタック IP トランスレーションに依存していないネットワーク環境の IPv6 ネットワーク状態を無効にすることもできます。</p> <p>注 - デュアルスタック IP トランスレーションでは、Oracle ILOM の IPv6 状態を有効にする必要があります。</p> <p>「IPv6 State」の CLI 構文:</p> <pre>set /SP CMM/network/ipv6 pendingaddress=enabled disabled</pre>

ユーザーインターフェースの構成可能なターゲットとユーザーの役割:

- CLI: /SP|CMM/network
- Web: 「ILOM Administration」 > 「Connectivity」 > 「Network」 > 「Network Settings」
- ユーザーの役割: admin (a) (すべてのプロパティ変更に必要)

要件:

- CLI で保留中のネットワーク変更を Oracle ILOM で有効にするには、コミットする必要があります。
- Web の「Network Settings」ページで行われたネットワーク変更を Oracle ILOM で有効にするには、保存する必要があります。

表 43 ネットワーク接続の構成プロパティー (続き)

プロパティー	デフォルト値	説明
IPv6 Autoconfig (/ipv6 autoconfig=)	Stateless、Enabled	<p>Oracle ILOM の「IPv6 Autoconfig」プロパティーは、デフォルトで「Stateless」に設定されています。「Autoconfig Stateless」プロパティーが有効の場合、Oracle ILOM はサーバー SP または CMM の IPv6 アドレスを、IPv6 用に構成されたネットワークルーターから取得します。</p> <p>「IPv6 Autoconfig Stateless」プロパティーが「None」に設定されている場合、Oracle ILOM は「Autoconfig Stateless」を使用してサーバー SP または CMM の IPv6 ネットワークアドレスを取得することができません。</p> <p>特別な考慮事項:</p> <ul style="list-style-type: none"> 「IPv6 Autoconfig Stateless」オプションは、DHCPv6 サーバーからの IP サポートなしで IP アドレスを判定します。 「dhcpv6_server_duid=」の読み取り専用プロパティー値が「none」に設定されるのは、Oracle ILOM の「IPv6 Autoconfig Stateless」プロパティーが有効の場合のみです。 Oracle ILOM の「IPv6 Auto config Stateless」プロパティーは「DHCPv6_Stateless」または「DHCPv6_Stateful」のどちらかが有効の場合に同時に有効にできます。 <p>「IPv6 Auto Config」の CLI 構文:</p> <pre>set /SP CMM/network/ipv6 autoconfig=stateless none</pre>

表 43 ネットワーク接続の構成プロパティ (続き)

ユーザーインターフェースの構成可能なターゲットとユーザーの役割:

- CLI: `/SP|CMM/network`
- Web: 「ILOM Administration」 > 「Connectivity」 > 「Network」 > 「Network Settings」
- ユーザーの役割: `admin (a)` (すべてのプロパティ変更に必要)

要件:

- CLI で保留中のネットワーク変更を Oracle ILOM で有効にするには、コミットする必要があります。
- Web の 「Network Settings」 ページで行われたネットワーク変更を Oracle ILOM で有効にするには、保存する必要があります。

プロパティ	デフォルト値	説明
DHCPv6 Autoconfig (/ipv6 autoconfig=)	None, Disabled	<p><code>DHCPv6_Stateless DHCP_Stateful None</code></p> <p>Oracle ILOM の 「DHCPv6 Autoconfig」 プロパティは、デフォルトで無効 (「None」 に設定) になっています。このプロパティが 「None」 に設定されている場合、Oracle ILOM は SP または CMM のネットワークアドレスおよび DNS 情報をネットワーク上の DHCPv6 サーバーから取得できません。</p> <p>ネットワーク管理者は、Oracle ILOM の 「DHCPv6 Autoconfig」 プロパティを次のいずれかの値に設定することで、ネットワークに接続された DHCPv6 サーバーが SP または CMM の IPv6 アドレスおよび DNS 情報を割り当てるように選択することもできます:</p> <ul style="list-style-type: none"> ■ DHCPv6 Stateless - 有効にすると、Oracle ILOM は DHCPv6 Stateless Autoconfig を使用してサーバー SP または CMM の IPv6 アドレスおよび DNS 情報を取得します。 ■ DHCPv6 Stateful - 有効にすると、Oracle ILOM は DHCPv6 stateful Autoconfig を使用してサーバー SP または CMM の IPv6 アドレスおよび DNS 情報を取得します。 <p>特別な考慮事項:</p> <ul style="list-style-type: none"> ■ Oracle ILOM の 「IPv6 Autoconfig Stateless」 プロパティは、「DHCPv6_Stateless」または「DHCPv6_Stateful」のどちらかを使用するように「DHCPv6 Autoconfig」が有効になっている場合に同時に有効にできます。 ■ デュアルスタック DHCP 構成の場合、Oracle ILOM の DNS 設定では、DNS 情報を IPv4 または IPv6 DHCP サーバーのいずれかから受信するように設定できます。 ■ DHCPv6 ネットワーク情報を取得するために Oracle ILOM が最後に使用した DHCPv6 サーバーの固有 ID は、「dhcpv6_server_ duid」プロパティによって識別されます。 <p>「DHCPv6 Autoconfig」の CLI 構文:</p> <pre>set /SP CMM/network/ipv6 autoconfig=dhcpv6_stateless dhcpv6_stateful none</pre>

表 43 ネットワーク接続の構成プロパティ (続き)

ユーザーインタフェースの構成可能なターゲットとユーザーの役割:

- CLI: `/SP|CMM/network`
- Web: 「ILOM Administration」 > 「Connectivity」 > 「Network」 > 「Network Settings」
- ユーザーの役割: `admin (a)` (すべてのプロパティ変更に必要)

要件:

- CLI で保留中のネットワーク変更を Oracle ILOM で有効にするには、コミットする必要があります。
- Web の 「Network Settings」 ページで行われたネットワーク変更を Oracle ILOM で有効にするには、保存する必要があります。

プロパティ	デフォルト値	説明
Link-Local IPv6 Address (<code>/ipv6 link_local_ipaddress=</code>)	読み取り専用	<p>読み取り専用の 「Link-Local IPv6 Address」 プロパティは、同じネットワーク上の IPv6 が有効な別のノードから Oracle ILOM SP (または CMM) への接続に使用できる、ルーティングの宛先とならないアドレスです。</p> <p>Oracle ILOM は、SP または CMM のリンクローカルアドレスの構築に次の原則を適用します:</p> <ul style="list-style-type: none"> ■ Oracle ILOM は、SP または CMM MAC アドレスとリンクローカル識別子プレフィックスを組み合わせ使用します。 ■ Oracle ILOM は、初期化の際に重複アドレス検出 (DAD) プロトコルを使用して、SP (または CMM) の報告されたローカルリンクアドレスが一意であることを確認します。 <p>「Link-Local Address」 の CLI 構文:</p> <pre>show /SP CMM/network/ipv6</pre>
IPv6 Static IP Address (<code>/ipv6 static_ipaddress=</code>)	なし	<p>IPv6 の状態が有効の場合、ネットワーク管理者は静的 IPv6 アドレスを SP または CMM に割り当てることもできます。</p> <p>IPv6 静的 IP およびネットマスクを指定するためのパラメータは次のとおりです: <code>IPv6_address/ subnet_mask_length_in_bits</code>。ゲートウェイアドレスは自動的に構成されます。</p> <p>例: <code>fec0:a:8:b7:214:4fff:feca:5f7e/64</code></p> <p>「Static IPv6 Address」 の CLI 構文:</p> <pre>set /SP CMM/network/ipv6 static_ipaddress=ipaddress/subnetmask</pre>
IPv6 Gateway (<code>/ipv6 ipgateway=</code>)	読み取り専用	<p>このプロパティに表示される読み取り専用の IPv6 ゲートウェイアドレスは、ネットワーク上の IPv6 ルーターから取得されます。</p> <p>「IPv6 Gateway」 の CLI 構文:</p> <pre>show /SP CMM/network/ipv6</pre>

表 43 ネットワーク接続の構成プロパティ (続き)

ユーザーインタフェースの構成可能なターゲットとユーザーの役割:

- **CLI:** `/SP|CMM/network`
- **Web:** 「ILOM Administration」 > 「Connectivity」 > 「Network」 > 「Network Settings」
- ユーザーの役割: `admin (a)` (すべてのプロパティ変更に必要)

要件:

- CLI で保留中のネットワーク変更を Oracle ILOM で有効にするには、コミットする必要があります。
- Web の 「Network Settings」 ページで行われたネットワーク変更を Oracle ILOM で有効にするには、保存する必要があります。

プロパティ	デフォルト値	説明
Dynamic IPv6 Address (<code>/ipv6 dynamic_ipaddress_n</code>)	読み取り専用	<p>Oracle ILOM は、次が発生した場合に動的 IPv6 アドレスを報告します:</p> <ul style="list-style-type: none"> ■ Oracle ILOM で 「Autoconfig Stateless」 と 「Autoconf DHCPv6_Stateful」 のプロパティの両方またはいずれかが有効になっている。 ■ IPv6 ネットワークルーターまたは DHCPv6 サーバーが、サーバー SP または CMM の複数の動的ネットワークアドレスを報告する。 <p>特別な考慮事項:</p> <ul style="list-style-type: none"> ■ Oracle ILOM は、内部構造に 10 個の動的アドレスを格納します。 ■ Oracle ILOM はすべての動的ネットワークアドレスに応答しません。 ■ 「Autoconfig DHCPv6_Stateless」 プロパティのみが設定されている場合、Oracle ILOM インタフェースでは動的ネットワークアドレスは報告されません。 <p>「Dynamic IPv6 Address」 の CLI 構文:</p> <pre>show /SP CMM/network/ipv6</pre>

表 43 ネットワーク接続の構成プロパティー (続き)

ユーザーインターフェースの構成可能なターゲットとユーザーの役割:

- **CLI:** `/SP|CMM/network`
- **Web:** 「ILOM Administration」 > 「Connectivity」 > 「Network」 > 「Network Settings」
- ユーザーの役割: **admin (a)** (すべてのプロパティー変更に必要)

要件:

- CLI で保留中のネットワーク変更を Oracle ILOM で有効にするには、コミットする必要があります。
- Web の「Network Settings」ページで行われたネットワーク変更を Oracle ILOM で有効にするには、保存する必要があります。

プロパティー	デフォルト値	説明
Save Button (<code>commitpending=true</code>)	All pending network modifications	<p>Web インタフェース - 「Network Settings」ページで行われたすべての変更を Oracle ILOM で有効にするには、保存する必要があります。</p> <p>CLI - 保留中のすべてのネットワーク変更は、<code>/network</code> ターゲットでコミットする必要があります。</p> <p>特別な考慮事項:</p> <ul style="list-style-type: none"> ■ 保留中の IPv4 の変更は、コミットまたは保存されたあとに有効になります。 ■ 管理対象デバイスに新しい静的 IPv4 アドレスを割り当てると、SP または CMM へのアクティブな Oracle ILOM セッションがすべて終了します。Oracle ILOM にログインし直すには、新しいブラウザセッションを開いて新しく割り当てられた IPv4 アドレスを入力します。 ■ 保留中の IPv6 の変更は、コミットまたは保存されたあとに有効になります。自動構成プロパティーへの変更は、CLI でコミットする必要はありません。 ■ 新しく取得した自動構成 IPv6 アドレスは、管理対象デバイス (SP または CMM) に現在接続されている Oracle ILOM セッションには影響しません。 <p>「IPv4 Commit Pending Modification」の CLI 構文:</p> <pre>set /SP CMM/network pendingstate=enabled disabled pendingipdiscovery=static dhcp pendingipaddress=value pendingipgateway=value pendingipnetmask=value commitpending=true</pre> <p>「IPv6 Commit Pending Modifications」の CLI 構文:</p> <pre>set /SP CMM/network pendingstate=enabled disabled pending_static_ipaddress=ip6_address/ subnet_mask_length_in_bits commitpending=true</pre> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 127 ページの「IPv4 および IPv6 の接続をテストする」

表 44 DNS 構成プロパティー

プロパティー	デフォルト値	説明
ユーザーインターフェースの構成可能なターゲットとユーザーの役割: <ul style="list-style-type: none"> ■ CLI: /SP CMM/clients/dns ■ Web: 「ILOM Administration」 > 「Connectivity」 > 「DNS」 > 「DNS Configuration」 ■ ユーザーの役割: admin (a) (プロパティー変更に必要な) 		
Auto DNS via DHCP (auto_dns=)	Enabled	Enabled Disabled Oracle ILOM の「Auto DNS via DHCP」プロパティーは、デフォルトで有効になっています。このプロパティーが有効の場合、Oracle ILOM は DNS 情報を DHCP サーバーから自動的に取得します。 ネットワーク管理者は、「Auto DNS」プロパティーを無効にして DNS 情報を Oracle ILOM で手動で構成することもできます。 「Auto DNS via DHCP」の CLI 構文: <pre>set /SP CMM/clients/dns auto_dns=enabled disabled</pre>
DNS Named Server (nameserver=)	なし	「Auto DNS」プロパティーが無効の場合、「DNS Named server」プロパティーで IP アドレスを 3 つまで手動で構成できます。 複数の IP アドレスを入力する場合は、次のガイドラインに従ってください: <ul style="list-style-type: none"> ■ 各アドレスはコンマで区切る必要があります。 ■ IPv4 アドレスと IPv6 アドレスが混在する場合は、IPv4 アドレスを先に記載します。 「DNS Named Server」の CLI 構文: <pre>set /SP CMM/clients/dns nameserver=ip_address_1, ipaddress_2, ipaddress_3</pre>
DNS Search Path (searchpath=)	なし	「Auto DNS」プロパティーが無効の場合、「DNS Search Path」プロパティーでドメイン接尾辞を 6 つまで手動で構成できます。各検索接尾辞はコンマで区切る必要があります。 「DNS Search Path」の CLI 構文: <pre>set /SP CMM/clients/dns searchpath= domain_1.com, domain_2.edu, and so on ...</pre>

表 44 DNS 構成プロパティ (続き)

プロパティ	デフォルト値	説明
DNS Timeout (timeout=)	5 seconds	<p>1 - 10 の整数</p> <p>「DNS Timeout」のプロパティ値は、DNS クエリーを完了するために DNS サーバーに割り当てられる秒数を指定します。</p> <p>ネットワーク管理者は、DNS サーバーに割り当てられているデフォルトのタイムアウト値を必要に応じて増減できます。</p> <p>「DNS Timeout」の CLI 構文:</p> <pre>set /SP CMM/clients/dns timeout=n</pre> <p>関連トピック:</p> <ul style="list-style-type: none"> ■ 118 ページの「動的 DNS の設定例」
DNS Retries (retries=)	1 retry	<p>0 - 4 の整数</p> <p>「DNS Retries」のプロパティ値は、タイムアウトの発生時に DNS クエリーを再試行する回数を指定します。</p> <p>ネットワーク管理者は、デフォルトの「DNS Retries」のプロパティ値を必要に応じて増減できます。</p> <p>「DNS Retries」の CLI 構文:</p> <pre>set /SP CMM/clients/dns retries=n</pre>
Save Button (Web のみ)		<p>Web インタフェース - 「DNS Configuration」ページで行われた変更を有効にするには、Oracle ILOM で保存する必要があります。</p>

表 45 シリアルポートの構成プロパティ

プロパティ	デフォルト値	説明
ユーザーインターフェースの構成可能なターゲット:		
■ CLI: /SP/serial/portsharing		
■ Web: 「ILOM Administration」 > 「Connectivity」 > 「Serial Port」 > 「Serial Port Settings」		
■ User Role: (a) Admin (プロパティ変更に必要な)		
Owner (owner =)	SP	<p>SP hostserver</p> <p>シリアルポートの「Owner」プロパティは一部の Oracle サーバーで構成できます。詳細は、88 ページの「シリアル管理ポートの所有者」を参照してください。</p> <p>「Serial Port Owner」の CLI 構文:</p> <pre>set /SP/serial/portsharing owner=SP hostserver</pre>
Host Serial Port (/host pendingspeed= flowcontrol=)	Baud Rate= 9600 Flow Control= None	<p>Baud Rate = 9600 Flow Control = Software Hardware None</p> <p>「Host Serial Port」プロパティは一部の Oracle サーバーで構成できます。</p> <p>「Host Serial Port」オプションのプロパティ値は、ホストサーバーのシリアルコンソールポート用に設定されているプロパティ値と一致する必要があります。多くの場合シリアルポート 0、COM1、または /dev/ttyS0 と呼ばれます。</p> <p>「Host Serial Port」の CLI 構文:</p> <pre>set /SP CMM/serial/host pendingspeed=value flowcontrol=value commitpending=true</pre>
External Serial Port (/external pendingspeed= flowcontrol=)	Baud Rate= 9600 Flow Control= None	<p>Baud Rate = 9600 Flow Control = None</p> <p>管理対象デバイスの外部シリアルポートはシリアル管理 (SER MGT) ポートです。</p> <p>ネットワーク管理者は、外部シリアルポートのデフォルトのボーレート速度を必要に応じて変更できます。</p> <p>「External Serial Port」の CLI 構文:</p> <pre>set /SP CMM/serial/external pendingspeed=value commitpending=true</pre>
Save Button (Web のみ)		<p>Web インタフェース - 「Serial Port Settings」ページで行われた変更を有効にするには、Oracle ILOM で保存する必要があります。</p>

動的 DNS の設定例

動的ドメインネームサービス (DDNS) を設定することで DHCP をさらに活用し、DHCP によって新しく追加されたすべての Oracle ILOM システムのホスト名を、使用しているネットワーク環境の DNS サーバーで自動的に認識できます。

DDNS を構成すると、ネットワーク管理者は製品のシリアル番号と SUNSP または SUNCMMn のどちらかの接尾辞を組み合わせることで特定の Oracle ILOM SP または CMM のホスト名を判定できます。たとえば、製品のシリアル番号が 0641AMA007 の場合、サーバー SP のホスト名は SUNSP-0641AMA007 となり、シャーシに取り付けられた 1 つの CMM のホスト名は SUNCMM-0641AMA007 となります。また、シャーシに取り付けられた 2 つの CMM のホスト名は SUNCMM0-0641AMA007 および SUNCMM1-0641AMA007 となります。

▼ 例: DDNS 構成を設定する

この例では、一般的な DDNS 構成の設定方法について説明します。

前提条件:

この DDNS 構成の例には、次の前提条件が適用されます:

- SP が存在するネットワーク上に、DNS と DHCP の両方を処理する 1 台のサーバーが存在する。
- SP のネットワークアドレスは 192.168.1.0 である。
- DHCP/DNS サーバーのアドレスは 192.168.1.2 である。
- 192.168.1.100 から 192.168.1.199 の IP アドレスは、SP およびその他のクライアントにアドレスを提供するためのプールとして使用される。
- ドメイン名は example.com である。
- 既存の DNS 構成または DHCP 構成は存在しない。存在する場合は、この例の .conf ファイルをガイドラインとして使用して、既存の構成を更新してください。

注 - DDNS の設定方法は、サイトで使用しているインフラストラクチャーによって異なります。Oracle Solaris、Linux、および Microsoft Windows オペレーティングシステムはすべて、DDNS 機能を提供するサーバーソリューションをサポートしています。この例の構成では、Debian r4.0 をサーバーのオペレーティングシステム環境として使用しています。

ここで紹介する手順とサンプルファイルにサイト固有の変更を加えることで、独自の DDNS 構成を設定できます。

- 1 **Debian** ディストリビューションから **bind9** パッケージと **dhcp3-server** パッケージをインストールします。
dnsutils パッケージをインストールすると、dig、nslookup、およびその他の便利なツールにもアクセスできるようになります。
- 2 **dnssec-keygen** を使用すると、DNS データへのアクセスを制御するために DHCP サーバーと DNS サーバーの間で共有される鍵が生成されます。
- 3 次を含む DNS 構成ファイルを **/etc/bind/named.conf** という名前で作成します:

```
options {
    directory "/var/cache/bind";
    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };
};
// prime the server with knowledge of the root servers
zone "." {
    type hint;
    file "/etc/bind/db.root";
};
// be authoritative for the localhost forward and reverse zones, // and for broadcast zones as per RFC 1912
zone "localhost" {
    type master;
    file "/etc/bind/db.local";
};
zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};
zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};
zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};
// additions to named.conf to support DDNS updates from dhcp server
key server.example.com {
    algorithm HMAC-MD5;
    secret "your-key-from-step-2-here"
};
zone "example.com" {
    type master;
    file "/etc/bind/db.example.com";
    allow-update { key server.example.com; };
};
zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.example.rev";
    allow-update { key server.example.com; };
};
```

- 4 ローカルネットワーク用に空のゾーンファイルを追加します。
空のゾーンファイルには、**/etc/bind/db.example.com** および **/etc/bind/db.example.rev** という名前を付けるようにしてください。

ディストリビューションによって提供される `db.empty` ファイルのコピーで十分です。これらが DNS サーバーによって自動的に更新されます。

5 次の含む `/etc/dhcp3/dhcpd.conf` ファイルを作成します:

```
ddns-update-style interim;
ddns-updates on;
server-identifier server;
ddns-domainname "example.com.";
ignore client-updates;
key server.example.com {
    algorithm hmac-md5;
    secret your-key-from-step-2-here;
}
zone example.com. {
    primary 127.0.0.1;
    key server.example.com;
}
zone 1.168.192.in-addr.arpa. {
    primary 127.0.0.1;
    key server.example.com;
}
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local7;
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.100 192.168.1.199;
    option domain-name-servers 192.168.1.2;
}
```

6 前述の手順 1 から 5 を完了したあと、`/etc/init.d` スクリプトを実行して DNS サーバーと DHCP サーバーを起動します。

いったんサーバーが稼動すると、DHCP 用に構成された新しい Oracle ILOM SP には、電源投入時にホスト名で自動的にアクセスできるようになります。必要に応じて、ログファイル、`dig`、`nslookup`、およびその他のユーティリティーを使用してデバッグを行います。

参考 参照情報

この例で使用している Linux の DHCP サーバーおよび DNS サーバーの詳細については、Internet Systems Consortium の Web サイトを参照してください:<http://www.isc.org/>

システム識別情報の割り当て

Oracle ILOM には、使用している環境で特定の管理対象デバイスを識別するのに役立つ一連の構成可能なプロパティが用意されています。システム管理者は、これらのパラメータを使用して管理対象デバイスの物理的な場所、管理対象デバイスの連絡先、および管理対象デバイスに割り当てられたホスト名を一意に識別できます。システム識別構成の詳細は、次の表を参照してください。

表 46 デバイス識別の構成プロパティ

プロパティ	デフォルト値	説明
ユーザーインターフェースの構成可能なターゲットとユーザーの役割: <ul style="list-style-type: none"> ■ CLI: /SP/ ■ Web: 「ILOM Administration」 > 「Identification」 ■ ユーザーの役割: Admin (a) (プロパティ変更に必要) 		
Host Name (hostname=)	なし	<p>「Host Name」は、定義した場合、コンピュータネットワークに接続されている管理対象デバイスの識別に役立ちます。</p> <p>「Host Name」のプロパティ値には、最大 60 文字まで含めることができます。先頭には英字を使用します。また、使用できる文字は英数字、ハイフン、およびアンダースコアのみです。</p> <p>「Host Name」の CLI 構文:</p> <pre>set /SP CMM hostname=value</pre>
System Identifier (/system_identifier=)	なし	<p>「System Identifier」は、定義した場合、SNMP トラップのペイロード要素内にある管理対象デバイスの識別に役立ちます。</p> <p>「System Identifier」のプロパティ値には、標準的なキーボードの任意のキー (引用符を除く) を使用して最大 60 文字まで含めることができます。</p> <p>このプロパティは、サーバー SP と CMM の両方で構成可能です。</p> <p>「System Identifier」の CLI 構文:</p> <pre>set /SP CMM system_identifier=value</pre>
System Contact (/system_contact=)	なし	<p>「System Contact」は、定義した場合、管理対象デバイスの連絡先、たとえばそのデバイスに責任を負う個人の名前や電子メールアドレスなどを識別するのに役立ちます。</p> <p>「System Contact」のプロパティ値には、標準的なキーボードの任意のキー (引用符を除く) を使用したテキスト文字列を使用できます。</p> <p>「System Contact」の CLI 構文:</p> <pre>set /SP CMM system_contact=value</pre>

表 46 デバイス識別の構成プロパティ (続き)

プロパティ	デフォルト値	説明
System Location (/system_location=)	なし	<p>「System Location」は、定義した場合、ラック識別子やデータセンターの場所といった管理対象デバイスの物理的な場所を識別するのに役立ちます。</p> <p>「system location」のプロパティ値には、標準的なキーボードの任意のキー (引用符を除く) を使用したテキスト文字列を使用できます。</p> <p>「System Location」の CLI 構文:</p> <pre>set /SP CMM system_location=value</pre>
Physical Presence Check (/check_physical_presence=)	Enabled	<p>「Physical Presence Check」は、事前構成された Oracle ILOM の root アカウントパスワードを復元するための動作に影響します。</p> <ul style="list-style-type: none"> Enabled (true) - 有効の場合、デフォルトの Oracle ILOM パスワードを復元するには物理システムの「Locator」ボタンを押す必要があります。 Disabled (false) - 無効の場合、デフォルトの Oracle ILOM 管理者パスワードは、物理システムの「Locator」ボタンを押すことなくリセットできます。 <p>「Physical Presence Check」の CLI 構文:</p> <pre>set /SP CMM check_physical_presence=true false</pre> <p>関連トピック:</p> <ul style="list-style-type: none"> 表 12
Save Button (Web のみ)		<p>Web インタフェース - 「Identification」ページで行われた変更を有効にするには、Oracle ILOM で保存する必要があります。</p>

SP または CMM クロックのプロパティの設定

Oracle ILOM をはじめて配備する場合、システム管理者は、Oracle ILOM によって記録されるシステム管理イベントが正しいタイムスタンプで表示されるように、Oracle ILOM でクロック設定を構成するようにしてください。

システム管理者は、Oracle ILOM クロックを NTP サーバーに同期させるか、ホストサーバーの UTC/GMT タイムゾーンを使用して Oracle ILOM で日付と時間をローカルに手動で構成するかを選択できます。

Oracle ILOM クロックの構成プロパティについては、次の表を参照してください。

表 47 Oracle ILOM クロックの構成プロパティ

プロパティ	デフォルト値	説明
ユーザーインタフェースの構成可能なターゲットとユーザーの役割: <ul style="list-style-type: none"> ■ CLI: /SP CMM/clock ■ Web: 「ILOM Administration」 > 「Date and Time」 > 「Clock Settings Timezones」 ■ ユーザーの役割: admin (a) (プロパティ変更に必要な) 		
Date and Time (datetime=)	なし	「Date」プロパティに、月、日、および年を入力します。「Time」プロパティに、時間と分を入力します。 「Date and Time」の CLI 構文: set /SP CMM/clock datetime=MMDDhhmmYYYY
Timezones (timezones=)	なし	タイムゾーンの略称 (PST、EST など) 「Timezones」プロパティに、適切なタイムゾーンを入力します。 「Timezones」の CLI 構文: set /SP CMM/clock timezones=3_to_4_characters
Synchronize Time with NTP Server (usentpserver=)	Disabled	Enabled Disabled Oracle ILOM にクロック設定とネットワーク NTP サービスを同期するように指示するには、このプロパティを有効にします。 注 - NTP サーバー用の IP アドレスの最小構成 1 つが必要です。NTP サーバーのプロパティを参照してください。 「Synchronize Time with NTP Server」の CLI 構文: set /SP CMM/clock usentpserver=enabled disabled
NTP Server 1 (2) (/SP/clients/ntp/servern=)	なし	「Server 1」または「Server 2」プロパティに NTP サーバーの IP アドレスを入力します。 NTP サーバーの IP アドレスを設定する CLI 構文: set /SP/clients/ntp/server1=ip_address
Save Button (Web のみ)		Web インタフェース - 「Clock Settings」ページおよび「Timezone Settings」ページで行われた変更を有効にするには、Oracle ILOM で保存する必要があります。

次を確認するには、Oracle サーバーのドキュメントを参照してください:

- Oracle ILOM の現在の時間が SP をリブートしても維持されるか。
- Oracle ILOM の現在の時間をホストのブート時にホストと同期させることができるかどうか。
- システムが時間を格納するリアルタイムクロック要素をサポートするかどうか。

ネットワーク接続の問題の推奨される解決策

- 124 ページの「Web ブラウザのセキュリティー設定の解決」
- 125 ページの「接続の問題の解決」
- 126 ページの「スパニングツリー構成についての推奨事項」
- 127 ページの「IPv4 および IPv6 の接続をテストする」

Web ブラウザのセキュリティー設定の解決

Oracle ILOM 3.1.0 では、Internet Explorer (IE) 6 ユーザーは2つのタスクのうち1つを実行しないと Web インタフェースに接続できません:

- **タスク 1** – ブラウザを IE7以降、または同等かより新しい別のブラウザにアップグレードします。
または
- **タスク 2** – Oracle ILOM Web サーバーのプロパティーおよび SSL 証明書と鍵を変更します。操作方法は、次の手順を参照してください。

▼ Internet Explorer 6 をサポートするようにデフォルトの Web サーバープロパティーを変更する

Oracle ILOM に付属している事前構成済み Web サーバー自己署名証明書はより強力な暗号化を使用しており、これは IE 6 ではサポートされていません。

IE 6 から IE 7 へのアップグレードを考えていないユーザーの場合、IE 6 から Oracle ILOM Web インタフェースへの接続を許可するように次の手順の Web サーバープロパティーを変更する必要があります。

始める前に

- Oracle ILOM で Web サーバープロパティーを変更するには Admin (a) の役割が必要です。

1 Oracle ILOM SP CLI にログインします。

2 次を入力して弱い暗号を有効にします:

```
set /SP|CMM/services/https weak_ciphers=enabled
```

3 次を入力してカスタム鍵をアップロードします:

```
set /SP|CMM/services/https/ssl/custom_key load_uri=<uri_string >
```

4 次を入力してカスタム証明書をアップロードします:

```
set /SP|CMM/services/https/ssl/custom_cert load_uri=<uri_string>
```

参考 関連情報:

- 表 35

接続の問題の解決

Oracle ILOM インタフェースへのネットワーク接続の確立に問題が発生している場合、推奨される解決策を次の IPv4 および IPv6 の情報で参照してください。

- 表 48
- 表 49

表 48 IPv4 接続問題のトラブルシューティング

問題	推奨される解決策
ネットワーククライアントから IPv4 を使用して Oracle ILOM にアクセスできません。	<p>Oracle ILOM Web インタフェースの「Network Settings」ページ、または Oracle ILOM CLI の /SP/network ターゲットで、「State」の設定が有効になっていることを確認します。IPv4 ネットワークの問題を診断するための推奨されるほかの方法には、次のものがあります:</p> <ul style="list-style-type: none"> ■ 物理的な管理ポート (NET MGT) への LAN 接続が確立されていることを確認します。 ■ Oracle ILOM の適切なネットワークサービスである SSH、HTTP、または HTTPS が使用可能になっていることを確認します。Web インタフェースで、「ILOM Administration」>「Connectivity」をクリックして、ネットワーク接続設定を検証および変更します。 ■ IPv4 Ping や Traceroute などの業界標準のネットワーク診断ツールを使用して、管理対象デバイスへのネットワーク接続をテストします。Web または CLI から ping を実行します。または、サービス Oracle ILOM 制限付きシェルから traceroute を実行します。
Internet Explorer 6 (IE 6) Web ブラウザを使用して Oracle ILOM Web インタフェースにアクセスできない。	<p>Internet Explorer 6 ユーザーは、Oracle ILOM Web インタフェースで SSL を使用するためにブラウザをアップグレードするか、カスタム証明書および非公開鍵をアップロードする必要があります。</p> <p>カスタム SSL 証明書をアップロードする手順については、表 36 を参照してください。</p>

表 49 IPv6 接続問題のトラブルシューティング

問題	推奨される解決策
IPv6 アドレスを使用して Oracle ILOM Web インタフェースにアクセスできません。	<p>URL 内の IPv6 アドレスが角括弧で囲まれていることを確認します。例: <code>https://[2001:db8:0:0:0:0:0:0]</code></p>

表 49 IPv6 接続問題のトラブルシューティング (続き)

問題	推奨される解決策
IPv6 アドレスを使用してファイルをダウンロードできません。	URL 内の IPv6 アドレスが角括弧で囲まれていることを確認します。例: <code>load -source tftp://[2001:db8:0:0:0:0:0:0]/desktop.pkg</code>
ネットワーククライアントから IPv6 を使用して Oracle ILOM にアクセスできません。	別のサブネット上の場合、次のことを試みます: <ul style="list-style-type: none"> ■ Oracle ILOM が (リンクローカルアドレスだけでなく) 動的または静的アドレスを持つことを確認します。 ■ ネットワーククライアントに (リンクローカルアドレスだけでなく) IPv6 アドレスが構成されていることを確認します。 <p>同じサブネットまたは別のサブネット上の場合、次のことを試みます:</p> <ul style="list-style-type: none"> ■ Oracle ILOM Web インタフェースの「Network Settings」ページ、または Oracle ILOM CLI の <code>/SP/network/ipv6</code> ターゲットで、「IPv6 State」のプロパティが有効になっていることを確認します。 ■ Oracle ILOM の適切なネットワークサービスである SSH、HTTP、または HTTPS が使用可能になっていることを確認します。 Web インタフェースで、「ILOM Administration」>「Connectivity」をクリックして、ネットワーク接続設定を検証および変更します。 ■ IPv6 Ping や Traceroute などの業界標準のネットワーク診断ツールを使用して、管理対象デバイスへのネットワーク接続をテストします。 Web または CLI から <code>ping6</code> を実行します。または、サービス Oracle ILOM 制限付きシェルから <code>traceroute</code> を実行します。
Internet Explorer 6 (IE 6) Web ブラウザを使用して Oracle ILOM Web インタフェースにアクセスできない。	Internet Explorer 6 ユーザーは、Oracle ILOM Web インタフェースで SSL を使用するためにブラウザをアップグレードするか、カスタム証明書および非公開鍵をアップロードする必要があります。 カスタム SSL 証明書をアップロードする手順については、表 36 を参照してください。

スパニングツリー構成についての推奨事項

SP ネットワーク管理ポートは、スイッチポートのような動作をするように設計されていないため、SP ネットワーク管理ポートはスパニングツリーポートファーストなどのスイッチポート機能をサポートしていません。

スパニングツリーパラメータを構成するときは、次の推奨事項を検討してください:

- SP ネットワーク管理ポートを隣接するネットワークスイッチに接続するために使用するポートでは、常に SP ネットワーク管理ポートをホストポートとして扱うようにしてください。
- 隣接するネットワークスイッチに接続するポートのスパニングツリーオプションは、完全に無効にするか、少なくとも次のパラメータを使用して構成するようにしてください:

スパンニングツリーパラメータ	推奨する設定
portfast	このインタフェースで、すぐに転送状態に移行できるようにします。
bpdufilter	このインタフェースでBPDUを送信または受信しません。
bpduguard	このインタフェースでBPDUを受け入れません。
cdp	このインタフェースで検出プロトコルを有効にしません。

▼ IPv4 および IPv6 の接続をテストする

Oracle ILOM で構成された IP アドレスおよびゲートウェイアドレスからネットワーク上のデバイスにネットワークテストを送信するには、次の手順に従います:

- 次のいずれかを実行します:

- **CLI:**

CLI から ping 接続テストを実行するには、次のいずれかを入力します:

```
set /SP|CMM/network/test ping=device_ipv4_address_on_network
```

```
set /SP|CMM/network/test ping6=device_ipv6_address_on_network
```

テストに失敗すると、エラーメッセージが表示されます。一部の Oracle サーバーではテストに成功すると成功メッセージが表示されます。

- **Web:**

Web から ping 接続テストを実行するには、次を実行します:

- 「ILOM Administration」 > 「Connectivity」 > 「Network」 > 「Network Tools」の順にクリックします。
- ツールダイアログで、テストの種類を選択し、ネットワーク上のデバイスの IP アドレスを指定して「Test」をクリックします。

参考 関連情報:

- 表 43

リモート KVMs コンソールを使用したホストサーバーのリダイレクション

説明	リンク
ホストサーバーの KVMs リダイレクションを行うための GUI ベースの Oracle ILOM リモートコンソールの設定と使用については、これらのセクションを参照してください。	<ul style="list-style-type: none">■ 129 ページの「Oracle ILOM リモートコンソールの最初の設定」■ 137 ページの「Oracle ILOM リモートコンソールの起動と使用」
ホストストレージリダイレクションを行うためのコマンド行の Oracle ILOM Storage Redirection コンソールの設定と使用については、これらのセクションを参照してください。	<ul style="list-style-type: none">■ 142 ページの「Oracle ILOM Storage Redirection CLI の最初の設定」■ 149 ページの「Oracle ILOM Storage Redirection CLI の起動と使用」
ホストサーバーのオペレーティングシステムに対するシリアルリダイレクションセッションを開始する手順については、このセクションを参照してください。	<ul style="list-style-type: none">■ 157 ページの「ホストシリアルリダイレクションセッションの開始と停止」

関連情報

- 『Oracle ILOM 3.1 セキュリティガイド』の「リモート KVMs のセキュアな使用方法」

Oracle ILOM リモートコンソールの最初の設定

Oracle ILOM リモートコンソールをはじめて使用するために設定するには、これらのトピックを参照してください:

- 130 ページの「Oracle ILOM リモートコンソールを使用するための要件」
- 131 ページの「ローカルクライアントの KVMs 設定の構成」
- 132 ページの「Windows IE Web ブラウザ用の 32 ビット JDK Java Plug-in の登録」
- 133 ページの「Mozilla Firefox Web ブラウザ用の 32 ビット JDK Java Plug-in の登録」
- 134 ページの「ホストサーバーのデスクトップをセキュリティー保護するためにロックモードを設定する (省略可能)」

Oracle ILOM リモートコンソールを使用するための要件

Oracle ILOM リモートコンソールをはじめて使用する前に、次の要件を満たす必要があります。

表 50 Oracle ILOM リモートコンソールを使用するための要件

設定要件	説明
KVMS の設定	<p>キーボード、ビデオ、およびマウスのリダイレクション動作に関する SP のローカルクライアントプロパティを構成します。</p> <p>デフォルト:</p> <p>「State」: 「enabled」、 「Mouse Mode」: 「absolute」、 「Display Quality」: 「YUV420」、 「Lock Mode」: 「disabled」</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 131 ページの「ローカルクライアントの KVMS 設定の構成」
Java Runtime Environment	<p>ローカルクライアントシステムに Java Runtime Environment (1.5 以降) がインストールされている必要があります。最新の Java Runtime Environment をダウンロードするには、http://java.com にアクセスしてください。</p>
必要な JDK および Web ブラウザ	<p>IPv4 ネットワークでは、32 ビット JDK が必要です。</p> <p>IPv6 ネットワークでは、JDK170b36 以降が必要です。</p> <p>サポートされている Web ブラウザについては、35 ページの「サポートされているオペレーティングシステムの Web ブラウザ」を参照してください。</p>
ビデオリダイレクション用の 32 ビット JDK の登録	<p>Oracle ILOM リモートコンソールを使用してビデオリダイレクションを行う前に、32 ビット JDK Java Plug-in がローカルクライアントの Web ブラウザに登録されている必要があります。</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 132 ページの「Windows IE Web ブラウザ用の 32 ビット JDK Java Plug-in の登録」 ■ 133 ページの「Mozilla Firefox Web ブラウザ用の 32 ビット JDK Java Plug-in の登録」
ユーザーの役割とホストサーバーのユーザー資格	<p>Oracle ILOM で KVMS のサービス状態を変更するには、Admin (a) の役割が必要です。</p> <p>Oracle ILOM で KVMS のプロパティ (サービスの「State」プロパティを除く) を変更したり、Oracle ILOM リモートコンソールを起動したりするには、Console (c) の役割が必要です。</p> <p>リダイレクトされたホストサーバーにアクセスするには、ホストサーバーのユーザー資格が必要です。</p>

