HPE iLO 5 2.30 ユーザーガイド

摘要

このガイドは、HPE iLO 5 ファームウェアを使用してサポートされるサーバーおよびコンピュートモジュールの構成、アップデート、および操作に関する情報を提供します。本書は、iLO 5 が含まれている Hewlett Packard Enterprise サーバーの構成と使用に関係するシステム管理者、Hewlett Packard Enterprise の担当者、および Hewlett Packard Enterprise 認定チャネルパートナーを対象としています。

部品番号: 880740-198
発行: 2020 年 9 月
版数: 1

© Copyright 2012-2020 Hewlett Packard Enterprise Development LP

ご注意

本書の内容は、将来予告なしに変更されることがあります。Hewlett Packard Enterprise 製品およびサービスに対する保証については、当該製品およびサービスの保証規定書に記載されています。本書のいかなる内容も、新たな保証を追加するものではありません。本書の内容につきましては万全を期しておりますが、本書中の技術的あるいは校正上の誤り、脱落に対して、責任を負いかねますのでご了承ください。

本書で取り扱っているコンピューターソフトウェアは秘密情報であり、 その保有、使用、または複製には、Hewlett Packard Enterprise から使用許諾を得る必要があります。 FAR 12.211 および 12.212 に従って、商業用コンピューターソフトウェア、コンピューターソフトウェアドキュメンテーション、および商業用製品の技術データ（Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items）は、ベンダー標準の商業用使用許諾のもとで、米国政府に使用許諾が付与されます。

他社の Web サイトへのリンクは、Hewlett Packard Enterprise の Web サイトの外に移動します。Hewlett Packard Enterprise は、Hewlett Packard Enterprise の Web サイト以外の情報を管理する権限を持たず、また責任を負いません。

商標

Microsoft®および Windows®は、米国および/またはその他の国における Microsoft Corporation の登録商標または商標です。

Java®および Oracle®は、Oracle および/またはその関連会社の登録商標です。

Google™は、Google Inc.の商標です。

Google Chrome™は、Google Inc.の商標です。

Linux®は、Linus Torvalds の米国およびその他の国における登録商標です。

Red Hat®は、米国およびその他の国における Red Hat, Inc.の商標または登録商標です。

VMware®は、VMware, Inc.の米国および各国での登録商標または商標です。

Intel®、インテル、およびインテル®Xeon®はインテルコーポレーションまたはその子会社のアメリカ合衆国およびその他の国における商標または登録商標です。

SD は SD-3C の米国およびその他の国における商標または登録商標です。

すべてのサードパーティのマークは、それぞれの所有者に帰属します。

改訂履歴

部品番号	出版日付	版数	変更のサマリー
880740-198	2020 年 9 月	1	· **One-button セキュア消去**機能は iLO Web インターフェイスから利用可能です。 · **ユーザーアカウントロール**は、定義済みの権限セットを提供するか、またはカスタムセットを定義することもできます。 · 新しい **HTML5 リモートコンソールモード**：スタンドアロンモードと新しいウィンドウモード。 · **ストレージ情報**ページのデザインが変更されました。 · **NVMe ドライブの電源をオンまたはオフにする**仮想電源ボタン。 · **構成可能な最小ファン速度** · NVMe 直接接続ストレージ用の**ドライブインジケーター LED のサポート**。 · **温度構成設定**の表示および構成。 · 構成可能な**インレット周囲センサーの事前警告しきい値アラート** · **Platform Level Data Model（PLDM）ファームウェアパッケージ**のサポート · **RDE 対応**デバイスの読み取りのサポート。 · 新しい**ライフサイクル管理**ナビゲーションツリーメニュー。このメニューには、Always On Intelligent Provisioning、One-button セキュア消去、および iLO のバックアップとリストア機能が含まれています。 · **iLO ネットワーク有効化モジュール**に関する情報。 · **iLO 機能で使用されるポート**のリストが追加されました。 · **IPMI アラート**が追加されました。

目次

iLO 18
iLO 機能 18
iLO Web インターフェイス 19
ROM ベースの構成ユーティリティ 20
iLO モバイルアプリケーション 20
iLO RESTful API 20
RESTful インターフェイスツール 20
iLO スクリプティングとコマンドライン 21
iLO Amplifier Pack 21
HPE InfoSight for Servers 21

iLO のセットアップ 22
iLO をセットアップするための準備 22
iLO ネットワーク接続オプション 22
共有ネットワークポート構成による NIC チーミング 23
iLO IP アドレスの取得 24
iLO アクセスセキュリティ 25
iLO 構成ツール 25
その他の iLO 構成ツール 26
初期セットアップ手順 26
iLO ネットワークに接続する 27
iLO の iLO 5 構成ユーティリティを使用したセットアップ 27
静的 IP アドレスの構成（iLO 5 構成ユーティリティ） 27
iLO 5 構成ユーティリティを使用したローカルユーザーアカウントの管理 28
Web インターフェイスによる iLO のセットアップ 30
iLO に初めてログインする方法 31
iLO のデフォルトの DNS 名とユーザーアカウント 31
iLO ライセンスが必要な機能 31
iLO ドライバーのサポート 31
iLO ドライバーのインストール 32

iLO Web インターフェイスの使用 34
サポートされているブラウザー 34
ブラウザーの要件 34
Internet Explorer の JavaScript の有効化 34
iLO Web インターフェイスへのログイン 35
ブラウザーインスタンスと iLO の間での Cookie の共有 35
iLO Web インターフェイスの概要 37
iLO 制御のアイコン 38
iLO ナビゲーションペイン 39
iLO ナビゲーションペインのリモートコンソールのサムネイル 39
ログインページからのリモート管理ツールの起動 39
ログインページからの言語の変更 40

iLO 情報およびログの表示 41
iLO の概要情報の表示 41

システム情報の詳細....41
システムステータスの詳細....42
HPE への接続ステータス....43
ネットワーク詳細....44
セキュリティダッシュボードの使用....44
セキュリティダッシュボード詳細....45
リスク詳細....46
セキュリティリスク状態の原因....47
iLO セッションの管理....48
セッションリスト詳細....49
iLO イベントログ....49
イベントログの表示....49
CSV ファイルへのイベントログの保存....51
イベントログのクリア....52
インテグレーテッドマネジメントログ....52
IML イベントタイプの例....52
IML の表示....53
IML エントリーの修正済みへの変更....55
IML にメンテナンスノートを追加する....55
CSV ファイルへの IML の保存....56
IML のクリア....56
セキュリティログ....56
セキュリティログの表示....57
CSV ファイルへのセキュリティログの保存....59
セキュリティログのクリア....59
Active Health System....59
Active Health System のデータ収集....59
Active Health System ログ....60
Active Health System ログのダウンロード方法....60
日付範囲を指定した Active Health System ログのダウンロード....61
Active Health System ログ全体のダウンロード....61
cURL を使用した Active Health System ログのダウンロード....62
Active Health System ログ（iLOREST）のダウンロード....64
Active Health System ログの消去....65

iLO とシステム診断の使用....67
iLO セルフテスト結果の表示....67
iLO セルフテストの詳細....67
iLO セルフテストの種類....67
iLO の再起動（リセット）....68
iLO の再起動（リセット）方法....68
Web インターフェイスを使用した iLO プロセッサーの再起動（リセット）....69
iLO の iLO 5 構成ユーティリティを使用した再起動（リセット）....69
サーバーの UID ボタンによる正常な iLO の再起動の実行....70
サーバーの UID ボタンによるハードウェア iLO の再起動の実行....70
アプライアンスのイメージの再構築....70
システム診断....71
NMI の生成....71
システムセーフモードでの起動....72
インテリジェント診断モードで起動....72
工場デフォルト設定のリストア....73
システムデフォルト設定のリストア....74

全般的なシステム情報の表示....76

ヘルスサマリー情報の表示....76
冗長ステータス....76
サブシステムおよびデバイスのステータス....76
サブシステムおよびデバイスステータスの値....77
プロセッサー情報の表示....77
プロセッサーの詳細....77
メモリ情報の表示....78
アドバンストメモリプロテクションの詳細....78
メモリの概要....80
物理メモリ詳細....81
メモリ詳細ペイン（物理メモリ）....82
ネットワーク情報の表示....83
物理ネットワークアダプター....84
論理ネットワークアダプター....86
デバイスインベントリの表示....86
デバイスインベントリの詳細....87
スロットの詳細ペイン....87
デバイスステータスの値....88
MCTP 検出の構成....89
MCTP 工場出荷時リセットの開始....89
ストレージ情報の表示....90
サポート対象のストレージコンポーネント....91
サポートされるストレージ製品....91
ストレージ詳細....91
NVMe ドライブの電源の管理....94