表 50 Oracle ILOM リモートコンソールを使用するための要件 (続き)

設定要件	説明
ビデオリダイレクションとシリアルリダイレクションの使用	<p>Oracle ILOM リモートコンソールを起動すると、ユーザーは次のいずれかのリダイレクション方法を使用してリモート KVMS セッションを開始できます:</p> <ul style="list-style-type: none"> ■ シリアルリダイレクション (SPARC のみ) - このオプションは、SPARC サーバー SP でのみ使用できます。有効にすると、Oracle ILOM にシリアルホストサーバーリダイレクション用のテキストベースのコンソールが表示されます。 ■ ビデオリダイレクション - このオプションは、CMM、x86 サーバー SP、および SPARC サーバー SP で使用できます。このオプションでは、ビデオがリダイレクトされるホストサーバー用の GUI ベースのコンソールが表示されます。
必要な TCP/IP 通信ポート	<p>Oracle ILOM リモートコンソールは、デフォルトで次の TCP/IP 通信ポートを使用します:</p> <ul style="list-style-type: none"> ■ ポート 5120 (CD リダイレクション用)。 ■ ポート 5123 (フロッピーリダイレクション用)。 ■ ポート 5556 (ユーザー認証のリダイレクション用)。 ■ ポート 7578 (ビデオリダイレクション用)。 ■ ポート 7579 (SPARC サーバーのリダイレクション専用)。 <p>Oracle ILOM で使用されるネットワークポートの完全なリストについては、表 34を参照してください。</p>

▼ ローカルクライアントの KVMS 設定の構成

- 1 Oracle ILOM でサーバー SP の KVMS 設定にアクセスするには、次を実行します:
 - Web - 「Remote Console」 > 「KVMS」 > 「KVMS Settings」の順にクリックします。
 - CLI - 次を入力します:


```
show /SP/services/kvms
```
- 2 必要に応じて次の KVMS プロパティを変更します:

プロパティ	説明
State (servicestate=)	<p>リダイレクション用の KVMS サービスの「State」はデフォルトで有効になっています。</p> <p>Oracle ILOM リモートコンソールを使用するには、この「State」プロパティを有効にする必要があります。この状態を無効にすると、Oracle ILOM リモートコンソールの使用も無効になります。</p> <p>「KVMS Service State」の CLI 構文:</p> <pre>set /SP/services/kvms servicestate=enabled disabled</pre>

プロパティ	説明
Mouse (mousemode=)	<p>適切なマウスモードオプションを設定します:</p> <ul style="list-style-type: none"> ■ Relative (デフォルト) - リモートホストで Linux OS が実行されている場合は、このローカルマウスモードを設定します。 ■ Absolute - リモートホストで Windows OS または Solaris が実行されている場合は、このローカルマウスモードを設定します。 <p>「KVMS Mouse Mode」の CLI 構文:</p> <pre>set /SP/services/kvms mousemode=<i>absolute relative</i></pre>
Display Quality (display_quality=)	<p>適切なビデオ品質オプションを選択します:</p> <ul style="list-style-type: none"> ■ YUV420 (初期の出荷時のデフォルト) - この設定を選択すると、高圧縮のカラー画像データスキームが送信され、その結果データ転送レートが最適化されます。 ■ YUV444 - この設定を選択すると、低圧縮のカラー画像データスキームが送信され、その結果画像の解像度が高くなります。 ■ VQ2 - この設定を選択すると、2色の端末ディスプレイ出力にもっとも適した低圧縮のビデオデータスキームが送信されます。 ■ VQ4 - この設定を選択すると、4色の端末ディスプレイ出力にもっとも適した低圧縮のビデオデータスキームが送信されます。 <p>注 - 「Display Quality」に設定したプロパティ値は、SPのレポート後も維持されます。したがって、変更を行うと、初期の出荷時のデフォルト値 (YUV420) は保持されません。</p> <p>KVMS の「Display Quality」の CLI 構文:</p> <pre>set /SP/services/kvms display_quality=<i>YUV420 YUV444 VQ2 VQ4</i></pre>
Host Lock Settings (lock_mode=)	<p>ホストロックプロパティについては、134 ページの「ホストサーバーのデスクトップをセキュリティー保護するためにロックモードを設定する (省略可能)」を参照してください。</p>

- 3 変更を適用するには、「KVMS Settings」ページで「Save」をクリックします。

▼ Windows IE Web ブラウザ用の 32 ビット JDK Java Plug-in の登録

- 1 Windows クライアントで、Windows エクスプローラ (Internet Explorer ではありません) を開きます。
- 2 Windows エクスプローラのダイアログボックスで、「ツール」 > 「フォルダオプション」の順にクリックし、「ファイルの種類」タブをクリックします。

- 3 「ファイルの種類」タブで、次を実行します
 - a. 「登録されているファイルの種類」リストで「JNLP」ファイルの種類を選択し、「変更」をクリックします。
 - b. 「ファイルを開くプログラムの選択」ダイアログボックスで、「参照」をクリックして32ビットJDKファイルを選択します。
 - c. 「この種類のファイルを開くときは、選択したプログラムをいつも使う」チェックボックスをオンにします。
 - d. 「OK」をクリックし、Oracle ILOM リモートコンソールを起動します。
手順については、137ページの「Oracle ILOM リモートコンソールの起動と使用」を参照してください。

▼ Mozilla Firefox Web ブラウザ用の32ビットJDK Java Plug-inの登録

- 1 Oracle ILOM Web インタフェースから Oracle ILOM リモートコンソールを起動します。
「Remote Console」>「Redirection」の順にクリックします。

「Launch Redirection」ページで、シリアルまたはビデオリダイレクション方法を選択して(表示された場合)、「Launch Remote Console」ボタンをクリックします。

注-または、Web インタフェースの「Summary」ページにある「Actions」パネルから Oracle ILOM リモートコンソールにアクセスすることもできます。

「Java Start Web Program」ダイアログが表示されます。

- 2 「Java Start Web Program」ダイアログで、次を実行します:
 - a. 「Open with...」をクリックして32ビットJDKファイルの場所を指定します。
 - b. 「Do this automatically for files like this from now on」チェックボックスをオンにします。

注-サイトの名前が証明書の名前と一致していないことを示す、証明書に関する警告メッセージが表示される場合は、「Run」をクリックして続行します。

「Oracle ILOM Remote Console」ウィンドウが表示されます。

Oracle ILOM リモートコンソールを使用して KVMs デバイスをリダイレクトする方法の詳細は、137 ページの「Oracle ILOM リモートコンソールの起動と使用」を参照してください。

ホストサーバーのデスクトップをセキュリティー保護するためにロックモードを設定する (省略可能)

Oracle ILOM には、必要に応じてリモート KVMs セッションが切断するたびにホストサーバーのデスクトップをロックする機能が用意されています。この機能により、KVMs セッションのユーザーがホストサーバーのデスクトップからログアウトする前に KVMs セッションを閉じると、後続の KVMs セッションのユーザーはシステムにアクセスするために自分のユーザー資格を入力するように求められます。

ロックモードオプションおよび Oracle ILOM でのロックモードの構成方法については、これらのトピックを参照してください:

- [表 51](#)
- [135 ページの「リモート KVMs セッション切断時のホストのデスクトップのロック」](#)

表 51 構成可能なホストサーバーロックオプション

ロックモードプロパティ値	説明
Windows (lock_mode=windows)	「Windows」ロックオプションは、Microsoft Windows オペレーティングシステムを実行しているホストサーバーで構成できます。 ホストロックモードプロパティを「Windows」に設定すると、Oracle ILOM は Windows オペレーティングシステムのデスクトップをロックする標準の Windows キーボードショートカット (Ctrl + Alt + Del) と連係して機能します。

表 51 構成可能なホストサーバーロックオプション (続き)

ロックモードプロパティ値	説明
Custom (lock_mode=custom)	<p>「Custom」ロックオプションは、Ctrl + Alt + Del キーシーケンスを使用しない Oracle Solaris オペレーティングシステム、Linux ベースのオペレーティングシステム、または Microsoft Windows オペレーティングシステムを実行しているホストサーバーで構成できます。</p> <p>Oracle ILOM でホストロックモードプロパティを「Custom」に設定すると、Oracle ILOM は次のキーシーケンスを使用したデスクトップのロックをサポートします。</p> <ul style="list-style-type: none"> ■ Oracle Solaris または Linux ベースのオペレーティングシステムでサポートされているカスタムロックキーシーケンス。Oracle ILOM で「Custom」ロックモードプロパティを有効にする前に、ホストオペレーティングシステム上でカスタムロックキーシーケンスを定義する必要があります。カスタムロックキーシーケンスを作成する手順については、オペレーティングシステムベンダーのドキュメントを参照してください。 ■ Windows でサポートされているカスタムロックキーシーケンス (Windows ログキー + L キーボードショートカットなど)。Oracle ILOM の「Custom」ロックモードオプションでは、デスクトップをロックする標準の Windows キーボードショートカット (Ctrl + Alt + Del) はサポートされません。
Disabled (lock_mode=disabled)	<p>ホストロックモードプロパティを「disabled」(デフォルト)に設定すると、Oracle ILOM はリモート KVMs セッションの終了時にホストサーバーのデスクトップを自動的にロックしません。</p>

▼ リモート KVMs セッション切断時のホストのデスクトップのロック

始める前に

- カスタムロックモード構成の場合は、Oracle ILOM でカスタムロックモードオプションを設定する前に、ホストサーバーのオペレーティングシステム上でカスタムキーシーケンスを定義する必要があります。
- Oracle ILOM でホストロックプロパティを変更するには、Console (c) の役割が必要です。

1 次を実行して、Oracle ILOM でホストロックモードプロパティの値を設定します:

- Web-「Remote Control」>「KVMs」の順にクリックします。「KVMs Settings」ページで、「Lock Mode」リストボックスをクリックして次のいずれかの値を選択します:「Windows」、「Custom」、または「Disable」。
- CLI-次を入力します:

```
set /SP/services/kvms lockmode=windows|custom|disabled
```

ロックモードプロパティを「Custom」に設定した場合は、手順2に進みません。それ以外で、Web インタフェースを使用している場合は、手順3に進みません。

- 2 手順1でロックモードプロパティを「Custom」に設定した場合は、次を実行して、カスタムロック修飾子とカスタムロックキーを指定します:

- Web- 「KVMS Settings」 ページで:

「Custom Lock Modifiers」 リストボックスをクリックし、ホストサーバー OS に定義されたカスタムキーシーケンスを選択します。

「Custom Lock Key」 リストボックスをクリックし、カスタムロックキーを選択します。

- CLI- 次を入力します:

```
set /SP/services/kvms lockmodifiers=value
```

```
set /SP/services/kvms custom_lock_key=value
```

カスタムロック修飾子に指定できる値:

`l_alt, r_alt, l_shift, r_shift, l_ctrl, r_ctrl, l_gui, r_gui`

最大4個のロック修飾子の値を指定できます。それぞれの修飾子をコンマで区切ることができます。

カスタムロックキーに指定できる値:`esc, end, tab, ins, del, home, enter, space, break, backspace, pg_up, pg_down, scr_lck, sys_rq, num_plus, num_minus, f1, f2, f3, f4, f5, f6, f7, f8, f9, f10, f11, f12, a-z, 0-9, !, @, #, $, %, ^, &, *, (,), -, _, =, +, ?, |, ~, ?, [, {,], }, ;, :, ?, <, ., >, /, ?`

この手順のあとに示す例(ホストロック構成)を参照してください。

- 3 「KVMS Setting」 ページで行なったプロパティの変更を適用するには、「Save」をクリックします。

参考 ホストロック構成の例:

ホストサーバーのオペレーティングシステムに次のカスタムロックキーシーケンス(キーボードショートカット)が定義されている場合:

Shift + Ctrl + バックスペース

Oracle ILOM SP で次の KVMS ロックプロパティを設定します:

```
/SP/services/kvms
```

Properties:

```
custom_lock_key = backspace
custom_lock_modifiers = l_shift, l_ctrl
lockmode = custom
mousemode = absolute
servicestate = enabled
```

Oracle ILOM リモートコンソールの起動と使用

KVMS リダイレクションのために GUI ベースの Oracle ILOM リモートコンソールを起動して使用するには、これらのトピックを参照してください:

- 137 ページの「[Oracle ILOM リモートコンソールの起動と使用](#)」
- 139 ページの「[キーボードとマウスの制御の切り替えキーシーケンス](#)」
- 139 ページの「[「Redirection」メニューのオプション](#)」
- 141 ページの「[「Keyboard」メニューのオプション](#)」
- 140 ページの「[「Devices」メニューのオプション](#)」

▼ Oracle ILOM リモートコンソールの起動と使用

始める前に

- 初回使用時の要件を満たしていることを確認します: [表 50](#)。
- Oracle ILOM リモートコンソールを起動して使用するには、Console (c) の役割が必要です。
- Oracle ILOM リモートコンソールを起動すると、SPARC サーバー SP の場合にのみ、ビデオおよびシリアルリダイレクションオプションが表示されます。x86 サーバー SP の場合は、Oracle ILOM リモートコンソールが自動的にビデオリダイレクションを開始します。
- Oracle ILOM リモートコンソールとホストのデスクトップの間でキーボードとマウスの使用を制御するには、[139 ページの「キーボードとマウスの制御の切り替えキーシーケンス」](#)を参照してください。
- ホストサーバーに対するリダイレクションセッションを確立するときは、ホストオペレーティングシステムのデスクトップにログインするためにユーザー資格が必要です。

1 Oracle ILOM リモートコンソールを起動するには、次を実行します。

- a. **Oracle ILOM Web** インタフェースで、「**Remote Console**」 > 「**Redirection**」の順にクリックします。

- b. 「**Launch Redirection**」 ページで、リダイレクションのオプションをクリックして (表示された場合)、「**Launch Remote Console**」 ボタンをクリックします。

リダイレクトされたホストサーバーのデスクトップが現在の状態で表示されます。たとえば、ホストサーバーの電源が投入されると、一連のブートメッセージが表示されます。ホストサーバーのオペレーティングシステムが起動すると、デスクトップのログインダイアログが表示されます。ホストサーバーの電源が入っていないと、空白の画面が表示されます。

注- または、SP および CMM のユーザーは Oracle ILOM Web インタフェースの「**Summary**」 ページにある「**Actions**」 パネルから Oracle ILOM リモートコンソールを起動することもできます。

- 2 リダイレクションセッションを停止、再開、または新規に開始するには、「**Redirection**」メニューをクリックして該当するメニューオプションを選択します。

メニューオプションについては、139 ページの「**Redirection**」メニューのオプション」を参照してください。

特別な考慮事項:

- 単一のホストサーバー SP から KVMS セッションが開始されると、自動的に単一のリダイレクションビューが表示されます。
- (1) 新しい KVMS セッションを手動で追加するか、(2) 最初の KVMS セッションを CMM (シャーシ) Web インタフェースから開始すると、複数のリダイレクションビューが可能になります。CMM の KVMS セッションでは、シャーシ管理 CPU ブレードサーバー SP のそれぞれに対して単一のリダイレクションビューが表示されます。

- 3 デバイスをリダイレクトするには、「**Devices**」メニューをクリックして該当するメニューオプションを選択します。

メニューオプションについては、140 ページの「**Devices**」メニューのオプション」を参照してください。

特別な考慮事項:

- 配布メディア (CD/DVD) からソフトウェアをインストールする場合は、ローカルクライアントにリダイレクトされたドライブにメディアが挿入されていることを確認します。
- ISO イメージからソフトウェアをインストールする場合は、ISO イメージがローカルクライアントまたはネットワーク共有ファイルシステムに保存されていることを確認します。
- Oracle Solaris クライアントのユーザーの場合は、ストレージデバイスをリダイレクトする前に、次の操作を実行する必要があります:

- ポリウムマネージャーが有効な場合は、この機能を無効にする必要があります。
- ストレージリダイレクションを開始するには、`root`としてログインします。
または、ストレージリダイレクションを開始するために、これらのコマンドを入力して、Oracle ILOM リモートコンソールを実行しているプロセッサに `root` 権限を割り当てることもできます:

```
su to root
```

```
priv -s +file_dac_read pid_javarconsole
```

- 4 キーボードのモードおよび送信オプションを設定するには、「**Keyboard**」メニューをクリックして該当するメニューオプションを選択します。
メニューオプションについては、141 ページの「**Keyboard**」メニューのオプション」を参照してください。
- 5 リモートコンソールを終了するには、「**Redirection**」メニューの「**Quit**」をクリックします。

キーボードとマウスの制御の切り替えキーシーケンス

Oracle ILOM リモートコンソールアプリケーションとローカルクライアントデスクトップの間でキーボードとマウスの使用を制御するには、次のいずれかの切り替えキーシーケンスを使用します。

ローカルクライアントのデバイス	切り替えキーシーケンス
マウス	Alt + M
キーボード	Alt + K

「Redirection」メニューのオプション

「Redirection」メニューのオプション	説明
Start Redirection (デフォルト)	リダイレクションサービスを有効にするには、「Start Redirection」をクリックします。 このオプションはデフォルトで有効になっているため、Oracle ILOM リモートコンソールのダイアログを起動すると、リダイレクションサービスが自動的に起動されます。

「Redirection」メニューのオプション	説明
Restart Redirection	「Restart Redirection」オプションは、アクティブなキーボード、ビデオ、マウス、およびストレージのリダイレクションを停止してから開始します。
Stop Redirection	「Stop Redirection」オプションは、アクティブなキーボード、ビデオ、マウス、およびストレージのリダイレクションを停止します。
New Session	新しいリダイレクションセッションを現在のタブセットに追加します。
Delete Session	現在のタブセットからリダイレクションセッションを削除します。

「Devices」メニューのオプション

「Devices」メニューのオプション	説明
Keyboard (デフォルトで有効)	ローカルクライアントのキーボードのリダイレクションサービスのオンとオフを切り替えるには、「Keyboard」をクリックします。 このオプションはデフォルトで有効になっているため、ローカルクライアントのキーボードのリダイレクションサービスは自動的に起動されます。
Mouse (デフォルトで有効)	ローカルクライアントのマウスのリダイレクションサービスのオンとオフを切り替えるには、「Mouse」をクリックします。 このオプションはデフォルトで有効になっているため、ローカルクライアントのマウスのリダイレクションサービスは自動的に起動されます。
CD-ROM	ローカルのCDデバイスをリモートホストサーバーに直接接続されているかのように動作させるには、「CD-ROM」をクリックします。
Floppy	ローカルのフロッピーデバイスをリモートホストサーバーに直接接続されているかのように動作させるには、「Floppy」を選択します。 このオプションは、SPARC ホストサーバーではサポートされていません。
CD-ROM Image	ローカルクライアントまたはネットワーク共有に格納されているCD-ROM イメージファイルの場所を指定するには、「CD-ROM Image」を選択します。

「Devices」メニューのオプション	説明
Floppy Image	ローカルクライアントまたはネットワーク共有に格納されているフロッピーイメージファイルの場所を指定するには、「Floppy Image」を選択します。 このオプションは、SPARC ホストサーバーではサポートされていません。
Save as host defaults	現在選択されている「Devices」メニューのオプションをデフォルト設定として設定するには、「Save as host defaults」をクリックします。

「Keyboard」メニューのオプション

注 - Oracle ILOM リモートコンソールでは、次の国際キーボードのすべての文字の使用がサポートされます: スウェーデン語、フランス語 (スイス)、およびフィンランド語。

「Keyboard」メニューのオプション	説明
Auto-Keyboard Mode (デフォルトで有効)	キー入力のために自動的にキーブレイクを送信するには、「Auto-keybreak Mode」をクリックします。 このオプションは、低速ネットワーク接続でキーボードに関する問題を解決する場合に役立ちます。
Stateful Key Locking	オプションは、XSun を実行する Oracle Solaris または OSX に適用されます。 ローカルクライアントでステートフルキーロックが使用される場合は、「Stateful Key Locking」をクリックします。ステートフルキーロックは、Caps Lock、Num Lock、および Scroll Lock の3つのロックキーに適用されます。
Left Alt Key	このオプションは、Windows クライアントでは使用できません。 左側の Alt キーのオンとオフを切り替えるには、「Left Alt Key」をクリックします。

「Keyboard」メニューのオプション	説明
Right Alt Key / Alt Graph Key	<p>このオプションは、英語以外のキーボードに適用されます。</p> <p>右側の Alt キーのオンとオフを切り替えるには、「Right Alt Key」(「Alt Graph Key」)をクリックします。</p> <p>このオプションが有効になっている場合は、キーの3番目のキー文字を入力できます。</p>
F10	<p>F10 ファンクションキーを適用するには、「F10」をクリックします。</p> <p>このオプションは、通常、x86 ホストサーバーの BIOS 機能に適用されます。</p>
Control Alt Delete	<p>Ctrl + Alt + Del シーケンスを送信するには、「Control Alt Delete」をクリックします。</p>
Control Space	<p>キーボード入力を有効にする Ctrl + スペースシーケンスをホストサーバーに送信するには、「Control Space」をクリックします。</p>
Caps Lock	<p>ロシア語およびギリシャ語キーボードでの入力を有効にする Caps Lock キーをホストサーバーに送信するには、「Caps Lock」をクリックします。</p>

Oracle ILOM Storage Redirection CLI の最初の設定

Oracle ILOM Storage Redirection をはじめて使用するために設定するには、これらのトピックを参照してください:

- 142 ページの「Oracle ILOM Storage Redirection CLI を使用するための要件」
- 143 ページの「Windows IE ブラウザ用の Java Plug-in の登録とサービスの最初の起動」
- 145 ページの「サービスの最初の起動と Mozilla Firefox ブラウザ用の Java Plug-in の登録」
- 146 ページの「Storage Redirection クライアントのインストール」
- 147 ページの「Storage Redirection のデフォルトのネットワークポート 2121 を変更する(省略可能)」

Oracle ILOM Storage Redirection CLI を使用するための要件

Oracle ILOM Storage Redirection CLI をはじめて使用する前に、次の要件を満たす必要があります。

表 52 Oracle ILOM Storage Redirection を使用するための要件

設定要件	説明
JRE 1.5 環境	<p>ストレージリダイレクションのサービスおよびクライアントは、ローカルクライアントシステムに Java Runtime Environment (1.5 以降) をインストールする必要がある Java Web Start アプリケーションです。</p> <p>最新の Java Runtime Environment (JRE) をダウンロードするには、http://java.com を参照してください。</p>
32 ビット JDK Plug-in の登録と Storage Redirection サービスの起動	<p>ストレージリダイレクションサービスは、ローカルにインストールするか、Oracle ILOM Web インタフェースから実行されるように設定する必要があります。</p> <p>また、ローカルクライアントの Web ブラウザに 32 ビット JDK Java Plug-in を登録する必要があります。</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 143 ページの「Windows IE ブラウザ用の Java Plug-in の登録とサービスの最初の起動」 ■ 145 ページの「サービスの最初の起動と Mozilla Firefox ブラウザ用の Java Plug-in の登録」
Storage Redirection クライアントのインストール	<p>ローカルクライアントの Web ブラウザに 32 ビット JDK plug-in を登録し、ストレージリダイレクションサービスをはじめて起動したあとは、ローカルクライアントシステムにストレージリダイレクションクライアントをインストールする必要があります。</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 146 ページの「Storage Redirection クライアントのインストール」
ユーザーの役割	<p>Oracle ILOM で Oracle ILOM Storage Redirection CLI を起動して使用するには、Console (c) の役割が必要です。</p>
必要な TCP/IP 通信ポート	<p>Oracle ILOM Storage Redirection CLI は、デフォルトで TCP/IP ポート 2121 を使用してホストサーバーと通信します。</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 147 ページの「Storage Redirection のデフォルトのネットワークポート 2121 を変更する (省略可能)」

▼ Windows IE ブラウザ用の Java Plug-in の登録とサービスの最初の起動

(1) Microsoft Windows IE ブラウザに 32 ビット JDK Java plug-in を登録し、(2) ストレージリダイレクションサービスをはじめて起動するには、この手順を実行します:

- 1 ローカル Windows クライアントで、**Windows エクスプローラ (Internet Explorer ではありません)** を開きます。
- 2 **Windows エクスプローラ** のダイアログボックスで、「ツール」 > 「フォルダオプション」の順にクリックし、「ファイルの種類」タブをクリックします。

- 3 「ファイルの種類」タブで、次を実行します:
 - a. 「登録されているファイルの種類」リストで「JNLP」ファイルの種類を選択し、「変更」をクリックします。
 - b. 「ファイルを開くプログラムの選択」ダイアログボックスで、「参照」をクリックしてローカルクライアントシステムに格納されている32ビットJDKファイルを選択します。
 - c. 「この種類のファイルを開くときは、選択したプログラムをいつも使う」チェックボックスをオンにします。
 - d. 「OK」をクリックします。
- 4 ストレージリダイレクションサービスをはじめて起動するには、**Oracle ILOM Web** インタフェースを開き、「**Remote Control**」>「**Redirection**」>「**Launch Service**」の順にクリックします。

「Opening Jnlpgenerator-cli」ダイアログボックスが表示されます。
- 5 「**Opening Jnlpgenerator-cli**」ダイアログボックスで、次のいずれかのオプションを選択して、ファイルをインストールするか、またはそれを**Web** インタフェースから実行します:
 - インストール- 「**Save to disk**」をクリックし、ファイルの格納場所を指定して「**OK**」をクリックします。
 - 実行- 「**Open it with**」をクリックし、ローカルシステム上の **javaws** (デフォルト) 32ビットJDKファイルを選択して「**OK**」をクリックします。**Storage Redirection** サービスが実行される前に、セキュリティ警告ダイアログボックスが表示されます。

特別な考慮事項:

- Jnlpgenerator-cli ファイルのインストールではなく実行を選択した場合、後続のユーザーは Oracle ILOM Storage Redirection CLI コンソールを使用する前に、Oracle ILOM Web インタフェースからストレージリダイレクションサービスを起動する必要があります。
- Jnlpgenerator-cli ファイルの実行を選択し、「*Always perform this action when handling this file type*」チェックボックスもオンにした場合は、今後 Jnlpgenerator-cli のダイアログボックスを使用してデフォルトのストレージネットワークポートを変更できなくなります。したがって、今後デフォルトのネットワークポート(2121)を変更する必要がある場合は、このチェックボックスをオンにするべきではありません。

- 6 次のいずれかを実行してストレージリダイレクションサービスを起動します:
- サービスの実行- 「Security」ダイアログボックスで、「Run」(または「Yes」)をクリックしてサービスを起動します。
 - コマンドウィンドウまたは端末からのサービスの起動-インストールされている **Jnlpgenerator-cli** ファイルの場所に続けて **javaws rconsole.jnlp** コマンドを入力し、サービスを起動します。

構文例:

```
cd jnlp file location javaws rconsole.jnlp
```

ストレージリダイレクションサービスの起動に失敗すると、エラー状況を示すエラーメッセージが表示されます。それ以外で、エラーメッセージが表示されなかった場合は、サービスが起動しており、ユーザー入力を待機しています。

▼ サービスの最初の起動と Mozilla Firefox ブラウザ用の Java Plug-in の登録

(1) ストレージリダイレクションサービスをはじめて起動し、(2) Mozilla Firefox Web ブラウザに 32 ビット JDK Java plug-in を登録するには、この手順を実行します。

- 1 **Oracle ILOM Web** インタフェースからストレージリダイレクションサービスを起動します。
 - 「Remote Console」 > 「Redirection」 > 「Launch Service」の順にクリックします。

jnlpgenerator-cli ファイルを開くためのダイアログボックスが表示されます。
- 2 「Opening Jnlpgenerator-cli」ダイアログで、次のいずれかのオプションを選択して、サービスをローカルにインストールするか、またはサービスを **Web** インタフェースから実行します:
 - インストール- 「Save to disk」をクリックし、ファイルの格納場所を指定して「OK」をクリックします。
 - 実行- 「Open it with」をクリックし、ローカルシステム上の **javaws** (デフォルト) 32 ビット **JDK** ファイルを選択して「OK」をクリックします。 **Storage Redirection** サービスが実行される前に、セキュリティー警告ダイアログボックスが表示されます。

特別な考慮事項:

- `Jnlpgenerator-cli` ファイルのインストールではなく実行を選択した場合、後続のユーザーは Oracle ILOM Storage Redirection CLI コンソールを使用する前に、Oracle ILOM Web インタフェースからストレージリダイレクションサービスを起動する必要があります。
- `Jnlpgenerator-cli` ファイルの実行を選択し、「*Always perform this action when handling this file type*」チェックボックスもオンにした場合は、今後 `Jnlpgenerator-cli` のダイアログボックスを使用してデフォルトのストレージネットワークポートを変更できなくなります。したがって、今後デフォルトのネットワークポート (2121) を変更する必要がある場合は、このチェックボックスをオンにするべきではありません。

3 次のいずれかを実行して **Storage Redirection** サービスを起動します:

- `Jnlpgenerator-cli` ファイルを実行するように構成している場合:
「Security」ダイアログボックスで、「Run」(または「Yes」)をクリックしてサービスを起動します。
- `Jnlpgenerator-cli` ファイルがローカルにインストールされている場合:
インストールされている `Jnlpgenerator-cli` ファイルの場所に続けて `javaws rconsole.jnlp` コマンドを入力し、サービスを起動します。

構文例:

```
cd jnlp file location javaws rconsole.jnlp
```

ストレージリダイレクションサービスの起動に失敗すると、エラー状況を示すエラーメッセージが表示されます。それ以外で、エラーメッセージが表示されなかった場合は、サービスが起動しており、ユーザー入力を待機しています

参考 関連情報:

- [146 ページの「Storage Redirection クライアントのインストール」](#)
- [147 ページの「Storage Redirection のデフォルトのネットワークポート 2121 を変更する \(省略可能\)」](#)

▼ **Storage Redirection** クライアントのインストール

ローカルクライアントシステムにストレージリダイレクションサービスをインストールするには、次の手順を実行します。

注 - これは、Oracle ILOM Storage Redirection CLI をはじめて使用する前に完了する必要がある一回限りのクライアントインストールです。

始める前に

- Java plug-in を登録し、ストレージリダイレクションサービスをはじめて起動するようにしてください。

手順については、次のいずれかを参照してください:

- [143 ページの「Windows IE ブラウザ用の Java Plug-in の登録とサービスの最初の起動」](#)
- [145 ページの「サービスの最初の起動と Mozilla Firefox ブラウザ用の Java Plug-in の登録」](#)

ストレージリダイレクションクライアントをインストールするには、これらの手順を実行します:

- 1 Oracle ILOM Web インタフェースで、「Remote Console」 > 「Redirection」 > 「Download Client」の順にクリックします。

StorageRedir.jar ファイルを開くためのダイアログボックスが表示されます。

- 2 「Opening StorageRedir.jar」ダイアログボックスで、次を実行します:

- 「Save it to disk」をクリックし、「OK」をクリックします。
- 「Save As」ダイアログで、StorageRedir.jar ファイルをローカルクライアントシステム上の場所に保存します。

参考 関連情報:

- [147 ページの「Storage Redirection のデフォルトのネットワークポート 2121 を変更する \(省略可能\)」](#)
- [149 ページの「Oracle ILOM Storage Redirection CLI の起動と使用」](#)

▼ Storage Redirection のデフォルトのネットワークポート 2121 を変更する (省略可能)

Oracle ILOM がストレージリダイレクションに使用するデフォルトのネットワークポート 2121 を必要に応じて変更するには、次の手順を実行します。

始める前に

- 次の手順には、Jnlpgenerator-cli ファイルへのアクセスが必要です。

注-以前にストレージリダイレクションサービス用の `Jnlpgenerator-cli` ファイルを Web インタフェースから実行するように構成し、以前に `Jnlpgenerator-cli` ファイルを開くためのダイアログを表示しないように構成した場合は、次の手順を使用してデフォルトのストレージリダイレクションネットワークポートを変更できません。

- Oracle ILOM Web インタフェースからストレージリダイレクションサービスを実行するには、Console (c) の役割が必要です。
- デフォルトのストレージリダイレクションポート番号を変更すると、Oracle ILOM ストレージリダイレクションのユーザーは、コマンドウィンドウまたは端末からストレージリダイレクションの開始、停止、または表示を行うときに必ずデフォルト以外のポート番号を指定する必要があります。

デフォルトのストレージリダイレクションネットワークポート 2121 を変更するには、これらの手順に従います:

1 Jnlpgenerator-cli ファイルにアクセスするため、次のいずれかを実行します:

- ストレージリダイレクションサービスの `Jnlpgenerator-cli` ファイルがインストールされている場合:
テキストエディタを使用して、ローカルに格納されている `Jnlpgenerator-cli` ファイルを開きます。
- ストレージリダイレクションサービスの `Jnlpgenerator-cli` ファイルを Web インタフェースから実行するように設定している場合:
 - a. Oracle ILOM Web インタフェースで、「Remote Console」 > 「Redirection」 > 「Launch Service」の順にクリックします。
Jnlpgenerator-cli ファイルを開くためのダイアログが表示されます。
 - b. 「Opening Jnlpgenerator-cli」ダイアログで、「Save to disk」をクリックし、「OK」をクリックします。
 - c. 「Save As」ダイアログで、ファイルを格納する場所を指定して「OK」をクリックします。
 - d. テキストエディタを使用して、ローカルクライアントシステム上に格納されている `Jnlpgenerator-cli` ファイルを開きます。

- 2 **Jnlpgenerator-cli** ファイル内で参照されるポート番号引数を変更し、変更をファイルに保存します。

ファイルの例:

```
<application-desc>
<argument>cli</argument>
<argument>2121</argument>
</application-desc>
```

デフォルトのネットワークポート 2121 を変更し、ローカルに格納されている **Jnlpgenerator-cli** ファイルに変更を保存したあとは、コマンドウィンドウまたは端末からストレージリダイレクションの開始、停止、または表示を行うときに必ずデフォルト以外のポート番号を指定する必要があります。

Oracle ILOM Storage Redirection CLI の起動と使用

Oracle ILOM Storage Redirection CLI を起動して使用するには、これらのトピックを参照してください:

- 149 ページの「Oracle ILOM Storage Redirection CLI の起動とストレージデバイスのリダイレクション」
- 154 ページの「対話型および非対話型シェルの構文」
- 154 ページの「Storage Redirection のコマンドおよびオプション」

▼ Oracle ILOM Storage Redirection CLI の起動とストレージデバイスのリダイレクション

Oracle ILOM Storage Redirection CLI コンソールを起動して使用するには、次の手順を使用します。

始める前に

- 初回使用時の要件を満たしていることを確認します: [表 52](#)。
- Oracle ILOM リモートコンソールを起動して使用するには、Console (c) の役割が必要です。
- シェルモードの構文とストレージリダイレクションのコマンドを確認します:
 - 154 ページの「対話型および非対話型シェルの構文」
 - 154 ページの「Storage Redirection のコマンドおよびオプション」

Storage Redirection CLI コンソールを起動してストレージデバイスをリダイレクトするには、これらの手順を実行します:

- 1 ストレージリダイレクションサービスを起動するには、次のいずれかを実行します:
 - Oracle ILOM Web インタフェースからストレージリダイレクションサービスを実行するには:
 - a. Oracle ILOM Web インタフェースで、「Remote Console」 > 「Redirection」 > 「Launch Service」の順にクリックします。
Jnlpgenerator-cli ファイルを開くためのダイアログが表示されます。
 - b. 「Opening Jnlpgenerator-cli」ダイアログで、「Open it with」をクリックし、javaws (デフォルト)(32 ビット JDK ファイル)を選択して「OK」をクリックします。
 - c. 「Warning Security」ダイアログボックスで、「Run」をクリックしてストレージリダイレクションサービスを起動します。
 - d. ローカルクライアントシステム上でコマンドウィンドウまたは端末を開き、Oracle ILOM Storage Redirection CLI を起動します。
Oracle ILOM Storage Redirection CLI の起動手順については、手順 2 を参照してください。
 - コマンドウィンドウから (インストールされている) ストレージリダイレクションサービスを起動するには:
 - a. ローカルクライアントシステム上でコマンドウィンドウまたは端末を開きます。
例:
Windows システム: 「スタート」メニューから「ファイル名を指定して実行」をクリックし、**cmd** と入力して「OK」をクリックします。
Oracle Solaris または **Linux** システム: デスクトップで端末ウィンドウを開きます。
 - b. **Jnlpgenerator-cli** ファイルがインストールされている場所に移動し、**javaws rconsole.jnlp** コマンドを実行してサービスを起動します。
例:

```
cd jnlp_file_location/javaws rconsole.jnlp
```
- 2 コマンドウィンドウまたは端末から **Storage Redirection CLI** コンソールを起動するには、使用しているシェルモードに応じて次のいずれかの手順を実行します。

シェルモード	説明および手順
対話型シェルモード	<p data-bbox="465 210 1322 262">対話型モードは、一連の Storage Redirection コマンドを入力する必要がある場合に便利です。</p> <p data-bbox="465 284 1322 336">対話型シェルモードを使用して Storage Redirection CLI コンソールを起動するには、これらの手順を実行します:</p> <ol data-bbox="465 343 1322 399" style="list-style-type: none"><li data-bbox="465 343 1322 399">a. コマンド行インタフェースで、<code>cd</code> コマンドを使用して、Storage Redirection クライアント (<code>StorageRedir.jar</code>) がインストールされているディレクトリに移動します。 <p data-bbox="504 406 532 427">例:</p> <pre data-bbox="504 440 872 461"><code>cd my_settings/storage_redirect_directory</code></pre> <ol data-bbox="465 482 1322 503" style="list-style-type: none"><li data-bbox="465 482 1322 503">b. 次のコマンドを入力して、Storage Redirection CLI を起動します。 <pre data-bbox="504 517 779 538"><code>java -jar StorageRedir.jar</code></pre> <p data-bbox="504 545 532 565">例:</p> <pre data-bbox="504 579 1193 600"><code>C:\Documents and Settings\redirectstorage java -jar StorageRedir.jar</code></pre> <p data-bbox="504 607 918 628"><code><storageredir></code> プロンプトが表示されます。</p> <p data-bbox="465 656 1322 743">注 - Windows を使用している場合は、ターゲットディスクドライブの大文字を指定する必要があります。たとえば、ターゲットディスクドライブに割り当てられた文字が <code>c:</code> である場合は、<code>c:</code> ではなく <code>C:</code> を指定する必要があります。</p> <p data-bbox="465 767 1322 819">ヒント - 「<code>java</code>」の前にスペースを1つだけ入力し、「<code>-jar</code>」の前後にスペースを1つ入力します。それ以外の場合、<code>java -jar StorageRedir.jar</code> コマンドが失敗します。</p> <p data-bbox="465 843 565 864">関連情報:</p> <ul data-bbox="465 878 1019 899" style="list-style-type: none"><li data-bbox="465 878 1019 899">■ 154 ページの「対話型および非対話型シェルの構文」

シェルモード	説明および手順
非対話型シェルモード	<p>非対話型モードは、バッチ手続きまたはスクリプトを実行する必要がある場合に便利です。</p> <p>非対話型シェルモードを使用して Storage Redirection CLI コンソールを起動するには、これらの手順を実行します:</p> <ol style="list-style-type: none"> コマンド行インタフェースで、シェルプロンプト (\$) に Storage Redirection CLI を起動するコマンド (<code>java -jar StorageRedir.jar</code>) を入力します。 <pre>\$ java -jar StorageRedir.jar</pre> <p>注 - JAVA_HOME 環境が構成されていない場合は、Java バイナリへのフルパスを使用しなければならないことがあります。たとえば、JDK パッケージを <code>/home/user_name/jdk</code> の下にインストールした場合は、次のように入力します:</p> <pre>/home/user_name/jdk/bin/java -jar ...</pre> Storage Redirection CLI の起動に失敗すると、エラー状況を示す詳細なエラーメッセージが表示されます。それ以外の場合、Storage Redirection CLI はユーザー入力を受け付ける準備ができています。 <p>注 - ローカルのコマンドウィンドウまたは端末から Storage Redirection コマンド (<code>-jar StorageRedir.jar</code>) を実行すると、複数の Storage Redirection CLI コンソールを起動できます。</p> <p>ヒント - 「<code>-jar</code>」の前後にスペースを1つだけ入力します。それ以外の場合、<code>java -jar StorageRedir.jar</code> コマンドが失敗します。</p> <p>関連情報:</p> <ul style="list-style-type: none"> ■ 154 ページの「対話型および非対話型シェルの構文」 ■ 154 ページの「Storage Redirection のコマンドおよびオプション」

- ストレージリダイレクションサービスが実行されていることを確認するには、次のコマンドを入力します:

test-service

リダイレクションサービスの成功または失敗を示すメッセージが表示されます。

コマンドの説明とシェルモードの構文については、これらのトピックを参照してください:

- 154 ページの「Storage Redirection のコマンドおよびオプション」
- 154 ページの「対話型および非対話型シェルの構文」

- ストレージリダイレクションを開始するには、次の **start** コマンドに続けて、リモート **SP** のリダイレクションデバイスの種類、デバイスへのパス、リモート **SP** ユーザー名とパスワード、および **IP** アドレスに関するサブコマンドとプロパティを入力します。

例:

注- 次の例で示すコマンドは、ひと続きの文字列として入力するようにしてください。

```
start -r redir_type -t redir_type_path -u remote_username [-s remote_user_password] [-p non_default_storageredir_port] remote_SP_IP
```

コマンドの説明とシェルモードの構文については、これらのトピックを参照してください:

- 154 ページの「[Storage Redirection のコマンドおよびオプション](#)」
- 154 ページの「[対話型および非対話型シェルの構文](#)」

- 5 アクティブなストレージリダイレクションを表示するには、**list** コマンドに続けて、リモートホストサーバー **SP** のデフォルト以外のストレージリダイレクションポートと **IP** アドレスに関するサブコマンドとプロパティーを入力します。

例:

```
list [-p non_default_storageredir_port] remote_SP
```

コマンドの説明とシェルモードの構文については、これらのトピックを参照してください:

- 154 ページの「[Storage Redirection のコマンドおよびオプション](#)」
- 154 ページの「[対話型および非対話型シェルの構文](#)」

- 6 ストレージデバイスのリダイレクションを停止するには、**stop** コマンドに続けて、リモートホストサーバー **SP** のストレージデバイスの種類、リモート **SP** ユーザー名とパスワード、ストレージリダイレクションポート、および **IP** アドレスに関するコマンドとプロパティーを入力します。

例:

```
stop -r redir_type -u remote_username [-s remote_user_password] [-p non_default_storageredir_port] remote_SP
```

コマンドの説明とシェルモードの構文については、これらのトピックを参照してください:

- 154 ページの「[Storage Redirection のコマンドおよびオプション](#)」
- 154 ページの「[対話型および非対話型シェルの構文](#)」

- 7 コマンド行のヘルプを表示するには、次のコマンドを入力します:

```
help
```

コマンドの構文と使用方法に関する次の情報が表示されます。

使用法:

```

list [-p storageredir_port] [remote_SP]

start -r redir_type -t redir_type_path -u remote_username [-s remote_user_password] [-p
storageredir_port] remote_SP stop -r redir_type -u remote_username [-s
remote_user_password] [-p storageredir_port] remote_SP

stop-service [-p storageredir_port]

test-service [-p storageredir_port]

help

version

quit

```

対話型および非対話型シェルの構文

これらのモードのいずれかで Storage Redirection のコマンドを入力するために必要な構文は、次のとおりです:

- 対話型シェルモードの構文

```
storageredir <command> <command_options> <sub_commands>
<sub_command_options>
```

- 非対話型シェルモードの構文

```
$ java -jar StorageRedir.jar <command> <command_options> <sub_commands>
<sub_command_options>
```

Storage Redirection のコマンドおよびオプション

- [表 53](#)
- [表 54](#)
- [表 55](#)
- [表 56](#)

表 53 Storage Redirection のコマンド

コマンド名	説明
java -jar StorageRedir.jar	java -jar コマンドは、コマンドウィンドウまたは端末から Storage Redirection クライアント (StorageRedir.jar) を起動するために使用します。
storageredir	storagedir コマンドは、すべてのストレージリダイレクション操作を実行します。

表 54 Storage Redirection のコマンドオプション

オプション名	説明
- h	-h コマンドオプションは、コマンド行のヘルプ情報を表示します。
- v	-v コマンドオプションは、Java コマンドのバージョン情報を表示します。

表 55 Storage Redirection のサブコマンド

サブコマンド名	説明
list	<p>list サブコマンドは、1つまたはすべてのリモート SP で現在アクティブなストレージリダイレクションのリストを提供します。</p> <p>構文の使用例:storageredir list [-p storageredir_port] [remote_SP]</p>
start	<p>start サブコマンドは、ローカルホストとリモートホストサーバーの間の指定されたリダイレクションを呼び出します。認証パスワードを入力しないと、システムがパスワードを要求します。</p> <p>構文の使用 例:storageredir start -r redir_type -t redir_type_path -u remote_username [-s remote_user_password] [-p storageredir_port] remote_SP</p> <p>注-リモートサーバーのストレージデバイスのリダイレクションを開始するには、有効な Admin (a) または Console (c) の役割のアカウントを Oracle ILOM で指定する必要があります。</p>
stop	<p>stop サブコマンドは、ローカルホストとリモートホストサーバーの間の指定されたリダイレクションを停止します。認証パスワードを入力しないと、システムがパスワードを要求します。</p> <p>構文の使用例:storageredir stop -r redir_type -u remote_username [-s remote_user_password] [-p storageredir_port] remote_SP</p> <p>注-リモートサーバーのストレージデバイスのリダイレクションを停止するには、有効な Admin (a) または Console (c) の役割のアカウントを Oracle ILOM で指定する必要があります。</p>
test-service	<p>test-service サブコマンドは、Storage Redirection サービスの接続がローカルホストでアクティブになっているかどうかを確認します。</p> <p>構文の使用例:storageredir test-service [-p storageredir_port]</p>
stop-service	<p>stop-service サブコマンドは、リモートホストサーバーへの Storage Redirection サービスの接続を停止します。</p> <p>構文の使用例:storageredir stop-service [-p storageredir_port]</p>

表 56 Storage Redirection のサブコマンドオプション

サブコマンドオプション名	説明
<code>-r redir_type</code>	<p><code>-r redir_type</code> は、リダイレクト対象のストレージメディアの種類を識別します。</p> <p><code>redir_type</code> の有効なデバイス値は、次のとおりです:</p> <ul style="list-style-type: none"> ■ CD-ROM デバイスの構文: <code>-r cdrom</code> ■ CD-ROM イメージ: 構文: <code>-r cdrom_img</code> ■ フロッピーデバイス: 構文: <code>-r floppy</code> ■ フロッピーイメージ: 構文: <code>-r floppy_img</code>
<code>-t redir_type_path</code>	<p><code>-t redir_type_path</code> は、Storage Redirection メディアが格納またはマウントされている場所へのフルパスを識別します。</p> <p>例: <code>-t /home/username/JRC_Test_Images/CDROM.iso</code></p>
<code>-u remote_username</code>	<p><code>-u remote_username</code> は、Oracle ILOM SP へのログインに必要なユーザー名を識別します。</p> <p>例:</p> <p><code>-u john_smith</code></p> <p>注 - Oracle ILOM で有効なユーザーアカウントはすべて、ローカルシステムで Storage Redirection サービスまたはクライアントをインストールまたは起動できます。ただし、リモートサーバー上のストレージデバイスのリダイレクションを開始または停止するには、有効な Admin (a) または Console (c) の役割が Oracle ILOM で必要です。</p>
<code>-s remote_user_password</code>	<p><code>-s remote_user_password</code> は、Oracle ILOM SP へのログインに必要なパスワードを識別します。</p> <p>例:</p> <p><code>-s my_password</code></p> <p>このパスワードコマンドがコマンド行で指定されていない場合、システムは自動的にパスワードの入力を要求します。</p>
<code>-p storageredir_port</code>	<p><code>-p storageredir_port</code> は、ローカルホストでの Storage Redirection 通信ポートを識別します。指定されているデフォルトポートは 2121 です。</p> <p>例:</p> <p><code>-p 2121</code></p>

ホストシリアルリダイレクションセッションの開始と停止

Oracle ILOM には、Oracle ILOM リモートコンソールと Storage Redirection CLI に加えて、ホストサーバーのオペレーティングシステムに対するテキストベースのシリアルリダイレクションセッションを開始する機能が用意されています。

Oracle ILOM の Console (c) の役割のユーザーは、CLI からホストシリアルリダイレクションコンソールを起動または停止できます。リダイレクションセッションを開始したあとは、ホストオペレーティングシステムにアクセスするためのホストユーザー資格が必要です。ホストユーザーは、Oracle ILOM からリダイレクションセッションを停止する前に、ホストオペレーティングシステムからログアウトするようにしてください。

CLI からホストシリアルコンソールを起動および停止する手順の詳細は、次の手順を参照してください。

▼ シリアルコンソールリダイレクションの開始とホストサーバー OS へのログイン

始める前に

- Oracle ILOM でホストサーバーのオペレーティングシステムに対するシリアルリダイレクションセッションを開始するには、Console (c) の役割が必要です。
- ホストオペレーティングシステムにアクセスするには、ホストサーバーのユーザー資格が必要です。ユーザーは、Oracle ILOM からホストリダイレクションセッションを終了する前に、ホストオペレーティングシステムからログアウトするようにしてください。
- ホストシリアルリダイレクションセッションは、Oracle ILOM SP CLI からのみ開始できます。

- 1 Oracle ILOM SP CLI からホストシリアルリダイレクションコンソールを起動するには、次を入力します:

```
start /host/console
```

ユーザー資格を指定するように促すメッセージが表示されます。

- 2 ホストサーバーのオペレーティングシステムにアクセスするために必要なユーザー資格を入力します。

これで、ホストシリアルコンソールを介してホストサーバーのオペレーティングシステムにログインしました。

注- 標準の Oracle ILOM CLI コマンドを実行するには、最初にホストシリアルコンソールを終了する必要があります。

- 3 ホストリダイレクションセッションを終了するには、ホストサーバーのオペレーティングシステムからログアウトし、**ESC** キーと (キーを押してホストシリアルコンソールセッションを終了します。

注- ホストにブレークを送信するには、Esc キーを押して大文字の B を入力します。

ホストサーバー管理操作の構成

説明	リンク
CMM および SP のホスト電源制御に関する構成可能なプロパティについては、このセクションを参照してください。	■ 160 ページの「サーバーまたはブレードシステムシャーシに対するホスト電源の制御」
SP の構成可能な診断プロパティについては、このセクションを参照してください。	■ 161 ページの「実行するホスト診断テストの設定」
x86 SP の次のブートデバイスに関する構成可能なプロパティについては、このセクションを参照してください。	■ 165 ページの「x86 ホストサーバーの次のブートデバイスの設定」
SPARC SP のホスト制御に関するプロパティについては、このセクションを参照してください。	■ 166 ページの「SPARC ホストサーバーのブート動作の設定」
SPARC SP の OpenBoot および LDom に関する構成可能なブートモードプロパティについては、このセクションを参照してください。	■ 170 ページの「SPARC ホストブートモードのオーバーライド」
SPARC SP のホストドメインに関する構成可能なブートプロパティ、および現在設定されている LDom 構成の一覧については、このセクションを参照してください。	■ 172 ページの「SPARC ホストドメインの管理」
SPARC SP のホストキースイッチ状態に関する構成可能なプロパティ値については、このセクションを参照してください。	■ 174 ページの「SPARC ホストキースイッチ状態の設定」
SPARC SP のホスト TPM 状態に関する構成可能なプロパティ値については、このセクションを参照してください。	■ 175 ページの「SPARC ホスト TPM 状態の設定」

関連情報

- [221 ページの「x86 BIOS 構成パラメータの保守」](#)

サーバーまたはブレードシステムシャーシに対するホスト電源の制御

Oracle ILOM には、システム管理者がホストサーバーまたはブレードシャーシシステムの電源状態を制御するために使用できる一連のパラメータが用意されています。

システム管理者は、Oracle ILOM の CLI または Web インタフェースから電源制御コマンドを実行できます。各電源制御コマンドの詳細は、次の表を参照してください。

表 57 ホスト管理対象デバイス用のリモート電源制御コマンド

ユーザーインタフェースの構成可能なターゲットとユーザーの役割:

- **CLI:** `<command> /System`
- **Web:** 「Host Management」 > 「Power Control」
- ユーザーの役割: Admin (a) の役割

要件:

- Web インタフェースで選択した電源オプションを適用するには、「Save」をクリックする必要があります。

Web	CLI	該当する対象:	説明
Reset	<ul style="list-style-type: none"> ■ x86 SP: <code>reset /System</code> ■ SPARC: <code>reset -force /System</code> 	<ul style="list-style-type: none"> ■ 任意の管理対象サーバー 	「Reset」は、システムコンポーネント (ディスクドライブなど) に適用される電源を維持しながら管理対象サーバーの電源を再投入することを表明するために使用します。
Graceful Reset	<ul style="list-style-type: none"> ■ <code>reset /System</code> 	<ul style="list-style-type: none"> ■ SPARC 管理対象サーバーのみ 	「Graceful Reset」は、ホストオペレーティングシステムを正常にシャットダウンしてから管理対象サーバーの電源を再投入するために使用します。
Immediate Power Off	<ul style="list-style-type: none"> ■ <code>stop -force /System</code> 	<ul style="list-style-type: none"> ■ 任意の管理対象サーバーまたはブレードシステムシャーシ 	「Immediate Power Off」は、管理対象デバイスの電源をすぐに停止するために使用します。
Graceful Shutdown and Power Off	<ul style="list-style-type: none"> ■ <code>stop /System</code> 	<ul style="list-style-type: none"> ■ 任意の管理対象サーバーまたはブレードシステムシャーシ 	「Graceful Shutdown and Power Off」は、ホストオペレーティングシステムを正常にシャットダウンしてから管理対象デバイスの電源を停止するために使用します。

表 57 ホスト管理対象デバイス用のリモート電源制御コマンド (続き)

ユーザーインタフェースの構成可能なターゲットとユーザーの役割:

- CLI: `<command> /System`
- Web: 「Host Management」 > 「Power Control」
- ユーザーの役割: Admin (a) の役割

要件:

- Web インタフェースで選択した電源オプションを適用するには、「Save」をクリックする必要があります。

Web	CLI	該当する対象:	説明
Power On	<ul style="list-style-type: none"> ■ <code>start /System</code> 	<ul style="list-style-type: none"> ■ 任意の管理対象サーバーまたはブレードシステムシャーシ 	「Power On」は、管理対象デバイスの電源を完全に投入するために使用します。
Power Cycle	<ul style="list-style-type: none"> ■ <code>stop /System</code> ■ <code>start /System</code> 	<ul style="list-style-type: none"> ■ 任意の管理対象サーバー 	「Power Cycle」は、すべてのシステムコンポーネントのシステム電源を切断してから、すべてのシステムコンポーネントの電源を完全に投入するために使用します。

実行するホスト診断テストの設定

Oracle ILOM には、システム管理者が起動時にシステム診断テストを実行するかどうかを制御するために使用できる一連のサーバー固有の診断プロパティーが用意されています。これらの診断プロパティーは、Oracle ILOM の CLI または Web インタフェースから構成できます。これらのプロパティーの詳細は、以降の表を参照してください:

- [表 58](#)
- [表 59](#)

表 58 x86 サーバー SP の診断プロパティ

ユーザーインターフェースの構成可能なターゲットとユーザーの役割:

- **SP CLI:** /HOST
- **Web:** 「Host Management」 > 「Diagnostics」
- ユーザーの役割: **Reset and Host Control (r)** の役割 (診断プロパティを変更するために必要)。

要件:

- Web インタフェースでの診断プロパティの変更を適用するには、「Save」をクリックする必要があります。

プロパティ	デフォルト値	説明
Run Diagnostics on Boot (/diag/state=disabled enabled extended manual)	Disabled	<p><i>Disabled Enabled Extended Manual</i></p> <ul style="list-style-type: none"> ■ Disabled - x86 サーバーの電源投入時に PC-Check 診断テストが実行されません。 ■ Enabled - x86 サーバーの電源投入時に基本的な PC-Check 診断テストが実行され、完了するまでに約 3 分かかります。 ■ Extended - x86 サーバーの電源投入時に拡張 PC-Check 診断テストが実行され、完了するまでに約 20 分かかります。 ■ Manual - サーバーの電源リセット時に PC-Check 診断テストがマニュアルモードで実行されます。サーバーの電源投入時に PC-Check 診断テストのメニューが表示され、テストを手動で有効にすることができます。 <p>「Diagnostics on Boot State」の CLI 構文:</p> <pre>set /HOST/diag state=disabled enabled extended manual</pre>
Generate NMI button (generate_host_nmi=true)	値なし	<p>このオプションを有効にすると、ホストオペレーティングシステムにマスク不可能割り込みが送信されます。</p> <p>注 - ホストオペレーティングシステムの構成によっては、この操作によってオペレーティングシステムがクラッシュしたり、応答しなくなったり、外部デバッガからの入力を待機したりする場合があります。</p> <p>「Generate NMI」の CLI 構文:</p> <pre>set /HOST/generate_host=true</pre>

表 59 SPARC サーバー SP の診断プロパティ

ユーザーインタフェースの構成可能なターゲットとユーザーの役割:

- **SP CLI:** /HOST/diag
- **Web:** 「Host Management」 > 「Diagnostics」
- ユーザーの役割: **Reset and Host Control (r)** の役割 (診断プロパティを変更するために必要)。

要件:

- Web インタフェースでの診断プロパティの変更を適用するには、「Save」をクリックする必要があります。

プロパティ	デフォルト値	説明
Trigger (trigger=error-reset hw-change power-on-resets)	HW-Change	<i>Power-On HW-Change Error-Reset</i> 電源投入時自己診断 (POST) を実行するには、次の 1 つまたは複数のトリガーを指定します。 <ul style="list-style-type: none"> ■ Power On - 有効にすると、SPARC サーバーの電源投入時に電源投入時自己診断 (POST) が実行されます。 ■ HW-Change - 有効にすると、起動時に次のハードウェア変更が発生した場合に電源投入時自己診断 (POST) が実行されます: FRU の交換、カバーの取り外し、または AC 電源の再投入。 ■ Error-reset - 有効にすると、エラーによる電源リセットが発生したあとで電源投入時自己診断 (POST) が実行されます。 「Trigger」の CLI 構文: set /HOST/diag/trigger=error-reset hw-change power-on-resets
Trigger Levels (power_on_level= hw_change_level= error_reset_level=)	Max	<i>Max Min</i> 有効にした各トリガーのテストレベルを別個に設定します。 <ul style="list-style-type: none"> ■ Max - 有効にすると、最大レベルの診断テストを実行します。 ■ Min - 有効にすると、最小レベルの診断テストを実行します。 「Trigger Levels」の CLI 構文: set /HOST/diag/error_reset_level=min max hw_change_level=min max power_on_level=min max

表 59 SPARC サーバー SP の診断プロパティ (続き)

ユーザーインタフェースの構成可能なターゲットとユーザーの役割:

- **SP CLI:** /HOST/diag
- **Web:** 「Host Management」 > 「Diagnostics」
- ユーザーの役割: **Reset and Host Control (r)** の役割 (診断プロパティを変更するために必要)。

要件:

- Web インタフェースでの診断プロパティの変更を適用するには、「Save」をクリックする必要があります。

プロパティ	デフォルト値	説明
Trigger Verbosity (power_on_verbosity= hw_change_verbosity= error_reset_verbosity=)	Min	<p><i>Normal Min Max Debug None</i></p> <p>有効にした各トリガーのレポートレベルを別個に設定します:</p> <ul style="list-style-type: none"> ■ Normal - 有効にすると、Oracle ILOM は中程度の量のデバッグ情報をシステムコンソールに出力します。出力には、各テスト実行の名前と結果が含まれています。 ■ Min - 有効にすると、Oracle ILOM は限られた量の出力をシステムコンソールに出力します (デフォルト)。 ■ Max - 有効にすると、Oracle ILOM は各 POST 手順のデバッグ情報をシステムコンソールに出力します。 ■ Debug - 有効にすると、Oracle ILOM は広範囲のデバッグ情報をシステムコンソールに出力します。出力には、各テスト実行のテストされたコンポーネントの名前とテスト結果が含まれています。 ■ None - 有効にすると、Oracle ILOM はシステムコンソールへのデバッグ情報の出力を無効にします。 <p>「Trigger Verbosity」の CLI 構文:</p> <pre>set /HOST/diag/error_reset_verbosity=normal min max debug none hw_change_verbosity=normal min max debug none power_on_verbosity=normal min max debug none</pre>
Mode (mode=)	Normal	<p><i>Off Normal</i></p> <p>有効にしたすべてのトリガーで電源投入時自己診断を有効または無効にするモードを設定します。</p> <ul style="list-style-type: none"> ■ Off - 有効にしたすべてのトリガーで電源投入時自己診断 (POST) を実行しません。 ■ Normal - 有効にしたすべてのトリガーで電源投入時自己診断 (POST) を実行します (デフォルト)。 <p>「Mode」の CLI 構文:</p> <pre>set /HOST/diag/mode=normal off</pre>

x86 ホストサーバーの次回のブートデバイスの設定

Oracle ILOM には、システム管理者がホストサーバーの次回のブートデバイスを設定するために使用できる一連の x86 サーバードプロパティが用意されています。ただし、Oracle ILOM のこれらの構成可能なブートデバイスプロパティは、x86 サーバーの次の電源投入時にのみ適用されます。

注- システムの電源が投入され、Oracle ILOM の (ユーザーが指定した) ブートデバイスがブートすると、システムはシステム BIOS ユーティリティで設定されたブートデバイスプロパティに戻ります。

システム管理者は、Oracle ILOM の CLI または Web インタフェースから x86 サーバーの次回のブートデバイスに関するプロパティを設定できます。x86 サーバーの次回のブートデバイスに関するこれらのプロパティの詳細は、次の表を参照してください。

表 60 x86 管理対象サーバーの次回のブートデバイスプロパティの設定

プロパティ値	説明
ユーザーインタフェースの構成可能なターゲットとユーザーの役割: <ul style="list-style-type: none"> ■ SP CLI: <code>/SP/HOST/boot_device=</code> ■ SP Web: 「Host Management」 > 「Host Control」 > 「Next Boot Device」 ■ ユーザーの役割: Reset and Host Control (r) の役割 	
要件:	
<ul style="list-style-type: none"> ■ Web インタフェースの次回のブートデバイスオプションを適用するには、「Save」をクリックする必要があります。 	
Default (Use BIOS Settings) (boot_device=default)	<p>「Default (Use BIOS Settings)」プロパティを設定すると、システム BIOS のブート順序で現在設定されている 1 つ目のデバイスから x86 システムがブートされます。</p> <p>CLI から構成可能なホストプロパティを設定するには、set コマンド (<code>set /Host property_name=value</code>) を実行します。</p>
PXE (boot_device=pxe)	<p>「PXE」プロパティを設定すると、システム BIOS のブート順序が一時的に無視され、PXE ブート仕様を使用してネットワーク経由で x86 システムがブートされます。</p>
Disk (boot_device=disk)	<p>「Disk」プロパティを設定すると、システム BIOS のブート順序が一時的に無視され、BIOS ユーティリティのブート順序の 1 つ目のディスクによって特定される 1 つ目のディスクデバイスがブートされます。</p>
Diagnostic (boot_device=diagnostic)	<p>「Diagnostic」プロパティを設定すると、システム BIOS のブート順序が一時的に無視され、診断パーティションからシステムがブートされます (構成されている場合)。</p>

表 60 x86 管理対象サーバーの次回のブートデバイスプロパティの設定 (続き)

ユーザーインタフェースの構成可能なターゲットとユーザーの役割:	
■ SP CLI: /SP/HOST/boot_device=	
■ SP Web: 「Host Management」 > 「Host Control」 > 「Next Boot Device」	
■ ユーザーの役割: Reset and Host Control (r) の役割	
要件:	
■ Web インタフェースの次回のブートデバイスオプションを適用するには、「Save」をクリックする必要があります。	
プロパティ値	説明
CDROM (boot_device=cdrrom)	「CDROM」プロパティを設定すると、システム BIOS のブート順序が一時的に無視され、接続されている CD-ROM または DVD デバイスからシステムがブートされます。
BIOS (boot_device=bios)	「BIOS」プロパティを設定すると、BIOS のブート順序が一時的に無視され、システムのブート時に BIOS ユーティリティの設定メニューが表示されます。

SPARC ホストサーバーのブート動作の設定

Oracle ILOM には、システム管理者がホスト制御情報を表示したり、必要に応じてシステムのブート動作を制御するプロパティを設定したりするために使用できる一連の SPARC サーバープロパティが用意されています。

システム管理者は、Oracle ILOM の CLI または Web インタフェースからホスト制御情報を表示したり、構成可能な SPARC サーバーブートプロパティを設定したりできます。これらのプロパティの詳細は、次の表を参照してください。

表 61 SPARC 管理対象サーバーのホスト制御情報およびブートのプロパティ

プロパティ	デフォルト値	説明
ユーザーインターフェースの構成可能なターゲットとユーザーの役割: <ul style="list-style-type: none"> ■ SP CLI: /HOST property_name ■ Web: 「Host Management」 > 「Host Control」 ■ ユーザーの役割: 構成可能なホストプロパティを変更するには、Reset and Host Control (r) の役割が必要です。 要件: <ul style="list-style-type: none"> ■ Web の 「Host Control」 ページで行われたプロパティの変更を適用するには、「Save」をクリックする必要があります。 		
Host Control Information /HOST	読み取り専用プロパティ	SPARC サーバーの次のホスト制御情報を表示します: <ul style="list-style-type: none"> ■ MAC Address - 管理対象デバイスに割り当てられた Ethernet MAC アドレスを表示します。 ■ Hypervisor Version - Hypervisor ファームウェアのバージョンを表示します。 ■ OBP - OpenBoot PROM (OBP) ファームウェアのバージョンを表示します。 ■ POST Version - 現在の POST のバージョンを表示します。 ■ SysFW Version - 現在インストールされている Oracle ILOM ファームウェアのバージョンを表示します。 ■ Host Status - ホストオペレーティングシステムの現在の電源状態を表示します。 「Host Control Information」の CLI 構文: show /HOST
Auto Run On Error (autorunonerror=false true)	False (無効)	False True 致命的でないブートエラーが発生しても SPARC サーバーのブートを続行するように Oracle ILOM を設定します。 「Auto Run On Error」の CLI 構文: set /HOST autorunonerror=true false

表 61 SPARC 管理対象サーバーのホスト制御情報およびブートのプロパティ (続き)

ユーザーインターフェースの構成可能なターゲットとユーザーの役割:

- **SP CLI:** /HOST property_name
- **Web:** 「Host Management」 > 「Host Control」
- ユーザーの役割: 構成可能なホストプロパティを変更するには、**Reset and Host Control (r)** の役割が必要です。

要件:

- Web の「Host Control」ページで行われたプロパティの変更を適用するには、「Save」をクリックする必要があります。

プロパティ	デフォルト値	説明
Auto Restart Policy (autorestart=)	Reset	<p><i>Reset Dump Core None</i></p> <p>ホストオペレーティングシステムがハングアップしたときに Oracle ILOM が実行する処理を設定します。</p> <ul style="list-style-type: none"> ■ Reset (デフォルト) - Oracle ILOM は、Oracle Solaris のウォッチドッグタイマーが期限切れになると、SPARC サーバーの電源リセットを試みます。 ■ None - Oracle ILOM は警告を発行し、それ以外の処理を行いません。 ■ Dump Core - Oracle ILOM は、Oracle Solaris のウォッチドッグタイマーが期限切れになると、オペレーティングシステムのコアダンプを強制的に試みます。 <p>「Auto Restart Policy」の CLI 構文:</p> <pre>set /HOST autorestart=reset dumpcore none</pre>
Boot Timeout (boottimeout=)	0 (タイマーが無効)	<p>0 から 36000 までの整数 (秒)</p> <p>SPARC サーバーのブートタイマーのタイムアウト値を設定します。</p> <p>「Boot Timeout」の CLI 構文:</p> <pre>set /HOST boottimeout=0 to 360000</pre>
Boot Restart Policy (bootrestart=)	None (ポリシーが無効)	<p><i>None Reset</i></p> <p>システムがタイムアウトしたときに Oracle ILOM が SPARC サーバーを再起動するかどうかを設定します。</p> <p>「Boot Restart Policy」の CLI 構文:</p> <pre>set /HOST bootrestart=reset none</pre>

表 61 SPARC 管理対象サーバーのホスト制御情報およびブートのプロパティー (続き)

プロパティー	デフォルト値	説明
Max Boot Fails Allowed (maxbootfails=)	3 (試行回数)	<p>0 から 10000 までの整数 (試行回数)</p> <p>Oracle Solaris のブートプロセスが失敗したときに許可される最大試行回数を設定します。</p> <p>max boot fail が示す試行回数内でホストが正常にブートしない場合、ホストは電源が切断または再投入されます (boot fail recovery の設定によって異なる)。いずれの場合も、boot timeout は 0 (ゼロ秒) に設定され、その後のホスト再起動の試行は無効になります。</p> <p>「Max Boot Fails Allowed」の CLI 構文:</p> <pre>set /HOST bootrestart=0 to 10000</pre>
Boot Fail Recovery (bootfailrecovery=)	Poweroff	<p>Powercycle Poweroff None</p> <p>このプロパティーを設定すると、最大ブート試行回数に達したあとでブートプロセスが失敗したときに Oracle ILOM が実行する処理が設定されます。</p> <ul style="list-style-type: none"> ■ Poweroff (デフォルト) - 許容される最大ブート試行回数に達すると、Oracle ILOM は SPARC サーバーの電源を切断します。 ■ Powercycle - 許容される最大ブート試行回数に達すると、Oracle ILOM は SPARC サーバーの電源を再投入します。 ■ None - 「Boot Fail Recovery」プロパティーが無効になります。 <p>「Boot Fail Recovery」の CLI 構文:</p> <pre>set /HOST bootfailrecovery=off none powercycle</pre>

SPARC ホストブートモードのオーバーライド

Oracle ILOM には、システム管理者が SPARC サーバー上のホストオペレーティングシステムをブートするデフォルトの方法をオーバーライドするために使用できる一連のホストブートモードプロパティが用意されています。

Oracle ILOM のホストブートモードプロパティは、OpenBoot または LDom の破損したブートモード設定を解決することを目的としています。Oracle ILOM で設定したブートモードプロパティは、シングルブートにのみ適用され、ホスト SPARC サーバーの電源がリセットされない場合は 10 分以内に期限切れになります。

システム管理者は、Oracle ILOM の CLI または Web インタフェースを使用してホストブートモードプロパティを設定できます。これらのプロパティの詳細は、次の表を参照してください。

表 62 ホスト SPARC サーバーのホストブートモードプロパティ

ユーザーインタフェースの構成可能なターゲットとユーザーの役割:

- **SP CLI:** /HOST/bootmode
- **SP Web:** 「Host Management」 > 「Host Boot Mode」
- ユーザーの役割: **Reset and Host Control (r)** の役割 (構成可能なホストブートモードプロパティを変更するために必要)。

要件:

- 「Host Boot Mode Settings」 ページでのブートモードプロパティの変更を適用するには、「Save」をクリックする必要があります。

プロパティ	デフォルト値	説明
State (state=)	Normal	<p><i>Normal</i> <i>Reset NVRAM</i></p> <p>SPARC サーバーの電源がリセットされたときに Oracle ILOM が実行する処理を設定します。</p> <ul style="list-style-type: none"> ■ Normal - Oracle ILOM は、現在の NVRAM 変数プロパティを保持します。 ■ Reset NVRAM - Oracle ILOM は、SPARC サーバーの次の電源リセット時にすべての OpenBoot 変数をデフォルトのプロパティ値に戻します。 <p>「Host Boot Mode」の「State」の CLI 構文:</p> <pre>set /HOST/bootmode state=<i>normal reset_nvram</i></pre>

表 62 ホスト SPARC サーバーのホストブートモードプロパティ (続き)

ユーザーインタフェースの構成可能なターゲットとユーザーの役割:

- **SP CLI:** /HOST/bootmode
- **SP Web:** 「Host Management」 > 「Host Boot Mode」
- ユーザーの役割: **Reset and Host Control (r)** の役割 (構成可能なホストブートモードプロパティを変更するために必要)。

要件:

- 「Host Boot Mode Settings」 ページでのブートモードプロパティの変更を適用するには、「Save」をクリックする必要があります。

プロパティ	デフォルト値	説明
Expiration Date (expires=)	値なし (読み取り専用プロパティ)	ブートモードプロパティは、10 分以内または SPARC サーバーの電源がリセットされたとき (どちらか早い方) に期限切れになります。 「LDOM Config」 および 「Script」 プロパティは期限切れにならず、次のサーバーリセット時または手動で値をクリアしたときにクリアされます。 「Host Boot Mode」 の 「State」 の CLI 構文: show /HOST/bootmode
Script (script=)	値なし	最大長は 64 バイトです。 スクリプトは、ホスト SPARC サーバーの OpenBoot PROM ファームウェアのブート方法を制御します。 このスクリプトは、次の場合に読み取られます: (1) 「State」 が 「Reset NVRAM」 に設定され、(2) SPARC サーバーの電源がリセットされ、(3) OpenBoot 変数がデフォルトにリセットされる。 注 - 保守作業員から、問題を解決するためのスクリプトを指定するように指示される場合があります。完全なスクリプトには、主にデバッグ用に用意されている、ドキュメントには記載されていない機能があります。

表 62 ホスト SPARC サーバーのホストブートモードプロパティ (続き)

プロパティ	デフォルト値	説明
LDOM Config (config=)	Factory-default	<p><i>Factory-default</i> <i>Valid LDOM Config</i></p> <p>ホスト SPARC サーバーの電源リセット時に Oracle ILOM が使用する LDOM 構成を設定します:</p> <ul style="list-style-type: none"> Factory-default - 出荷時のデフォルト構成は、プラットフォームが1つのオペレーティングシステムのみをホストする単一のシステムとして表示される初期構成です。 Oracle ILOM で出荷時のデフォルト構成を使用すると、ほかのドメインに割り当てられている可能性があるすべてのシステムリソース (CPU、メモリー、I/O) に再度アクセスできるようになります。「Factory-default」のプロパティ値は、論理ドメインの OS ソフトウェアを使用して出荷時のデフォルトを復元する前に論理ドメインマネージャーを削除した場合に必要なことがあります。 Valid LDOM Config - 有効でアクティブな論理ドメイン構成の名前を入力します。 <p>「Host Boot Mode」の「LDOM Config」の CLI 構文:</p> <pre>set /HOST/bootmode config=factory-default valid_LDOM_configuration</pre>

SPARC ホストドメインの管理

Oracle ILOM には、システム管理者がホスト SPARC サーバーに現在設定されている論理ドメイン構成を表示したり、ホストドメインの自動ブートおよびブートゲストのプロパティを設定したりするために使用できる一連のホストドメインプロパティが用意されています。

Oracle ILOM のホストドメインプロパティは、Oracle ILOM の CLI および Web インタフェースから表示および構成できます。これらのプロパティの詳細は、以降の表を参照してください:

- 表 63
- 表 64

表 63 ホスト SPARC サーバーで検出された論理ドメイン構成の表示

ユーザーインターフェースの構成可能なターゲット:

- **SP CLI:** /HOST/domain/configs
- **Web:** 「Host Management」 > 「Host Domain」

要件:

- ホスト SPARC サーバーのオペレーティングシステム上に論理ドメイン構成を作成する必要があります。論理ドメイン構成を作成する方法については、Oracle VM Server for SPARC のドキュメントを参照してください。
- 論理ドメイン構成を表示するには、show コマンド (show /HOST/domain/configs) を実行します。

プロパティ	説明
Domain Configurations (読み取り専用)	Oracle ILOM には、ホストオペレーティングシステム上で検出された論理ドメイン構成の一覧が表示されます。 Oracle は、検出された論理ドメイン構成を非揮発性メモリーに保存し、変更が発生したときにその一覧を更新します。

表 64 ホスト SPARC サーバーの構成可能なホストドメインプロパティ

ユーザーインターフェースの構成可能なターゲット:

- **SP CLI:** /HOST/domain/control
- **Web:** 「Host Management」 > 「Host Domain」
- ユーザーの役割: **Reset and Host Control (r)** の役割 (構成可能なホストドメインプロパティを変更するために必要)。

要件:

- ホスト SPARC サーバーのオペレーティングシステム上に論理ドメイン構成を作成する必要があります。論理ドメイン構成を作成する方法については、Oracle VM Server for SPARC のドキュメントを参照してください。
- 「Host Domain Settings」 ページでのホストドメインプロパティの変更を適用するには、「Save」をクリックする必要があります。

プロパティ	デフォルト値	説明
Auto-Run (auto-boot=)	Enabled	<i>Enabled Disabled</i> 「Auto-Run」のプロパティを有効にすると、Oracle ILOM は次の電源投入またはリセット後に制御ドメインを自動的にブートします。 「Auto-Run」のプロパティを無効にすると、自動ブートが回避され、次にサーバーの電源が投入またはリセットされたときに OpenBoot の OK プロンプトでホストの制御ドメインが停止します。 「Host Domain」の「Auto-Run」の CLI 構文: set /HOST/domain/control auto-boot=enabled disabled

表 64 ホスト SPARC サーバーの構成可能なホストドメインプロパティ (続き)

プロパティ	デフォルト値	説明
Boot Guests (boot_guests=)	Enabled	<p><i>Enabled Disabled</i></p> <p>「Boot Guests」のプロパティを有効にすると、Oracle ILOM はサーバーの次の電源投入またはリセット時にゲストドメインをブートします。</p> <p>「Boot Guests」のプロパティを無効にすると、構成済みのゲストドメインがサーバーの次の電源投入またはリセット時にブートしません。</p> <p>「Host Domain」の「Boot Guests」の CLI 構文:</p> <pre>set /HOST/domain/control boot_guests=enabled disabled</pre>

SPARC ホストキースイッチ状態の設定

Oracle ILOM には、システム管理者がホスト SPARC サーバーのキースイッチ状態を設定するために使用できる「KeySwitch」プロパティが用意されています。「KeySwitch」プロパティは、Oracle ILOM の CLI または Web インタフェースから構成できます。構成可能な「KeySwitch」プロパティ値の詳細は、次の表を参照してください。