ファームウェアおよびソフトウェアの表示および管理....95
ファームウェアのアップデート....95
オンラインでのファームウェアアップデート....95
オフラインでのファームウェアアップデート....96
iLO ファームウェアとソフトウェアの管理....96
インストール済みファームウェア情報の表示....97
ファームウェアの種類....98
ファームウェアの詳細....98
冗長なシステム ROM でアクティブなシステム ROM を交換....98
フラッシュファームウェア機能を使用した iLO またはサーバーのファームウェアのアップデート....99
日次のファームウェアフラッシュ制限....101
サポートされるファームウェアタイプ....101
ファームウェアアップデートを有効にするための要件....102
iLO ファームウェアイメージファイルの入手....102
サポートされるサーバーファームウェアイメージファイルの入手....103
ソフトウェア情報の表示....104
HPE ソフトウェアの詳細....104
実行中のソフトウェアの詳細....104
インストールされたソフトウェアの詳細....104
メンテナンスウィンドウ....104
メンテナンスウィンドウの追加....105
メンテナンスウィンドウの編集....105
メンテナンスウィンドウの削除....106
すべてのメンテナンスウィンドウを削除....107
メンテナンスウィンドウの表示....107
iLO レポジトリ....108
iLO レポジトリへのコンポーネントの追加....108
iLO レポジトリからコンポーネントをインストールする....109

iLO レポジトリからのコンポーネントの削除....111
iLO レポジトリからすべてのコンポーネントを削除する....111
iLO レポジトリの概要とコンポーネントの詳細の表示....111
インストールセット....112
インストールセットのインストール....113
インストールセットを削除する....114
すべてのインストールセットを削除する....115
インストールセットを表示する....115
システムリカバリセット....116
システムリカバリセットの作成....117
インストールキュー....119
インストールキューへのタスクの追加....119
インストールキューのタスクの編集....122
インストールキューからのタスクの削除....124
インストールキューからのすべてのタスクの削除....124
インストールキューの表示....125

iLO 連携の構成と使用....128
iLO 連携....128
iLO 連携の構成....128
iLO 連携機能を使用するための前提条件....128
iLO 連携のネットワーク要件....129
iLO 連携マルチキャストオプションの構成....129
iLO 連携グループ....130
iLO 連携グループメンバーシップを管理する（ローカル iLO システム）....132
iLO 連携グループメンバーシップの追加（複数の iLO システム）....134
エンクロージャー iLO 連携サポートの設定....137
iLO 連携機能の使用....138
選択されたグループのリスト....138
iLO 連携情報を CSV ファイルにエクスポートする方法....139
iLO 連携マルチシステムビュー....140
iLO 連携マルチシステムマップの表示....141
iLO 連携グループ仮想メディア....142
iLO 連携グループ電力....145
グループ消費電力上限の構成....147
iLO 連携グループファームウェアアップデート....149
ライセンスキーのインストール（iLO 連携グループ）....152

iLO リモートコンソール....155
リモートコンソールのアクセス設定の表示....156
リモートコンソールのアクセス設定の詳細....156
統合リモートコンソールの起動....157
HTML5 IRC の起動....157
概要ページからの HTML5 IRC の起動....157
HTML5 スタンドアロンリモートコンソールの起動....158
HTML5 リモートコンソールモード....159
HTML5 リモートコンソールのコントロール....160
.NET IRC の起動....162
概要ページからの.NET IRC の起動....162
.NET IRC 要件....163
Java IRC の起動（Oracle JRE）....164
概要ページから Java IRC（Oracle JRE）の起動....164
Java IRC の起動（OpenJDK JRE）....165
リモートコンソールの取得....166

共有リモートコンソールセッションへの参加（.NET IRC 専用）.....167
リモートコンソールのステータスバーの表示.....168
統合リモートコンソールの機能.....169
IRC を使用したキーボード操作.....169
仮想電源 IRC の機能.....171
仮想メディア IRC の機能.....173
コンソールのキャプチャー（.NET IRC）.....180
IRC を使用したスクリーンキャプチャー.....184
リモートコンソールのホットキー.....185
リモートコンソールのホットキーの作成.....185
リモートコンソールコンピューターのロックキーおよびホットキーを構成するキー.. 186
ホットキーのリセット.....187
リモートコンソールの構成済みホットキーの表示（Java IRC）.....187
リモートコンソールセキュリティの設定.....188
リモートコンソールのコンピューターロック設定を構成する.....188
リモートコンソールの信頼設定の構成（.NET IRC）.....189

テキストベースのリモートコンソールの使用.....190
iLO 仮想シリアルポート.....190
iLO 仮想シリアルポートの使用.....191
UEFI システムユーティリティでの iLO 仮想シリアルポートの構成.....191
iLO 仮想シリアルポートを使用するための Linux の設定.....192
iLO 仮想シリアルポート搭載の Windows EMS コンソール.....194
iLO 仮想シリアルポートセッションの開始.....195
iLO 仮想シリアルポートログの表示.....196
テキストベースのリモートコンソール（Textcons）.....196
テキストベースのリモートコンソールの使用.....197
テキストベースのリモートコンソールと組み合わせた Linux.....197
テキストベースのリモートコンソールのカスタマイズ.....197

ホスト上での iLO の使用.....199
仮想 NIC についてのオペレーティングシステムのサポート.....199
仮想 NIC を使用するための前提条件.....199
仮想 NIC 機能の構成.....200
仮想 NIC インターフェイスを静的から DHCP に変更する（ネットワークマネージャー）.....201
仮想 NIC インターフェイスを静的から DHCP に変更する（CLI）.....201
iLO Web インターフェイスにアクセスするための仮想 NIC の使用.....202
ホスト上での iLOREST の使用.....203
仮想 NIC での SSH 接続の使用.....203

iLO 仮想メディアの使用.....205
仮想メディアに関する留意事項.....205
仮想メディアを使用するためのオペレーティングシステム要件.....206
オペレーティングシステムの USB 要件.....206
オペレーティングシステムに関する注意事項：仮想ディスケット/USB キー.....206
オペレーティングシステムに関する注意事項：仮想 CD/DVD-ROM.....207
オペレーティングシステムに関する注意事項：仮想フォルダー.....208
iLO Web インターフェイスの仮想メディアオプション.....208
仮想メディアのステータスおよびポート構成の表示.....208
接続されているローカルメディアの表示.....209
ローカル仮想メディアデバイスの取り出し.....209
URL ベースのメディアの接続.....210

接続されている URL ベースのメディアの表示....211
URL ベースの仮想メディアデバイスの取り出し....211
スクリプト仮想メディア用 IIS のセットアップ....212
IIS の設定....212
読み出し/書き込みアクセス用の IIS の設定....212
ヘルパーアプリケーションによる仮想メディアの挿入....213
仮想メディアヘルパーアプリケーションのサンプル....214

電力および温度機能の使用....216
サーバーの電源オン....216
電圧低下からの復旧....216
正常なシャットダウン....217
電力効率....217
電源投入時の保護....217
電力割り当て（ブレードサーバーおよびコンピュートモジュール）....218
サーバー電力の管理....218
仮想電源ボタンのオプション....219
システム電力リストア設定....219
自動電源オン....220
電源オン遅延....220
サーバー電力使用量の表示....221
電力メーターグラフ表示オプション....222
現在の電源状態の表示....223
サーバー電力履歴の表示....224
電力設定....225
パワーレギュレーターの設定....225
消費電力上限の構成....226
バッテリバックアップユニット設定の構成....227
電力しきい値設定超過の SNMP アラートの構成....228
マウスとキーボードの持続接続の設定....229
電力情報の表示....229
電源装置概要の詳細....230
電源装置のリスト....231
Power Discovery Services iPDU 概要....232
電力測定値....233
パワーマイクロコントローラー....233
バッテリバックアップユニットの詳細....234
Smart Storage Energy Pack のリスト....234
電力監視....235
高効率モード....235
ファンの構成と表示....235
最小ファン速度の構成....235
温度構成設定の構成....236
ファン情報の表示....236
温度情報....238
温度グラフの表示....238
温度センサーデータの表示....238
温度の監視....239
インレット周囲センサーの事前警告しきい値アラートの構成....240

パフォーマンス管理機能の使用....241
パフォーマンス管理....241
Jitter Smoothing 設定の構成....241
Jitter Smoothing オプション....242

iLO 5 および Always On Intelligent Provisioning を使用したワークロードプロファイルの選択....243
ワークロードプロファイル....244
iLO 5 および Always On Intelligent Provisioning を使用したコアブーストの構成....245
コアブーストのオプション....246
パフォーマンス設定の表示....247
パフォーマンス監視....247
パフォーマンスデータの表示....248
パフォーマンスアラートの構成....250
ワークロードアドバイザー....251
サーバーワークロード詳細の表示....252
パフォーマンスチューニングオプションの構成....253

iLO ネットワーク設定の構成....256
iLO ネットワーク設定....256
ネットワーク構成の概要の表示....256
ネットワーク情報の概要....256
IPv4 概要の詳細....257
IPv6 概要の詳細....257
IPv6 アドレスリスト....257
ネットワーク共通設定....258
iLO ホスト名の設定....258
NIC 設定....259
IPv4 設定の構成....263
DHCPv4 構成設定....264
静的 IPv4 アドレス構成設定....264
IPv4 DNS 構成設定....265
IPv4 の WINS 構成設定....265
IPv4 の静的経路構成設定....265
その他の IPv4 設定....265
IPv6 設定の構成....266
グローバル IPv6 構成設定....266
DHCPv6 構成設定....267
IPv6 DNS 構成設定....267
静的 IPv6 アドレス構成設定....268
IPv6 の静的経路構成設定....268
IPv6 をサポートしている iLO の機能....268
iLO SNTP 設定の構成....269
SNTP オプション....270
iLO のクロック同期....271
DHCP NTP アドレスの選択....271
iLO NIC 自動選択....271
NIC 自動選択のサポート....272
NIC 自動選択が有効になっている場合の iLO 起動時の動作....272
iLO NIC 自動選択の有効化....272
NIC フェイルオーバーの構成....273
Windows ネットワークフォルダー内の iLO システムの表示....273

リモートサポートの管理....275
HPE 内蔵リモートサポート....275
デバイスサポート....276
HPE リモートサポートにより収集されるデータ....276
HPE プロアクティブケアサービス....277
リモートサポート登録に関する前提条件....277