表 65 ホスト SPARC サーバーのキースイッチ状態プロパティ値

ユーザーインタフェースの構成可能なターゲットとユーザーの役割:

- **SP CLI:** /SYS
- **Web:** 「Host Management」 > 「KeySwitch」 > 「KeySwitch」
- ユーザーの役割: Admin (a) の役割 (「KeySwitch」プロパティを変更するために必要)。

要件:

- Web インタフェースでの「KeySwitch」プロパティの変更を適用するには、「Save」をクリックする必要があります。

プロパティ	デフォルト値	説明
Keyswitch (keyswitch_state=)	Normal	<p><i>Normal Standby Diag Locked</i></p> <ul style="list-style-type: none"> ■ Normal - SPARC サーバー自体の電源を入れて、ブートプロセスを開始できます。 ■ Standby - SPARC サーバーの電源を入れることができません。 ■ Diag - SPARC サーバーの電源を入れ、Oracle ILOM のデフォルトのホスト診断プロパティ値を使用して障害カバレッジを表示できます。このオプションを有効にすると、ユーザーが指定した Oracle ILOM の診断プロパティ値がオーバーライドされます。 ■ Locked - SPARC サーバー自体の電源を入れることができませんが、フラッシュデバイスの更新または /HOST send_break_action=break に設定された CLI プロパティ値の変更は許可されません。 <p>「KeySwitch」の CLI 構文:</p> <pre>set /SYS keyswtich_state=normal standby diag locked</pre>

SPARC ホスト TPM 状態の設定

Oracle ILOM には、システム管理者がホスト SPARC サーバー上の Trusted Platform Module (TPM) 機能の状態を管理するために使用できる一連の Oracle Solaris TPM プロパティが用意されています。「TPM」プロパティは、Oracle ILOM の CLI または Web インタフェースから構成できます。構成可能な「TPM」プロパティ値の詳細は、次の表を参照してください。

注 - x86 サーバーの TPM プロパティは BIOS ユーティリティで管理されます。x86 オペレーティングシステムの TPM プロパティおよび要件の詳細は、Oracle x86 サーバーの管理ガイドを参照してください。

表 66 ホスト SPARC サーバーの TPM プロパティ値

ユーザーインターフェースの構成可能なターゲットとユーザーの役割:

- **SP CLI:** /HOST/tpm
- **Web:** 「Host Management」 > 「TPM」 > 「TPM Settings」
- ユーザーの役割: **Reset and Host Control (r)** の役割 (「TPM」プロパティを変更するために必要)。

要件:

- ホスト SPARC サーバーで、TPM をサポートする Oracle Solaris オペレーティングシステムのバージョンが実行されている必要があります。
- Web インタフェースでの「TPM」プロパティの変更を適用するには、「Save」をクリックする必要があります。

プロパティ	デフォルト値	説明
TPM (activate= enable= forceclear=)	Disabled	<p><i>Active Enable Forceclear</i></p> <ul style="list-style-type: none"> ■ Enable (TPM 状態) - TPM 構成の変更を適用するには、Oracle ILOM でこのオプションを有効に (true に設定) する必要があります。 ■ Activate - TPM 構成を有効にするには、Oracle ILOM でこのオプションと「Enable」オプションを有効に (true に設定) する必要があります。 ■ Forceclear - 次回の電源リセット時に TPM 状態を消去するには、このオプションと「Enable」オプションを無効に (false に設定) する必要があります。 <p>「KeySwitch」の CLI 構文:</p> <pre>set /tpm activate=false true enable=false clear forceclear=false enable</pre>

警告通知とイベントログ用の Syslog サーバーの設定

説明	リンク
警告通知の構成、テスト、および無効化については、このセクションを参照してください。	■ 177 ページの「警告通知の構成」
Oracle ILOM イベントをリモートホストに記録するための Syslog サーバーの構成については、このセクションを参照してください。	■ 183 ページの「イベントログ用の Syslog の構成」

関連情報

- 『ユーザーズガイド』の「Oracle ILOM のログエントリの管理」
- 『SNMP、IPMI、CIM、WS-MAN プロトコル管理』の「Oracle ILOM を使用して SNMP トラップ警告を管理する」
- [表 37](#)

警告通知の構成

システム管理者は、発生する可能性があるシステム障害を事前に警告する警告通知を Oracle ILOM で構成できます。Oracle ILOM では、IPMI PET 警告、SNMP トラップ警告、および電子メール警告通知の構成がサポートされています。

Oracle ILOM では、Oracle ILOM CLI、Oracle ILOM Web インタフェース、または SNMP クライアントを使用して、最大 15 個の警告通知を構成できます。システム管理者は、必要に応じて構成済みの各警告通知のテストメッセージを生成し、宛先の受信者がテストメッセージを正常に受信することを確認できます。

Oracle ILOM で警告通知を構成する方法の詳細は、以降のトピックを参照してください:

- [178 ページの「警告通知の構成プロパティ」](#)
- [180 ページの「警告通知の構成とテスト \(IPMI PET、SNMP、または電子メール\)」](#)
- [181 ページの「警告通知の無効化 \(IPMI PET、SNMP、または電子メール\)」](#)

- 182 ページの「電子メール警告用の SMTP クライアントを構成する」

警告通知の構成プロパティ

Oracle ILOM では、それぞれの警告通知にこれら 3 つのプロパティが設定されている必要があります: `alert type`、`alert destination`、および `alert level`。構成されている警告の種類によっては、その他のプロパティを必要に応じて構成できます。

警告通知の構成プロパティの詳細は、次の表を参照してください。

表 67 警告通知の構成プロパティ

プロパティ	要件	説明
Alert Type	必須	<p>「Alert Type」プロパティは、Oracle ILOM が警告メッセージを作成して送信する際に使用するメッセージの形式と配信方法を指定します。</p> <p>選択できる警告の種類は次のとおりです:</p> <ul style="list-style-type: none"> ■ IPMI PET 警告 - 必須プロパティは、警告の宛先 IP アドレスと警告レベルです。指定した警告の宛先は、それぞれ IPMI PET メッセージの受信をサポートしている必要があります。 ■ SNMP トラップ警告 - 必須プロパティは、警告の宛先 IP アドレス、警告の宛先ポート番号、および警告レベルです。指定した宛先は、それぞれ SNMP トラップメッセージの受信をサポートしている必要があります。 ■ 電子メール警告 - 必須プロパティは、宛先の電子メールアドレスと警告レベルです。電子メール警告を有効にする前に、Oracle ILOM で SMTP 電子メールサーバーのプロパティを構成する必要があります。 <p>関連情報:</p> <ul style="list-style-type: none"> ■ 『SNMP、IPMI、CIM、WS-MAN プロトコル管理』の「電子メール通知警告用に SMTP クライアントを構成する (SNMP)」
Alert Destination	必須	<p>「Alert Destination」プロパティは、警告メッセージの送信先を指定します。IPMI PET 警告と SNMP 警告では、IP アドレスの宛先を構成する必要があります。電子メール警告では、電子メールアドレスの宛先を構成する必要があります。</p>
Alert Destination Port	省略可能	<p>TCP/UDP 宛先ポートは、SNMP 警告の構成にのみ適用されます。</p> <p>Oracle ILOM は、標準の TCP/UDP 宛先ポート番号を自動的に選択します。システム管理者は、標準のポート番号 (162) を受け入れるか、手動で TCP/UDP ポート番号を指定するかを必要に応じて選択できます。</p>

表 67 警告通知の構成プロパティ (続き)

プロパティ	要件	説明
Alert Level	必須	<p>すべての警告通知の構成で、警告レベルを設定する必要があります。</p> <p>警告レベルによって、警告通知の送信が有効になります。さらに、IPMI PET 警告および電子メール警告では、警告レベルは、警告の受信者が受信することにもっとも関心のある警告メッセージのみを受信できるようにするフィルタメカニズムとして機能します。</p> <p>Oracle ILOM には次の警告レベルがあり、もっとも低いレベルの警告は「Minor」です:</p> <ul style="list-style-type: none"> ■ Minor - 情報イベント、メジャーイベント、およびクリティカルイベントに関する警告を生成します。 ■ Major - すべての非クリティカル、回復不能、およびクリティカルイベントに関する警告を生成します。 ■ Critical - すべてのクリティカルおよび回復不能イベントに関する警告を生成します。 ■ Disabled - 警告の構成を無効にします。Oracle ILOM は警告メッセージを生成しません。 <p>重要 - Oracle ILOM は、すべての IPMI PET 警告の構成および電子メール警告の構成の警告レベルフィルタリングをサポートしています。Oracle ILOM は、SNMP 警告の構成の警告レベルフィルタリングをサポートしていません。ただし、Oracle ILOM で SNMP 警告を生成できるようにするには、次のいずれかの警告レベルを指定する必要があります: <i>Minor</i>、<i>Major</i>、または <i>Critical</i>。</p>
Email Custom Sender	電子メール警告で省略可能	<p>システム管理者は、電子メール警告の構成でのみ、このプロパティを必要に応じて構成できます。</p> <p><code>email_custom_sender</code> プロパティを使用すると、次のいずれかの文字列を使用して SMTP カスタム送信者アドレスをオーバーライドできます: <code><IPADDRESS></code> または <code><HOSTNAME></code>。</p> <p>例: <code>alert<IPADDRESS></code></p>
Email Message Prefix	電子メール警告で省略可能	<p>システム管理者は、電子メール警告の構成でのみ、このプロパティを必要に応じて構成できます。</p> <p>「Email Message Prefix」プロパティを使用すると、Oracle ILOM でユーザーが指定した情報をメッセージ本文に付加できます。</p>
Event Class Filter	電子メール警告で省略可能	<p>システム管理者は、電子メール警告の構成でのみ、このプロパティを必要に応じて構成できます。</p> <p>「Event Class Filter」プロパティを使用すると、Oracle ILOM で選択したイベントクラスを除くすべての情報を除外できます。フィルタをクリアし、すべてのクラスに関する情報を送信するには、空の二重引用符(″)を入力します。</p>

表 67 警告通知の構成プロパティ (続き)

プロパティ	要件	説明
Event Type Filter	電子メール警告で省略可能	システム管理者は、電子メール警告の構成でのみ、このプロパティを必要に応じて構成できます。 「Event Type Filter」プロパティを使用すると、Oracle ILOM で選択したイベントの種類を除くすべての情報を除外できます。フィルタをクリアし、すべてのイベントの種類に関する情報を送信するには、空の二重引用符 ("") を入力します。
SNMP Version	SNMP 警告で省略可能	システム管理者は、「SNMP Version」プロパティを使用して、送信される SNMP トラップのバージョンを指定できます。サポートされている SNMP バージョンは 1、2c、および 3 です。
SNMP Community Name または User Name	SNMP 警告で省略可能	システム管理者は、SNMPv1 または 2c のコミュニティ文字列、あるいは SNMPv3 のユーザー名を必要に応じて指定できます。 注 - SNMPv3 ユーザー名が構成されている場合は、Oracle ILOM で SNMPv3 ユーザー名を構成する必要があります。SNMP ユーザー名が構成されていない場合は、警告が配信時に認証されません。

▼ 警告通知の構成とテスト (IPMI PET、SNMP、または電子メール)

次の手順は、Oracle ILOM CLI および Web インタフェースを使用して警告通知を構成およびテストする手順を示しています。SNMP アプリケーションクライアントから警告通知を構成およびテストする手順については、を参照してください。

始める前に

- 電子メール警告の構成では、SMTP サーバーを構成する必要があります。SMTP サーバーが構成されていないと、Oracle ILOM は電子メール警告を生成できません。構成の詳細は、182 ページの「電子メール警告用の SMTP クライアントを構成する」を参照してください。
- SNMP 警告の構成では、SNMP セットのプロパティを有効にして、SNMP 用に少なくとも 1 つのユーザーアカウントを構成する必要があります。構成の詳細は、表 37 を参照してください。
- Oracle ILOM で警告通知のプロパティを構成するには、Admin (a) の役割が必要です。

1 15 個の警告構成 ID のいずれかのプロパティを設定するには、次を実行します:

■ Web:

「ILOM Administration」 > 「Notifications」 > 「Alerts」の順にクリックし、「Alert ID」をクリックしてから「Edit」をクリックします。必須プロパティ（レベル、種類、および宛先）を定義して、「Save」をクリックします。

必須プロパティと省略可能なプロパティの詳細は、表 67 を参照してください。

- **CLI:**

必須の警告プロパティを設定するには、次を入力します:

```
set /SP|CMM/alertmgmt/rules/n type=email|snmptrap|ipmipet
destination=ip_address port=required_for_snmptrap level=minor|major|critical|disable
```

必須プロパティと省略可能なプロパティの詳細は、表 67 を参照してください。

2 警告通知の構成をテストするには、次を実行します:

- **Web:**

「ILOM Administration」 > 「Notifications」 > 「Alerts」の順にクリックし、構成された警告 ID をクリックしてから「Test Rule」をクリックします。

成功または失敗のステータスメッセージが表示されます。

- **CLI:**

構成された警告通知をテストするには、次を入力します:

```
set /SP|CMM/alertmgmt/rules/n testalert=true
```

成功または失敗のステータスメッセージが表示されます。

参考 関連情報:

- 表 67
- 182 ページの「電子メール警告用の SMTP クライアントを構成する」
- 表 37
- 『ユーザーズガイド』の「Oracle ILOM のログエントリの管理」
- 『SNMP、IPMI、CIM、WS-MAN プロトコル管理』の「Oracle ILOM を使用して SNMP トラップ警告を管理する」

▼ 警告通知の無効化 (IPMI PET、SNMP、または電子メール)

次の手順は、Oracle ILOM CLI および Web インタフェースを使用して構成済みの警告通知を無効にする手順を示しています。SNMP アプリケーションクライアントから構成済みの警告通知を無効にする手順については、を参照してください。

始める前に

- Oracle ILOM で警告通知のプロパティを変更するには、Admin (a) の役割が必要です。
- 警告通知の構成を無効にするには、次を実行します:
 - **Web:**

「ILOM Administration」 > 「Notifications」 > 「Alerts」の順にクリックし、構成された警告IDをクリックしてから「Edit」をクリックします。「Level」リストボックスで「Disable」をクリックし、「Save」をクリックします。

成功または失敗のステータスメッセージが表示されます。
 - **CLI:**

構成された警告通知を無効にするには、次を入力します:

```
set /SP|CMM/alertmgmt/rules/n level=disable
```

成功または失敗のステータスメッセージが表示されます。

▼ 電子メール警告用のSMTPクライアントを構成する

次の手順は、Oracle ILOM CLI および Web インタフェースを使用して Oracle ILOM を SMTP クライアントとして構成する方法について説明します。電子メール警告通知を正常に送信するには、Oracle ILOM が SMTP クライアントとして動作する必要があります。

始める前に

- Oracle ILOM を SMTP クライアントとして構成する前に、電子メール通知を処理する送信 SMTP 電子メールサーバーの IP アドレスとポート番号を確認してください。
- カスタム送信者の「SMTP Client」プロパティは省略可能です。このプロパティを使用すると、Oracle ILOM で次のいずれかの文字列を使用して SMTP 送信者アドレスをオーバーライドできます: <IPADDRESS> または <HOSTNAME>。例: alert@[IPADDRESS]
- Oracle ILOM で「SMTP Client」プロパティを構成するには、Admin (a) の役割が必要です。
- Oracle ILOM を SMTP クライアントとして構成するには、次を実行します:
 - **Web:**

「ILOM Administration」 > 「Notifications」 > 「SMTP Client」の順にクリックします。

SMTP の状態を有効にし、必須プロパティ (SMTP サーバーの IP アドレスとポート番号) を設定し、必要な場合は省略可能なプロパティ (カスタム送信者) を設定して、「Save」をクリックします。

- **CLI:**

次を入力します:

```
set /SP|CMM/clients/smtp state=enable address=smtp_server_ip
port=smtp_server_port custom_send=optional_string
```

参考 関連情報:

- 180 ページの「警告通知の構成とテスト (IPMI PET、SNMP、または電子メール)」

イベントログ用の Syslog の構成

Syslog は、リモートログホストにイベントを記録するために使用されるプロトコルサービスです。システム管理者は、Oracle ILOM で Syslog サーバーの IP アドレスを構成して、Syslog サービスを有効にすることができます。

Syslog サーバーに記録されるイベントには、クラス、種類、重要度、説明など、ローカル Oracle ILOM イベントログに表示される情報と同じものがすべて含まれています。Oracle ILOM には、最大 2 つの Syslog サーバーを構成するためのプロパティが用意されています。

▼ イベントログ用の Syslog IP アドレスの構成

始める前に

- Oracle ILOM で Syslog のプロパティを変更するには、Admin (a) の役割が必要です。
- 2 つの Syslog プロパティのいずれかの IP アドレスを設定するには、次を実行します:

- **Web:**

「ILOM Administration」 > 「Notifications」 > 「Syslog」の順にクリックします。

「Server 1」または「Server 2」テキストボックスに Syslog サーバーの IP アドレスを入力して「Save」をクリックします。

- **CLI:**

次を入力します:

```
set /SP|CMM/clients/syslog destination_ip=syslog_server_ip
```

参考 関連情報:

- 『ユーザーズガイド』の「Oracle ILOM のログエントリの管理」

システム管理ポリシー構成の設定

説明	リンク
サーバー SP から構成できるシステム管理ポリシーの説明については、このセクションを参照してください。	■ 185 ページの「サーバー SP から構成できるシステム管理ポリシー」
CMM から構成できるシステム管理ポリシーの説明については、このセクションを参照してください。	■ 187 ページの「CMM から構成できるシステム管理ポリシー」

関連情報

- [191 ページの「電源警告通知の設定とシステムの電力使用の管理」](#)

サーバー SP から構成できるシステム管理ポリシー

システム管理者は、必要に応じて、サーバー SP からシステム管理ポリシーを設定し、ブート時の電源投入ポリシーと電源切断ポリシー、およびシステムコンポーネントの冷却ポリシーを制御できます。

デフォルトでは、すべてのシステム管理ポリシーは、Oracle ILOM SP で無効にされています。サーバー SP から構成できるシステム管理ポリシーのプロパティの説明については、次の表を参照してください。

表 68 サーバー SP のシステム管理ポリシー

ユーザーインターフェースの構成可能なターゲットとユーザーの役割:	
<ul style="list-style-type: none"> ■ CLI: <code>/SP/policy</code> ■ Web: 「System Management」 > 「Policy」 > 「Policy Configuration」 ■ ユーザーの役割: <code>admin (a)</code> (すべてのプロパティ変更が必要) 	
システム管理ポリシー	説明
Auto-Power-On Host on Boot (HOST_AUTO_POWER_ON=)	<p><i>Disabled</i> (デフォルト) <i>Enabled</i></p> <p>ブート時にホストサーバーのオペレーティングシステムの電源を自動的に入れる場合は、このポリシーを有効にします。</p> <p>注 - このポリシーを有効にすると、「Set host power to last power state policy」のポリシーが自動的に無効になります (有効にされていた場合)。</p> <p>「Auto-Power-On-Host on Boot」の CLI 構文</p> <p>Set /SP/policy HOST_AUTO_POWER_ON=<i>enabled disabled</i></p>
Set Host to Last Power State on Boot (HOST_LAST_POWER_STATE=)	<p><i>Disabled</i> (デフォルト) <i>Enabled</i></p> <p>ブート時に、ホストサーバーの電源状態を最後に認識された状態に設定するには、このポリシーを有効にします。</p> <p>注 - このポリシーを有効にすると、「Auto power-on host policy」のポリシーが自動的に無効になります (有効にされていた場合)。</p> <p>「Set Host to Last Power State on Boot」の CLI 構文</p> <p>Set /SP/policy HOST_LAST_POWER_STATE=<i>enabled disabled</i></p>
Set to Delay Host Power On (SPARC サーバーのみ) (HOST_AUTO_POWER_ON=)	<p><i>Disabled</i> (デフォルト) <i>Enabled</i></p> <p>ブート時に、ホストオペレーティングシステムの電源投入を遅延するには、Oracle SPARC サーバーでこのポリシーを有効にします。</p> <p>「Set to Delay Host Power On」の CLI 構文</p> <p>Set /SP/policy HOST_AUTO_POWER_ON=<i>enabled disabled</i></p>

表 68 サーバー SP のシステム管理ポリシー (続き)

システム管理ポリシー	説明
ユーザーインタフェースの構成可能なターゲットとユーザーの役割: <ul style="list-style-type: none"> ■ CLI: <code>/SP/policy</code> ■ Web: 「System Management」 > 「Policy」 > 「Policy Configuration」 ■ ユーザーの役割: <code>admin (a)</code> (すべてのプロパティ変更に必要な) 	
Set Enhanced PCIe Cooling Mode (x86 サーバーのみ) (ENHANCED_PCIE_COOLING_MODE=)	<p><i>Disabled</i> (デフォルト) <i>Enabled</i></p> <p>特定の x86 サーバーの PCIe カードで要求される低い動作温度に適合するようにするには、Oracle x86 サーバーでこのポリシーを有効にします。</p> <p>PCIe クールダウンポリシーモードを有効にすると、シャーシの出力温度センサーのしきい値を低くするように、Oracle ILOM に指示されます。このしきい値は、要求された温度範囲内で PCIe カードが動作するように、シャーシのファンアルゴリズムで使用されません。</p> <p>「Set Enhanced PCIe Cooling Mode」の CLI 構文</p> <pre>Set /SP/policy ENHANCED_PCIE_COOLING_MODE=enabled disabled</pre>
Enable a Cooldown Period Before Host Shuts Down (HOST_AUTO_POWER_ON=)	<p><i>Disabled</i> (デフォルト) <i>Enabled</i></p> <p>ホストサーバーの電源切断時にクールダウンモードに入るようにするには、SPARC サーバーでこのプロパティを有効にします。クールダウンモードでは、ユーザーに危険を及ぼさないために、特定のコンポーネントが最低温度より低い状態であることを監視するように、Oracle ILOM に指示されます。サーバーのサブコンポーネントが最低温度より低くなると、サーバーの電源が切断されるか、処理が完了するまでに 4 分を超えた場合は、ホストの電源が切断されます。</p> <p>「Enable a Cooldown Period Before Host Shuts Down」の CLI 構文</p> <pre>Set /SP/policy HOST_AUTO_POWER_ON=enabled disabled</pre>

CMM から構成できるシステム管理ポリシー

システム管理者は、必要に応じて、CMM からシステム管理ポリシーを設定して、シャーシの電源の需要、電源装置のファン速度、ストレージブレード SAS-2 の機能、およびシャーシの電源を管理できます。

CMM から構成できるシステム管理ポリシーのプロパティの説明については、次の表を参照してください。

表 69 CMM のサーバー管理ポリシー

システム管理ポリシー	デフォルト値	説明
ユーザーインターフェースの構成可能なターゲットとユーザーの役割: ■ CLI: /CMM/policy - または - /CH/BLn/SP/policy ■ Web: 「System Management」 > 「Policy」 > 「Policy Configuration」 ■ ユーザーの役割: admin (a) (すべてのプロパティ変更が必要)		
Light Load Efficiency Mode (LIGHT_LOAD_EFFICIENCY_MODE=)	Disabled	<i>Disabled Enabled</i> 効率を向上させるために、シャードシステムの電源使用を監視して、電源ユニット (PSU) の各サイドを自動的にシャットダウンするには、このポリシーを有効にします。 「Light Load Efficiency Mode」の CLI 構文 Set /CMM/policy LIGHT_LOAD_EFFICIENCY_MODE=enabled disabled
Monitor Power Supply 0 Side 0 for power (MONITOR_PS0_SIDE0=)	Enabled	<i>Disabled Enabled</i> 「Light Load Efficiency Mode」で電源装置 0 サイド 0 の監視を有効にするには、このポリシーを有効にします。 「Monitor Power Supply 0 Side 0」の CLI 構文 Set /CMM/policy MONITOR_PS0_SIDE0=enabled disabled
Monitor Power Supply 0 Side 1 for power (MONITOR_PS0_SIDE1=)	Enabled	<i>Disabled Enabled</i> 「Light Load Efficiency Mode」で電源装置 0 サイド 1 の監視を有効にするには、このポリシーを有効にします。 「Monitor Power Supply 0 Side 1」の CLI 構文 Set /CMM/policy MONITOR_PS0_SIDE1=enabled disabled
Monitor Power Supply 1 Side 0 for power (MONITOR_PS1_SIDE0=)	Enabled	<i>Disabled Enabled</i> 「Light Load Efficiency Mode」で電源装置 1 サイド 0 の監視を有効にするには、このポリシーを有効にします。 「Monitor Power Supply 1 Side 0」の CLI 構文 Set /CMM/policy MONITOR_PS1_SIDE0=enabled disabled
Monitor Power Supply 1 Side 1 for power (MONITOR_PS1_SIDE1=)	Enabled	<i>Disabled Enabled</i> 「Light Load Efficiency Mode」で電源装置 1 サイド 1 の監視を有効にするには、このポリシーを有効にします。 「Monitor Power Supply 1 Side 1」の CLI 構文 Set /CMM/policy MONITOR_PS1_SIDE1=enabled disabled

表 69 CMM のサーバー管理ポリシー (続き)

システム管理ポリシー	デフォルト値	説明
ユーザーインターフェースの構成可能なターゲットとユーザーの役割: ■ CLI: /CMM/policy-または-/CH/BLn/SP/policy ■ Web: 「System Management」 > 「Policy」 > 「Policy Configuration」 ■ ユーザーの役割: admin (a) (すべてのプロパティ変更に必要)		
Sun Cooling Door Installed (COOLING_DOOR_INSTALLED=)	Disabled	Disabled Enabled Sun Blade 6048 シャーシに取り付けられている冷却ドアをサポートするには、このポリシーを有効にします。 「Cooling Door Installed」の CLI 構文 Set /CMM/policy COOLING_DOOR_INSTALLED=enabled disabled
Force Power Supply Fans to High Speed (PS_FANS_HIGH=)	Disabled	Disabled Enabled 電源装置のファンが100%の出力で動作するように強制するには、このポリシーを有効にします。 「Force Power Supply Fans to High Speed」の CLI 構文 Set /CMM/policy PS_FANS_HIGH=enabled disabled
Force Power Supply Fans to Low Speed (PS_FANS_LOW=)	Disabled	Disabled Enabled 電源装置のファンが80%の出力で動作するように強制するには、このポリシーを有効にします。 「Force Power Supply Fans to Low Speed」の CLI 構文 Set /CMM/policy PS_FANS_LOW=enabled disabled
Force server blade to be SAS2 Capable at 3Gbps (BLn_FORCE_SAS2_3GBPS= disabled)	Disabled	Disabled Enabled このアクションが必要となる例外的な場合に、NEMがSASリンクを遅いレートで実行するように強制するには、このポリシーを有効にします。 「Force Server Blade to be SAS2 Capable at 3Gbps」の CLI 構文 Set /CH/BLn/SP/policy PS_FANS_LOW=enabled disabled
Manage chassis power.Warning: Disabling may lead to chassis shutdown (POWER_MANAGEMENT=)	Enabled	Disabled Enabled シャーシに取り付けられる新しいサーバーモジュールの電源を入れた場合に、シャーシに十分な電源があるかどうかを判別するには、このポリシーを有効にします。 「Manage Chassis Power.Warning: Disabling May Lead to Chassis Shutdown」の CLI 構文 Set /CMM/policy POWER_MANAGEMENT=enabled disabled

電源警告通知の設定とシステムの電力使用の管理

説明	リンク
消費電力警告通知に関する CMM および SP の構成可能なプロパティの説明は、このセクションを参照してください。	<ul style="list-style-type: none">■ 191 ページの「消費電力警告通知の設定」
システムの電力使用の管理に対する CMM および SP の構成可能なプロパティの説明は、これらのセクションを参照してください。	<ul style="list-style-type: none">■ 192 ページの「SP 電力制限および CMM 電力許可プロパティの設定」■ 195 ページの「電力制限を実施するための SP 詳細電力上限ポリシーの設定」■ 197 ページの「CMM 電源装置冗長性ポリシーの設定」

関連情報

- 『ユーザーズガイド』の「Oracle ILOM インタフェースを介したリアルタイム電力監視」
- 『SNMP、IPMI、CIM、WS-MAN プロトコル管理』の「SPARC 診断、POST、およびブートモードの操作の管理 (SNMP)」
- [177 ページの「警告通知とイベントログ用の Syslog サーバーの設定」](#)

消費電力警告通知の設定

Oracle ILOM には、2つの消費電力通知に対する構成プロパティがあります。有効にすると、システムの電力が設定されているしきい値を超えた場合に、構成されている電子メール受信者が警告通知を受信します。

消費電力のしきい値および電子メール警告通知は、Oracle ILOM の CLI または Web インタフェースから構成できます。

電子メール警告通知の構成の詳細は、[177 ページの「警告通知の構成」](#)を参照してください。

電力通知しきい値に対する構成プロパティの詳細は、次の表を参照してください。

表 70 消費電力通知しきい値の構成プロパティ

プロパティ	デフォルト値	説明
Notification Threshold 1 および 2 (threshold1= <i>n</i> threshold2= <i>n</i>)	Disabled	<p><i>Disabled</i> <i>Enabled</i></p> <ul style="list-style-type: none"> Disabled - 無効の場合、Notification Threshold プロパティの状態およびワット数プロパティの値 (0) は無効になります。 Enabled - 有効の場合、Notification Threshold プロパティの状態およびユーザー指定のワット数プロパティの値を構成できます。ワット数のしきい値は 1 - 65535 の間で指定してください。システムの電力が設定されたしきい値を超えると Oracle ILOM が警告イベントを生成します。電子メール警告の受信者が構成されている場合は、Oracle ILOM は構成されている受信者への消費電力の電子メール警告も生成します。 <p>消費電力通知しきい値の CLI 構文</p> <pre>set /SP/CMM/powermgmt threshold1=<0 - 65535> threshold2=<0 - 65535></pre> <p>関連情報:</p> <ul style="list-style-type: none"> 177 ページの「警告通知の構成」

SP 電力制限および CMM 電力許可プロパティの設定

Oracle ILOM には、管理対象システムの電力使用を制限および許可するための、SP および CMM の構成可能なプロパティがあります。これらの電力制限および電力許可のプロパティは、Oracle ILOM CLI およびファームウェアバージョン 3.1.1 以降の Web インタフェースから構成できます。

電力制限および電力許可に対して Oracle ILOM で構成可能なプロパティの詳細については、次のトピックを参照してください:

- 193 ページの「SP の「Power Target Limit」プロパティを設定する」
- 194 ページの「CMM の「Blade Slot Grant Limit」プロパティを設定する」

▼ SP の「Power Target Limit」プロパティを設定する

始める前に

- 管理対象のサーバーに Oracle ILOM SP ファームウェアバージョン 3.1.2 以降がインストールされている必要があります。
- Oracle ILOM で「Power Limit」プロパティを変更するには Admin (a) の役割が必要です。
- 「Power Target Limit」は、有効の場合、管理対象のサーバーに許容する消費電力の量を制御します。

この手順では、Web および CLI SP の両方の手順について説明します。

- SP の「Power Target Limit」プロパティを有効にするには、次の Oracle ILOM インタフェースの手順のいずれかを実行します:

Oracle ILOM インタフェース	「Power Target Limit」の設定手順
Web	<ul style="list-style-type: none"> a. 「Power Management」 > 「Power Limit」の順にクリックします。 b. 制限目標値をワット数またはパーセントで入力します。 制限目標は、取り付けられているハードウェアコンポーネントによって取り込まれる最小電力と管理対象のサーバーが許容されている最大消費電力 (許容ピーク) の間に設定するようにしてください。 c. 「Power Limiting」のアクティブ化状態を有効にします。 Oracle ILOM で電力制限目標の構成をアクティブ化するには、「Power Limiting」の状態が有効になっている必要があります。 d. 「Save」をクリックして変更を適用します。
CLI	<ul style="list-style-type: none"> ■ 次を入力します: set /SP/powermgmt/budget pending_power_limit=value pendingactivation_state=enabled commit_pending=true ここでは、<i>value</i> はワット数の制限目標値またはパーセントの制限目標値です。制限目標は、取り付けられているハードウェアコンポーネントによって取り込まれる最小電力と管理対象のサーバーが許容されている最大消費電力 (許容ピーク) の間に設定するようにしてください。

参考 関連情報

- 『ユーザーズガイド』の「電力割り当ての監視」
- [195 ページの「電力制限を実施するための SP 詳細電力上限ポリシーの設定」](#)

▼ CMM の「Blade Slot Grant Limit」プロパティを設定する

始める前に

- Oracle ILOM CMM ファームウェアバージョン 3.1.1 以降が必要です。
- Oracle ILOM で「Blade Slot Grant Limit」プロパティを変更するには Admin (a) の役割が必要です。
- 「Blade Slot Grant Limit」プロパティは、CMM が CPU ブレードサーバーに許容する消費電力の量を制御します。デフォルトでは、「Blade Slot Grant Limit」は 1200 ワットに設定されています (最大ブレードスロット電力制限)。

システム管理者は、デフォルトのブレードスロット許可制限 (1200 ワット) を受け入れるか変更するかを選択できます。ただし、許可制限のプロパティは CMM によってすでに許可されているブレードスロットの電力 (ワット数、許可電力) よりも少なく設定してはいけません。「Blade Slot Grant Limit」を 0 に設定すると、取り付けられている CPU ブレードサーバーの電源を投入できなくなります。

注 - 「Blade Slot Grant Limit」は取り付けられているストレージブレードサーバーからは無視されます。ストレージブレードサーバーには自動的に送電されます。

この手順では、Web および CLI CMM の両方の手順について説明します。

- CMM の「Blade Slot Grant Limit」プロパティを設定するには、次の Oracle ILOM インタフェースの手順のいずれかを実行します:

Oracle ILOM インタフェース

CMM の「Blade Slot Grant Limit」の設定手順

Web

- a. 「Power Management」 > 「Allocation」の順にクリックします。
- b. 「Power Grants」テーブルで、CPU ブレードサーバーの横のラジオボタンをクリックし、「Edit」をクリックします。
注。ストレージブレードサーバーはテーブル内に「Ignored Auto-Powered blade」として表示されません。「Blade Slot Grant Limit」プロパティはストレージブレードサーバーには無視されます。
- c. 「Edit」ダイアログで、次のいずれかの「Blade Slot Grant Limit」オプションを有効にします:
Slot Maximum (デフォルトは **1200** ワット)-有効にすると、CMM はリクエスト元の CPU ブレードサーバーに対して最大 1200 ワットの電力を許可できます。
または
Custom -有効にする場合は、CMM がリクエスト元の CPU ブレードサーバーに許可できる許容電力のワット数を入力します。電力のワット数は、CMM によってすでに許可されているブレードスロットへの電力のワット数 (許可電力) よりも少なくしてはいけません。電力のワット数を 0 に設定すると、取り付けられている CPU ブレードサーバーの電源を投入できなくなります。
- d. 「Save」をクリックして変更を適用します。

CLI

- 次を入力します:
`set /CMM/powermgmt/powerconf/bladeslots/BLn grant_limit=watts`
ここでは:
n - 取り付けられている CPU ブレードサーバーのブレードスロット番号を入力します。
watts - CMM がリクエスト元の CPU ブレードサーバーに許可できる許容電力のワット数を入力します。電力のワット数は、CMM によってすでに許可されているブレードスロットへの電力のワット数 (許可電力) よりも少なくしてはいけません。電力のワット数を 0 に設定すると、取り付けられている CPU ブレードサーバーの電源を投入できなくなります。

参考 関連情報

- 『ユーザーズガイド』の「消費電力の用語とプロパティ」
- 『ユーザーズガイド』の「電力割り当ての監視」
- シャーシ電力管理の CMM ポリシー、[187 ページの「CMM から構成できるシステム管理ポリシー」](#)

電力制限を実施するための SP 詳細電力上限ポリシーの設定

Oracle ILOM には、システムの電力制限を実施するための SP 電力上限ポリシーのプロパティがあります。これらの電力上限ポリシーのプロパティは、Oracle ILOM CLI およびファームウェアバージョン 3.1.1 以降の Web インタフェースから構成できます。

Oracle ILOM の電力上限ポリシープロパティの構成についての詳細は、次の手順を参照してください。

▼ 詳細電力上限ポリシーを設定する

始める前に

- Oracle ILOM SP ファームウェアバージョン 3.1.2 以降が必要です。
- Oracle ILOM で詳細電力ポリシープロパティを変更するには Admin (a) の役割が必要です。
- 詳細電力上限ポリシーを使用すると、システム管理者は猶予期間および違反動作を伴うソフト上限を設定したり、許容ピーク消費電力を電力制限目標内に抑えるハード上限を設定したりできるため、システムの電力制限目標の実施に役立ちます。

この手順では、Web および CLI SP の両方の手順について説明します。

- SP 電力上限ポリシーを設定するには、次の Oracle ILOM インタフェースの手順のいずれかを実行します：

Oracle ILOM インタフェース

詳細電力上限ポリシーの設定手順

Web

- a. 「Power Management」 > 「Power Limit」の順にクリックします。
 - b. 次のいずれかの詳細電力上限ポリシーオプションを有効にします：
Soft Cap (デフォルト) - 有効にすると、システム消費電力 (実際の電力) が電力制限目標およびユーザー構成可能な猶予期間 (デフォルトは 10 秒) を超えた場合にのみシステムの電力が制限されます。
システム管理者は、デフォルトの 10 秒の猶予期間を受け入れるか、「Custom」をクリックして許容される猶予期間の秒数 (0 - 99999) を入力し、デフォルトの猶予期間を変更するかを選択できます。
または
Hard Cap - 有効にすると、許容ピーク電力を電力制限目標内に抑えるようにシステムの消費電力が制限されます。
 - c. 次のいずれかのポリシー違反動作を有効にします：
None (デフォルト) - 有効にすると、システムの消費電力が電力ポリシーに違反しても動作は行われません。
または
Hard Power Off - 有効にすると、システムの消費電力が電力ポリシーに違反した場合すぐにシステムの電源が切断されます。
 - d. 「Save」をクリックして変更を適用します。
-

Oracle ILOM イン
タフェース

詳細電力上限ポリシーの設定手順

CLI

- a. 詳細電力上限ポリシーを設定するには、次を入力します:

```
set /SP/powermgmt policy=performance|elastic|none
```

ここでは:

performance (Web の「Soft Cap」と同じ、デフォルト) - 設定すると、システムの消費電力 (実際の電力) が電力制限目標およびユーザー構成可能な `timelimit` プロパティ (デフォルトは 10 秒) を超えた場合にのみシステム電力が制限されます。

または

elastic (Web の「Hard Cap」と同じ) - 設定すると、許容ピーク電力を電力制限目標内に抑えるようにシステムの消費電力が制限されます。

none - 設定すると、Oracle ILOM の電力ポリシーが無効になります。

- b. 電力ポリシーに「Performance」プロパティを設定した場合の `timelimit` および `violation_actions` を設定するには、次を入力します:

```
set /SP/powermgmt/budget pendingtimelimit=seconds pendingviolation_actions=none|hardpoweroff  
commit_pending=true
```

ここでは:

seconds - 猶予期間として許容される秒数 (0 - 99999) を入力します (デフォルトは 10 秒)。

none|hardpoweroff - 電力ポリシーに違反してもシステムによる動作を行わないようにするには、`none` と入力します。システムの消費電力が電力ポリシーに違反した場合すぐにシステムの電源を切断するには、`hardpoweroff` と入力します。

参考 関連情報

- 『ユーザーズガイド』の「消費電力の用語とプロパティ」
- 『ユーザーズガイド』の「電力割り当ての監視」
- シャーシ電力管理の CMM ポリシー、187 ページの「CMM から構成できるシステム管理ポリシー」

CMM 電源装置冗長性ポリシーの設定

Oracle ILOM には、ブレードシステムシャーシコンポーネントへの電力損失を防ぐための CMM 電源装置冗長性ポリシーがあります。電源装置冗長性ポリシーは、Oracle ILOM の CMM CLI および Web インタフェースから構成できます。

Oracle ILOM CMM からブレードシステムシャーシの電源装置冗長性ポリシーを構成する場合の詳細は、次の手順を参照してください。

▼ CMM 電源装置冗長性ポリシーを設定する

始める前に

- Oracle ILOM CMM ファームウェアバージョン 3.1.1 以降が必要です。

- 電源装置冗長性ポリシーをサポートするには、ブレードシステムシャーシ内に少なくとも2台の電源ユニット (PSU) が最初に取り付けられている必要があります。

注 - Sun Blade 6000 PSU には2つの電源サイドがあります。Sun Blade 6048 PSU には3つの電源サイドがあります。システム管理者は、システム管理ポリシーの軽負荷効率モード (LLEM) を有効にすることで一方の PSU の電源を切断できます。LLEM は、冗長 PSU と非冗長 PSU の両方をサポートしています。

- Oracle ILOM で CMM 許可制限のプロパティを変更するには Admin (a) の役割が必要です。
- 電源装置冗長性ポリシーは、PSU の障害に備えて CMM が各 PSU から蓄えておく電力量を制御します。Oracle ILOM のデフォルトでは、CMM 電源装置ポリシーは各 PSU から半分の電力 (N+N) を蓄えておくよう設定されています。ブレードシャーシ内で PSU に障害が発生した場合、CMM はシャーシシステムコンポーネントへの電力損失を防ぐために残りの PSU から蓄えられた電力を割り当てます。システム管理者は、デフォルトの電源装置冗長性ポリシー (N+N) を受け入れるか無効にするかを選択できます。

注 - PSU の冗長性ポリシーが変更された場合、この変更は CMM が CPU ブレードサーバーに割り当てることができる電力のワット数に影響します。たとえば、冗長性ポリシーが有効の場合 (N+N)、CMM は許容ピーク電力を PSU が提供できるワット数から蓄えておく分を引いたワット数に再調整します。冗長性ポリシーが無効の場合に PSU に障害が発生すると、CMM は許容ピークシステム電力のワット数を削減します。許容ピークシステムワット数が削減されてすでに割り当てられている電力のワット数を下回った場合、システム管理者はシャーシ電力の割り当てを削減するために CPU ブレードサーバーの電源を切断する手順を実行するようにしてください。

この手順では、Web および CLI CMM の両方の手順について説明します。

- **CMM 電源装置冗長性ポリシーを設定するには、次のいずれかの Oracle ILOM インタフェースの手順を実行します:**

Oracle ILOM インタフェース	CMM PSU 冗長性ポリシーの設定手順
---------------------	----------------------

Web	<ol style="list-style-type: none">「Power Management」 > 「Redundancy」の順にクリックします。次のいずれかの電源冗長性ポリシーを有効にします: N+N (デフォルト) - 有効にすると、CMM が各シャーシ PSU から電源冗長性のために電力の半分を蓄えておきます。 または None - 有効にすると、冗長 PSU のポリシー構成は無効になります。「Save」をクリックして変更を適用します。
-----	---

CLI	<ul style="list-style-type: none">■ 次を入力します: <code>set /CMM/powermgmt redundancy=redundancy none</code> ここでは: redundancy (デフォルト) - 設定すると、CMM が各シャーシ PSU から電源冗長性のために電力の半分を蓄えておきます。 none - 設定すると、冗長 PSU のポリシー構成は無効になります。
-----	--

参考 関連情報

- CMM 電源装置のファン速度を調整する、187 ページの「CMM から構成できるシステム管理ポリシー」
- シャーシ電力管理の CMM ポリシー、187 ページの「CMM から構成できるシステム管理ポリシー」

Oracle ILOM の保守および構成管理タスクの実行

説明	リンク
アップグレード可能なシステムデバイスのファームウェア更新の実行については、このセクションを参照してください。	■ 201 ページの「ファームウェア更新の実行」
SP、CMM、またはブレードシャーシコンポーネントの電源のリセットについては、このセクションを参照してください。	■ 210 ページの「サービスマニモジュールまたはシャーシ監視モジュールの電源のリセット」
SP または CMM の Oracle ILOM 構成をバックアップ、復元、またはリセットする手順については、このセクションを参照してください。	■ 211 ページの「Oracle ILOM 構成のバックアップ、復元、またはリセット」

関連情報

- 『ユーザーズガイド』の「スナップショットを作成する: Oracle ILOM SP の状態」

ファームウェア更新の実行

ユーザーが Oracle ILOM の最新機能と製品拡張にアクセスできるようにするため、アップグレード可能なすべてのシステムデバイスを最新の Oracle ILOM ファームウェアリリースで更新するようにしてください。

システム管理者は、Oracle ILOM の Web インタフェースまたは CLI を使用して、アップグレード可能な任意のシステムデバイスのファームウェアを更新できます。

Oracle ILOM のファームウェア更新の詳細は、これらのトピックを参照してください:

- [202 ページの「ファームウェアをアップグレードできるデバイス」](#)
- [202 ページの「Oracle ILOM 構成の保持」](#)
- [202 ページの「ファームウェア更新を開始する前に」](#)
- [203 ページの「サーバー SP または CMM のファームウェアイメージを更新する」](#)
- [207 ページの「ブレードシャーシコンポーネントのファームウェアイメージを更新する」](#)

- 210 ページの「ファームウェア更新時のネットワーク障害から回復する」

ファームウェアをアップグレードできるデバイス

次の Oracle ILOM 管理対象デバイスのファームウェアイメージを Oracle 製品ダウンロード Web サイトから入手できます:

- サービスプロセッサ (SP) を含むラック搭載型またはブレードサーバー (x86 および SPARC)
- ブレードシステムのシャーシ監視モジュール (CMM)
- サービスプロセッサを含むブレードシステムシャーシネットワーク拡張モジュール (NEM)
- ブレードシステムシャーシのストレージブレードサーバー

ファームウェアのダウンロード手順については、[8 ページ](#)の「製品のソフトウェアおよびファームウェアのダウンロード」を参照してください。

Oracle ILOM 構成の保持

新しいファームウェアリリースに更新するときに、「Preserve Configuration」オプションが有効になっていると、既存の Oracle ILOM 構成が保存され、ファームウェア更新の完了後にユーザー定義の構成設定が復元されます。しかし、「Preserve Configuration」オプションが有効になっていない場合は、ファームウェア更新プロセスの完了時に Oracle ILOM 構成設定 (ネットワーク設定を含む) が出荷時のデフォルト値にリセットされます。

注- 構成という用語は、Oracle ILOM でユーザーによって構成された設定を指します。これらの設定には、ユーザーアカウント設定、SP ネットワーク設定、管理アクセス設定、警告構成設定、リモート管理構成などがあります。

以前のファームウェアリリースに更新する場合、Oracle ILOM がそのリリース用に保持されている構成を検出すると、「Preserve Configuration」オプションが有効であれば、更新プロセスの完了後に以前のリリースの構成に戻ります。

一般に、システムのファームウェアは以前のリリースに更新しないでください。ただし、システム上で以前のバージョンのファームウェアを実行する必要があると判断される場合は、ダウンロード可能な以前の任意のファームウェアリリースにファームウェアを更新できます。

ファームウェア更新を開始する前に

Oracle ILOM ファームウェアを更新する前に、次を実行すべきです:

1. 管理対象のサーバー SP または CMM がネットワークに接続され、ファームウェアイメージを更新できることを確認します。
たとえば、サーバー SP または CMM がネットワークに接続されていることを確認するには、リモート Web ブラウザクライアントまたはリモート CLI ssh クライアントを使用して、サーバー SP または CMM にログインします。手順については、[30 ページの「Oracle ILOM SP または CMM へのログイン」](#)を参照してください。
2. 管理対象デバイス (サーバー SP、ストレージサーバー、NEM SP、または CMM) で実行されている Oracle ILOM ファームウェアのバージョンを識別します。
すべてのアップグレード可能なデバイスのファームウェアバージョンは、Web インタフェースの「Firmware」ページまたは /System/Firmware CLI ターゲットに表示されます。
3. アップグレード可能なデバイスのファームウェアイメージを Oracle 製品ダウンロード Web サイトからダウンロードし、そのイメージをローカルまたはネットワーク共有上、あるいは TFTP、FTP、HTTP、または HTTPS サーバー上に配置します。
ファームウェアのダウンロード手順については、[8 ページの「製品のソフトウェアおよびファームウェアのダウンロード」](#)を参照してください。
4. Admin (a) の役割のアカウント権限を持つ Oracle ILOM ユーザー名とパスワードを取得します。ファームウェアイメージを更新するには、Admin (a) 権限が必要です。
5. SP または CMM のユーザーにファームウェア更新のスケジュールを通知し、ファームウェア更新が完了するまですべてのクライアントセッションを閉じるように求めます。
システム管理者は、バナーメッセージを使用してこのメッセージをユーザーに伝えることができます。ログイン時のバナーメッセージを作成して有効にする手順については、[表 42](#)を参照してください。
6. ホストサーバーのプラットフォームで必要な場合は、SP のファームウェアイメージを更新する前にホストオペレーティングシステムの電源を切断します。
ホストサーバーの電源が入っていて、プラットフォームサーバーの電源を切断する必要がある場合は、「Summary」Web ページの「Actions」パネルのボタンをクリックして、ホストオペレーティングシステムおよびサーバーの電源を正常に切断します。または、CLI で次のコマンドを実行して、ホストオペレーティングシステムおよびサーバーの電源を正常に切断することもできます: **stop /System**

▼ サーバー SP または CMM のファームウェアイメージを更新する

システム管理者は、アップグレード可能なデバイスのファームウェア更新プロセスを、Web インタフェースの「Actions」パネル、「Maintenance」の「Firmware Upgrade」ページ、または CLI ターゲットから開始できます。

次の手順では、CLI および Web インタフェースの「Maintenance」ページを使用したファームウェア更新プロセスについて説明します。

始める前に

- SP または CMM のファームウェアイメージを更新するための初期要件が満たされていることを確認してください。202 ページの「[ファームウェア更新を開始する前に](#)」を参照してください。
- ファームウェア更新処理の完了には、数分かかります。この間、ほかの Oracle ILOM タスクを実行しないでください。ファームウェア更新プロセスが完了すると、システムがリブートします。

ファームウェア更新プロセスを開始し、更新プロセスが正常に完了したことを確認するには、これらの手順に従います:

- 1 サーバー SP または CMM イメージのファームウェア更新プロセスを開始するには、いずれかの **Oracle ILOM** インタフェースを使用して次の手順を実行します:

Oracle ILOM インタフェース	SP または CMM のファームウェア更新手順を開始して実行するには
Web	<p>a. 「Maintenance」 > 「Firmware Upgrade」の順にクリックします。</p> <p>b. 「Enter Firmware Upgrade Mode」ボタンをクリックし、アップグレード確認ダイアログボックスで「OK」をクリックして処理を続行します。 「Firmware Upgrade」ページにファームウェアイメージをアップロードするためのプロパティが表示されます。 注 - Oracle 製品ダウンロード Web サイトからファームウェアイメージをダウンロードしていない場合は、これらの手順を参照して、更新されたイメージをダウンロードしてください。 8 ページの「製品のソフトウェアおよびファームウェアのダウンロード」。</p> <p>c. 「Firmware Upgrade」ページで、次のいずれかの操作を実行します: 「Browse」をクリックしてアップロードするファームウェアイメージを指定し、「Upload」ボタンをクリックします。 または ファームウェアイメージをアップロードする URL を入力し、「Upload」ボタンをクリックします。 Oracle ILOM によってファームウェアイメージが検証され、「Firmware Verification」ページにオプションが表示されます。</p> <p>d. 「Firmware Verification」ページで、適用可能なオプションを有効にします: Preserve Configuration - 既存の Oracle ILOM ファームウェア設定を保存し、ファームウェア更新の完了後に復元するには、このオプションを有効にします。このオプションの詳細は、202 ページの「Oracle ILOM 構成の保持」を参照してください。 Preserve BIOS Configuration (x86 サーバー SP のみ) - 既存の BIOS 構成を保存し、更新プロセスの完了後に復元するには、このオプションを有効にします。このオプションは、一部の x86 サーバーではサポートされていません。そのため、このオプションが表示されない場合、Oracle ILOM はアップグレードプロセスの完了後にデフォルトの BIOS 設定を復元します。 Delay BIOS Upgrade (x86 サーバー SP のみ) - システムの次回の電源再投入後まで x86 BIOS のアップグレードを延期するには、このオプションを有効にします。</p> <p>e. 「Start」をクリックして更新プロセスを開始します。</p> <p>f. 一連のプロンプトで「OK」をクリックし、「Update Status」ページが表示されるまで処理を続行します。</p> <p>g. 「Update Status」が 100% になると、システムが自動的にリポートします。サーバー SP または CMM で正しいファームウェアバージョンが実行されていることを確認するには、この手順の手順 2を参照してください。</p>

Oracle ILOM インタフェース SP または CMM のファームウェア更新手順を開始して実行するには

- CLI
- a. CLI を使用して Oracle ILOM ファームウェアイメージを読み込むには、`load -source` コマンドの後ろにインストールするファームウェアイメージの場所を示すパスを指定して実行します。
例:
`load -source protocol://username:password@server_ip/<path_to_image>/<image.pkg>`
ここでは、`protocol` には次を指定できます:`http`、`https`、`ftp`、`tftp`、`sftp`、`scp`
一連のプロンプトが表示されます。
 - b. `y` と入力してイメージファイルを読み込み、`y` と入力して適用可能な更新オプション (SP 構成の保持、x86 BIOS 設定の保持、x86 BIOS 更新の遅延など) を有効にします
注 - 一部の x86 サーバー SP では、BIOS 構成設定を保持するオプションはサポートされていません。x86 BIOS オプションが表示されない場合、Oracle ILOM は自動的にデフォルトの BIOS 設定を保持します。
SP 構成の保持の詳細は、202 ページの「Oracle ILOM 構成の保持」を参照してください。
 - c. ファームウェアプロセスが完了すると、Oracle ILOM によってステータスメッセージが表示されます。システムが自動的にリブートし、新しいファームウェアイメージが適用されます。サーバー SP で正しいファームウェアバージョンが実行されていることを確認するには、この手順の[手順 2](#)を参照してください。
-

- 2 更新されたファームウェアバージョンがインストールされていることを確認するには、次のいずれかを実行します:

- **Web:**

Oracle ILOM にログインし、「System Information」 > 「Firmware」の順にクリックして、インストールされているファームウェアバージョンを表示します。

注 - ファームウェア更新のあとで Oracle ILOM Web インタフェースが適切にリフレッシュされない場合があります。Oracle ILOM の Web ページで情報が欠落している場合やエラーメッセージが表示される場合は、以前のバージョンのキャッシュされているページが表示されている可能性があります。ブラウザのキャッシュをクリアし、ブラウザをリフレッシュしてから続行してください。

- **CLI:**

次を入力します: `show /System/Firmware`

参考 関連情報:

- 210 ページの「ファームウェア更新時のネットワーク障害から回復する」
- 表 13

▼ ブレードシャーシコンポーネントのファームウェアイメージを更新する

Oracle ILOM CMM には、次のアップグレード可能なブレードシャーシコンポーネントのファームウェア更新を管理するための一元化されたユーザーインターフェースが用意されています:

- ストレージブレードサーバー
- CPU ブレードサーバー
- SP を含む NEM

システム管理者は、CMM の Web インタフェースまたは CLI を使用して、シャーシコンポーネントのファームウェアバージョンを表示したり、シャーシコンポーネントのファームウェア更新を開始したりできます。

次の手順では、Web インタフェースの「Firmware Update」ページおよびファームウェア更新を読み込むための CLI シャーシコンポーネントターゲットを使用してシャーシコンポーネントのファームウェアイメージを更新するプロセスについて説明します。

始める前に

- ファームウェア更新の初期要件が満たされていることを確認してください。[202 ページの「ファームウェア更新を開始する前に」](#)を参照してください。
- ファームウェア更新処理の完了には、数分かかります。この間、ほかの Oracle ILOM タスクを実行しないでください。ファームウェア更新プロセスが完了すると、システムがリブートします。

ファームウェア更新プロセスを開始し、更新プロセスが正常に完了したことを確認するには、これらの手順に従います:

- 1 サーバー SP または CMM イメージのファームウェア更新プロセスを開始するには、次のいずれかの Oracle ILOM インタフェース手順を実行します:

Oracle ILOM インタフェース ブレードシャーシコンポーネント(ブレードまたは NEM)のファームウェア更新手順を開始して実行するには

- Web
- a. CMM の Web インタフェースで、「Firmware」をクリックします。
 - b. 表内で、ファームウェアをアップグレードするシャーシコンポーネントの横のラジオボタンをクリックし、「Actions」リストボックスの「Firmware Update」オプションをクリックします。
「Firmware Upgrade」ページにファームウェアイメージをアップロードするためのプロパティが表示されます。
 - c. 「Firmware Upgrade」ページで、次のいずれかの操作を実行します:
「Browse」をクリックしてアップロードするファームウェアイメージを指定し、「Upload」ボタンをクリックします。
または
ファームウェアイメージをアップロードする URL を入力し、「Upload」ボタンをクリックします。
Oracle ILOM によってファームウェアイメージが検証され、シャーシコンポーネントに応じて Oracle ILOM で、ファームウェア更新プロセスを開始するためのボタンが表示されるか、または CPU ブレードサーバー SP の構成オプションの選択肢が表示されます。
CPU ブレードサーバー SP のファームウェアを更新する場合は手順 4 に進み、それ以外の場合は手順 5 に進みます。
 - d. (CPU ブレードの更新のみ) 「Firmware Verification」ページで、CPU ブレードサーバーで利用できる適用可能なオプションを有効にします:
Preserve Configuration – 既存の Oracle ILOM ファームウェア設定を保存し、ファームウェア更新の完了後に復元するには、このオプションを有効にします。このオプションの詳細は、[202 ページの「Oracle ILOM 構成の保持」](#)を参照してください。
Preserve BIOS Configuration (x86 サーバー SP のみ) – 既存の BIOS 構成を保存し、更新プロセスの完了後に復元するには、このオプションを有効にします。このオプションは、一部の x86 サーバーではサポートされていません。そのため、このオプションが表示されない場合、Oracle ILOM はアップグレードプロセスの完了後にデフォルトの BIOS 設定を復元します。
Delay BIOS Upgrade (x86 サーバー SP のみ) – システムの次の電源再投入後まで x86 BIOS のアップグレードを延期するには、このオプションを有効にします。
 - e. 「Start」をクリックして更新プロセスを開始します。
 - f. 一連のプロンプトで「OK」をクリックし、「Update Status」ページが表示されるまで処理を続行します。
 - g. 「Update Status」が 100% に達すると、システムが自動的にリブートします。サーバー SP または CMM で正しいファームウェアバージョンが実行されていることを確認するには、この手順の[手順 2](#)を参照してください。
-

Oracle ILOM インタフェース ブレードシャーシコンポーネント(ブレードまたはNEM)のファームウェア更新手順を開始して実行するには

CLI

- a. 次の例のように、ブレードまたはNEMのファームウェアのターゲットに移動します:
`cd /System/Firmware/Other_Firmware/Firmware_#`
 ここで、**Firmware_#**は特定のブレードサーバーまたはNEMに割り当てられた番号です。
 - b. CLIを使用してOracle ILOMファームウェアイメージを読み込むには、`load -source` コマンドの後ろにインストールするファームウェアイメージの場所を示すパスを指定して実行します。
 例:
`load -source protocol://username:password@server_ip/<path_to_image>/<image.pkg>`
 ここでは、*protocol*には次を指定できます:*http*、*https*、*ftp*、*tftp*、*sftp*、*scp*。
 イメージを読み込むかどうかを確認するメッセージが表示されます。
 - c. **y** と入力してイメージファイルを読み込みます。
 CPUブレードのファームウェア更新の場合は手順4に進み、それ以外(ストレージブレードまたはNEMのファームウェア更新)の場合は手順5に進みます。
 - d. (CPUブレードの更新のみ)**y** と入力して適用可能な更新オプション(SP構成の保持、x86 BIOS設定の保持、x86 BIOS更新の遅延など)を有効にします
 注-一部のx86サーバーSPでは、BIOS構成設定を保持するオプションはサポートされていません。x86 BIOSオプションが表示されない場合、Oracle ILOMは自動的にデフォルトのBIOS設定を保持します。
 SP構成の保持の詳細は、[202 ページの「Oracle ILOM 構成の保持」](#)を参照してください。
 - e. ファームウェアプロセスが完了すると、Oracle ILOMによってステータスメッセージが表示されます。シャーシコンポーネントが自動的にリブートし、新しいファームウェアイメージが適用されます。正しいシャーシコンポーネントのファームウェアバージョンが実行されていることを確認するには、この手順の[手順2](#)を参照してください。
-

2 更新されたファームウェアバージョンがインストールされていることを確認するには、次のいずれかを実行します:

■ Web:

Oracle ILOM CMM にログインし、「System Information」 > 「Firmware」の順にクリックして、アップグレード可能なシャーシコンポーネントのそれぞれにインストールされているファームウェアバージョンを表示します。

注-ファームウェア更新のあとでOracle ILOM Web インタフェースが適切にリフレッシュされない場合があります。Oracle ILOM の Web ページで情報が欠落している場合やエラーメッセージが表示される場合は、以前のバージョンのキャッシュされているページが表示されている可能性があります。ブラウザのキャッシュをクリアし、ブラウザをリフレッシュしてから続行してください。

■ CLI:

次を入力します: `show /System/Firmware/Other_Firmware/Firmware_n`

参考 関連情報:

- 210 ページの「ファームウェア更新時のネットワーク障害から回復する」
- 表 13

▼ ファームウェア更新時のネットワーク障害から回復する

ファームウェア更新の実行中にネットワーク障害が発生した場合、Oracle ILOM は自動的にセッションをタイムアウトし、システムをリブートします。システムがリブートしたら、これらのガイドラインに従ってファームウェア更新プロセスを回復してください。

- 1 ネットワークの問題に対処し、解決します。
- 2 Oracle ILOM SP または CMM に再接続します。
- 3 ファームウェア更新プロセスを再起動します。

サービスプロセッサまたはシャーシ監視モジュールの電源のリセット

アップグレードを完了したり、エラー状態をクリアしたりするために、サーバーまたは Network Express Module (NEM) のブレードシャーシ監視モジュール (CMM) またはサービスプロセッサ (SP) をリセットする必要がある場合があります。SP および CMM のリセット操作は、すべてのアクティブな処理が終了し、システムがリブートする PC のリセットと似ています。

サーバー SP または CMM の電源をリセットすると、現在の Oracle ILOM セッションが自動的に切断され、リセットプロセスが完了するまでサービスプロセッサが管理不可能な状態になります。ただし、ラック搭載型サーバー SP または CPU ブレードサーバー SP がリセットされても、サーバー上のホストオペレーティングシステムは影響を受けません。

システム管理者は、Web インタフェースまたは CLI からサーバー SP、NEM SP、および CMM をリセットできます。SP および CMM のリセット手順については、次の手順を参照してください。

▼ サーバー SP、NEM SP、または CMM の電源をリセットする 始める前に

- SP または CMM をリセットするには、Host Control and Reset (r) の役割が必要です。

- Web の「Reset」ボタンをクリックするか、または CLI の `reset` コマンドを実行すると、CLI の `-script` オプション (`reset [options] target`) を指定しないかぎり、Oracle ILOM によってリセット操作を確認するプロンプトが自動的に表示されます。

この手順では、Web と CLI の両方の手順について説明します。

- **SP または CMM の電源をリセットするには、次のいずれかを実行します:**

Oracle ILOM インタフェース	SP または CMM の電源をリセットする
Web	<p>次のいずれかを実行します:</p> <ul style="list-style-type: none"> ■ サーバー SP: <ul style="list-style-type: none"> 「ILOM Administration」 > 「Maintenance」 > 「Reset SP」の順にクリックして、「Reset SP」ボタンをクリックします。 ■ CMM およびブレードシャーシコンポーネント: <ul style="list-style-type: none"> 「ILOM Administration」 > 「Maintenance」 > 「Reset Components」の順にクリックします。 シャーシコンポーネント (CMM、ブレード、NEM) の横のラジオボタンをクリックし、「Reset」ボタンをクリックします。
CLI	<p>次のいずれかを実行します:</p> <ul style="list-style-type: none"> ■ サーバー SP: <ul style="list-style-type: none"> サーバー SP をリセットするには、次を入力します: <code>reset /SP</code> ■ CMM ブレードシャーシコンポーネント: <ul style="list-style-type: none"> CMM をリセットするには、次を入力します: <code>reset /CMM</code> ブレード SP をリセットするには、次を入力します: <code>reset /Servers/Blades/BLn/SP</code> NEM SP をリセットするには、次を入力します: <code>reset /System/IO_Modules/NEMn/SP</code>

Oracle ILOM 構成のバックアップ、復元、またはリセット

システム管理者は、Oracle ILOM に用意されているバックアップおよび復元プロパティを使用して、現在の Oracle ILOM 構成をバックアップ XML ファイルにコピーし、必要に応じてその構成を復元できます。システム管理者は、バックアップ XML 構成ファイルを使用して現在の SP または CMM 上に設定を復元したり、バックアップファイルを使用してほかの CMM またはサーバー SP に構成設定をインストールしたりできます。

システム管理者は、Oracle ILOM に用意されている「Reset Default」プロパティを使用して、ユーザーが設定した Oracle ILOM 構成プロパティをクリアし、それらを出荷時のデフォルト値に復元できます。

システム管理者は、Web インタフェースまたは CLI から、Oracle ILOM 構成のバックアップ、復元、および構成設定のデフォルトへのリセットを行うことができます。Oracle ILOM のバックアップ、復元、またはデフォルトへのリセット機能の詳細は、次のトピックを参照してください:

- 212 ページの「バックアップ、復元、およびデフォルトへのリセット操作の使用」
- 213 ページの「ユーザーの役割によってバックアップまたは復元される構成設定が決まる」
- 213 ページの「Oracle ILOM 構成設定をバックアップする」
- 215 ページの「Oracle ILOM のバックアップ XML 構成ファイルを編集する (省略可能)」
- 218 ページの「Oracle ILOM のバックアップ XML ファイルを復元する」
- 219 ページの「Oracle ILOM 構成を出荷時のデフォルトにリセットする」

バックアップ、復元、およびデフォルトへのリセット操作の使用

システム管理者は、次の方法でバックアップ、復元、およびデフォルトへのリセットの操作を使用できます:

Oracle ILOM 構成をほかのシステム上で使用するためにレプリケートする。

システム管理者は、次の手順に従って Oracle ILOM 構成をほかの Oracle サーバー SP または CMM で使用するためにレプリケートできます:

1. 必要に応じて Oracle ILOM 構成をカスタマイズします
たとえば、ユーザーアカウントの定義、デフォルトのネットワーク設定の変更、警告通知の設定、システムポリシーの定義など。
2. Oracle ILOM 構成をバックアップ XML ファイルに保存します。
3. バックアップ XML ファイルを編集して、特定のシステムに固有の設定 (IP アドレスなど) を削除します。
4. 復元操作を実行して、構成をほかの Oracle サーバー SP または CMM にレプリケートします。

既存の **Oracle ILOM** 構成が機能しなくなったときに、正常に機能する **Oracle ILOM** 構成を回復する。

最後のバックアップ操作以降に Oracle ILOM 構成が変更され、現在の Oracle ILOM 構成が機能しなくなった場合、システム管理者はこれらの手順に従って正常に機能するバックアップ構成を回復できます:

1. Oracle ILOM 構成をデフォルトにリセットします。
 2. Oracle ILOM 構成を正常に機能する最新の既知の構成に復元します。
-

ユーザーの役割によってバックアップまたは復元される構成設定が決まる

セキュリティ上の理由から、XML 構成ファイルをバックアップまたは復元するときには、使用するユーザーアカウントに現在割り当てられているユーザーの役割権限によって、バックアップまたは復元操作にどの程度の構成が含まれるかが決まります。

XML ファイル内のすべての構成設定がバックアップまたは復元されるようにするには、完全なユーザーの役割権限が必要です。したがって、バックアップおよび復元操作を実行するシステム管理者は、Administrator (administrator) プロファイルの役割を割り当ててもらおうか、または次のユーザーの役割をすべて割り当ててもらおうようにしてください:

- Admin (a)
- User Management (u)
- Console (c)
- Reset and Host Control (r)
- Read Only (o)

十分な権限がないユーザーアカウントを使用してバックアップおよび復元操作を実行すると、構成設定の一部がバックアップまたは復元されないことがあります。ユーザー権限不足のためにバックアップまたは復元されない構成プロパティごとに、Oracle ILOM イベントログにログエントリが作成されます。

Oracle ILOM のユーザーの役割について説明する一覧については、[表 9](#)を参照してください。ユーザーの役割を割り当てる手順については、[46 ページの「ローカルユーザーアカウントの構成」](#)を参照してください。

Oracle ILOM によって記録されたイベントの表示およびフィルタリングの詳細は、『ユーザーズガイド』の「Oracle ILOM のログエントリの管理」を参照してください。

▼ Oracle ILOM 構成設定をバックアップする

システム管理者は、サーバー SP または CMM 上でアクティブに実行されている Oracle ILOM 構成ファイルのバックアップコピーを保存できます。バックアップ操作を開始すると、SP または CMM に対するすべての Oracle ILOM クライアントセッションが一時的に停止します。バックアップ操作が完了すると、停止したセッションは正常な状態に戻ります。通常、バックアップ操作が完了するには 2-3 分かかります。

始める前に

- Oracle ILOM で構成のバックアップ操作を実行するには、Administrator (administrator) プロファイルの役割を使用するか、または次のユーザーの役割が割り当てられている必要があります: Admin (a)、User Management (u)、Console (c)、Reset and Host Control (r)、および Read Only (o)。

詳細は、213 ページの「ユーザーの役割によってバックアップまたは復元される構成設定が決まる」を参照してください。

次の Oracle ILOM 構成バックアップ手順では、SP および CMM 用の Web と CLI の両方の手順を示します。

- **Oracle ILOM 構成を XML ファイルにバックアップするには、次に示すいずれかの Oracle ILOM ユーザーインターフェースの手順を実行します。**

Oracle ILOM ユーザーインターフェース	Oracle ILOM 構成設定の XML ファイルへのバックアップ
Web	<ol style="list-style-type: none">「ILOM Administration」 > 「Configuration Management」 > 「Backup/Restore」の順にクリックします。「Operations」ボックスの「Backup」をクリックします。「Transfer Method」ボックスをクリックし、Oracle ILOM 構成ファイルの転送方法を指定します。 各ファイル転送方法のプロパティについては、表 13 を参照してください。バックアップ構成ファイルを暗号化するには、「Passphrase」テキストボックスにパスフレーズを入力し、「Confirm Passphrase」テキストボックスにパスフレーズを再入力します。指定したパスフレーズを使用してバックアップファイルが暗号化されます。 注 - 機密性のあるデータ (パスワード、SSH 鍵、証明書、LDom など) をバックアップするには、パスフレーズを指定する必要があります。「Run」をクリックしてバックアップ操作を開始します。 バックアップ操作を実行しているときは、Oracle ILOM SP または CMM に対するクライアントセッションが一時的に停止します。バックアップ操作が完了すると、セッションは正常な状態に戻ります。

Oracle ILOM ユーザーインタ
フェース

Oracle ILOM 構成設定の XML ファイルへのバックアップ

CLI

- a. 次の例のように、`config CLI` ターゲットに移動します:


```
cd /SP/config
cd /CMM/config
```
- b. バックアップ構成ファイルを暗号化するには、次の例のように、`passphrase` プロパティの値を設定します:


```
set passphrase=value
```

 指定したパスフレーズを使用してバックアップファイルが暗号化されます。
 注 - 機密性のあるデータ(パスワード、SSH 鍵、証明書、LDom など)をバックアップするには、パスフレーズを指定する必要があります。
- c. バックアップ操作を開始するには、`/SP/config` または `/CMM/config` ディレクトリ内から次のコマンドを入力します。例:


```
set
dump_uri=transfer_method://username:password@ipaddress_or_hostname/directorypath/filename
```

 ここでは、`transfer method` には次を指定できます: `tftp`、`ftp`、`sftp`、`scp`、`http`、または `https`
 各ファイル転送方法のプロパティについては、表 13 を参照してください。
 例:


```
set dump_uri=scp://adminuser:userpswd@1.2.3.4/Backup/Lab9/SP123.config
```

 バックアップ操作を実行しているときは、Oracle ILOM SP または CMM に対するクライアントセッションが一時的に停止します。バックアップ操作が完了すると、セッションは正常な状態に戻ります。

参考 関連情報:

- 215 ページの「Oracle ILOM のバックアップ XML 構成ファイルを編集する (省略可能)」
- 218 ページの「Oracle ILOM のバックアップ XML ファイルを復元する」
- 212 ページの「バックアップ、復元、およびデフォルトへのリセット操作の使用」

▼ Oracle ILOM のバックアップ XML 構成ファイルを編集する (省略可能)

上級ユーザーは、バックアップ XML ファイルを使用して、ネットワーク上のほかの Oracle サーバー SP または CMM を同じ Oracle ILOM 構成でプロビジョニングできます。システム管理者は、バックアップ XML ファイルを別のシステムで使用する前に、ファイルを編集して、特定のシステムに固有の情報 (IP アドレスなど) をすべて削除するようにしてください。

XML ファイルの例:

バックアップされた XML ファイルの例を次に示します。ファイルの内容は、この手順に合わせて省略されています。

```
<SP_config version="3.0">
<entry><entry><property>/SP/clock/datettime</property><value>Mon May 12 15:31:09 2010</value></entry>...
<property>/SP/check_physical_presence</property><entry><property>/SP/config/passphrase</property>
<value encrypted="true">89541176be7c</value></entry>...
<value>>false</value><entry><property>/SP/network/pendingipaddress</property><value>1.2.3.4</value></entry>...
</entry><entry><property>/SP/network/commitpending</property><value>>true</value></entry>...
<entry><entry><property>/SP/services/snmp/sets</property><value>enabled</value></entry>...
<property>/SP/hostname</property><entry><property>/SP/users/john/role</property><value>aucro</value></entry>
<entry><property>/SP/users/john/password</property><value encrypted="true">c21f5a3df51db69fdf</value></entry>
</SP_config>
<value>labssystem12</value>
</entry>
<entry>
<property>/SP/system_identifiser</property>
<value>SUN BLADE X8400 SERVER MODULE, ILOM v3.0.0.0, r32722</value>
</entry>
.
.
.
```

1 この XML ファイルの例で、次を確認します:

- パスワードとパスフレーズ以外の構成設定は平文です (暗号化されていません)。
- ファイルの最初の構成エントリである `check_physical_presence` プロパティは、`false` に設定されています。デフォルト設定は `true` であるため、この設定はデフォルトの Oracle ILOM 構成が変更されていることを表しています。
- `pendingipaddress` および `commitpending` の構成設定は、サーバーごとに異なります。これらの設定は、バックアップ XML ファイルを別のサーバーの復元操作に使用する前に削除するようにしてください。
- ユーザーアカウント `john` には、`a`、`u`、`c`、`r`、`o` の役割が構成されています。デフォルトの Oracle ILOM 構成ではユーザーアカウントが構成されていないため、このアカウントはデフォルトの Oracle ILOM 構成が変更されていることを表しています。
- SNMP の `sets` プロパティは、`enabled` に設定されています。デフォルト設定は `disabled` です。

- 2 平文の構成設定を変更するには、値を変更するか、新しい構成設定を追加します。

例:

- ユーザー **john** に割り当てられている役割を変更するには、テキストを次のように変更します:

```
<entry>
<property>/SP/users/john/role</property>
<value>auo</value>
</entry>
```

- 新しいユーザーアカウントを追加し、そのアカウントに **a**、**u**、**c**、**r**、**o** の役割を割り当てるには、ユーザー **john** のエントリのすぐ下に次のテキストを追加します:

```
<entry>
<property>/SP/users/bill/role</property>
<value>aucro</value>
</entry>
```

- パスワードを変更するには、**encrypted="true"** の設定と暗号化されたパスワード文字列を削除し、新しいパスワードを入力します。たとえば、ユーザー **john** のパスワードを変更するには、**XML** ファイルを次のように変更します:

変更箇所:

```
<entry>
<property>/SP/users/john/password</property>
<value encrypted="true">c21f5a3df51db69fdf</value>
</entry>
```

変更後:

```
<entry>
<property>/SP/users/john/password</property>
<value>newpassword</value>
</entry>
```

- 3 バックアップ **XML** ファイルに変更を加えたら、同じシステムや別のシステムでの復元操作に使用できるようにファイルを保存します。

参考 関連トピック

- [215 ページの「Oracle ILOM のバックアップ XML 構成ファイルを編集する \(省略可能\)」](#)
- [218 ページの「Oracle ILOM のバックアップ XML ファイルを復元する」](#)
- [212 ページの「バックアップ、復元、およびデフォルトへのリセット操作の使用」](#)

▼ Oracle ILOM のバックアップ XML ファイルを復元する

システム管理者は、復元操作を実行することで、リモートシステムから XML ファイルを取得し、その内容を解析して、バックアップされた構成データで SP (または CMM) を更新できます。復元操作を開始すると、復元しているサーバー SP または CMM に対するすべての Oracle ILOM クライアントセッションが一時的に停止します。復元操作が完了すると、停止したセッションは正常な状態に戻ります。通常、復元操作の完了には 2-3 分かかります。

始める前に

- Oracle ILOM で構成の復元操作を実行するには、Administrator (administrator) プロファイルの役割を使用するか、または次のユーザーの役割が割り当てられている必要があります: Admin (a)、User Management (u)、Console (c)、Reset and Host Control (r)、および Read Only (o)。

詳細は、213 ページの「ユーザーの役割によってバックアップまたは復元される構成設定が決まる」を参照してください。

次の Oracle ILOM 構成復元手順では、SP および CMM 用の Web と CLI の両方の手順を示します。

- バックアップされた Oracle ILOM 構成 XML ファイルを復元するには、次に示すいずれかの Oracle ILOM ユーザーインターフェースの手順を実行します。

Oracle ILOM ユーザーインターフェース

Oracle ILOM 構成設定のバックアップコピーの復元

Web

- 「ILOM Administration」 > 「Configuration Management」 > 「Backup/Restore」の順にクリックします。
 - 「Operations」ボックスの「Restore」をクリックします。
 - 「Transfer Method」ボックスをクリックし、Oracle ILOM 構成ファイルの転送方法を指定します。
各ファイル転送方法のプロパティについては、表 13 を参照してください。
 - バックアップ構成ファイルがパスフレーズで暗号化されている場合は、「Passphrase」テキストボックスにパスフレーズを入力し、「Confirm Passphrase」テキストボックスにパスフレーズを再入力します。
注 - 入力するパスフレーズは、バックアップ構成ファイルを暗号化するために使用したパスフレーズと一致する必要があります。
 - 「Run」をクリックして復元操作を開始します。
復元操作を実行しているときは、Oracle ILOM SP または CMM に対するクライアントセッションが一時的に停止します。復元操作が完了すると、セッションは正常な状態に戻ります。
-