HPE 組み込みリモートサポートでサポートされるブラウザー....278
リモートサポート登録用の ProLiant サーバーのセットアップ....279
Insight Online Direct Connect のネットワーク要件....280
Insight Remote Support Central Connect 環境のセットアップ....281
Insight Online へのアクセスの確認....282
Insight Online Direct Connect の登録....282
Insight Online Direct Connect の登録（手順 1）....283
Insight Online Direct Connect の登録（手順 2）....283
登録が完了したことの確認（iLOWeb インターフェイス）....284
登録後の手順（オプション）の完了....284
Web プロキシ設定を編集する (Insight Online Direct Connect のみ)....285
Insight Remote Support Central Connect の登録....285
Insight Online Direct Connect からの登録の解除....286
Insight Remote Support Central Connect の登録解除....286
リモートサポートサービスイベント....286
サービスイベントの送信....287
メンテナンスモードの設定....287
メンテナンスモードの有効期限の編集....288
メンテナンスモードのクリア....288
メンテナンスモードのステータスの表示....288
テストサービスイベントの送信....289
サービスイベントログの表示....290
サービスイベントログのクリア....292
リモートサポートのデータ収集....292
データ収集情報の送信....292
Active Health System が報告する情報の送信....293
iLO でのデータ収集ステータスの表示....293
iLO での Active Health System レポートステータスの表示....294
Insight Online でのデータ収集ステータスの表示....294
Insight RS Console（Insight Remote Support Central Connect のみ）でのデータ収集ステータスの表示....294
Insight Online Direct Connect のホストサーバーとして使用する ProLiant サーバーの登録....295
サポートされるデバイスのリモートサポート設定の変更....295
サポートされるデバイスの Central Connect から Direct Connect リモートサポートへの変更....296
サポートされるデバイスの Direct Connect から Central Connect リモートサポートへの変更....296

iLO の管理機能の使用....297
iLO ユーザーアカウント....297
ローカルユーザーアカウントの追加....297
ローカルユーザーアカウントの編集....298
ユーザーアカウントの削除....299
iLO ユーザーアカウントオプション....299
iLO ユーザーアカウントの権限....300
iLO ユーザーアカウントロール....301
パスワードに関するガイドライン....301
IPMI/DCMI ユーザー....302
ユーザーアカウントの表示....302
iLO ディレクトリグループ....303
ディレクトリグループの追加....303
ディレクトリグループの編集....304
ディレクトリグループの削除....305
ディレクトリグループのオプション....305
Active Directory の入れ子型グループ（スキーマフリー構成のみ）....305

ディレクトリグループ権限 306
ディレクトリグループの表示 306
ブート順序 307
サーバーブートモードの設定 307
サーバーブート順序の構成 307
ワンタイムブートステータスの変更 308
ROM ベースユーティリティを次回のリセット時に起動 310
ライセンスキーのインストール 310
ライセンス情報の表示 311
iLO ライセンス 311
iLO でのキーマネージャーの使用 312
サポートされているキーマネージャー 312
リモートキー管理の構成 312
キーマネージャーサーバーの構成 313
キーマネージャー構成の詳細の追加 314
キーマネージャー構成のテスト 316
キーマネージャーイベントの表示 316
キーマネージャーログのクリア 317
言語パック 317
フラッシュファームウェア機能で言語パックをインストール 318
言語パックの選択 319
デフォルト言語設定の構成 319
現在の iLO Web インターフェイスセッション言語の構成 319
言語パックのアンインストール 320
ファームウェア検証 320
ファームウェア検証設定の構成 321
ファームウェア検証スキャンの実行 322
ファームウェアヘルスステータスの表示 322
隔離されたファームウェアの表示 323
隔離されたファームウェアのダウンロード 324
隔離されたファームウェアの削除 324
フルシステムリカバリの開始 324

iLO のセキュリティ機能の使用 326
セキュリティガイドライン 326
重要なセキュリティ機能 328
iLO の機能によって使用されるポート 328
iLO アクセス設定 331
iLO アクセス設定の構成 331
iLO 機能の無効化 332
サーバーアクセス設定オプション 334
アカウントサービスのアクセス設定オプション 334
iLO アクセス設定オプション 335
サービスアクセス設定オプションのアップデート 339
ネットワークアクセス設定オプション 339
iLO サービスポート 343
iLO サービスポート経由での Active Health System ログのダウンロード 343
iLO サービスポートを通じて iLO にクライアントを接続する 344
iLO サービスポート設定の構成 345
iLO サービスポートを通じて接続するクライアントを設定する 346
iLO サービスポートのサポート対象デバイス 346
iLO サービスポートを通じた Active Health System ログダウンロードのサンプルテキストファイル 347
SSH キーの管理 348
Web インターフェイスを使用した新しい SSH キーの認証 348

CLI を使用した新しい SSH キーの認証....349
SSH キーの削除....349
HPE SIM サーバーからの SSH キーを認証するための要件....350
SSH ホストキーの表示....350
認証済み SSH キーの表示....351
SSH キー....351
サポートされている SSH キー形式の例....352
CAC Smartcard 認証....353
CAC Smartcard 認証設定の構成....353
CAC Smartcard 認証用の信頼済み証明書の管理....355
証明書マッピング....357
SSL 証明書の管理....358
SSL 証明書情報の表示....359
SSL 証明書の取得とインポート....359
SSL 証明書の削除....361
iLO のディレクトリの認証と認可設定....362
認証およびディレクトリサーバー設定を構成するための前提条件....362
iLO で Kerberos 認証の設定を構成します....363
iLO におけるスキーマフリーディレクトリ設定の構成....364
iLO における HPE 拡張スキーマディレクトリ設定の構成....365
ディレクトリユーザーコンテキスト....367
ディレクトリサーバー CA 証明書....368
Kerberos 認証およびディレクトリ統合によるローカル ユーザー アカウント....368
ディレクトリテストの実行....368
iLO 暗号化設定....371
製品または「高セキュリティ」セキュリティ状態の有効化....372
FIPS および CNSA セキュリティ状態を有効にする....372
高いセキュリティ状態を使用する場合の iLO への接続....374
iLO による FIPS 承認済み環境の構成....375
FIPS セキュリティ状態の無効化....375
CNSA セキュリティ状態の無効化....376
iLO セキュリティ状態....377
SSH 暗号、キー交換、および MAC のサポート....379
SSL 暗号および MAC のサポート....380
HPE SSO....381
HPE SSO 用の iLO の設定....382
信頼済みの証明書の追加....383
HPE SIM SSO 証明書の取得....383
直接 DNS 名のインポート....384
信頼済みの証明書とレコードの表示....384
信頼済みの証明書とレコードの削除....385
ログインセキュリティバナーの構成....385
システムメンテナンススイッチ....386
iLO セキュリティを無効にする理由....387

iLO 管理設定の構成....388
Agentless Management と AMS....388
Agentless Management Service....389
AMS のインストール....389
AMS のインストールの確認....390
AMS の再起動....391
System Management Assistant....391
SNMP 設定の構成....395
SNMP オプション....396
SNMPv3 認証....396

SNMP アラートの送信先の追加 396
SNMP アラートの送信先のオプション 397
SNMP アラート送信先の編集 397
SNMP アラート送信先の削除 398
SNMPv3 ユーザーの構成 398
SNMPv3 ユーザーオプション 399
SNMPv3 ユーザーの削除 400
SNMPv3 設定の構成 400
SNMPv3 の設定オプション 400
SNMP アラートの構成 401
SNMP アラートの設定 401
AMS コントロールパネルを使用した SNMP および SNMP アラートの設定（Windows 専用） 402
SNMP トラップ 403
REST アラート 417
IPMI アラート 427
iLO アラートメール 428
アラートメールを有効にする 428
アラートメールを無効にする 431
リモート syslog 431
iLO リモート syslog の有効化 431
iLO リモート syslog の無効化 432
リモート Syslog アラートレベル（Linux） 432

ライフサイクル管理機能の使用 433
Always On Intelligent Provisioning 433
iLO からの Intelligent Provisioning の起動 433
One-button セキュア消去 433
One-button セキュア消去アクセス方式 433
iLO から One-button セキュア消去プロセスを開始するための前提条件 434
iLO からの One-button セキュア消去プロセスの開始 434
One-button セキュア消去後にシステムを動作状態に戻す 436
One-button セキュア消去レポートの表示 437
CSV ファイルへの One-button セキュア消去レポートの保存 438
One-button セキュア消去レポートの削除 438
One-button セキュア消去の完了後のシステムへの影響 439
One-button セキュア消去の FAQ 441
iLO のバックアップとリストア 445
バックアップとリストアの操作中にリストアされる情報 445
バックアップとリストアの操作中にリストアされない情報 445
iLO 構成を手動でリストアする理由 446
iLO 構成のバックアップ 447
iLO 構成のリストア 447
システムボード交換後の iLO 構成のリストア 448

エンクロージャー、フレーム、およびシャーシの操作 449
Onboard Administrator 449
OA 情報の表示 449
OA Web インターフェイスの起動 450
サーバーまたはエンクロージャー UID LED の切り替え 450
iLO オプション 450
フレーム情報の表示 451
フレームの詳細 451
フレームまたはコンピュートモジュール UID の切り替え 452

シャーシ情報の表示....452
シャーシ情報....452
電源装置のリスト....453
各電源装置の詳細....453
インテリジェント PDU の詳細....455
Smart Storage Energy Pack のリスト....455
個々の Energy Pack の詳細....455
パワーレギュレーション....456
電力レギュレーターモード設定の構成....456
グローバルパワーレギュレーション設定の構成....457
ゾーンマッピングの構成....458
ゾーンの優先度設定の構成....459
消費電力上限値設定の構成....460
電力較正の構成....461
較正データの表示....462
ドライブベイのマッピング....462
ドライブベイのマッピング情報の表示....463
ドライブベイのマッピングの構成....464
ドライブベイのマッピング構成をデフォルト構成に設定....465
ドライブベイのマッピング構成のエクスポートとインポート....465

iLO と他のソフトウェア製品およびツールとの使用....469
iLO およびリモート管理ツール....469
リモート管理ツールの iLO からの起動....469
リモートマネージャー構成の削除....469
iLO を HPE OneView と一緒に使用する....470
IPMI サーバー管理....471
Linux 環境での IPMI ツールの高度な使用方法....471
HPE SIM での iLO の使用....472
HPE SIM の機能....472
HPE SIM での SSO の確立....473
iLO の識別および関連付け....473
HPE SIM での SNMP アラートの受信....473
iLO と HPE SIM の HTTP ポート一致要件....474
HPE SIM での iLO ライセンス情報の確認....474