CLI

- a. 次の例のように、`config CLI` ターゲットに移動します:


```
cd /SP/config
cd /CMM/config
```
- b. バックアップ構成ファイルがパスフレーズで暗号化されている場合は、次の例のように、`passphrase` プロパティの値を、ファイルを暗号化するために使用したパスフレーズに設定します:


```
set passphrase=value
```

注 - 入力するパスフレーズは、バックアップ構成ファイルを暗号化するために使用したパスフレーズと一致する必要があります
- c. 復元操作を開始するには、`/SP/config` または `/CMM/config` ディレクトリ内から次のコマンドを入力します。例:


```
set
load_uri=transfer_method://username:password@ipaddress_or_hostname/directorypath/filename
```

ここでは、`transfer method` には次を指定できます: `tftp`、`ftp`、`sftp`、`scp`、`http`、または `https`。
各ファイル転送方法のプロパティについては、表 13 を参照してください。
例:

```
set load_uri=scp://adminuser:userpswd@1.2.3.4/Backup/Lab9/SP123.config
```

 復元操作を実行しているときは、Oracle ILOM SP または CMM に対するクライアントセッションが一時的に停止します。復元操作が完了すると、セッションは正常な状態に戻ります。

参考 関連情報:

- 212 ページの「バックアップ、復元、およびデフォルトへのリセット操作の使用」
- 218 ページの「Oracle ILOM のバックアップ XML ファイルを復元する」
- 213 ページの「ユーザーの役割によってバックアップまたは復元される構成設定が決まる」

▼ Oracle ILOM 構成を出荷時のデフォルトにリセットする

システム管理者は、SP または CMM の現在の Oracle ILOM 構成設定を元の出荷時のデフォルト設定に復元できます。

デフォルトへのリセット操作に設定できる値については、次の表を参照してください。

リセットプロパティ値	説明
All	サービスプロセッサの次回のリセット時に Oracle ILOM 構成データのすべてをデフォルト設定にリセットするには、「All」オプションを設定します。この操作では、ログファイルのエントリは消去されません。
Factory	サービスプロセッサの次回のリセット時に Oracle ILOM 構成データのすべてをデフォルト設定にリセットし、すべてのログファイルを消去するには、「Factory」オプションを設定します。
None (デフォルト)	現在の構成を使用しながら通常の動作を行うには、「None」オプションを設定します。また、サービスプロセッサの次回のリセット前に保留中のデフォルトへのリセット操作(「All」または「Factory」)を取り消す場合にも、「None」オプションを使用します。

- サーバー SP または CMM に対してデフォルトへのリセット操作を実行するには、次に示すいずれかの Oracle ILOM ユーザーインターフェースの手順を実行します。

Oracle ILOM インタフェース	SP または CMM のデフォルトへのリセット操作
Web	<ol style="list-style-type: none">「ILOM Administration」 > 「Configuration Management」 > 「Reset Defaults」の順にクリックします。「Reset Defaults」リストボックスをクリックして、次のいずれかの値を指定します: 「None」、「All」、または「Factory」。「Reset Defaults」ボタンをクリックします。
CLI	次のいずれかを実行します: <ul style="list-style-type: none">■ サーバー SP: 次を入力します: <code>set /SP reset_to_defaults=all none factory</code>■ CMM: 次を入力します: <code>set /CMM reset_to_defaults=all none factory</code>

参考 関連情報:

- 210 ページの「サービスプロセッサまたはシャーシ監視モジュールの電源のリセット」

x86 BIOS 構成パラメータの保守

説明	リンク
x86 BIOS の構成を管理する方法を特定するには、このトピックを参照してください。	■ 221 ページの「BIOS 構成の管理」
Oracle ILOM BIOS 構成の機能、用語、およびプロパティについては、これらのトピックを参照してください。	■ 222 ページの「Oracle ILOM: BIOS 構成機能」 ■ 223 ページの「Oracle ILOM: BIOS の用語」 ■ 223 ページの「Web および CLI: BIOS プロパティ」
Oracle ILOM から BIOS 構成タスクを実行する方法については、このセクションを参照してください。	■ 228 ページの「Oracle ILOM からの BIOS 構成タスクの実行」

関連情報

- x86 Sun サーバーの管理ガイド、Oracle System Assistant
- x86 Sun サーバーの管理ガイド、BIOS 設定ユーティリティ

BIOS 構成の管理

Oracle x86 サーバーの BIOS 構成パラメータは、ホスト BIOS 設定、Oracle System Assistant インタフェース、および Oracle ILOM の CLI と Web インタフェースから管理できます。このセクションの以降のトピックでは、Oracle ILOM インタフェースから BIOS 構成を管理する方法について説明します。

- 222 ページの「Oracle ILOM: BIOS 構成機能」
- 222 ページの「Oracle ILOM: BIOS に関する特別な考慮事項」
- 223 ページの「Oracle ILOM: BIOS の用語」
- 223 ページの「Web および CLI: BIOS プロパティ」

注 - ホスト BIOS 設定または Oracle System Assistant から BIOS 構成を管理する手順については、Oracle x86 サーバーの管理ガイドを参照してください。

Oracle ILOM: BIOS 構成機能

Oracle ILOM には、Oracle ILOM で管理されている x86 サーバーの BIOS 構成パラメータを管理するために使用できる一連の構成可能なプロパティが用意されています。これらの構成可能な Oracle ILOM プロパティを使用して、次のことができます:

- BIOS 非揮発性データストア内の構成パラメータのコピーをバックアップする。
- バックアップした構成パラメータのコピーを BIOS 非揮発性データストアに復元する。
- BIOS 非揮発性データストア内のパラメータを出荷時のデフォルトにリセットする。

さらに、Oracle ILOM は BIOS 非揮発性データストア内のパラメータを動的に監視し、それらが Oracle ILOM BIOS 構成ファイル内のパラメータと同期していることを確認します。CLI および Web インタフェースに表示される構成同期ステータスは、Oracle ILOM BIOS 構成ファイルに格納されている BIOS パラメータの現在の状態を示します。

注 - BIOS 構成を別の Oracle x86 サーバーにプロビジョニングする必要がある上級ユーザーは、215 ページの「Oracle ILOM のバックアップ XML 構成ファイルを編集する (省略可能)」を参照してください。

Oracle ILOM: BIOS に関する特別な考慮事項

- Oracle ILOM BIOS 構成では、Oracle ILOM BIOS 構成ファイルがホスト BIOS 非揮発性データストアと同期していないと、ホストのブート時間が増加することがあります。
- 「Preserve existing BIOS configuration」のオプションが有効になっている場合は、サーバー SP の Oracle ILOM ファームウェアを更新すると、Oracle ILOM BIOS 構成パラメータに影響することがあります。ファームウェア更新の実行および Oracle ILOM で保守される BIOS 構成パラメータの保存の詳細は、201 ページの「ファームウェア更新の実行」を参照してください。

Oracle ILOM: BIOS の用語

Oracle ILOM の用語	説明
BIOS	Oracle x86 サーバー上の BIOS は、ホストサーバーの電源が投入されてからオペレーティングシステムに引き継がれるまでのシステムを制御するブートファームウェアプログラムです。BIOS では、バッテリー駆動の非揮発性データストアにシステムの日付、時間、および構成情報が格納されます。
BIOS バージョン	Oracle x86 サーバーにインストールされている現在の BIOS ファームウェアのバージョンを示す読み取り専用プロパティ。
BIOS 非揮発性データストア	非揮発性メモリーチップに現在格納されている Oracle x86 サーバーの BIOS 構成パラメータ。
Oracle ILOM BIOS 構成ファイル	サーバー SP 上で動的に保守される XML ファイルで、BIOS 非揮発性データストアから最後に取得された BIOS 構成パラメータのリストが含まれています。
Backup BIOS configuration	Oracle ILOM 内の構成可能なプロパティで、これによって BIOS 非揮発性データストアに現在設定されているパラメータのコピーを取得し、それらをサーバー SP 上の Oracle ILOM BIOS 構成ファイルに保存できます。
Restore BIOS configuration	Oracle ILOM 内の構成可能なプロパティで、これによって Oracle ILOM BIOS 構成ファイル内のパラメータを BIOS 非揮発性データストアにエクスポートできます。
BIOS 構成パラメータ	一般に、Oracle ILOM でコピーまたはエクスポートされる BIOS 構成パラメータには、設定、ブートリスト、およびブートデバイスの値が含まれています。

Web および CLI: BIOS プロパティ

- [表 71](#)
- [表 72](#)
- [表 73](#)

表 71 BIOS の Web ナビゲーションと CLI ターゲット

Web ナビゲーション	CLI ターゲット
「System Management」 > 「BIOS」	/System/BIOS
	/System/BIOS/Config

表 72 BIOS の Web プロパティと CLI プロパティ

プロパティ名	種類	値	説明
System BIOS Version (system_bios_version=)	読み取り専用		「System BIOS Version」プロパティは、管理対象 Oracle x86 サーバーに現在インストールされている BIOS ファームウェアのバージョンを識別します。
BIOS Configuration: Sync Status (config_sync_status=)	読み取り専用	OK <i>Reboot Required</i> <i>Internal Error</i>	<p>「BIOS Configuration Sync Status」プロパティは、次のいずれかの状態を示します:</p> <ul style="list-style-type: none"> ■ OK - Oracle ILOM によって保守される BIOS 構成パラメータが BIOS 非揮発性データストア内の構成パラメータと同期しています。 ■ Reboot Required - Oracle ILOM によって保守される BIOS 構成パラメータが BIOS 非揮発性データストア内の構成パラメータと同期していません。BIOS パラメータを同期するには、Oracle x86 サーバーをリブートする必要があります。 ■ Internal Error - Oracle ILOM は、BIOS 非揮発性データストアを読み取ることができず、BIOS のバックアップまたは復元操作を開始できません。詳細は、Oracle サービスにお問い合わせください。
BIOS Configuration: Reset To Defaults (reset_to_defaults=)	読み取り 書き込み	Factory None	<p>「Reset To Defaults」プロパティには、次のいずれかの値を指定します:</p> <ul style="list-style-type: none"> ■ Factory - BIOS 非揮発性データストア内の構成パラメータを出荷時のデフォルトに設定します。 ■ None - この値 (None) は、BIOS 非揮発性データストア内のパラメータを出荷時のデフォルトにリセットしたあとで表示されます。
BIOS Configuration: Backup (dump_uri=)	書き込み専用		<p>「BIOS Configuration Backup」プロパティを使用すると、BIOS 非揮発性データストア内のパラメータのコピーを作成し、それらのパラメータを ILOM ファイルシステム内の BIOS 構成ファイルに保存できます。</p> <p>BIOS 構成をバックアップする手順については、232 ページの「BIOS 構成のバックアップ」を参照してください。</p>

表 72 BIOS の Web プロパティと CLI プロパティ (続き)

プロパティ名	種類	値	説明
BIOS Configuration: Restore Status (restore_status=)	読み取り専用	OK Restore pending Partial restore: invalid configuration entry Partial restore: invalid boot order entry Partial restore: invalid configuration and boot order entries	<p>「BIOS Configuration Restore Status」プロパティは、次のいずれかの状態を示します:</p> <ul style="list-style-type: none"> ■ OK – Oracle ILOM BIOS 構成パラメータをホスト BIOS 非揮発性データストアに復元する前回の復元操作が正常に完了しました。 ■ Restore pending – ホストの電源が切断されるまで復元操作が保留になっています。注 – 復元操作は、ホストサーバーの電源が切断されたときに Oracle ILOM によって実行されます。 ■ Partial restore: invalid configuration entry – 前回の復元操作で 1 つ以上のホスト BIOS 構成パラメータを復元できませんでした。 ■ Partial restore: invalid boot order entry – 前回の復元操作でホストブート順序リスト内の 1 つ以上のブートデバイスを復元できませんでした。 ■ Partial restore: invalid configuration and boot order entries – 前回の復元操作で、1 つ以上の BIOS 構成パラメータおよびホストブート順序リスト内の 1 つ以上のブートデバイスを復元できませんでした。

表 72 BIOS の Web プロパティと CLI プロパティ (続き)

プロパティ名	種類	値	説明
BIOS Configuration: Restore (load_uri=restore_options)	読み取り 書き込み	All Configuration only Bootlist only Cancel Restore	<p>「BIOS Configuration Restore」プロパティを使用すると、以前に Oracle ILOM によって保存された BIOS パラメータをホスト BIOS 非揮発性データストアに復元できます。BIOS パラメータの復元には次のオプションがあります:</p> <ul style="list-style-type: none"> ■ All - 以前に Oracle ILOM によって保存されたすべての BIOS 構成パラメータを復元します。 ■ Configuration only - 以前に保存された設定パラメータを復元します。 ■ Bootlist only - 以前に Oracle ILOM によって保存されたホストブートリストパラメータを復元します。 ■ Cancel Restore (または action=cancel) - 開始された復元操作を取り消します。 <p>注 - Web インタフェースで「Cancel Restore」オプションを使用できるのは、(1) 復元操作を開始し、(2) 管理対象 Oracle x86 サーバー上のホストオペレーティングシステムの電源切断やリセットがまだ行われていない場合だけです。</p> <p>BIOS 構成を復元する手順については、233 ページの「BIOS 構成の復元」を参照してください。</p>

表 72 BIOS の Web プロパティと CLI プロパティ (続き)

プロパティ名	種類	値	説明
Transfer Method Options	読み取り 書き込み	Browser TFTP FTP SFTP SCP HTTP HTTPS	<p>Oracle ILOM BIOS 構成パラメータをインポートまたはエクスポートするときは、次のいずれかの転送方法を指定できます:</p> <ul style="list-style-type: none"> ■ Browser - Web インタフェースオプションのみ。このオプションを使用するときは、ファイルの場所を指定します。 ■ TFTP - このオプションを使用するときは、TFTP ホストの IP アドレスまたは名前とファイルへのディレクトリパスを指定します。 ■ FTP - このオプションを使用するときは、ホストの IP アドレスまたは名前、FTP サーバーのユーザー名とパスワード、およびファイルの場所へのディレクトリパスを指定します。 ■ SFTP - このオプションを使用するときは、ホストの IP アドレスまたは名前、SFTP サーバーのユーザー名とパスワード、およびファイルの場所へのディレクトリパスを指定します。 ■ SCP - このオプションを使用するときは、ホストのネットワークアドレス、SCP サーバーのユーザー名とパスワード、およびファイルの場所へのディレクトリパスを指定します。 ■ HTTP - このオプションを使用するときは、ホストのネットワークアドレス、HTTP サーバーのユーザー名とパスワード、およびファイルの場所へのディレクトリパスを指定します。 ■ HTTPS - このオプションを使用するときは、ホストのネットワーク IP アドレスまたは名前、HTTPS サーバーのユーザー名とパスワード、およびファイルの場所へのディレクトリパスを指定します。

表 73 CLI コマンド load および dump の -force オプション

```
load_uri=-force restore_option/transfer_method://username:password@ipaddress_or_hostname /directorypath/filename
```

表 73 CLI コマンド load および dump の -force オプション (続き)

```
dump_uri=-force transfer_method://username:password@ipaddress_or_hostname /directorypath/filename
```

使用法- 次の場合に load または dump コマンドが失敗しないようにするには、-force オプションを指定する必要があります: (1) 「Restore Status」に「Pending Restore」状態が表示される (restore_status=pending_restore) か、または (2) 「BIOS Configuration Sync」に「Reboot Needed」状態が表示される (config_sync_status=reboot_needed) 場合。

注意- 次の場合は、同期していないホスト BIOS 構成ファイルが Oracle ILOM ファイルシステムにコピーされます: (1) 「BIOS Configuration Sync」に「Reboot Needed」状態が表示され (sync_status=reboot_needed)、(2) dump_uri=-force オプションを使用して BIOS 構成ファイルをバックアップする場合。

注意- 次の場合は、既存の復元保留中の BIOS 構成ファイルに含まれるパラメータが前回バックアップされた BIOS 構成ファイルのパラメータで置換されます: (1) 「Restore Status」に「Restore Pending」状態が表示され (restore_status=restore_pending)、(2) load_uri=-force オプションを使用してホスト BIOS 非揮発性データストア内のパラメータを復元する場合。

Oracle ILOM からの BIOS 構成タスクの実行

- 228 ページの「BIOS 構成タスクの要件」
- 229 ページの「BIOS 構成同期ステータスの表示と構成パラメータの同期」
- 231 ページの「SP および Oracle ILOM BIOS の出荷時のデフォルトへのリセット」
- 232 ページの「BIOS 構成のバックアップ」
- 233 ページの「BIOS 構成の復元」

BIOS 構成タスクの要件

BIOS 構成パラメータをバックアップまたは復元する前に、次の要件を満たす必要があります:

- Oracle ILOM で BIOS 構成パラメータを同期、復元、またはバックアップするには、次のユーザーの役割が必要です:

BIOS 構成タスク	Oracle ILOM ユーザーの役割	説明:
BIOS 構成の復元 (load_uri=)	Reset and Host Control (r) Admin (a)	ホスト BIOS 非揮発性データストア内の構成パラメータを読み込むには、Reset and Host Control (r) の役割と Admin (a) の役割が必要です。
注- Oracle ILOM は、ホスト BIOS 非揮発性データストア内のパラメータを Oracle ILOM BIOS 構成ファイルに最後に設定されたパラメータで置換します。		

BIOS 構成タスク	Oracle ILOM ユーザーの役割	説明:
BIOS 構成のバックアップ (dump_uri=)	Reset and Host Control (r) Admin (a)	Oracle ILOM 構成ファイル内の構成パラメータを置換するには、Reset and Host Control (r) の役割と Admin (a) の役割の両方が必要です。 注 - Oracle ILOM は、Oracle ILOM BIOS 構成ファイル内のパラメータをホスト BIOS 非揮発性データストアに最後に設定されたパラメータで置換します。
BIOS 構成の同期 (reset /System または stop /System)	Admin (a)	管理対象 Oracle x86 サーバーの電源をリセット (または電源を切断) するには、Admin (a) の役割が必要です。

- このセクションに記載されている BIOS 構成タスクを実行する前に、223 ページの「Web および CLI: BIOS プロパティ」を確認してください。
- 管理対象 Oracle x86 サーバーが新しい場合は、電源を投入し、ホスト BIOS のブートプロセスによってブートデバイスを検出し、初期のブート順序を作成し、これらのパラメータを BIOS 非揮発性データストアに保存するようにしてください。次に、管理対象 Oracle x86 サーバーの電源を再投入し、BIOS 非揮発性データストアを Oracle ILOM BIOS 構成ファイルと同期するようにしてください。
- /SP または /System/BIOS に出荷時のデフォルトを設定すると、相互に意図しない影響を及ぼす可能性があります。たとえば、/SP/reset_to_defaults を *factory* に設定すると、Oracle ILOM で /System/BIOS/reset_to_defaults の設定が消失することがあります。SP および BIOS 構成に出荷時のデフォルトを設定する手順については、231 ページの「SP および Oracle ILOM BIOS の出荷時のデフォルトへのリセット」に記載されている手順に従ってください。

▼ BIOS 構成同期ステータスの表示と構成パラメータの同期

始める前に

- 228 ページの「BIOS 構成タスクの要件」を確認してください。

BIOS 構成同期ステータスを表示し、必要に応じてホストの非揮発性データストア内の BIOS 構成パラメータを Oracle ILOM BIOS 構成ファイル内のパラメータと同期するには、これらの手順に従います。

- 1 Oracle ILOM BIOS 構成ファイル内の現在のパラメータの状態を表示するには、次のいずれかを実行します:

- Web インタフェースでは、「System Management」 > 「BIOS」の順にクリックします。
- CLI では、**show /System/BIOS/Config** と入力します。

「OK」状態は、Oracle ILOM BIOS 構成ファイル内のパラメータが BIOS 非揮発性データストアと同期していることを示します。

「Reboot_Required」状態は、Oracle ILOM BIOS 構成ファイルが BIOS 非揮発性データストアと同期していないことを示します。

「Internal_Error」状態は、Oracle ILOM が BIOS 非揮発性データストアを読み取れないことを示します。この内部エラーが発生すると、Oracle ILOM で BIOS 構成のバックアップおよび復元操作を開始できなくなります。詳細は、Oracle サービスにお問い合わせください。

- 2 BIOS 非揮発性データストア内のパラメータを **Oracle ILOM BIOS** 構成ファイルと同期するには、次のいずれかの操作を実行して、管理対象 **x86 Sun** サーバーの電源を再投入します。

- Web インタフェースで、「Host Management」 > 「Power Control」 > 「Power Cycle」の順にクリックします。
- CLI で、次を入力します: **reset /System**

Oracle ILOM は、BIOS 非揮発性データストアに設定されたパラメータを取得し、それらを Oracle ILOM BIOS 構成ファイルに保存して、「Configuration Sync Status」の状態を更新します。

参考 関連情報:

- 230 ページの「BIOS 構成の出荷時のデフォルトへのリセット」
- 231 ページの「SP および Oracle ILOM BIOS の出荷時のデフォルトへのリセット」
- 232 ページの「BIOS 構成のバックアップ」
- 233 ページの「BIOS 構成の復元」

▼ BIOS 構成の出荷時のデフォルトへのリセット

始める前に

- 228 ページの「BIOS 構成タスクの要件」を確認してください。
- BIOS 非揮発性データストアのパラメータを出荷時のデフォルトにリセットするには、次のいずれかの操作を実行します:
 - Web インタフェースで、「System Management」 > 「BIOS」の順にクリックし、「Reset To Defaults」リストボックスから「Factory」を選択して「Save」をクリックします。

- CLI で、次を入力します: **set /System/BIOS reset_to_defaults=factory**

Oracle ILOM は、非揮発性データストア内の BIOS 設定パラメータを出荷時のデフォルトにリセットします。出荷時のデフォルトのパラメータが適用されると、「Reset To Defaults」の値は「None」に戻ります。

参考 関連情報:

- 229 ページの「BIOS 構成同期ステータスの表示と構成パラメータの同期」
- 231 ページの「SP および Oracle ILOM BIOS の出荷時のデフォルトへのリセット」
- 232 ページの「BIOS 構成のバックアップ」
- 233 ページの「BIOS 構成の復元」

▼ SP および Oracle ILOM BIOS の出荷時のデフォルトへのリセット

始める前に

- 228 ページの「BIOS 構成タスクの要件」を確認してください

Oracle ILOM CLI または Web インタフェースから Oracle ILOM の構成およびホスト BIOS の構成を出荷時のデフォルトにリセットするには、これらの手順に従います。

- 1 次のいずれかを実行して、管理対象 Oracle x86 サーバー上のホストオペレーティングシステムの電源を切断します:
 - Web インタフェースで、「Host Management」 > 「Power Control」 > 「Power Cycle」の順にクリックします。
 - CLI で、次を入力します: **stop -force /System**
- 2 次のいずれかを実行して、BIOS 非揮発性データストア内のパラメータを出荷時のデフォルトにリセットします:
 - Web インタフェースで、「System Management」 > 「BIOS」の順にクリックし、「Reset To Defaults To Factory」リストボックスから「Factory」を選択して「Save」をクリックします。
 - CLI で、次を入力します: **set /System/BIOS reset_to_defaults=factory**

注 - /System/BIOS の reset_to_defaults が *factory* から *none* に変化するまで待つてから、手順 3 に進んでください。ホスト BIOS 非揮発性データストアに出荷時のデフォルトが適用されると、reset_to_default の値は *none* に戻ります。

- 3 次のいずれかを実行して、Oracle ILOM の構成を出荷時のデフォルトにリセットします:

- Web インタフェースで、「ILOM Administration」 > 「Configuration Management」 > 「Reset Defaults」の順にクリックし、「Reset Defaults」リストボックスから「Factory」を選択して「Reset Defaults」をクリックします。
 - CLI で、次を入力します: **set /SP reset_to_default=factory**
- 4 次のいずれかを実行して、Oracle ILOM SP の電源を再投入します:
- Web インタフェースで、「Host Management」 > 「Power Control」 > 「Reset」の順にクリックします。
 - CLI で、次を入力します: **reset /SP**

Oracle ILOM は、BIOS 構成パラメータを出荷時のデフォルトにリセットし、「Sync Status」の状態を「None」に戻します。

参考 関連情報:

- 229 ページの「BIOS 構成同期ステータスの表示と構成パラメータの同期」
- 230 ページの「BIOS 構成の出荷時のデフォルトへのリセット」
- 232 ページの「BIOS 構成のバックアップ」
- 233 ページの「BIOS 構成の復元」

▼ BIOS 構成のバックアップ

始める前に

- 228 ページの「BIOS 構成タスクの要件」を確認してください。
- 通常、BIOS 構成のバックアップ操作が完了するには2-3分かかります。

BIOS 非揮発性データストア内のパラメータを Oracle ILOM BIOS 構成ファイルにバックアップするには、この手順に従います。

- 1 BIOS 構成をバックアップするには、次のいずれかを実行します:
- Web インタフェースで、「System Management」 > 「BIOS」の順にクリックし、「Backup」セクションの「Transfer Method」リストボックスからオプションを選択し、その転送方法の必須パラメータを指定して「Start Backup」をクリックします。
 - CLI で、次を入力します:

```
set dump_uri transfer_method://username:password@ipaddress_or_hostname  
/directorypath/filename
```

ここでは:
 - *transfer_method* には、tftp、ftp、sftp、scp、http、https のいずれかを入力します。

- *username* には、選択した転送方法のサーバーのユーザーアカウントの名前を入力します。ユーザー名は *scp*、*sftp*、および *ftp* に必要です。ユーザー名は *tftp* には不要で、*http* および *https* では省略可能です。
- *password* には、選択した転送方法のサーバーのユーザーアカウントパスワードを入力します。パスワードは *scp*、*sftp*、および *ftp* に必要です。パスワードは *tftp* には使用されず、*http* と *https* では省略可能です。
- *ipaddress_or_hostname* には、選択した転送方法のサーバーの IP アドレスまたはホスト名を入力します。
- *directorypath* には、転送方法のサーバー上のファイルの格納場所を入力します。
- *filename* には、バックアップ構成ファイルに割り当てられた名前を入力します (例: *foo.xml*)。

2 Oracle ILOM による BIOS のバックアップ操作が完了するまで待機します。

Oracle ILOM は、BIOS 非揮発性データストアの構成ファイルのコピーを取得し、それを Oracle ILOM のファイルシステムに保存します。

参考 関連情報:

- [223 ページの「Web および CLI: BIOS プロパティ」](#)
- [表 73](#)
- [229 ページの「BIOS 構成同期ステータスの表示と構成パラメータの同期」](#)
- [230 ページの「BIOS 構成の出荷時のデフォルトへのリセット」](#)
- [231 ページの「SP および Oracle ILOM BIOS の出荷時のデフォルトへのリセット」](#)
- [233 ページの「BIOS 構成の復元」](#)

▼ BIOS 構成の復元

始める前に

- [228 ページの「BIOS 構成タスクの要件」](#)を確認してください。
- Oracle ILOM 構成ファイルのブートデバイスセクション内のデータは読み取り専用で、BIOS 非揮発性データストアに復元されるパラメータには影響しません。
- 通常、BIOS 構成の復元操作が完了するには 2-3 分かかります。

Oracle ILOM BIOS 構成ファイル内のパラメータを BIOS 非揮発性データストアに復元するには、この手順に従います。

1 BIOS 構成を復元するには、次のいずれかを実行します:

- Web インタフェースで、「System Management」 > 「BIOS」の順にクリックし、復元オプションを選択し、転送方法オプションを選択し、その転送方法の必須パラメータを指定して「Start Restore」をクリックします。

- CLI で、次を入力します:

```
set load_uri=restore_option/transfer_method://username:password@ipaddress_
or_hostname/directorypath/filename
```

ここでは:

- *restore option* には、all、config-only、bootlist-only のいずれかを入力します。
- *transfer_method* には、tftp、ftp、sftp、scp、http、https のいずれかを入力します。
- *username* には、選択した転送方法のサーバーのユーザーアカウント名を入力します。ユーザー名は scp、sftp、および ftp に必要です。ユーザー名は tftp には不要で、http および https では省略可能です。
- *password* には、選択した転送方法のサーバーのユーザーアカウントパスワードを入力します。パスワードは scp、sftp、および ftp に必要です。パスワードは tftp には使用されず、http と https では省略可能です。
- *ipaddress_or_hostname* には、選択した転送方法のサーバーの IP アドレスまたはホスト名を入力します。
- *directorypath* には、転送方法のサーバー上の Oracle ILOM 構成ファイルの格納場所 (/System/BIOS/Config) を入力します。
- *filename* には、Oracle ILOM 構成ファイルに割り当てられた名前を入力します (例: foo.xml)。

注 - 保留中の BIOS 構成復元操作を取り消すには、次を入力します: set
action=cancel

- 2 Oracle ILOM による復元操作が完了するまで待機します。

Oracle ILOM は、Oracle ILOM BIOS 構成ファイルの BIOS 構成パラメータを BIOS 非揮発性データストアにエクスポートし、「Restore Status」の状態を更新します。

- 3 「Restore Status」の状態を確認して、復元操作が正常に完了したかどうかを判定します。

「Restore Status」の状態を説明する一覧については、223 ページの「Web および CLI: BIOS プロパティ」を参照してください。

注 - 復元操作の結果は、Oracle ILOM イベントログ (/SP/logs/event list) に記録されます。

参考 関連情報

- 223 ページの「Web および CLI: BIOS プロパティ」
- 表 73
- 229 ページの「BIOS 構成同期ステータスの表示と構成パラメータの同期」

- 230 ページの「BIOS 構成の出荷時のデフォルトへのリセット」
- 231 ページの「SP および Oracle ILOM BIOS の出荷時のデフォルトへのリセット」
- 232 ページの「BIOS 構成のバックアップ」

シャreshiブレードストレージリソースのSASゾーン機能

説明	リンク
シャreshiレベルのストレージデバイスのゾーン作成でサポートされる管理オプションの詳細は、このセクションを参照してください。	■ 238 ページの「シャreshiレベルのSAS-2 対応リソースのゾーン管理」
Oracle ILOM Sun Blade Zone Manager のプロパティの詳細は、このセクションを参照してください。	■ 239 ページの「Sun Blade Zone Manager のプロパティ」
SASゾーンの構成パラメータの保存、バックアップ、および回復に関する重要な情報については、このセクションを参照してください。	■ 248 ページの「SASゾーンの割り当てに関する重要な考慮事項」
Sun Blade Zone Manager を有効にしてSASゾーンの割り当てを作成する手順については、このセクションを参照してください。	■ 249 ページの「ゾーン機能の有効化およびSAS-2ゾーンの割り当ての作成」
既存のストレージの割り当てを表示または変更する手順については、このセクションを参照してください。	■ 266 ページの「既存のSAS-2 ストレージリソースの割り当ての管理」
保存されているすべてのストレージの割り当てを出荷時のデフォルトにリセットする場合は、このセクションを参照してください。	■ 275 ページの「Sun Blade Zone Manager の割り当てを出荷時のデフォルトにリセットする」
必要に応じて、帯域内管理のパスワードをリセットする場合は、このセクションを参照してください。	■ 276 ページの「サードパーティーの帯域内管理でのゾーンのパスワードを出荷時のデフォルトにリセットする」

シャーシレベルの SAS-2 対応リソースのゾーン管理

Oracle ILOM は、Sun ブレードシャーシシステムに取り付けられているシャーシレベルの SAS-2 ストレージデバイスに対してゾーン管理をサポートしています。Sun ブレードのシャーシレベルのストレージリソースへのアクセスを管理するために、Oracle ILOM Sun Blade Zone Manager またはサードパーティー製の帯域内アプリケーションを使用することを選択できます。詳細は、次を参照してください:

- 238 ページの「サードパーティー製の帯域内管理アプリケーションを使用したゾーン管理」
- 238 ページの「Oracle ILOM Sun Blade Zone Manager を使用したゾーン管理」
- 239 ページの「管理可能な SAS-2 ゾーン対応デバイス」

サードパーティー製の帯域内管理アプリケーションを使用したゾーン管理

サードパーティー製の帯域内管理アプリケーションを使用した、シャーシレベルのストレージデバイスのアクセスの管理が使用している環境でサポートされている場合は、Oracle ILOM の Sun Blade Zone Manager の状態が無効になっている (デフォルト) ことを確認するようにしてください。帯域内管理のパスワードを出荷時のデフォルトにリセットする必要がある場合は、Oracle ILOM でこのパスワードをリセットできます。手順については、276 ページの「サードパーティーの帯域内管理でのゾーンのパスワードを出荷時のデフォルトにリセットする」を参照してください。

Oracle ILOM Sun Blade Zone Manager を使用したゾーン管理

Sun Blade Zone Manager が Oracle ILOM CMM で有効にされている場合は、シャーシに取り付けられている Sun ブレード CPU サーバーに対するシャーシレベルの SAS-2 ストレージのアクセス権を管理できます。Oracle ILOM Sun Blade Zone Manager の使用方法については、次のトピックを参照してください:

- 239 ページの「管理可能な SAS-2 ゾーン対応デバイス」
- 239 ページの「Sun Blade Zone Manager のプロパティ」
- 248 ページの「SAS ゾーンの割り当てに関する重要な考慮事項」
- 249 ページの「ゾーン機能の有効化および SAS-2 ゾーンの割り当ての作成」
- 266 ページの「既存の SAS-2 ストレージリソースの割り当ての管理」
- 275 ページの「Sun Blade Zone Manager の割り当てを出荷時のデフォルトにリセットする」

管理可能な SAS-2 ゾーン対応デバイス

Oracle ILOM CMM は、Sun ブレードシャーシシステム内の次のデバイスを管理可能な SAS-2 ゾーン対応デバイスとして認識します:

- SAS-2 RAID 拡張モジュール (REM) を装備した Sun ブレード CPU サーバー
- Sun ブレードシャーシシステムの Network Express Module (NEM)
- Sun ブレードストレージサーバー (Sun Blade Storage Module M2 など)

注 - Oracle ILOM は、次に対するゾーン管理をサポートしません: (1) Sun ブレード CPU サーバーに取り付けられている内部ストレージモジュール、(2) Sun ストレージブレード上のファブリック拡張モジュール (FMOD)、または (3) NEM の外部 SAS-2 ポートを使用して Sun ブレードシャーシシステムに接続されている外部ネットワーク SAS-2 ストレージリソース。

注 - Sun Blade Zone Manager の CLI は、サポート対象外の管理できない SAS-2 ストレージデバイスが存在することを認識または表示しません。ただし、Sun Blade Zone Manager の Web インタフェースは、サポート対象外の管理できない SAS-2 ストレージデバイスが存在することを認識および表示する場合があります。この場合、Sun Blade Zone Manager の Web インタフェース内の SAS-2 以外のストレージデバイスは、SAS-2 以外のリソースとして表示されます。

Sun Blade Zone Manager のプロパティ

Oracle ILOM は、シャーシレベルの SAS-2 ストレージデバイスへのアクセス権を設定および管理するための使いやすい一連のプロパティを提供しています。詳細は、次を参照してください:

- 239 ページの「Sun Blade Zone Manager Web: プロパティ」
- 246 ページの「Sun Blade Zone Manager の CLI: ターゲットとプロパティ」

Sun Blade Zone Manager Web: プロパティ

「Sun Blade Zone Manager Settings」ページは、Oracle ILOM CMM の Web インタフェースから、「System Management」>「SAS Zoning」をクリックすることによりアクセスできます。「Sun Blade Zone Manager Settings」ページには、SAS ゾーンのアクセス権の有効化、設定、および管理を行うための次のオプションがあります:

- 240 ページの「Sun Blade Zone Manager: 状態」
- 240 ページの「Whole Chassis Setup: Quick Setup」
- 245 ページの「Full Resource Control: Detailed Setup」

- [246 ページの「ゾーンのリセット: Reset All」](#)

Sun Blade Zone Manager: 状態

Oracle ILOM CMM の Web インタフェースでは、Sun Blade Zone Manager の状態は、「Sun Blade Zone Manager Settings」ページに表示されます。

この状態を有効にすると、Sun Blade Zone Manager によって、シャーシに取り付けられている SAS-2 ストレージデバイスに対するテンプレートベースの機能 (Quick Setup) またはカスタムのゾーン機能 (Detailed Setup) が提供されます。

この状態を無効 (デフォルト) にすると、Oracle ILOM は、シャーシに取り付けられている SAS-2 ストレージデバイスへのアクセス権を管理できなくなり、「Sun Blade Zone Manager Settings」ページのビューから「Quick Setup」および「Detailed Setup」オプションが非表示になります。

Sun Blade Zone Manager の状態を有効にする手順については、[250 ページの「Sun Blade Zone Manager にアクセスして有効にする」](#) を参照してください。

Whole Chassis Setup: Quick Setup

Web インタフェースの Whole Chassis Setup 機能は、通常、すべてのシャーシレベルの SAS-2 ストレージデバイスのゾーンへのアクセスを最初に設定するときに使用します。この機能は、次の Quick Setup のゾーン機能オプションを提供します:

- [240 ページの「オプション 1: 個別のディスクへの割り当て \(Quick Setup\)」](#)
- [241 ページの「オプション 2: 隣接する個別のディスクへの割り当て \(Quick Setup\)」](#)
- [242 ページの「オプション 3: 個別のストレージブレードへの割り当て \(Quick Setup\)」](#)
- [243 ページの「オプション 4: 隣接するストレージブレードへの割り当て \(Quick Setup\)」](#)

オプション 1: 個別のディスクへの割り当て (Quick Setup)

「Quick Setup」ダイアログに表示される最初のゾーンオプションは、ラウンドロビンアルゴリズムを使用して、シャーシ内のすべての CPU ブレードサーバーにストレージの所有権を均等に割り当てます。

オプション 1 は、単一のストレージブレードサーバーに障害が発生したり、取り外されたりしてもすべてのストレージアレイが停止することがない耐障害シャーシシステムの運用にもっとも適しています。

Quick Setup

Select how you would like all chassis storage resources allocated and click 'Save':

1. Assign per individual disks.
 2. Assign per adjacent individual disks.
 3. Assign per storage blade.
 4. Assign per adjacent storage blade.