Kerberos 認証とディレクトリサービスの設定....475
iLO での Kerberos 認証....475
Kerberos 認証の設定....475
Kerberos 認証用の iLO ホスト名とドメイン名の構成....475
ドメインコントローラーでの Kerberos サポートの準備....476
Windows 環境での iLO 用キータブファイルの生成....477
ご使用の環境が Kerberos 認証の時刻要件を満たしていることの確認....479
サポートされるブラウザーでのシングルサインオンの設定....479
ディレクトリ統合の利点....481
iLO で使用するディレクトリ構成の選択....482
スキーマフリーディレクトリ認証....482
ディレクトリ統合の設定（スキーマフリー構成）....484
スキーマフリーディレクトリ統合を使用するための前提条件....484
HPE 拡張スキーマディレクトリ認証....484
ディレクトリサービスのサポート....484
ディレクトリ統合の設定（HPE 拡張スキーマ構成）....485
HPE 拡張スキーマ構成で Active Directory を設定するための前提条件....486
iLO ディレクトリサポートソフトウェアのインストール....486

Schema Extender の実行....488
ディレクトリサービスオブジェクト....489
HPE Active Directory スナップインによって追加される管理オプション....489
ディレクトリ対応リモート管理（HPE 拡張スキーマ構成）....493
Active Directory と HPE 拡張スキーマの構成（構成例）....498
ディレクトリサービスによるユーザーログイン....501
一度に複数の iLO システムを構成するためのツール....501
ProLiant 管理プロセッサー用のディレクトリサポート（HPLOMIG）....502
HPLOMIG によるディレクトリ認証の設定....503
管理プロセッサーの検出....504
（オプション）管理プロセッサーのファームウェアのアップグレード（HPLOMIG）..505
ディレクトリ構成オプションの選択....507
マネジメントプロセッサーの命名（HPE 拡張スキーマのみ）....508
HPE 拡張スキーマを選択したときのディレクトリの設定....509
管理プロセッサーの設定（スキーマフリー構成のみ）....512
ディレクトリ用の管理プロセッサーのセットアップ....513
LDAP CA 証明書のインポート....514
（オプション）HPLOMIG を使用したディレクトリテストの実行....515
ディレクトリサービススキーマ....517
HPE Management コア LDAP OID クラスおよび属性....517
コアクラスの定義....518
コア属性の定義....519
Lights-Out Management 固有の LDAP OID クラスおよび属性....522
Lights-Out Management 属性....522
Lights-Out Management クラスの定義....522
Lights-Out Management 属性の定義....523

iLO の工場出荷時設定へのリセット....526
iLO の工場出荷時デフォルト設定へのリセット（iLO 5 構成ユーティリティ）....526

iLO モバイルアプリの使用....528
iLO モバイルアプリケーションの機能....528
iLO モバイルアプリの制限事項....528
Android デバイスでの iLO モバイルアプリの使用....529
モバイルアプリへの iLO システムの追加....529
QR コードのスキャンによるモバイルアプリへの iLO システムの追加....529
iLO システムのリストの編集....530
リストからの iLO システムの削除....530
iLO システムのリストの表示....530
リモートコンソールの起動....530
リモートコンソールの使用方法....531
モバイルアプリのキーボードの使用方法....531
サポートされるリモートコンソールのジェスチャー....532
Web サーバーに保存されたスクリプトの起動....532
iLO Web インターフェイスの起動....532
iLO モバイルアプリの履歴のクリア....533
iOS デバイスでの iLO モバイルアプリの使用....533
モバイルアプリへの iLO システムの追加....533
QR コードのスキャンによるモバイルアプリへの iLO システムの追加....533
iLO システムのリストの編集....534
リストからの iLO システムの削除....534
iLO システムのリストの表示....534
リモートコンソールの起動....535
リモートコンソールの使用方法....535

モバイルアプリのキーボードの使用方法.....535
サポートされるリモートコンソールのジェスチャー.....536
Web サーバーに保存されたスクリプトの起動.....536
iLO Web インターフェイスの起動.....536
iLO モバイルアプリの履歴のクリア.....537
iLO モバイルアプリのフィードバック.....537

Web サイト.....538

サポートと他のリソース.....540
Hewlett Packard Enterprise サポートへのアクセス.....540
アップデートへのアクセス.....540
リモートサポート（HPE 通報サービス）.....541
保証情報.....541
規定に関する情報.....541
ドキュメントに関するご意見、ご指摘.....542

iLO

iLO 5 は、HPE サーバーおよびコンピュートモジュールのシステムボードに組み込まれたリモートサーバー管理プロセッサーです。iLO では、リモートの場所からサーバーを監視および制御できます。iLO 管理は、サーバーをリモートで構成、アップデート、監視、および修復するための複数の方法を提供する強力なツールです。

iLO 機能

iLO には、次の標準機能およびライセンスされた機能が含まれています。これらの機能のライセンス要件を確認するには、iLO のライセンスガイドを参照してください。

- **Active Health System ログ** - Active Health System ログをダウンロードします。オープンサポートケースがある場合はログファイルを Hewlett Packard Enterprise に送信できます。または、ログを Active Health System Viewer にアップロードできます。
- **Agentless Management** - Agentless Management とともに、管理ソフトウェア（SNMP）はホスト OS ではなく iLO ファームウェア内で動作します。この構成により、ホスト OS 上のメモリおよびプロセッサーリソースがサーバーアプリケーション用に解放されます。iLO はすべての重要な内部サブシステムを監視し、ホスト OS がインストールされていない場合でも、中央管理サーバーに直接 SNMP アラートを送信できます。
- **展開とプロビジョニング** - 展開およびプロビジョニングの自動化などのタスクに仮想電源および仮想メディアを使用します。
- **組み込みリモートサポート** - サポート対象サーバーを HPE リモートサポートに登録できます。
- **ファームウェア管理** -iLO レポジトリ、インストールセット、インストールキューなどを含む iLO ファームウェア機能を使用して、ファームウェアのアップデートを管理します。
- **ファームウェアの検証とリカバリ** - スケジュール済みまたはオンデマンドでファームウェアの検証スキャンを実行して、問題が検出されたときに実装するリカバリ操作を設定します。
- バックアップ **iLO バックアップとリストア** - iLO の構成をバックアップして、同じハードウェア構成のシステムに復元できます。
- **iLO 連携管理** - iLO 連携機能を使用して、一度に複数のサーバーを検出および管理します。
- **iLO インターフェイスの管理** - セキュリティを強化するために、選択した iLO インターフェイスおよび機能を有効または無効にします。
- **iLO RESTful API および RESTful インターフェイスツール（iLOREST）** - iLO 5 には、Redfish API 準拠である iLO RESTful API が含まれています。
- **iLO サービスポート** - サポート対象の USB イーサネットアダプターを使用してクライアントを iLO サービスポートに接続し、サーバーに直接アクセスします。Hewlett Packard Enterprise は、Ethernet アダプターに HPE USB（部品番号 Q7Y55A）を使用することをお勧めします。また、USB キーを接続して、Active Health System ログをダウンロードすることもできます。
- **インテグレーテッドマネジメントログ** - サーバーイベントを表示し、SNMP アラート、リモート syslog、およびメールアラート経由での通知を設定します。
- **統合リモートコンソール** - サーバーとのネットワーク接続があれば、安全で高パフォーマンスのコンソールにより、世界中どこからでもサーバーにアクセスして管理できます。
- **IPMI** - iLO ファームウェアは、IPMI バージョン 2.0 仕様に基づくサーバー管理を提供します。
- **Jitter smoothing** - スムージングレベルを微小変動し、プロセッサーの周波数変動を分散させます。

- **詳細情報へのリンク** - サポート対象イベントのトラブルシューティング情報が**インテグレーテッドマネジメントログ**ページに表示されます。
- **One-button セキュア消去** - サーバーを安全に使用停止にしたり、別の用途のために準備したりします。
- **パフォーマンス監視** - Innovation Engine のサポートによってサーバーでサポートされたセンサーから収集したパフォーマンスデータを表示します。収集したデータに基づいてアラートを構成できます。
- **消費電力と電力設定** - サーバーの消費電力を監視し、サーバーの電力を設定し、サポートされているサーバーの消費電力上限を設定します。
- **電源管理** - リモートから安全に管理対象サーバーの電源状態を制御できます。
- **安全なリカバリ** - 電源の作動時に iLO ファームウェアを検証します。ファームウェアが無効な場合、iLO ファームウェアは自動的にフラッシュされます（iLO Standard ライセンス）。

  サーバーの起動時に、システム ROM を検証します。有効なシステム ROM が検出されないと、サーバーは起動できません。リカバリオプションには、アクティブおよび冗長 ROM のスワッピングや、ファームウェアの検証スキャンとリカバリアクションの起動などがあります。スケジュール済みのファームウェア検証スキャンと自動リカバリを行うには、iLO Advanced のライセンスが必要です。
- **セキュリティログ** - iLO ファームウェアによって記録されたセキュリティイベントのレコードを表示します。
- **セキュリティダッシュボード** - 重要なセキュリティ機能のステータスを表示したり、潜在的なリスクがあるかどうか設定を評価したりします。リスクが検知されたら、詳細情報とシステムセキュリティを向上させる方法についてのアドバイスを見ることができます。
- **セキュリティ状態** - ご使用の環境に合ったセキュリティ状態を設定します。iLO は、本番稼働（デフォルト）のセキュリティ状態や、高セキュリティ、FIPS、CNSA などのより高いセキュリティ状態をサポートします。
- **サーバーヘルスの監視** - iLO はサーバー内部の温度を監視し、修正信号をファンに送信して適切なサーバー冷却を維持します。さらに、インストールされているファームウェアとソフトウェアのバージョン、および他の監視対象のサブシステムとデバイスのステータスも監視します。
- **システム診断** - セーフモードまたはインテリジェント診断モードで起動してシステムを診断します。工場デフォルト設定またはシステムデフォルト設定をリストアできます。
- **Two-Factor 認証** - Two-Factor 認証は、Kerberos および CAC Smartcard 認証でサポートされます。
- **ユーザーアクセス** - ローカルまたはディレクトリベースのユーザーアカウントを使用して iLO にログインします。ローカルまたはディレクトリベースのアカウントで CAC Smartcard 認証を使用できます。
- **仮想 NIC** - ホストオペレーティングシステムから iLO に安全にアクセスします。
- **仮想メディア** - リモートから高性能仮想メディアデバイスをサーバーにマウントできます。
- **ワークロードアドバイザー** - 選択されたサーバーワークロード特性を表示します。監視対象データに基づき、推奨のパフォーマンスチューニング設定を表示したり、構成したりできます。
- **Workload Matching** - 構成済みのワークロードプロファイルを使用して、サーバーのリソースを微調整できるようにします。

iLO Web インターフェイス

iLO Web インターフェイスを使用して、サポートされるブラウザーを介して iLO にアクセスし、管理対象サーバーを監視および構成できます。

詳しくは

iLO Web インターフェイスの概要

ROM ベースの構成ユーティリティ

UEFI システムユーティリティの iLO 5 構成ユーティリティを使用すると、ネットワークパラメーター、グローバル設定、およびユーザーアカウントを構成できます。

iLO 5 構成ユーティリティは、初期の iLO セットアップのために設計されていて、継続的な iLO 管理のためのものではありません。このユーティリティはサーバーが起動するときに起動でき、リモートコンソールを使用してリモートから実行できます。

ユーザーが iLO 5 構成ユーティリティにアクセスするときにログインを要求するように iLO を構成できます。または、すべてのユーザー用のユーティリティを無効にすることもできます。これらの設定は、**アクセス設定**ページで構成できます。iLO 5 構成ユーティリティを無効にすると、iLO セキュリティを無効にするようにシステムメンテナンススイッチが設定されないかぎり、ホストからの再構成を防止します。

iLO 5 構成ユーティリティにアクセスするには、POST の実行時に **F9** キーを押して UEFI システムユーティリティを起動します。**システム構成**、**iLO 5 構成ユーティリティ**の順にクリックします。

詳しくは

iLO アクセス設定の構成

iLO モバイルアプリケーション

iLO モバイルアプリケーションは、モバイルデバイスからサポートされるサーバーへのアクセスを提供します。モバイルアプリケーションは、iLO プロセッサーと直接やり取りし、サーバーがプラグインされている限りサーバーを総合的に制御できるようにします。たとえば、正常な状態にあるサーバーにアクセスすることも、空のハードドライブを備えた電源が入っていないサーバーにアクセスすることもできます。IT 管理者は、ほとんどどこからでも、問題のトラブルシューティングを行い、ソフトウェアの展開を実行することができます。

詳しくは

iLO モバイルアプリの使用

iLO RESTful API

iLO には、Redfish API 準拠である iLO RESTful API が含まれています。iLO RESTful API は、基本的な HTTPS 操作（GET、PUT、POST、DELETE、および PATCH）を iLO Web サーバーに送信することで、サーバー管理ツールからサーバーの構成、インベントリ、および監視を実行できる管理インターフェイスです。

iLO RESTful API について詳しくは、Hewlett Packard Enterprise の Web サイト（**https://www.hpe.com/support/restfulinterface/docs**）を参照してください。

iLO RESTful API を使用したタスクの自動化について詳しくは、**https://www.hpe.com/info/redfish** にあるライブラリとサンプルコードを参照してください。

詳しくは、**Redfish & How it works with HPE Server Management** のビデオを見てください。

RESTful インターフェイスツール

RESTful インターフェイスツール（iLOREST）は、HPE サーバー管理タスクを自動化するためのスクリプティングツールです。これは、iLO RESTful API を利用する、簡素化されたコマンドのセットを提供します。ツールは、ご使用のコンピューターにインストールしてリモートで使用することも、Windows または Linux オペレーティングシステムを搭載するサーバーにローカルでインストールすることもできま

す。RESTful インターフェイスツールでは、自動化時間を短縮するための対話型モード、スクリプト可能なモード、および CONREP のようなファイルベースモードが提供されます。

詳しくは、次の Web サイトを参照してください。**https://www.hpe.com/info/resttool**

iLO スクリプティングとコマンドライン

iLO スクリプティングツールを使用して、複数のサーバーを設定したり、展開プロセスに標準設定を組み込んだり、サーバーやサブシステムを制御したりできます。

iLO スクリプティングおよび CLI ガイドには、コマンドラインインターフェイスまたはスクリプティングインターフェイスを通じて iLO を使用するために利用できる構文およびツールに関する説明が記載されています。

iLO Amplifier Pack

iLO Amplifier Pack は、高度なサーバーインベントリおよびファームウェアおよびドライバーのアップデートソリューションです。iLO Advanced 機能を使用して高速検出、詳細なインベントリレポート、およびファームウェアとドライバーのアップデートを有効にします。iLO Amplifier Pack は、ファームウェアとドライバーの大規模アップデートを目的として、サポートされている数千台のサーバーの迅速なサーバー検出およびインベントリを実行します。

iLO Amplifier Pack について詳しくは、次の Web サイトを参照してください。**https://www.hpe.com/servers/iloamplifierpack**

HPE InfoSight for Servers

HPE InfoSight ポータルは、HPE によってホストされている安全な Web インターフェイスで、サポートされているデバイスをグラフィカルインターフェイスによって監視できます。

HPE InfoSight for Servers：

- HPE InfoSight の機械学習と予測分析を、Active Health System（AHS）および HPE iLO のヘルスとパフォーマンス監視と組み合わせて、パフォーマンスを最適化し、問題を予測して防止します
- AHS からのセンサーデータとテレメトリデータを自動的に収集および分析し、インストールベースの動作から洞察を導き出して、問題の解決とパフォーマンスの向上に関する推奨事項を提供します

HPE InfoSight for Servers を使用するための準備について詳しくは、**https://www.hpe.com/info/infosight-servers-docs** を参照してください。

iLO のセットアップ

iLO をセットアップするための準備

iLO 管理プロセッサーをセットアップする前に、ネットワークとセキュリティの処理方法を決める必要があります。以下の質問に回答していくと、iLO の設定方法が明らかになります。

手順

1. **iLO はどの方法でネットワークに接続しますか。**
2. **共有ネットワークポート構成で NIC チーミングを使用しますか。**
3. **iLO はどの方法で IP アドレスを取得しますか。**
4. **どのようなアクセスセキュリティおよびユーザーアカウントと権限が必要ですか。**
5. **iLO の設定にどのようなツールを使用しますか。**

iLO ネットワーク接続オプション

iLO は、専用の管理ネットワークまたは本番環境ネットワークの共有接続を使用してネットワークに接続できます。

専用管理ネットワーク

この設定では、独立したネットワークに iLO ポートを配置します。ネットワークが独立しているため、性能が向上し、どのワークステーションをネットワークに接続するかを物理的に制御できるので、セキュリティが強化されます。また、本番環境ネットワーク内のハードウェアに障害が発生した場合には、サーバーへの冗長アクセスが提供されます。この構成では、本番環境ネットワークから直接 iLO にアクセスすることはできません。専用管理ネットワークは、優先される iLO ネットワーク構成です。

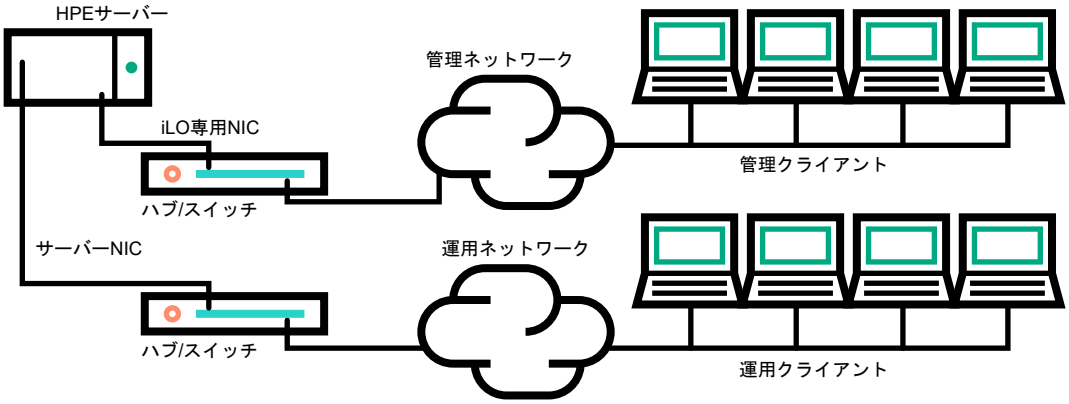


図 1: 専用管理ネットワーク

本番環境ネットワーク

この設定では、NIC と iLO ポートの両方を本番環境ネットワークに接続します。iLO で、このタイプの接続は、共有ネットワークポート構成と呼ばれます。特定の Hewlett Packard Enterprise 内蔵 NIC とアドオンカードが、この機能を提供します。この接続により、ネットワークのどこからでも iLO にアクセスできます。共有ネットワークポート構成を使用すると、iLO をサポートするために必要なネットワークハードウェアやインフラストラクチャの量が減ります。

この設定の使用にはいくつかの欠点があります。

- 共有ネットワーク接続では、トラフィックによって、iLO のパフォーマンスが低下することがあります。
- サーバーの起動時、およびオペレーティングシステム NIC ドライバーのロードおよびアンロード時に、短時間（2～8 秒）、ネットワークから iLO にアクセスできません。この短い時間の経過後に、iLO の通信が復元され、iLO がネットワークトラフィックに応答します。