SUN BLADE 6000 MODULAR SYSTEM - bur_02_core_ilom

Slot 0	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7	Slot 8	Slot 9
Server Blade Sun Blade X6270 M2	Server Blade Sun Blade X6270 M2	Storage Blade Sun Blade Storage Module M2	Server Blade Sun Blade X6270 M2	Server Blade Sun Blade X6270 M2	Storage Blade Sun Blade Storage Module M2	Storage Blade Sun Blade Storage Module M2	Server Blade Sun Blade X6270 M2	Storage Blade Sun Blade Storage Module M2	Storage Blade Sun Blade Storage Module M2
		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1			HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1	HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1	HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1
		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty			empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty	empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty	empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty

NEM Slot 0				NEM Slot 1					
SAS NEM NEM-2	EXT 0	EXT 1	EXT 2	EXT 3	SAS NEM NEM-2	EXT 0	EXT 1	EXT 2	EXT 3

NAC name:	/CH/BL9/FMOD1
Disk type:	SAS
WWN:	80205010.33333336 80205010.33333337

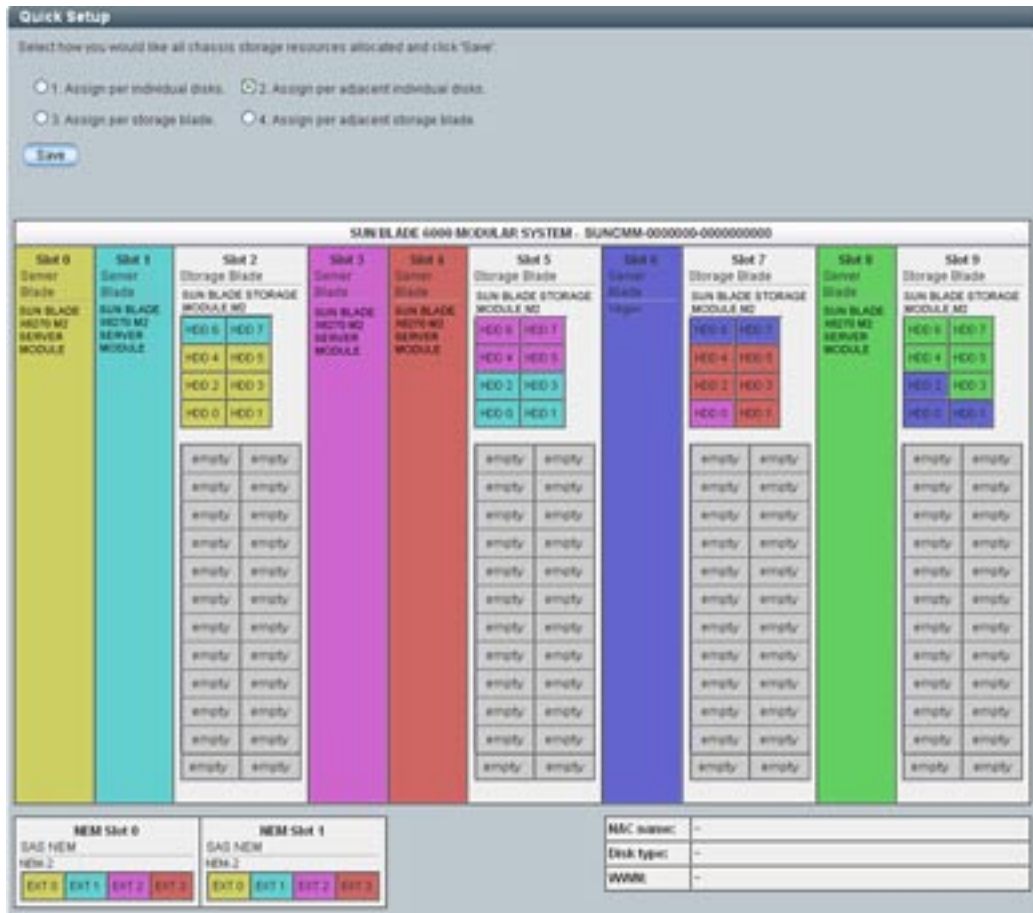
注- 「Quick Setup」ダイアログに表示されている空のスロットは、空のシャーシブレードスロット (何も取り付けられていない) を表しています。

オプション2: 隣接する個別のディスクへの割り当て (Quick Setup)

「Quick Setup」ダイアログに表示される2番目のゾーン割り当てオプションは、隣接するCPUブレードサーバー間でブレードストレージディスクの数を均等に分割します。

オプション2は、隣接する各CPUブレードサーバーにできるだけ同じ数のストレージディスクを割り当てることを試みます。CPUブレードに隣接するストレージブレードがない場合、Sun Blade Zone Managerはできるだけ近くのストレージブレードのストレージディスクを割り当てます。

隣接するストレージディスクへのCPUブレードの割り当ては次の場合にもっとも適しています:1)ストレージブレードサーバーよりCPUブレードサーバーが多いSunブレードシャーシシステム、および2)各CPUブレードサーバー間でストレージリソースを均等に配備する場合。



オプション3:個別のストレージブレードへの割り当て(Quick Setup)

「Quick Setup」ダイアログに表示される3番目のゾーン割り当てオプションは、SunブレードシャーシシステムでCPUブレードサーバーをスキャンして(スロット0から開始)、利用可能なもっとも近いストレージブレードのストレージディスクを割り当てます。

オプション3は、ストレージブレードサーバーとCPUブレードサーバーの数が同一のシャーシシステム、またはCPUブレードサーバーよりストレージブレードサーバーが多いシャーシシステムにもっとも適しています。それ以外で、シャーシ内でCPUブレードサーバーよりストレージブレードサーバーのほうが少ない場合、Sun Blade Zone Manager はいくつかのCPUブレードサーバーにストレージを割り当てることができません。

Quick Setup

Select how you would like all chassis storage resources allocated and click 'Save'.

1. Assign per individual disks. 2. Assign per adjacent individual disks.
 3. Assign per storage blade. 4. Assign per adjacent storage blade.

SUN BLADE 6000 MODULAR SYSTEM - bur_02_core_ilom

Slot 0	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7	Slot 8	Slot 9
Server Blade Sun Blade X6270 M2	Server Blade Sun Blade X6270 M2	Storage Blade Sun Blade Storage Module M2	Server Blade Sun Blade X6270 M2	Server Blade Sun Blade X6270 M2	Storage Blade Sun Blade Storage Module M2	Storage Blade Sun Blade Storage Module M2	Server Blade Sun Blade X6270 M2	Storage Blade Sun Blade Storage Module M2	Storage Blade Sun Blade Storage Module M2
		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1			HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1	HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1	HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1
		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty			empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty	empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty	empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty

NEM Slot 0 SAS NEM NEM-2 EXT 0 EXT 1 EXT 2 EXT 3				NEM Slot 1 SAS NEM NEM-2 EXT 0 EXT 1 EXT 2 EXT 3				NAC name: /CH/BL9/FMOD1	
								Disk type: SAS	
								WWN: 80205010.33333336 80205010.33333337	

オプション4:隣接するストレージブレードへの割り当て(Quick Setup)

「Quick Setup」ダイアログに表示される4番目のゾーン割り当てオプションは、隣接するスロットにストレージブレードがあるCPUブレードサーバーをSunブレードシャーシシステムでスキャンします。CPUブレードサーバーに隣接するシャーシスロットにストレージブレードサーバーがない場合、Sun Blade Zone ManagerはそのCPUブレードサーバーにストレージを割り当てません。

オプション4は、次のシャーシシステムにもっとも適しています:(1) ストレージブレードサーバーと CPU ブレードサーバーの数が同じである、および(2) ストレージブレードサーバーに隣接するシャーシスロットに各 CPU ブレードサーバーが取り付けられている。

Quick Setup

Select how you would like all chassis storage resources allocated and click 'Save'.

1. Assign per individual disks.
 2. Assign per adjacent individual disks.
 3. Assign per storage blade.
 4. Assign per adjacent storage blade.

SUN BLADE 6000 MODULAR SYSTEM - bur_02_core_ilom

Slot 0	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7	Slot 8	Slot 9
Server Blade Sun Blade X8270 M2	Server Blade Sun Blade X8270 M2	Storage Blade Sun Blade Storage Module M2	Server Blade Sun Blade X8270 M2	Server Blade Sun Blade X8270 M2	Storage Blade Sun Blade Storage Module M2	Storage Blade Sun Blade Storage Module M2	Server Blade Sun Blade X8270 M2	Storage Blade Sun Blade Storage Module M2	Storage Blade Sun Blade Storage Module M2
		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1			HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1	HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1	HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1
		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty			empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty	empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty	empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty

NEM Slot 0

SAS NEM
NEM-2

EXT 0 | EXT 1 | EXT 2 | EXT 3

NEM Slot 1

SAS NEM
NEM-2

EXT 0 | EXT 1 | EXT 2 | EXT 3

NAC name: /CH/BL9/FMOD1

Disk type: SAS

WWN: 80205010:33333336 80205010:33333337

注 - NEM0 および NEM1 が取り付けられていると、これらの NEM ターゲットが Zone Manager に表示されますが、SAS-2 ネットワークストレージデバイスへの外部 NEM 接続は、Sun Blade Zone Manager でサポートされておらず、表示されません。

シャーシ全体に SAS ゾーンの割り当てを作成する手順については、[252 ページ](#)の「シャーシ全体へのストレージの割り当て: Quick Setup (Web)」を参照してください。

Full Resource Control: Detailed Setup

Web インタフェースの Full Resource Control: Detailed Setup オプションでは、ストレージリソースに新しい割り当てを作成したり、既存のストレージリソースの割り当てを変更したりできます。たとえば、Full Resource Control: Detailed Setup オプションを使用すると、次を行うことを選択できます：

- ストレージの割り当てを CPU ブレードサーバーに追加するために、色分けされたサーバーグループの外側にあるコンポーネントをクリックします。
- CPU ブレードサーバーに割り当てられているストレージリソースの割り当てを削除するために、色分けされたサーバーグループ内のコンポーネントをクリックします。
- 単一のリソースの割り当てを 1 つ以上の CPU ブレードサーバー間で共有します。

Modify Group

Indicated below is your selected group of components that currently have assigned access. Click on those within the group that you would like to remove access to. Click on any components outside the group that you want added. When you are ready to apply the changes, click Save.

Save Cancel

SUN BLADE 6000 BR/CLAR SYSTEM - 8LPCVMB-0000000-000000000

Slot 0	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7	Slot 8	Slot 9
Server Blade SUN BLADE M270 M2 SERVER MODULE	Server Blade SUN BLADE M270 M2 SERVER MODULE	Storage Blade SUN BLADE STORAGE MODULE M0	Server Blade SUN BLADE M270 M2 SERVER MODULE	Server Blade SUN BLADE M270 M2 SERVER MODULE	Storage Blade SUN BLADE STORAGE MODULE M2	Server Blade SUN BLADE M270 M2 SERVER MODULE	Storage Blade SUN BLADE STORAGE MODULE M0	Server Blade SUN BLADE M270 M2 SERVER MODULE	Storage Blade SUN BLADE STORAGE MODULE M2
		HEC 0 HEC 7 HEC 4 HEC 5 HEC 2 HEC 3 HEC 6 HEC 1			HEC 8 HEC 9 HEC 4 HEC 5 HEC 2 HEC 3 HEC 6 HEC 1		HEC 6 HEC 7 HEC 4 HEC 5 HEC 2 HEC 3 HEC 8 HEC 1		HEC 8 HEC 7 HEC 4 HEC 5 HEC 2 HEC 3 HEC 6 HEC 1
		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty			empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty

MEM Slot 0		MEM Slot 1	
SAD MEM MEM 2	SAD MEM MEM 2	SAD MEM MEM 2	SAD MEM MEM 2
EXT 0 EXT 1 EXT 2 EXT 3	EXT 0 EXT 1 EXT 2 EXT 3	EXT 0 EXT 1 EXT 2 EXT 3	EXT 0 EXT 1 EXT 2 EXT 3

N/C Name:	-
Disk Type:	-
WWN:	-

リソースの割り当てを作成または変更するために「Detailed Setup」オプションを使用する手順については、次を参照してください:

- 254 ページの「単一のブレードサーバーへのストレージリソースの割り当て: Detailed Setup (Web)」
- 259 ページの「複数のブレードサーバーへの単一のストレージリソースの割り当て: Detailed Setup (Web)」
- 269 ページの「既存のブレードグループの割り当ての変更 (Web)」

ゾーンのリセット:Reset All

Sun Blade Zone Manager の状態を有効にすると、ゾーン構成を出荷時のデフォルトにリセットするオプションが「Sun Blade Zone Manager Settings」ページに表示されます (「System Management」 > 「SAS Zoning」)。

Sun Blade Zone Manager のパラメータを出荷時のデフォルトにリセットする手順については、275 ページの「ゾーンの割り当てを出荷時のデフォルトにリセットする (Web)」を参照してください。

Sun Blade Zone Manager の CLI: ターゲットとプロパティ

Oracle ILOM CMM の CLI を使用すると、/STORAGE/sas_zoning ネームスペースの下にあるゾーンのターゲットおよびプロパティにアクセスできます。

SAS ゾーンのプロパティ	値	デフォルト値	説明
zone_management_state=	<i>disabled</i> <i>enabled</i>	Disabled	無効に設定すると、Sun Blade Zone Manager は SAS-2 シャーシストレージリソースを管理できません。 有効に設定すると、Sun Blade Zone Manager によって、シャーシに取り付けられている SAS-2 リソースに対するテンプレートベースの機能またはカスタムのゾーン機能が提供されます。
reset_password_action=	<i>true</i>		true に設定すると、CMM の帯域内管理のゾーンのパスワードが、出荷時のデフォルト (すべてゼロ) に設定されます。
reset_access_action=	<i>true</i>		true に設定すると、CMM に現在保存されているストレージリソースの割り当てのパラメータが、出荷時のデフォルトに設定されます。

ゾーン機能が有効になっている場合、SAS-2 対応のブレードと NEM が CLI ターゲットとして /STORAGE/sas_zoning の下に表示されます。例:

```
-> show /STORAGE/sas_zoning
```

Targets

```
BL0
BL6
BL7
BL8
BL9
NEM0
NEM1
```

Properties

```
zone_management_state = enabled
reset_password_action = (Cannot show property)
reset_access_action = (Cannot show property)
```

Commands:

```
cd
set
show
```

注 - NEM0 および NEM1 が取り付けられていると、これらの NEM ターゲットが Zone Manager に表示されますが、現時点では、Sun Blade Zone Manager で外部 SAS 接続はサポートされていません。

ブレードサーバー上の SAS-2 対応ストレージデバイスが、sas_zoning/BLn の下にターゲットとして表示されます。例:

```
-> show /STORAGE/sas_zoning/BL9
```

Targets:

```
HDD0
HDD2
HDD3
HDD5
```

ブレードターゲット (BLn) またはストレージデバイス (HDDn) ターゲットの下にある利用可能な SAS ゾーンのプロパティには、次のものがあります:

ブレードとストレージのプロパティ	SAS ゾーンのターゲット	説明
add_storage_access=	/BLn	/sas_zoning/BLn ターゲットの下にある add_storage_access= プロパティは、CPU ブレードサーバーにストレージを割り当てるために使用します。
remove_storage_access=	/BLn	/sas_zoning/BLn ターゲットの下にある remove_storage_access= プロパティは、CPU ブレードサーバーからストレージを削除するために使用します。

ブレードとストレージのプロパティ	SASゾーンのターゲット	説明
add_host_access=	/BLn/HDDn	/sas_zoning/BLn/HDDn ターゲットの下にある add_host_access= プロパティは、CPU ブレードサーバーにストレージを割り当てるために使用します。
remove_host_access=	/BLn/HDDn	/sas_zoning/BLn/HDDn ターゲットの下にある remove_host_access= プロパティは、CPU ブレードサーバーからストレージを削除するために使用します。

ストレージリソースの割り当てを Oracle ILOM の CLI から管理する手順については、次を参照してください:

- 263 ページの「SAS-2 ゾーンの割り当ての手動での作成 (CLI)」
- 273 ページの「既存のストレージの割り当ての表示と変更 (CLI)」
- 276 ページの「ゾーンの割り当てを出荷時のデフォルトにリセットする (CLI)」
- 277 ページの「ゾーンのパスワードのリセット (CLI)」

SASゾーンの割り当てに関する重要な考慮事項

- 248 ページの「ストレージの割り当ての保存」
- 249 ページの「SAS-2 ゾーンの割り当てのバックアップおよび回復」

ストレージの割り当ての保存

ブレードに対するストレージの割り当てを保存する場合は、次を考慮してください:

- Oracle ILOM に保存されるストレージの割り当ては、シャーシに現在取り付けられているハードウェア (SAS-2 NEM またはストレージブレード) に基づいています。シャーシのハードウェア構成を変更すると、ストレージブレードグループが失われることがあります。このため、Oracle ILOM でシャーシ内のすべてのストレージの割り当てをバックアップするようにしてください。詳細は、249 ページの「SAS-2 ゾーンの割り当てのバックアップおよび回復」を参照してください。

注-シャーシコンポーネントのホットプラグ (NEM、ストレージブレードなど) も、ストレージブレードグループの割り当てに影響することがあります。NEM やストレージブレードをホットプラグした場合の影響については、Oracle Sun ストレージブレードまたは NEM ハードウェアのドキュメントを参照してください。

- 「Save」操作を実行している間は、「Sun Blade Zone Manager」ダイアログ (「Modify Group」または「New Assignments」) を開いておく必要があります。「Save」操作が行われているときに「Sun Blade Zone Manager」ダイアログを閉じると、ストレージブレードグループの一部のみが保存されます。

- 「Save」操作が行われている間は、ストレージブレードグループの一部であるシャーシハードウェアコンポーネントを削除したり、電源を再投入したりしないでください。これを行うと、グループの割り当てが正常に保存されません。

SAS-2 ゾーンの割り当てのバックアップおよび回復

Oracle ILOM には、次を行うことができるバックアップおよび復元の機能があります: (1) Oracle ILOM の構成ファイルに保存されているすべてのパラメータのバックアップコピーの作成、および (2) Oracle ILOM の構成ファイルのバックアップコピーの復元。Oracle ILOM の構成ファイルのバックアップコピーの作成、またはバックアップコピーの復元を行う方法については、237 ページの「シャーシブレードストレージリソースの SAS ゾーン機能」を参照してください。

ゾーン機能の有効化および SAS-2 ゾーンの割り当ての作成

- 249 ページの「シャーシのハードウェア要件」
- 250 ページの「Sun Blade Zone Manager にアクセスして有効にする」
- 252 ページの「シャーシ全体へのストレージの割り当て: Quick Setup (Web)」
- 254 ページの「単一のブレードサーバーへのストレージリソースの割り当て: Detailed Setup (Web)」
- 259 ページの「複数のブレードサーバーへの単一のストレージリソースの割り当て: Detailed Setup (Web)」
- 263 ページの「SAS-2 ゾーンの割り当ての手動での作成 (CLI)」

シャーシのハードウェア要件

- PCIe 2.0 準拠のミッドプレーンが、Sun Blade 6000 シャーシに存在する必要があります。これを確認する方法の詳細については、『Sun Blade 6000 モジュラーシステムプロダクトノート』を参照してください。
- 最低でもソフトウェアリリース 3.2.1 が CMM にインストールされている必要があります。このリリースには、SAS-2 をサポートする最低のバージョン (3.0.10.15a) の Oracle ILOM CMM ファームウェアと、Sun Blade Zone Manager が含まれています。
- すべての SAS-2 ストレージデバイス (SAS-2 REM を装備したブレードサーバーモジュール、SAS-2 NEM、および SAS-2 ストレージモジュール) が適切に取り付けられ、Sun ブレードシャーシシステムで電源が投入されている必要があります。

注-SAS-2 ストレージデバイスの状態が障害状態である場合、Sun Blade Zone Manager は障害が発生した SAS-2 ストレージデバイスを認識できない場合があります。Oracle ILOM を使用したハードウェア障害の識別および解決の詳細は、を参照してください。

- SAS-2 NEM は、ゾーン機能をサポートしているファームウェアバージョンレベルである必要があります。NEM のプロダクトノートで、バージョン情報と利用可能な更新を確認してください。
- Oracle ILOM CMM の初期設定および構成が完了している必要があります。Oracle ILOM CMM への管理接続の確立の詳細は、11 ページの「Oracle ILOM への管理接続の設定とログイン」を参照してください。

▼ Sun Blade Zone Manager にアクセスして有効にする

始める前に Oracle ILOM で Sun Blade Zone Manager を有効にすると、ストレージリソース (HDD、FMOD、外部 SAS ポート) にアクセス可能な SAS ドメイン内の CPU ブレードサーバーを制限する方法を使用できるようになります。

始める前に

- Oracle ILOM で SAS ゾーンのプロパティを変更するには Admin (a) の役割が必要です。
- 249 ページの「シャーシのハードウェア要件」を確認します。
- 248 ページの「SAS ゾーンの割り当てに関する重要な考慮事項」を確認します。

注-Oracle ILOM の Web インタフェースにシャーシのストレージブレードが存在していても、「CMM Manage」メニューには表示されません。ストレージブレードサーバーに取り付けられているストレージディスクは、「System Information」 > 「Storage」ページで表示できます。Sun ストレージブレードのリソースの割り当ては、「System Management」 > 「SAS Zoning」 > 「Sun Blade Zone Manager Settings」ページで管理できます。

1 CMM の Web インタフェースから Sun Blade Zone Manager にアクセスして有効にするには、次の手順を実行します:

- a. 「System Management」 > 「SAS Zoning」をクリックします。
「Sun Blade Zone Manager Settings」ページが表示されます。

- b. 「Enabled」チェックボックスにチェックマークを付けて、「Save」をクリックし、SAS ゾーン機能を有効にします。

Sun Blade Zone Manager を有効にすると、Oracle ILOM のインタフェースを使用して、SAS-2 ゾーンの作成、表示、および設定の管理を行うことができます。

Oracle ILOM CMM サービスがまだ初期化中の場合は、次のメッセージが表示されることがあります。

```
Sun Blade Zone Manager Not Ready
The Sun Blade Zone Manager is initializing and not ready for operation.
Please wait several minutes and then refresh to check the status.
```

上記のメッセージが表示された場合は、5分間待ってから、再度実行してください。この Web インタフェースのページを閉じてから再度開くか、リフレッシュする必要があります。

- 2 CMM CLI から SAS ゾーンのプロパティを有効にするには、次を入力します:

```
set /STORAGE/SAS_zoning zone_management_state=enabled
```

- 次のメッセージが表示されます。

```
Enabling the Sun Blade Zone Manager will result in the clearing of all zoning
configuration in the installed chassis SAS hardware, and any SAS disk I/O in
progress will be interrupted.
```

```
Are you sure you want to enable the Sun Blade Zone Manager (y/n)?
```

- 続行するには、次を入力します:y

次のメッセージが表示されます。

```
Set 'zone_management_state' to 'enabled'
```

- Oracle ILOM CMM が Sun Blade Zone Manager を初期化できない場合は、次のメッセージが表示されます:

```
set: The Sun Blade Zone Manager is initializing and not ready for operation.
Please wait several minutes and try again.
```

上記のメッセージが表示された場合は、5分間待ってから、コマンドを再度実行してください。

参考 関連情報

- 252 ページの「シャーシ全体へのストレージの割り当て: Quick Setup (Web)」
- 254 ページの「単一のブレードサーバーへのストレージリソースの割り当て: Detailed Setup (Web)」
- 263 ページの「SAS-2 ゾーンの割り当ての手動での作成 (CLI)」
- 266 ページの「既存の SAS-2 ストレージリソースの割り当ての管理」

- 275 ページの「Sun Blade Zone Manager の割り当てを出荷時のデフォルトにリセットする」

▼ シャーシ全体へのストレージの割り当て:**Quick Setup (Web)**

始める前に:

- Oracle ILOM で SAS ゾーンのプロパティを変更するには Admin (a) の役割が必要です。
 - 249 ページの「シャーシのハードウェア要件」を確認します。
 - ゾーンを割り当てるこの Quick Setup の手順を実行する前に、Oracle ILOM で SAS ゾーン機能を有効にする必要があります。手順については、250 ページの「Sun Blade Zone Manager にアクセスして有効にする」を参照してください。
- 1 Web インタフェースの「Sun Blade Zone Manager Settings」ページにアクセスするには、「System Management」>「SAS Zoning」の順にクリックします。
 - 2 「Sun Blade Zone Manager」セクションで、「Quick Setup」ボタンをクリックします。警告メッセージが表示されます。



- 3 既存のゾーンの割り当てを上書きするには、「OK」をクリックします。
「Quick Setup」画面が表示されます。

Quick Setup

Select how you would like all chassis storage resources allocated and click 'Save'.

1. Assign per individual disks. 2. Assign per adjacent individual disks.
 3. Assign per storage blade. 4. Assign per adjacent storage blade.

SUN BLADE 6000 MODULAR SYSTEM - bur_02_core_ilotm

Slot 0 Server Blade Sun Blade X6270 M2	Slot 1 Server Blade Sun Blade X6270 M2	Slot 2 Storage Blade Sun Blade Storage Module M2	Slot 3 Server Blade Sun Blade X6270 M2	Slot 4 Server Blade Sun Blade X6270 M2	Slot 5 Storage Blade Sun Blade Storage Module M2	Slot 6 Storage Blade Sun Blade Storage Module M2	Slot 7 Server Blade Sun Blade X6270 M2	Slot 8 Storage Blade Sun Blade Storage Module M2	Slot 9 Storage Blade Sun Blade Storage Module M2
		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1			HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1	HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1		HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1	HDD 6 HDD 7 HDD 4 HDD 5 HDD 2 HDD 3 HDD 0 HDD 1
		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty			empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty	empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty		empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty	empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty empty

NEM Slot 0				NEM Slot 1				NAC name: /CH/BL6/FMOD22	
SAS NEM NEM-2				SAS NEM NEM-2				Disk type: SAS	
EXT 0	EXT 1	EXT 2	EXT 3	EXT 0	EXT 1	EXT 2	EXT 3	WWN: 80205010:33333336 80205010:33333337	

注 - シャーシ内の現在HDDが取り付けられていないHDDシャーシスロットは、「empty」と表示されます。空のHDDシャーシスロットは、Quick Setupでのストレージの割り当てに使用されません。

- 4 シャーシにストレージリソースを割り当てる方法を指定するために、Quick Setupのいずれかのオプションを選択します。
各 Quick Setup オプションの詳細は、240 ページの「Whole Chassis Setup: Quick Setup」を参照してください。

Quick Setup のオプションを選択すると、Sun Blade Zone Manager は、CPU ブレードサーバー、およびストレージブレードサーバーに取り付けられているストレージデ

バイス (HDD) との間のゾーンの割り当てを色分けして表示します。Sun Blade Zone Manager に NEM0 と NEM1 の外部 SAS 接続が表示されますが、これらの接続はサポートされていません。

注- 「Save」 ボタンをクリックするまで、シャーシのストレージの割り当ては保存されません。

- 5 **Quick Setup** によるシャーシのストレージの割り当てを保存するには、「Save」をクリックします。
- 6 新しく保存したブレードストレージグループの割り当てをバックアップする場合は、[249 ページの「SAS-2 ゾーンの割り当てのバックアップおよび回復」](#)を参照してください。

参考 関連情報

- [248 ページの「SAS ゾーンの割り当てに関する重要な考慮事項」](#)
- [254 ページの「単一のブレードサーバーへのストレージリソースの割り当て: Detailed Setup \(Web\)」](#)
- [259 ページの「複数のブレードサーバーへの単一のストレージリソースの割り当て: Detailed Setup \(Web\)」](#)
- [269 ページの「既存のブレードグループの割り当ての変更 \(Web\)」](#)
- [263 ページの「SAS-2 ゾーンの割り当ての手動での作成 \(CLI\)」](#)
- Sun Blade 6000 モジュラーシステムのドキュメント

▼ 単一のブレードサーバーへのストレージリソースの割り当て: **Detailed Setup (Web)**

始める前に:

- Oracle ILOM で SAS ゾーンのプロパティを変更するには Admin (a) の役割が必要です。
- [249 ページの「シャーシのハードウェア要件」](#)を確認します。
- この手順を実行する前に、Oracle ILOM で Sun Blade Zone Manager を有効にする必要があります。手順については、[250 ページの「Sun Blade Zone Manager にアクセスして有効にする」](#)を参照してください。

- 1 「Sun Blade Zone Manager Settings」 ページで、「Detailed Setup」 ボタンをクリックします。

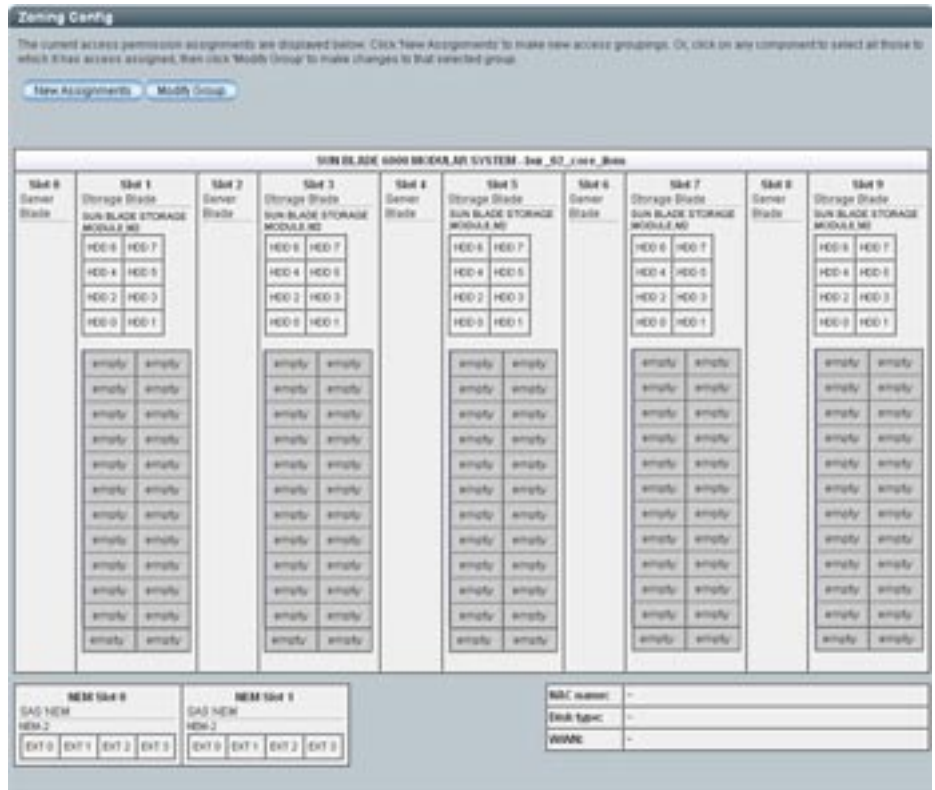
次のいずれかが表示されます:

- 「Zoning Config」 ダイアログが表示されます。手順 3 に進みます。

- ゾーンの割り当てが存在しないことを示す次のメッセージが表示されます。手順 2 に進みます。



- 2 ゾーンの割り当てが存在しないことを示すメッセージ内で、次のいずれかを実行します:
 - **Detailed Setup** オプションを使用して **SAS** ゾーンの割り当てを手動で作成する場合は、「Cancel」をクリックして手順 4 に進みます。
「Cancel」をクリックすると、「Detailed Setup Zoning Config」ページが開きます。



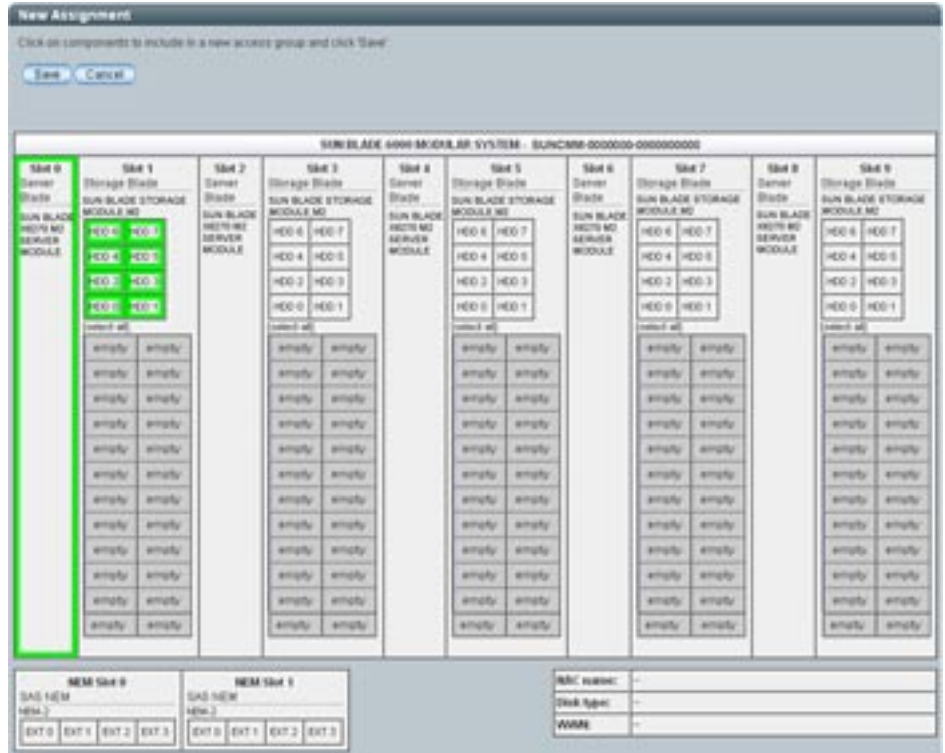
- **Sun Blade Zone Manager** の **Quick Setup** オプションを使用して初期のゾーンの割り当てを設定する場合は、「OK」をクリックして、[252 ページの「シャーシ全体へのストレージの割り当て: Quick Setup \(Web\)」](#)に進みます。
- 3 ストレージリソースを単一のブレードサーバーに割り当てるには、「**Zoning Config**」ダイアログで次の手順を実行します:
- a. 「**New Assignments**」をクリックします。
「New Assignments」ダイアログが表示されます。
 - b. ブレードサーバーをクリックし、その選択したブレードサーバーに割り当てるストレージリソース (**HDD**) をクリックします。

注 - HDD ストレージデバイスが取り付けられていないすべての HDD シャーシスロットは「empty」と表示されます。空の HDD シャーシスロットは、CPU ブレードサーバーに割り当てられません。

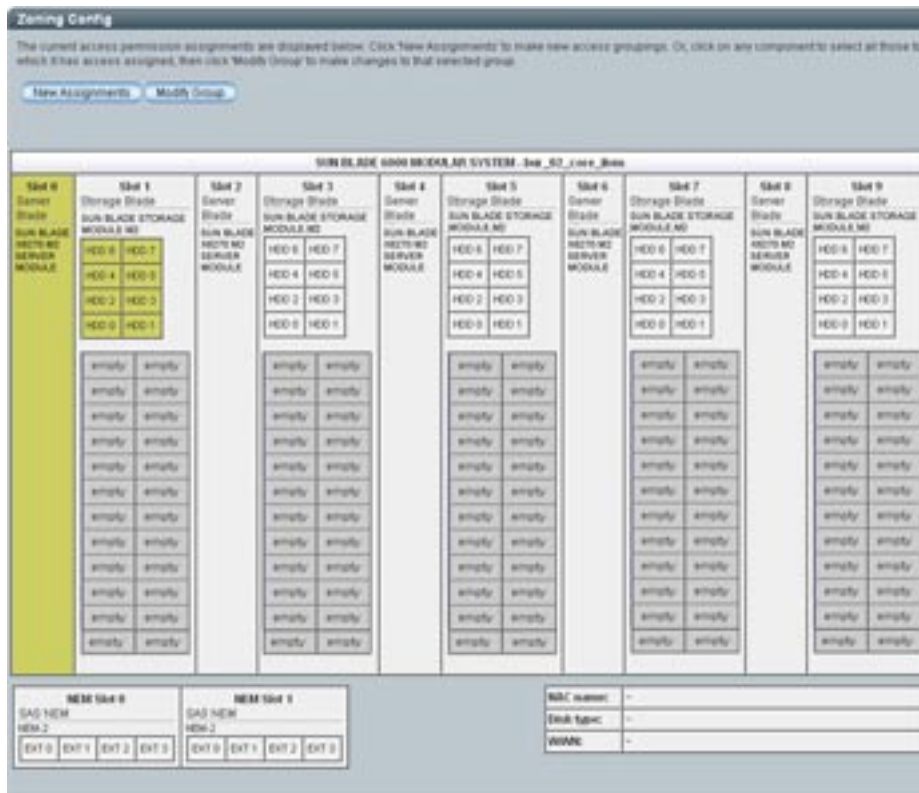


注意 - 代替の方法として、ストレージリソースを複数のブレードサーバーに割り当てることができます。ただし、サーバーでマルチパスが有効にされている必要があります。手順については、[259 ページの「複数のブレードサーバーへの単一のストレージリソースの割り当て: Detailed Setup \(Web\)」](#)を参照してください。

Sun Blade Zone Manager に NEM0 と NEM1 の外部 SAS 接続が表示されますが、これらの接続はサポートされていません。



- c. 新しく作成したブレードストレージグループの割り当てを保存するには、「Save」をクリックします。



4. 新しく保存したブレードストレージグループの割り当てをバックアップする場合は、249 ページの「SAS-2 ゾーンの割り当てのバックアップおよび回復」を参照してください。

参考 関連情報

- 269 ページの「既存のブレードグループの割り当ての変更(Web)」
- 248 ページの「SAS ゾーンの割り当てに関する重要な考慮事項」
- 259 ページの「複数のブレードサーバーへの単一のストレージリソースの割り当て: Detailed Setup (Web)」
- Sun Blade 6000 モジュラーシステムのドキュメント

▼ 複数のブレードサーバーへの単一のストレージリソースの割り当て: **Detailed Setup (Web)**

始める前に



注意 - Sun ブレードサーバーモジュールで、ほかの Sun ブレードサーバーモジュールとのストレージリソースの共有が有効になっているかどうかを判別する場合は、Sun ブレードサーバーのドキュメントを参照してください。

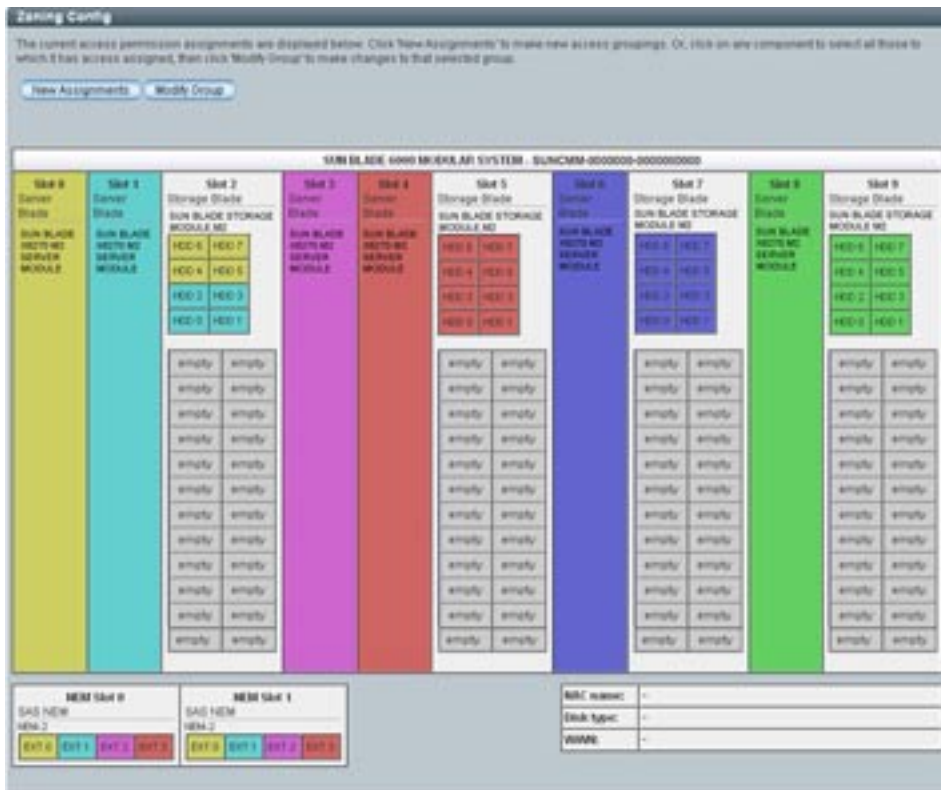


注意 - 単一のストレージリソースを共有するオプションは、Oracle でサポートされるクラスタ化ソリューションでのみ使用するようになっています。クラスタ化ソリューションの詳細は、Sun Blade Storage Module の管理ガイドを参照してください。