  このようなシチュエーションが起きた場合は、リモートコンソールと、接続されている iLO 仮想メディアデバイスが切断されることがあります。

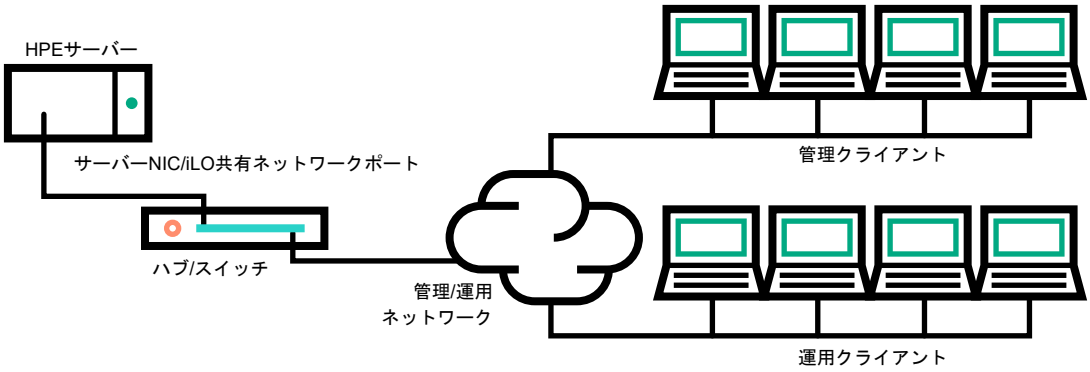


図 2: 共有ネットワーク接続

iLO ネットワーク有効化モジュール

一部のサーバーでは、専用管理ネットワーク（デフォルト）または共有ネットワーク接続によるリモート管理のサポートを追加するために、オプションの iLO ネットワーク有効化モジュールが必要です。iLO ネットワーク有効化モジュールがインストールされていない場合、iLO アクセスは、ホストベース（インバンド）のアクセス方式でのみサポートされます。サポートされているホストベースのアクセス方式の例には、iLO RESTful API、UEFI システムユーティリティ、iLO サービスポート（利用可能な場合）、および仮想 NIC が含まれます。

サーバーでサポートされているネットワーク接続を確認するには、サーバーのユーザーガイドを参照してください。

共有ネットワークポート構成による NIC チーミング

NIC チーミングは、サーバー NIC のパフォーマンスと信頼性を向上させるために使用できる機能です。

NIC チーミングの制限

iLO で共有ネットワークポートを使用するように構成する際に、チーミングモードを選択した場合：

- 次の状況で iLO ネットワーク通信がブロックされます。
  - 選択された NIC チーミングモードによって、iLO が接続されているスイッチは、iLO が共有するように構成されているサーバー NIC/ポートからのトラフィックを無視するようになります。
  - 選択された NIC チーミングモードによって、iLO 宛てのすべてのトラフィックが、iLO が共有するように構成されていない NIC/ポートに送信されます。
- iLO とサーバーは同じスイッチポートで送受信するため、選択された NIC チーミングモードでは、スイッチが同じスイッチポートでの 2 つの異なる MAC アドレスを持つトラフィックを許容するように

する必要があります。LACP（802.3ad）の一部の実装では、同じリンク上の複数の MAC アドレスを許容しません。

Hewlett Packard Enterprise NIC チーミングモード

サーバーで Hewlett Packard Enterprise NIC チーミングを使用するように構成した場合、次のガイドラインに従ってください。

ネットワークフォールトトレランス（NFT）

サーバーは 1 つだけの NIC（プライマリアダプター）で送受信します。チームに含まれる他の NIC（セカンダリアダプター）はトラフィックを送信せず、受信したトラフィックを無視します。このモードにより、iLO 共有ネットワークポートが正常に動作します。

iLO が**優先プライマリアダプター**として使用する NIC/ポートを選択します。

送信ロードバランシング（TLB）

サーバーは、複数のアダプターで送信しますが、プライマリアダプターでのみ受信します。このモードにより、iLO 共有ネットワークポートが正常に動作します。

iLO が**優先プライマリアダプター**として使用する NIC/ポートを選択します。

スイッチアシストロードバランシング（SLB）

このモードタイプは、以下のことを指します。

- HPE ProCurve ポートトランキング
- Cisco Fast EtherChannel/Gigabit EtherChannel（静的モードのみ、PAgP なし）
- IEEE 802.3ad リンクアグリゲーション（静的モードのみ、LACP なし）
- ベイネットワークマルチリンクトランキング
- Extreme Network Load Sharing

このモードでは、プライマリアダプターとセカンダリアダプターの概念はありません。すべてのアダプターはデータを送受信する目的で等しいと見なされます。このモードは、iLO 宛のトラフィックを受信できるサーバー NIC/ポートが 1 つだけであるため、iLO 共有ネットワークポート構成で最も問題となる可能性があります。スイッチアシストロードバランシングの実装に対するスイッチベンダーの制限を判断するには、スイッチベンダーのドキュメントを参照してください。

サーバーで、別の NIC チーミングの実装を使用する場合の NIC チーミングモードの選択については、**NIC チーミングの制限**およびベンダーのドキュメントを参照してください。

iLO IP アドレスの取得

iLO がネットワークに接続されてからアクセスを可能にするには、iLO 管理プロセッサーが IP アドレスとサブネットマスクを取得する必要があります。動的アドレスまたは静的アドレスを使用することができます。

動的 IP アドレス

動的 IP アドレスは、デフォルトで設定されます。iLO は、DNS または DHCP サーバーから IP アドレスとサブネットマスクを取得します。この方法が最も簡単です。

DHCP を使用する場合：

- iLO 管理ポートは、DHCP サーバーに接続されたネットワークに接続する必要があります。また、iLO をネットワークに接続してから電源を入れなければなりません。DHCP は、電源が投入される

とただちに要求を送信します。iLO が最初に起動したときに DHCP の要求に対する回答がない場合、DHCP は、90 秒間隔で要求を再発行します。

- DHCP サーバーは、DNS および WINS 名前解決を提供するように設定しなければなりません。

静的 IP アドレス

ネットワークで DNS または DHCP サーバーを使用できない場合、静的 IP アドレスが使用されます。静的 IP アドレスは、iLO 5 構成ユーティリティを使用して構成できます。

静的 IP アドレスの使用を予定する場合は、iLO セットアッププロセスを開始する前に IP アドレスが必要です。

iLO アクセスセキュリティ

次の方法で iLO へのアクセスを管理できます。

ローカルアカウント

iLO には、最大 12 のユーザーアカウントを格納できます。この構成は、研究所や中小企業のような小規模環境に最適です。

ローカルアカウントによるログインセキュリティは iLO アクセス設定およびユーザー権限によって管理します。

ディレクトリサービス

13 ユーザー以上をサポートするには、ディレクトリサービスを使用してアクセスの認証や権限付与を行うよう iLO を構成します。この構成により、ユーザーの数の制限がなくなります。また、この構成は、エンタープライズ内の iLO デバイスの数に合わせて、簡単に拡張できます。

ディレクトリサービスを使用する場合でも、代替アクセスとして少なくとも 1 つのローカル管理者アカウントを有効にしておきます。

ディレクトリにより iLO デバイスとユーザーを集中的に管理することができ、より強力なパスワードポリシーを適用できます。

CAC スマートカード認証

ローカルアカウントとディレクトリサービスと共に Common Access Smartcard を設定して、iLO ユーザーアクセスを管理できます。

詳しくは

iLO のディレクトリの認証と認可設定
CAC Smartcard 認証
iLO アクセス設定の構成
iLO ユーザーアカウント

iLO 構成ツール

iLO は、設定と操作用にさまざまなインターフェイスをサポートしています。このガイドで説明する主なインターフェイスは、次のとおりです。

iLO Web インターフェイス

iLO の Web インターフェイスは、Web ブラウザーを使用してネットワーク上の iLO に接続できる場合に使用します。また、iLO 管理プロセッサーの設定を変更する場合も、この方法を使用できます。

ROM ベースセットアップ

システム環境が DHCP、DNS、または WINS を使用しない場合は、iLO 5 構成ユーティリティを使用します。

その他の iLO 構成ツール

このガイドでは説明しませんが、以下の iLO 構成オプションがあります。

Intelligent Provisioning

Intelligent Provisioning を起動するには、POST 中に **F10** キーを押します。

iLO の Web インターフェイスから Always On Intelligent Provisioning にアクセスすることもできます。詳しくは、Intelligent Provisioning のユーザーガイドを参照してください。

iLO RESTful API

サーバー管理ツールから使用することで iLO 経由でサポート対象サーバーの構成、インベントリ、および監視を実行できる管理インターフェイスです。詳しくは、次の Web サイトを参照してください。**https://www.hpe.com/info/redfish**

HPE OneView

iLO 管理プロセッサーと対話して ProLiant サーバーまたは Synergy コンピュートモジュールを構成、監視、および管理をする管理ツールです。詳しくは、HPE OneView のユーザーガイドを参照してください。

HPE Scripting Toolkit

このツールキットは、サーバーの無人/自動での大量インストールを可能にする、IT エキスパート向けのサーバーインストール製品です。詳しくは、Windows または Linux 用の Scripting Toolkit ユーザーガイドを参照してください。

スクリプティング

スクリプティングを使用して複数の iLO 管理プロセッサーを設定できます。スクリプトは、RIBCL と呼ぶスクリプティング言語用に記述された XML ファイルです。iLO は､RIBCL スクリプトを使用して設定できます。ネットワーク経由での設定、初期展開の際の設定、展開済みのホストからの設定などさまざまな設定が可能です。

以下の方法を使用できます。

- **HPQLOCFG** - ネットワーク経由で RIBCL スクリプトを iLO に送信する Windows コマンドラインユーティリティです。
- **HPONCFG** - ホスト上で実行され、RIBCL スクリプトをローカルの iLO に転送する、ローカルでのオンラインのスクリプトによるセットアップユーティリティです。
- カスタムスクリプティング環境（LOCFG.PL） - iLO スクリプティングサンプルには、RIBCL スクリプトをネットワーク経由で iLO に送信するために使用できる Perl サンプルが含まれています。
- **SMASH CLP** - SSH または物理シリアルポートからコマンドラインにアクセスできるときに使用できるコマンドラインプロトコルです。

これらの方法について詳しくは、iLO スクリプティング/コマンドラインガイドを参照してください。

iLO のサンプルスクリプトは、次の Web サイトから入手できます。**https://www.hpe.com/support/ilo5**

初期セットアップ手順

iLO はデフォルト設定のままでも、ほとんどの機能を使用できます。ただし iLO では、複数の企業環境のために柔軟なカスタム設定が可能です。この章では、初期の iLO セットアップ手順について説明します。