- Oracle ILOM で SAS ゾーンのプロパティを変更するには Admin (a) の役割が必要です。
- 249 ページの「シャーシのハードウェア要件」を確認します。
- この手順を実行する前に、Oracle ILOM で Sun Blade Zone Manager を有効にする必要があります。手順については、250 ページの「Sun Blade Zone Manager にアクセスして有効にする」を参照してください。

- 1 「Sun Blade Zone Manager Settings」 ページで、「Detailed Setup」 ボタンをクリックします。

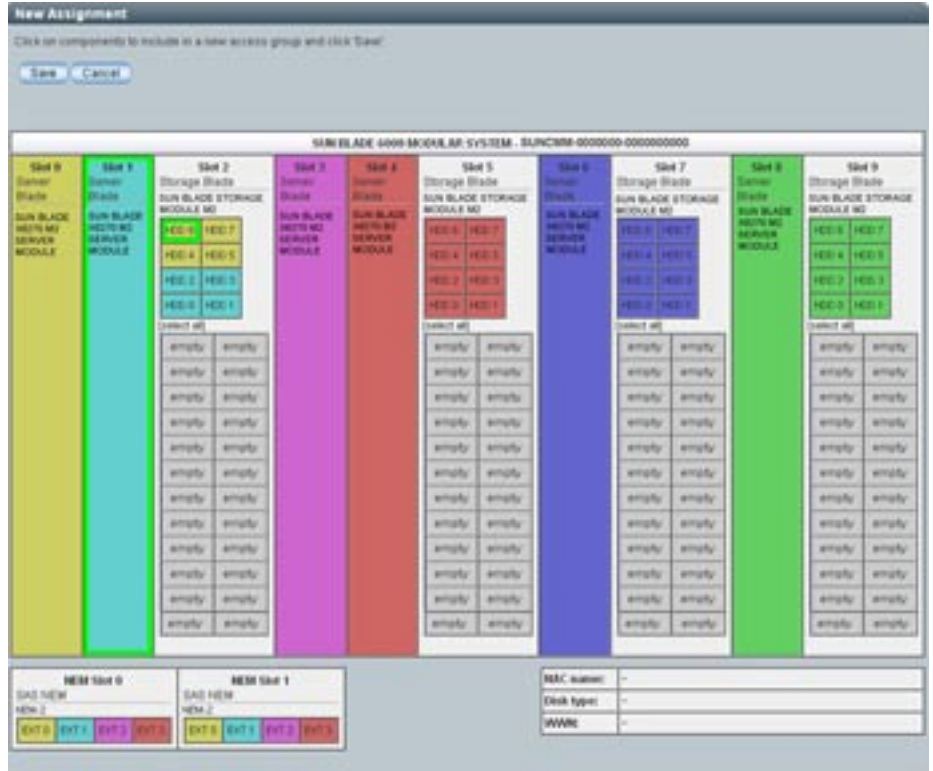
「Zoning Config」 ダイアログが表示されます。例:



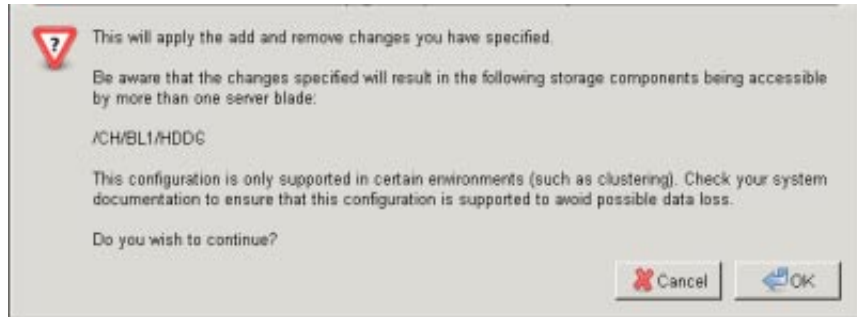
- 2 単一のストレージリソースを複数のブレードサーバーに割り当てるには、次の手順を実行します:

- a. 「New Assignments」 をクリックします。

- b. 単一のブレードサーバー (例: スロット 0 にある) に現在割り当てられている単一のストレージブレードリソース (例: スロット 2 の HDD6) を別のブレードサーバー (例: スロット 1 にある) と共有するには、追加のブレードサーバーターゲット (例: スロット 1 にある) をクリックして、このターゲット (例: スロット 1 にある) と共有するストレージブレードリソース (例: スロット 2 の HDD6) をクリックします。



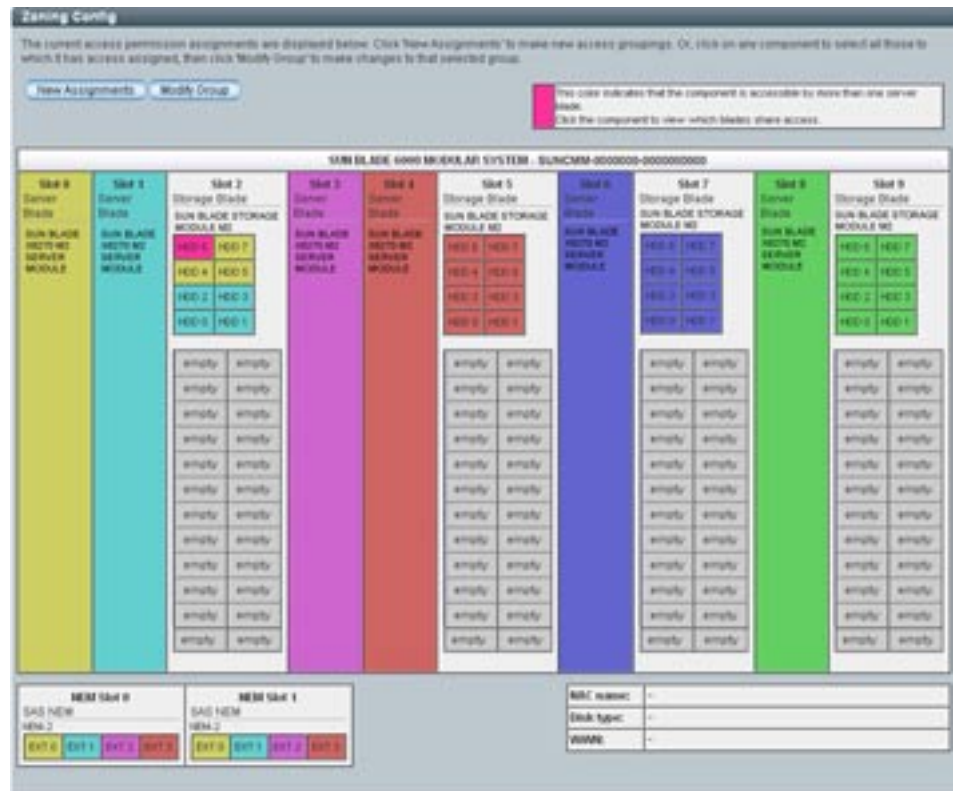
- c. ブレードストレージグループに対する割り当ての変更を保存するには、「Save」をクリックします。
次のメッセージが表示されます。



- d. ブレードストレージグループの割り当ての保存を続行するには、「OK」をクリックします。
Sun Blade Zone Manager で、共有されたストレージリソースがピンクで強調表示されます。

例:

スロット2のHDD6のストレージリソースが、複数のCPUブレードサーバーで共有されていることを示すためにピンクで強調表示されます。



- 3 新しく割り当てたブレードストレージグループをバックアップする場合は、[249 ページの「SAS-2 ゾーンの割り当てのバックアップおよび回復」](#)を参照してください。

参考 関連情報

- [248 ページの「SASゾーンの割り当てに関する重要な考慮事項」](#)
- [266 ページの「既存のSAS-2ストレージリソースの割り当ての管理」](#)
- [Sun Blade 6000 モジュラーシステムのドキュメント](#)

▼ SAS-2 ゾーンの割り当ての手動での作成 (CLI)

始める前に

- シャーシの構成が、[249 ページの「シャーシのハードウェア要件」](#)の要件を満たしていることを確認します。

- Oracle ILOM で SAS ゾーンの割り当てを手動で作成するには、Admin (a) 役割権限が必要です。
- Oracle ILOM で Sun Blade Zone Manager を有効にする必要があります。

1 CLI から Sun Blade Zone Manager にアクセスします。

手順については、250 ページの「[Sun Blade Zone Manager にアクセスして有効にする](#)」を参照してください。

2 次のいずれかの方法を使用して、ストレージリソースを CPU ブレードサーバーに割り当てます:

- **方法 1:** ストレージディスクを CPU ブレードサーバーに割り当てるために、次のコマンドを使用します:

```
-> cd /STORAGE/sas_zoning/BLn
```

```
-> set add_storage_access=path_to_storage_disk
```

ここでは、BLn は CPU ブレードサーバーのシャーシスロット番号、path_to_storage_disk はその CPU ブレードサーバーに割り当てるストレージブレードディスクのパスを表しています。

たとえば、ストレージブレードのスロットの場所 0 にあるハードディスクドライブを、シャーシのスロットの場所 1 にある CPU ブレードサーバーに割り当てるには、次を入力します:

```
-> set add_storage_access=/CH/BL1/HDD0.
```

- **方法 2:** CPU ブレードサーバーをストレージリソースに割り当てるために、次を入力します:

```
-> cd /STORAGE/sas_zoning/BLn/HDDn
```

```
-> set add_host_access=path_to_blade_server
```

ここでは、BLn はシャーシ内の CPU ブレードサーバーがあるスロットの場所、HDDn はストレージブレードのハードディスクドライブがあるスロットの場所、および path_to_blade_server はストレージディスクに割り当てる CPU ブレードサーバーのターゲットを表しています。

たとえば、ストレージブレードサーバー内のハードディスクドライブをシャーシ内の CPU ブレードサーバーに割り当てるには、次を入力します:

```
-> cd /STORAGE/sas_zoning/BL1/HDD0
```

```
-> set add_host_access=/CH/BL0
```

次の例では、これらのコマンドを使用して、スロット 1 にあるストレージブレードのストレージデバイスと、スロット 0 にあるサーバーブレードとの間にゾーンの割り当てを設定する方法について説明します。

- **方法 1 -** ストレージリソースを CPU ブレードサーバーに割り当てるためのコマンドの例:

CLIコマンド構文の例	手順
-> <code>cd /STORAGE/sas_zoning/BL0</code>	a. 最初のコマンド構文の例を使用して、ストレージリソースを割り当てるCPUブレードサーバーにアクセスします。
-> <code>set add_storage_access=/CH/BL1/HDD0</code>	b. 2番目のコマンド構文の例を使用して、ストレージブレードサーバー (BL1) のストレージモジュール (HDD0) をシャーシのスロット0のホストCPUブレードサーバー (BL0) に割り当てます。
-> <code>set add_storage_access=/CH/BL1/HDD0,/CH/BL1/HDD1</code>	c. 必要に応じて、3番目のコマンド構文を使用して、単一のコマンド行で複数のデバイスを割り当てることもできます。ストレージリソースのフルパスを指定して、各リソースをコンマ(スペースではなく)で区切ってください。
-> <code>show</code> /STORAGE/sas_zoning/BL0 Targets: 0 (/CH/BL1/HDD0) 1 (/CH/BL1/HDD1)	d. <code>show</code> コマンドを使用して、ストレージの割り当てがCPUブレードサーバー (/CH/BL1/HDD0 および CH/BL1/HDD1) に保存されていることを確認します。

- 方法2 - CPUサーバーブレード (BL0) をストレージブレードのリソース (BL1/HDD0) に割り当てるためのコマンドの例:

CLIコマンド構文の例	手順
-> <code>cd /STORAGE/sas_zoning/BL1/HDD0</code>	a. 最初のコマンド構文の例を使用して、ストレージブレードサーバー (BL1/HDD0) に取り付けられているストレージリソース (HDD0) にアクセスします。
-> <code>set add_host_access=/CH/BL0</code>	b. 2番目のコマンド構文の例を使用して、ストレージリソース (HDD0) をホストCPUブレードサーバー (BL0) に割り当てます。
-> <code>show</code> /STORAGE/sas_zoning/BL1/HDD0 Targets: 0 (/CH/BL0)	c. <code>show</code> コマンドを使用して、ストレージの割り当てが適切なCPUブレードサーバー (/CH/BL0) に保存されていることを確認します。

- 3 新しく保存したサーバストレージグループをバックアップします。

参考 関連情報

- [249 ページの「SAS-2 ゾーンの割り当てのバックアップおよび回復」](#)
- [263 ページの「SAS-2 ゾーンの割り当ての手動での作成 \(CLI\)」](#)
- [Sun Blade 6000 モジュラーシステムのドキュメント](#)

既存の SAS-2 ストレージリソースの割り当ての管理

Oracle ILOM の Sun Blade Zone Manager では、シャーシ内のストレージリソースの既存の割り当てを次の方法で管理できます:

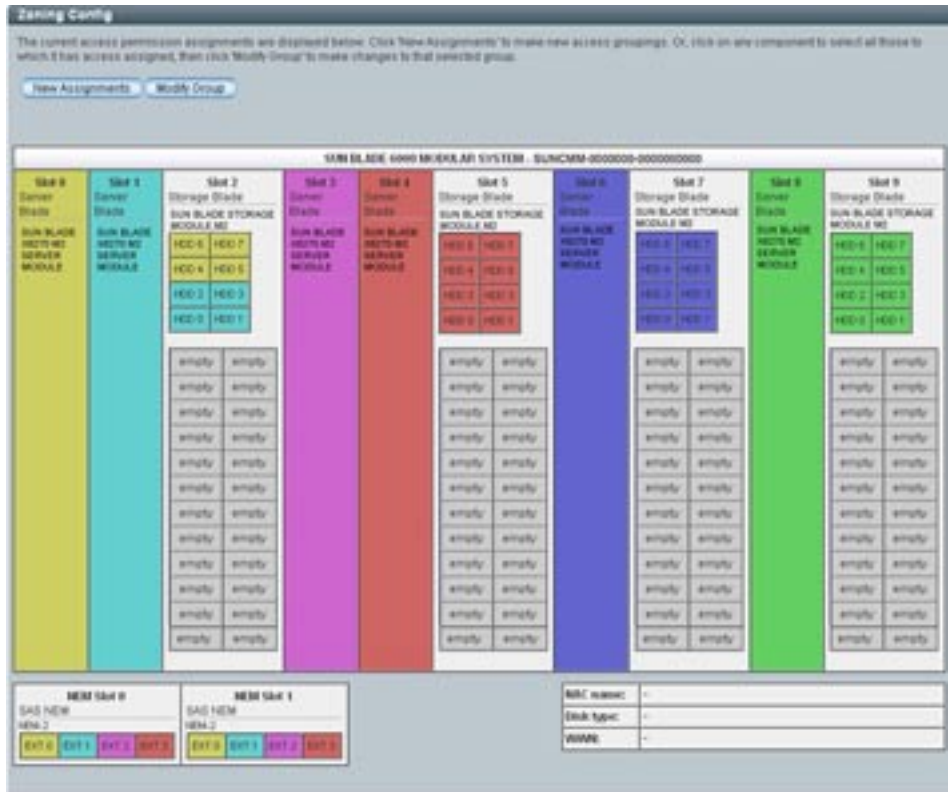
- [266 ページの「既存の CPU ブレードサーバーのストレージの割り当ての表示 \(Web\)」](#)
- [269 ページの「既存のブレードグループの割り当ての変更 \(Web\)」](#)
- [273 ページの「既存のストレージの割り当ての表示と変更 \(CLI\)」](#)

▼ 既存の CPU ブレードサーバーのストレージの割り当ての表示 (Web)

始める前に

- Oracle ILOM で Sun Blade Zone Manager の割り当てを表示するには、Admin (a) 役割権限が必要です。
 - Oracle ILOM で Sun Blade Zone Manager を有効にする必要があります。
- 1 **Sun Blade Zone Manager** にアクセスして、「**Detailed Setup**」をクリックします。
Sun Blade Zone Manager にアクセスする手順については、[250 ページの「Sun Blade Zone Manager にアクセスして有効にする」](#)を参照してください。

「Zoning Config」ダイアログが表示され、現在のシャーシのストレージの割り当てが表示されます。



- 2 選択した CPU ブレードサーバーのリソースの割り当てをすべて表示するには、次の手順を実行します:
 - a. CPU ブレードサーバーの slots を選択します。
この例では、slot 0 が選択されています。

b. 「Current Assignments」表までスクロールダウンします。

選択した CPU ブレードサーバーに現在割り当てられているすべてのストレージリソースが「Current Assignments」表に表示されます。

Component	Type	WWN
/CH/BLD	Server Blade (Virgo*)	-
/CH/NEM0/EXT0	SAS Port	-
/CH/NEM1/EXT0	SAS Port	-
/CH/BL2/HDD6	SAS HDD	80205010:12124558 80205010:12124557
/CH/BL2/HDD4	SAS HDD	80205010:12124558 80205010:12124557
/CH/BL2/HDD5	SAS HDD	80205010:12124558 80205010:12124557
/CH/BL2/HDD7	SAS HDD	80205010:12124558 80205010:12124557
/CH/BL2/FMOD23	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD21	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD19	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD18	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD20	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD22	SAS FMOD	80205010:33333336 80205010:33333337

3 選択した CPU ブレードサーバーの「Current Assignments」表とシャーシのほかの CPU ブレードサーバーのリソースの割り当てを同時に表示するには、「Detach Table」をクリックします。

切り離された「Current Assignments」表が別のダイアログボックスに表示されます。

Component	Type	WWN
/CH/BLD	Server Blade (Virgo*)	-
/CH/NEM0/EXT0	SAS Port	-
/CH/NEM1/EXT0	SAS Port	-
/CH/BL2/HDD6	SAS HDD	80205010:12124558 80205010:12124557
/CH/BL2/HDD4	SAS HDD	80205010:12124558 80205010:12124557
/CH/BL2/HDD5	SAS HDD	80205010:12124558 80205010:12124557
/CH/BL2/HDD7	SAS HDD	80205010:12124558 80205010:12124557
/CH/BL2/FMOD23	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD21	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD19	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD18	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD20	SAS FMOD	80205010:33333336 80205010:33333337
/CH/BL2/FMOD22	SAS FMOD	80205010:33333336 80205010:33333337

参考 関連情報

- 269 ページの「既存のブレードグループの割り当ての変更 (Web)」
- 248 ページの「SAS ゾーンの割り当てに関する重要な考慮事項」
- 263 ページの「SAS-2 ゾーンの割り当ての手動での作成 (CLI)」

- Sun Blade 6000 モジュラーシステムのドキュメント

▼ 既存のブレードグループの割り当ての変更 (Web)

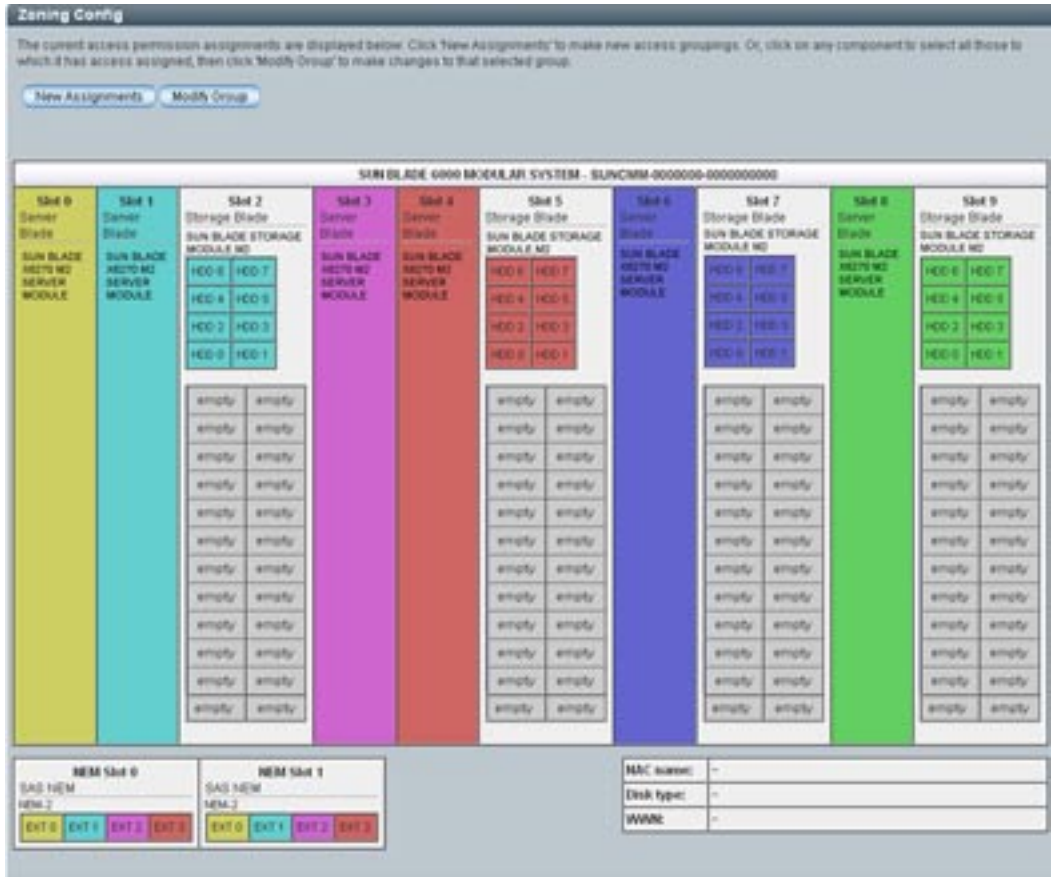
始める前に 始める前に

- シャーシのハードウェア構成が、[249 ページの「シャーシのハードウェア要件」](#)で説明されている要件を満たしていることを確認します。
- Oracle ILOM で Sun Blade Zone Manager のプロパティを変更するには、Admin (a) 役割権限が必要です。
- Oracle ILOM で Sun Blade Zone Manager を有効にする必要があります。

- 1 **Sun Blade Zone Manager** にアクセスするには、「System Management」 > 「SAS Zoning」をクリックします。

「SAS Zoning」ページが表示されます。

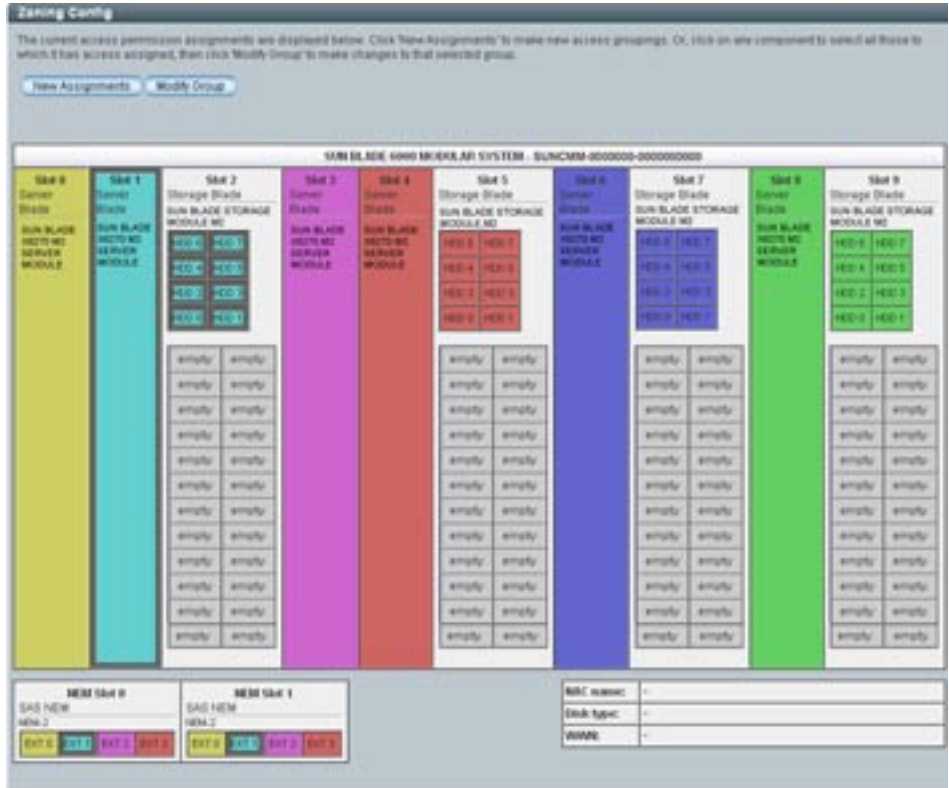
- 「Sun Blade Zone Manager」セクションで、「Detailed Setup」をクリックします。「Zoning Config」ダイアログが表示され、既存のストレージの割り当てが色分けされたグループで示されます。



注-ストレージデバイスが取り付けられていないHDDスロットは「empty」と表示されます。空のHDDスロットは、CPUブレードサーバーに割り当てられません。

- ブレードストレージグループのストレージの割り当てを変更するために、このグループの一部であるブレードを選択します。

Sun Blade Zone Manager の「Zoning Config」ダイアログで、ブレードストレージグループに割り当てられているストレージが強調表示されます。



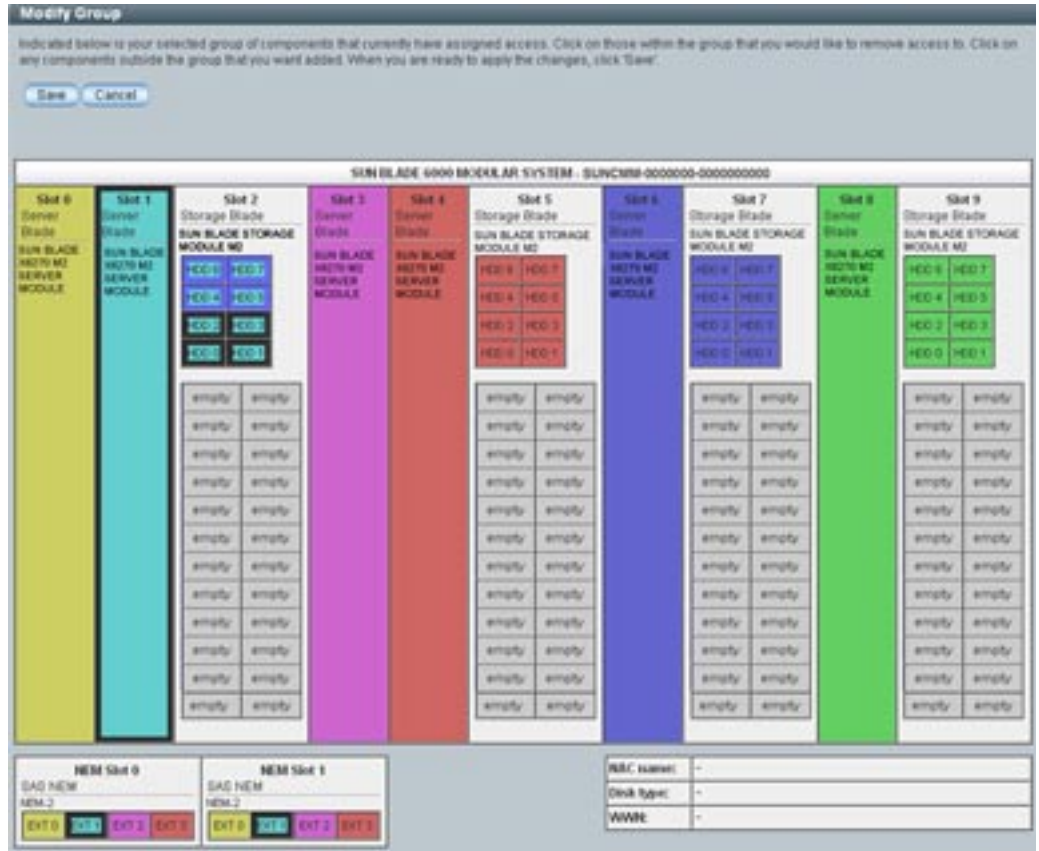
- 選択したブレードストレージグループに割り当てられているストレージリソースを変更するには、「Modify Group」をクリックします。

Sun Blade Zone Manager で、選択したブレードストレージグループが強調表示されます (CPU ブレードサーバーに現在割り当てられているストレージリソースを含む)。

5 選択したグループに対して、次のストレージの変更を1つまたは複数行います:

- 選択したブレードストレージグループに割り当てられているストレージリソースを削除するには、削除するリソースをクリックします。

例: 次の図は、スロット1のCPUブレードサーバーから削除するために選択されたリソース HDD 4-7 を示しています。



- 追加のストレージリソースをブレードストレージグループに割り当てるには、色分けされたグループの外側にある追加するストレージリソースをクリックします。

6 選択したブレードストレージグループに対する割り当ての変更を適用するには、「Save」をクリックします。

7 変更して保存したリソースの割り当てをバックアップします。

参考 関連情報

- 248 ページの「SAS ゾーンの割り当てに関する重要な考慮事項」
- 249 ページの「SAS-2 ゾーンの割り当てのバックアップおよび回復」
- 273 ページの「既存のストレージの割り当ての表示と変更 (CLI)」
- Sun Blade 6000 モジュラーシステムのドキュメント

▼ 既存のストレージの割り当ての表示と変更 (CLI)

始める前に 始める前に

- シャーシのハードウェア構成が、249 ページの「シャーシのハードウェア要件」の要件を満たしていることを確認します。
- Oracle ILOM で Sun Blade Zone Manager のプロパティを表示および変更するには、Admin (a) 役割権限が必要です。
- Oracle ILOM で Sun Blade Zone Manager を有効にする必要があります。

1 CLI から Sun Blade Zone Manager にアクセスします。

250 ページの「Sun Blade Zone Manager にアクセスして有効にする」を参照してください。

2 CPU ブレードサーバーに割り当てられているストレージリソースを表示するには、次のいずれかを実行します。

- CPU ブレードサーバーのストレージの割り当てを表示するには、**show** コマンドの後ろに **/STORAGE/sas_zoning/BLn** ターゲットを指定して使用します。例:

```
-> show /STORAGE/sas_zoning/BL0
```

```
Targets:
  0      (/CH/BL2/HDD0)
  1      (/CH/BL2/HDD1)
```

この例では、シャーシのスロット 2 のストレージブレードサーバーに現在取り付けられている HDD0 と HDD1 が、シャーシのスロット 0 の CPU ブレードサーバーに割り当てられています。

- ストレージブレードのリソースが割り当てられている場所を表示するには、**show** コマンドの後ろに **/STORAGE/BLn/HDDn** ターゲットを指定して使用します。例:

```
-> show /STORAGE/BL2/HDD0
```

```
Targets:
  0      (/CH/BL0)
```

```
-> show /STORAGE/BL2/HDD1
```

```
Targets:
  0      (/CH/BL0)
```

この例では、シャーシの スロット 2 のストレージブレードサーバーに取り付けられているリソース HDD0 と HDD1 が、シャーシの スロット 0 の CPU ブレードサーバーに割り当てられています。

3 ストレージの割り当てを変更するには、次のいずれかの方法を実行します:

方法 1: CPU ブレードサーバーごとにストレージリソースの追加または割り当ての解除を行います。

- ストレージリソースを CPU ブレードサーバーに割り当てするには、次を入力します:

```
-> cd /STORAGE/sas_zoning/BLn -> set add_storage_access=path_to_storage_device
```

ここでは、BLn はシャーシ内の CPU ブレードサーバーがあるスロットの場所、path_to_storage_device はストレージブレードのリソースのパスを表しています。

- CPU ブレードサーバーからストレージリソースの割り当てを解除するには、次を入力します:

```
-> cd /STORAGE/sas_zoning/BLn -> set  
remove_storage_access=path_to_storage_device
```

ここでは、BLn はシャーシ内の CPU ブレードサーバーがあるスロットの場所、path_to_storage_device はストレージブレードサーバー上のリソースのパスを表しています。たとえば、/CH/BL1/HDD0 です。

方法 2: ストレージデバイスへのサーバーブレードのアクセスの追加または割り当ての解除を行います。

- CPU ブレードサーバーをストレージリソースに割り当てするには、次を入力します:

```
-> cd /STORAGE/sas_zoning/BLn/HDDn  
-> set add_host_access=path_to_blade_server
```

- ストレージデバイスへのホストサーバーブレードのアクセスの割り当てを解除するには、次を入力します:

```
-> cd /STORAGE/sas_zoning/BLn/HDDn  
-> set remove_host_access=path_to_blade_server
```

ここでは、BLn はシャーシ内のストレージブレードサーバーがあるスロットの場所、HDDn はストレージリソースがあるスロットの場所、および path_to_blade_server はリソースの割り当てまたは割り当ての解除を行う CPU ブレードサーバーのシャーシ内のスロットの場所を表しています。たとえば、/CH/BL0 です。

注 - 単一のコマンド行で複数のストレージデバイスの追加または割り当ての解除を行うこともできます。これを行うには、リソースのフルパスを指定して、各リソースをコンマ(スペースではなく)で区切ります。例: `-> set add_storage_access=/CH/BL1/HDD0,/CH/BL1/HDD1`

- 4 ブレードストレージグループの割り当てをバックアップします。

参考 関連情報

- 248 ページの「SAS ゾーンの割り当てに関する重要な考慮事項」
- 249 ページの「SAS-2 ゾーンの割り当てのバックアップおよび回復」
- 263 ページの「SAS-2 ゾーンの割り当ての手動での作成 (CLI)」
- Sun Blade 6000 モジュールシステムのドキュメント

Sun Blade Zone Manager の割り当てを出荷時のデフォルトにリセットする

Sun Blade Zone Manager に保存されているシャーシ内のストレージの割り当てをすべて消去して、Sun Blade Zone Manager を出荷時のデフォルトから開始するには、次のいずれかの手順を実行します。

- 275 ページの「ゾーンの割り当てを出荷時のデフォルトにリセットする (Web)」
- 276 ページの「ゾーンの割り当てを出荷時のデフォルトにリセットする (CLI)」

▼ ゾーンの割り当てを出荷時のデフォルトにリセットする (Web)

始める前に 始める前に

- Oracle ILOM で Sun Blade Zone Manager のプロパティを変更するには、Admin (a) 役割権限が必要です。



注意 - この手順は、Oracle ILOM に現在保存されている SAS ゾーンの割り当てをすべて消去する場合にのみ使用します。

- 1 CMM の Web インタフェースの「Sun Blade Zone Manager」ページにアクセスするには、「System Management」 > 「SAS Zoning」の順にクリックします。

Sun Blade Manager の状態が有効になっている場合は、「Sun Blade Zone Manager」ページの「Zoning Reset」セクションに「Reset All」ボタンが表示されません。

- 2 保存されているすべてのリソースの割り当てを消去して、Sun Blade Zone Manager を出荷時のデフォルトにリセットするには、「Reset All」をクリックします。

▼ ゾーンの割り当てを出荷時のデフォルトにリセットする (CLI)

始める前に 始める前に

- Oracle ILOM で Sun Blade Zone Manager のプロパティを変更するには、Admin (a) 役割権限が必要です。



注意 - この手順は、Oracle ILOM に現在保存されている SAS ゾーンの割り当てをすべて消去する場合にのみ使用します。

- 1 CMM の CLI で、次のコマンドを使用して `/STORAGE/sas_zoning` に移動します:
-> `cd /STORAGE/sas_zoning`
- 2 保存されているすべてのリソースの割り当てを消去して、**Sun Blade Zone Manager** を出荷時のデフォルトにリセットするには、次を入力します:
-> `set reset_access_action=true`

Zone Manager が無効になっている場合は、次の警告が表示されます:

```
set: The CMM is not the SAS Zone Manager
```

このメッセージが表示された場合は、Zone Manager を有効にして、リセットのコマンドを再度実行します。詳細は、[250 ページの「Sun Blade Zone Manager にアクセスして有効にする」](#)を参照してください。

サードパーティの帯域内管理でのゾーンのパスワードを出荷時のデフォルトにリセットする

サードパーティ製の帯域内ゾーン管理アプリケーションを使用して、シャーシレベルのストレージデバイスのストレージの割り当てを管理していて、ゾーン管理のパスワードを出荷時のデフォルトにリセットする必要がある場合は、次のいずれかの手順を実行します。

- [276 ページの「ゾーンのパスワードのリセット \(Web\)」](#)
- [277 ページの「ゾーンのパスワードのリセット \(CLI\)」](#)

▼ ゾーンのパスワードのリセット (Web)

始める前に 始める前に

- Oracle ILOM で Sun Blade Zone Manager のプロパティを変更するには、Admin (a) 役割権限が必要です。



注意 - この手順は、Oracle ILOM Zone Manager を使用せずに、サードパーティー製の帯域内管理アプリケーションを使用して、シャーシのストレージの割り当てを管理する場合にのみ使用します。

- 1 **Sun Blade Zone Manager** の状態が無効であることを **CMM** の **Web** インタフェースで確認するには、「**System Management**」 > 「**SAS Zoning**」の順にクリックします。

「Sun Blade Zone Manager」ページが表示されます。

Sun Blade Zone Manager が無効になっている場合は、パスワードをリセットするオプションが「In-band Zoning Manager」セクションに表示されます。

- 2 ゾーンのパスワードをデフォルト値(すべてゼロ)にリセットするには、「**Reset**」をクリックします。

▼ ゾーンのパスワードのリセット (CLI)

始める前に 始める前に

- Oracle ILOM で Sun Blade Zone Manager のプロパティを変更するには、Admin (a) 役割権限が必要です。



注意 - この手順は、Oracle ILOM Zone Manager を使用せずに、サードパーティー製の帯域内管理アプリケーションを使用して、シャーシのストレージの割り当てを管理する場合にのみ使用します。

- 1 次のコマンドを使用して、`/STORAGE/sas_zoning` に移動します:

```
-> cd /STORAGE/sas_zoning
```

- 2 現在のゾーンのパスワードをリセットするには、次を入力します:

```
-> set reset_password_action=true
```

パスワードがデフォルト (すべてゼロ) に設定されます。

索引

C

CLI

- Sun Blade Zone Manager, 246
- Sun Blade Zone Manager のシャーシストレージ構成の作成に使用する, 263

D

- dnssec-keygen, 119

I

- ILOM にログインする, root ユーザーアカウントのパスワードを使用, 34
- init.d スクリプト, 120
- IPMI PET 警告, 178

N

- nslookup, 120

S

- SNMP トラップ警告, 178
- Sun Blade Zone Manager
 - CLI, 246
 - シャーシのストレージアクセス構成の作成
 - CLI の使用, 263
 - detailed setup の使用, 254

- Sun Blade Zone Manager, シャーシのストレージアクセス構成の作成 (続き)
 - quick setup の使用, 252
 - ストレージアクセス構成の保存, 248
 - ストレージアクセス構成表, 266
 - ストレージ構成の表示と変更
 - Web インタフェースを使用する, 269, 273, 275, 276
 - ゾーン構成のリセット
 - Web インタフェースを使用する, 275
 - ゾーンのパスワードのリセット
 - Web インタフェースを使用する, 277
- Sun Blade Zone Manager の Detailed Setup, 254
- Sun Blade Zone Manager の Quick Setup, 252
- Sun Blade Zone Manager のストレージアクセス構成表, 266

W

- Web インタフェース
 - ストレージ構成の表示と変更を使用する, 269, 273, 275, 276
 - ストレージのゾーン構成を回復する, 275
 - ゾーンのパスワードのリセット, 277

け

警告

- 宛先の指定, 178
- サポートされている種類, 178
- レベルの種類, 179

す

ストレージアクセス構成の保存, 248

て

電子メール通知警告, 178

と

動的 DNS

Debian r4.0 環境, 118

dnssec-keygen, 119

サポートされているオペレーティングシステム, 118

トピックのガイドライン, 221-235, 237-277