手順

1. iLO のセットアップと使用方法については、**一般的なセキュリティガイドライン**を参照してください。
2. **iLO をネットワークに接続します**。
3. 動的 IP アドレスを使用しない場合は、ROM ベースセットアップユーティリティを使用して**静的 IP アドレスを設定します**。
4. ローカルアカウント機能を使用する場合は、ROM ベースセットアップユーティリティを使用して**ユーザーアカウントを設定します**。
5. （オプション）**iLO ライセンスをインストールします**。
6. **必要に応じて、iLO ドライバーをインストールします**。

iLO ネットワークに接続する

本番環境ネットワークまたは専用の管理ネットワークを使用して iLO をネットワークに接続します。

iLO は、標準 Ethernet ケーブル（RJ-45 コネクターの付いた CAT 5 UTP ケーブルなど）を使用します。標準的な Ethernet ハブまたはスイッチへのハードウェアリンクを確立するには、ストレートケーブルが必要です。

ハードウェアのセットアップについて詳しくは、サーバーのユーザーガイドを参照してください。

詳しくは

iLO ネットワーク接続オプション

iLO の iLO 5 構成ユーティリティを使用したセットアップ

Hewlett Packard Enterprise は、初めて iLO をセットアップする場合と、DHCP、DNS、または WINS を使用しない環境に iLO のネットワークパラメーターを構成する場合に、iLO 5 構成ユーティリティを使用することをおすすめします。

静的 IP アドレスの構成（iLO 5 構成ユーティリティ）

この手順は、静的 IP アドレスを使用する場合にのみ必要です。動的 IP アドレスを使用する場合は、DHCP サーバーによって iLO の IP アドレスが自動的に割り当てられます。

インストールを簡単にするために、Hewlett Packard Enterprise は iLO で DNS または DHCP を使用することをおすすめします。

手順

1. （オプション）サーバーにリモートアクセスする場合、iLO リモートコンソールセッションを開始します。
2. サーバーを再起動するかまたは電源を入れます。
3. サーバーの POST 画面で **F9** キーを押します。

   UEFI システムユーティリティが起動します。
4. **システム構成**をクリックします。
5. **iLO 5 構成ユーティリティ**をクリックします。
6. DHCP を無効にします。

a. **ネットワークオプション**をクリックします。

b. **DHCP 有効**メニューで**オフ**を選択します。

IP アドレス、**サブネットマスク**、および**ゲートウェイ IP アドレス**ボックスが編集可能になります。DHCP 有効が**オン**に設定されている場合は、これらの値を編集できません。

7. **IP アドレス**、**サブネットマスク**、および**ゲートウェイ IP アドレス**ボックスに値を入力します。

8. 変更を保存して終了するには、**F12** キーを押します。

iLO 5 構成ユーティリティによって、保留中の構成変更を保存するか確認するメッセージが表示されます。

9. 保存して終了するには、**はい - 変更を保存します**をクリックします。

iLO 5 構成ユーティリティから、変更を反映するために iLO をリセットする必要があることが通知されます。

10. **OK** をクリックします。

iLO がリセットされ、iLO セッションが自動的に終了します。約 30 秒で再接続することができます。

11. 通常の起動プロセスを再開します。

a. iLO リモートコンソールを起動します。

iLO 5 構成ユーティリティは、前のセッションから開いたままになっています。

b. **ESC** キーを数回押して、**システム構成**ページに移動します。

c. システムユーティリティを終了し、通常のブートプロセスを再開するには、**システムを終了して再起動**をクリックします。

iLO 5 構成ユーティリティを使用したローカルユーザーアカウントの管理

ユーザーアカウントの追加（iLO 5 構成ユーティリティ）

手順

1. （オプション）サーバーにリモートアクセスする場合、iLO リモートコンソールセッションを開始します。

2. サーバーを再起動するかまたは電源を入れます。

3. サーバーの POST 画面で **F9** キーを押します。

UEFI システムユーティリティが起動します。

4. **システム構成**、**iLO 5 構成ユーティリティ**、**ユーザー管理**、**ユーザーの追加**の順にクリックします。

5. 新しいユーザーの権限を選択します。

権限を割り当てるには、権限名の横にあるメニューで**はい**を選択します。権限を削除するには、**いいえ**を選択します。

ログイン権限はデフォルトですべてのユーザーに割り当てられるため、iLO 5 構成ユーティリティでは表示されません。

リカバリセット権限は iLO 5 構成ユーティリティを通じて割り当てることができないため、リストにありません。

6. **新しいユーザー名**ボックスと**ログイン名**ボックスにユーザー名とログイン名を入力します。

7. パスワードを入力します。

   a. カーソルを**パスワード**ボックスに移動し、**Enter** キーを押します。

      新しいパスワードを入力しますボックスが開きます。

   b. パスワードを入力してから **Enter** キーを押します。

      新しいパスワードを確認してくださいボックスが開きます。

   c. 確認のためもう一度パスワードを入力して、**Enter** キーを押します。

   iLO 5 構成ユーティリティは、新しいアカウントの作成を確認します。

8. 確認ダイアログボックスを閉じるには、**OK** をクリックします。
9. 必要な数のユーザーアカウントを作成し、**F12** キーを押して変更を保存し、システムユーティリティを終了します。
10. 変更を確認するよう求められた場合は、**はい - 変更を保存します**をクリックしてユーティリティを終了し、ブートプロセスを再開します。

詳しくは

iLO ユーザーアカウントの権限
iLO ユーザーアカウントオプション
パスワードに関するガイドライン

ユーザーアカウントの編集（iLO 5 構成ユーティリティ）

手順

1. （オプション）サーバーにリモートアクセスする場合、iLO リモートコンソールセッションを開始します。
2. サーバーを再起動するかまたは電源を入れます。
3. サーバーの POST 画面で **F9** キーを押します。

   UEFI システムユーティリティが起動します。

4. **システム構成**、**iLO 5 構成ユーティリティ**、**ユーザー管理**、**ユーザーの編集/削除**の順にクリックします。
5. 編集または削除するユーザー名の**アクション**メニューを選択し、**編集**を選択します。

   アカウントのプロパティが表示されます。

6. **ログイン名**をアップデートします。
7. **パスワード**をアップデートします。

   a. カーソルを**パスワード**ボックスに移動し、**Enter** キーを押します。

      新しいパスワードを入力しますボックスが開きます。

   b. パスワードを入力してから **Enter** キーを押します。

      新しいパスワードを確認してくださいボックスが開きます。

   c. 確認のためもう一度パスワードを入力して、**Enter** キーを押します。

8. ユーザーアカウントの権限を変更します。

権限を割り当てるには、権限名の横にあるメニューで**はい**を選択します。権限を削除するには、**いいえ**を選択します。

ログイン権限はデフォルトですべてのユーザーに割り当てられるため、iLO 5 構成ユーティリティでは利用できません。

リカバリセット権限は iLO 5 構成ユーティリティを通じて割り当てることができないため、リストにありません。

9. 必要な数のユーザーアカウントをアップデートし、**F12** キーを押して変更を保存し、システムユーティリティを終了します。
10. 変更を確認するよう求められた場合は、**はい - 変更を保存します**をクリックしてユーティリティを終了し、ブートプロセスを再開します。

詳しくは

iLO ユーザーアカウントの権限
iLO ユーザーアカウントオプション
パスワードに関するガイドライン

ユーザーアカウントの削除（iLO 5 構成ユーティリティ）

手順

1. （オプション）サーバーにリモートアクセスする場合、iLO リモートコンソールセッションを開始します。
2. サーバーを再起動するかまたは電源を入れます。
3. サーバーの POST 画面で **F9** キーを押します。

   システムユーティリティが起動します。
4. **システム構成**、**iLO 5 構成ユーティリティ**、**ユーザー管理**、**ユーザーの編集/削除**の順にクリックします。
5. 削除するユーザーの**アクション**メニューで、**削除**を選択します。

   このページで変更を保存するときに削除するユーザー名にマークが付けられます。
6. 必要に応じて、削除する他のユーザーアカウントにマークを付けてから **F12** キーを押して変更を保存し、システムユーティリティを終了します。
7. 変更を確認するよう求められた場合は、**はい - 変更を保存します**をクリックしてユーティリティを終了し、ブートプロセスを再開します。

Web インターフェイスによる iLO のセットアップ

Web ブラウザーを使用してネットワーク上の iLO に接続できる場合は、iLO Web インターフェイスを使用して iLO を構成できます。また、iLO 管理プロセッサーの設定を変更する場合も、この方法を使用できます。

サポートされているブラウザーを使用して、デフォルトの DNS 名、ユーザー名、およびパスワードを入力して、リモートのネットワーククライアントから iLO にアクセスします。

詳しくは

サポートされているブラウザー
iLO Web インターフェイスの使用

iLO に初めてログインする方法

手順

1. **`https://<iLO`** ホスト名または **`IP`** アドレス**`>`**を入力します。

   iLO の Web インターフェイスのアクセスには HTTPS（SSL 暗号セッションで交換される HTTP）が必要です。

2. デフォルトのユーザー認証情報を入力して、**ログイン**をクリックします。

   ヒント: 初めて iLO にログインした後、Hewlett Packard Enterprise は、デフォルトのユーザーアカウントのパスワードを変更することをおすすめします。

詳しくは

ローカルユーザーアカウントの編集
パスワードに関するガイドライン

iLO のデフォルトの DNS 名とユーザーアカウント

iLO ファームウェアは、デフォルトのユーザー名、パスワード、および DNS 名が設定されています。デフォルトの情報は、iLO マネジメントプロセッサーを搭載するサーバーに取り付けられているシリアルラベルプルタブに記載されています。これらの値を使用し、Web ブラウザーを使用して、ネットワーククライアントからリモートで iLO にアクセスしてください。

- **ユーザー名** - Administrator
- **パスワード** - ランダムな 8 文字の文字列または共通のデフォルトパスワード。パスワードのタイプは工場出荷時に定義されており、サーバーの注文に含まれる SKU 番号によって異なります。
- **DNS 名** - ILOXXXXXXXXXXXX（**X** は、サーバーのシリアル番号）

重要: Hewlett Packard Enterprise は、初めて iLO にログインした後で、デフォルトのパスワードを変更することをお勧めします。

iLO を工場出荷時のデフォルト設定にリセットした場合は、リセット後にデフォルトの iLO アカウント認証情報（シリアルラベルプルタブに表示）を使用してログインします。

iLO ライセンスが必要な機能

iLO（Standard）は、追加コストまたはライセンスなしで Hewlett Packard Enterprise サーバーに事前設定されています。生産性を向上させる機能にはライセンスが必要です。詳しくは、**https://www.hpe.com/support/ilo-docs** にある iLO ライセンスガイドを参照してください。

iLO ライセンス機能を有効化するには、iLO ライセンスをインストールします。

詳しくは

ライセンスキーのインストール

iLO ドライバーのサポート

iLO は、内蔵のオペレーティングシステムを実行する独立したマイクロプロセッサーです。このアーキテクチャーでは、ホストのオペレーティングシステムとは関係なく、iLO のほとんどの機能を使用できま

す。iLO ドライバーは、HPONCFG や Agentless Management Service などのソフトウェアが iLO と通信できるようにします。インストールされている OS とシステム構成によって、インストール要件が決定します。

Windows

iLO で Windows を使用する場合は、以下のドライバーを使用できます。

- iLO 5 Channel Interface ドライバー for Windows - このドライバーは、Agentless Management Service、HPQLOCFG、ファームウェアのフラッシュコンポーネント、および他のユーティリティが iLO と通信する場合に必要です。SUM はこのドライバーを使用して、システムのファームウェアのインベントリを実行します。すべての構成でこのドライバーをインストールしてください。
- iLO 5 自動サーバー復旧ドライバー - このドライバーは、オペレーティングシステムがクラッシュまたはロックアップした場合にサーバーをリセットする ASR ハードウェアタイマーを管理します。

Linux

iLO で Linux を使用する場合は、`hpilo` 1.5.0 以降のドライバーを使用できます。

このドライバーは、エージェントおよびツールアプリケーションの iLO へのアクセスを管理します。

`hpilo` は、このバージョンの iLO ファームウェアでサポートされているすべてのサーバーオペレーティングシステム用の Linux カーネルの一部です。

`hpilo` は起動時に自動的にロードされます。

VMware

iLO で VMware を使用する場合は、`ilo` ドライバーを使用できます。

このドライバーは、Agentless Management Service、WBEM プロバイダー、およびツールアプリケーションの iLO へのアクセスを管理します。これは、カスタマイズされた Hewlett Packard Enterprise VMware イメージに含まれています。元の VMware イメージを使用するには、手動でドライバーをインストールする必要があります。

iLO ドライバーのインストール

手順

1. お使いの OS 用の iLO ドライバーを入手します。
   - **Windows の場合** - **SPP をダウンロード**するか、Hewlett Packard Enterprise サポートセンター（**https://www.hpe.com/support/ilo5**）からドライバーをダウンロードします。
   - **VMware の場合** - **SPP をダウンロード**するか、Hewlett Packard EnterpriseSoftware Delivery Repository の Web サイト（**https://www.hpe.com/support/SDR-Linux**）の **vibsdepot** セクションからドライバーをダウンロードします。

   注記: iLO ドライバーは Red Hat Enterprise Linux と SUSE Linux Enterprise Server の両方の Linux ディストリビューションに含まれています。

2. ドライバーをインストールします。

- Hewlett Packard Enterprise サポートセンターからドライバーをダウンロードした場合、ソフトウェアに付属のインストール手順を実行します。
- SPP をダウンロードした場合、SPP ドキュメント（**https://www.hpe.com/info/spp/documentation**）の指示に従ってください。

iLO Web インターフェイスの使用

サポートされているブラウザー

iLO 5 は以下のブラウザーの最新バージョンをサポートします。

推奨ブラウザー

- Google Chrome モバイルおよびデスクトップ
- Mozilla Firefox
- Microsoft Edge

Chrome、Firefox、Edge が iLO 5 で最高のパフォーマンスを提供します。

レガシーブラウザー

Microsoft Internet Explorer 11

ブラウザーの要件

- **JavaScript** - iLO はクライアントサイド JavaScript を広範に使用します。

  この設定は、すべての Internet Explorer バージョンでデフォルトでは無効です。この設定を確認または変更するには、**Internet Explorer の JavaScript の有効化**を参照してください。
- **Cookies** - 一部の機能が正常に動作するために、Cookie を有効にする必要があります。
- **ポップアップウィンドウ** - 一部の機能が正常に動作するために、ポップアップウィンドウを有効にする必要があります。ポップアップブロックが無効になっていることを確認してください。
- **TLS** - Web ブラウザーから iLO にアクセスするには、ブラウザーで TLS 1.0 以降を有効にする必要があります。

Internet Explorer の JavaScript の有効化

一部の Internet Explorer バージョンでは JavaScript がデフォルトで無効になっています。JavaScript を有効にするには、以下の手順を使用します。

手順

1. Internet Explorer を起動します。
2. **ツール** > **インターネットオプション**の順に選択します。
3. **セキュリティ**をクリックします。
4. **レベルのカスタマイズ**をクリックします。
5. **スクリプト**セクションで、**アクティブスクリプト**を**有効**に設定します。

6. **OK** をクリックします。
7. ブラウザーウィンドウを更新します。

iLO Web インターフェイスへのログイン

手順

1. **`https://<iLO`** のホスト名または **`IP`** アドレス**`>`**を入力します。

   iLO Web インターフェイスにアクセスするには、HTTPS を使用する必要があります（HTTPS は SSL 暗号セッションで交換される HTTP です）。

   iLO ログインページが開きます。

   - ログインセキュリティバナーが構成されている場合は、バナーテキストが**通知**セクションに表示されます。
   - **システムヘルス**ステータスが**劣化**または**クリティカル**の場合は、システムヘルスアイコンが iLO ホスト名の横に表示されます。
   - iLO ヘルスステータスが**劣化**で**匿名データ**アクセスオプションが有効な場合は、ヘルスステータスと問題の説明が iLO のログインページに表示されます。セキュリティ侵害の可能性があるセルフテスト障害は、説明には表示されません。

2. ディレクトリまたはローカルアカウントログイン名とパスワードを入力して、**ログイン**をクリックします。

   iLO が Kerberos ネットワーク認証用に設定されている場合は、**ログイン**ボタンの下に **Zero サインイン**ボタンが表示されます。**Zero サインイン**ボタンを使用して、ユーザー名とパスワードを入力せずにログインできます。

   iLO が CAC Smartcard 認証用に設定されている場合は、**ログイン**ボタンの下に **Smartcard でログイン**ボタンが表示されます。スマートカードを接続して、**Smartcard でログイン**ボタンをクリックすることができます。CAC Smartcard 認証を使用する場合、ログイン名とパスワードを入力しないでください。

詳しくは

iLO での Kerberos 認証
CAC Smartcard 認証
ログインセキュリティバナーの構成
iLO のデフォルトの DNS 名とユーザーアカウント

ブラウザーインスタンスと iLO の間での Cookie の共有

iLO にアクセスし、ログインすると、1 つのセッション Cookie が、ブラウザーのアドレスバーで iLO URL を共有する、開いているすべてのブラウザーウィンドウで共有されます。この結果、開いているすべてのブラウザーウィンドウが 1 つのユーザーセッションを共有します。1 つのウィンドウでログアウトすると、開いているすべてのウィンドウでユーザーセッションが終了します。新しいウィンドウで別のユーザーとしてログインすると、他のウィンドウでセッションが置き換えられます。

これは、ブラウザーの標準的な動作です。iLO は、同一クライアント上の同じブラウザー内の 2 つの異なるブラウザーウィンドウから複数のユーザーがログインすることをサポートしません。

共有インスタンス

iLO の Web インターフェイスが別のブラウザーウィンドウまたはタブ（ヘルプファイルなど）を開く場合、このウィンドウは、iLO への同じ接続とセッション Cookie を共有します。

iLO の Web インターフェイスにログインしているときに、手動で新しいブラウザーウィンドウを開くと、元のブラウザーウィンドウの複製インスタンスが開きます。アドレスバーのドメイン名が元のブラウザーセッションと一致する場合、新しいインスタンスは元のブラウザーウィンドウとセッション Cookie を共有します。

Cookie の順序

ログイン時に、ログインページは、ウィンドウを iLO ファームウェアの適切なセッションにリンクさせるブラウザーセッション Cookie を作成します。ファームウェアは、ブラウザーログインを、**セッションリスト**ページに示される個別のセッションとして追跡します。

たとえば、User1 がログインすると、Web サーバーは、アクティブユーザーとして User1 を示し、ナビゲーションペインにメニュー項目を示し、右のペインにページデータを示す初期フレームビューを表示します。User1 が各リンクをクリックすると、メニュー項目とページデータだけがアップデートされます。

User1 がログインしているときに、User2 が同じクライアントでブラウザーウィンドウを開いてログインすると、User1 セッションで作成された Cookie は、2 番目のログインによって上書きされます。User2 が異なるユーザーアカウントである場合、異なる現在のフレームが作成され、新しいセッションが許可されます。2 番目のセッションは、**セッションリスト**ページに User2 として表示されます。

2 番目のログインによって、User1 のログイン時に作成された Cookie が上書きされ、事実上、最初のセッションが親ブラウザーから切り離されています。この動作は、User1 のブラウザーが、ログアウトせずに閉じられた場合と同じです。親ブラウザーから切り離された User1 のセッションは、タイムアウトしたときに再要求されます。

ブラウザーのページ全体が強制的に更新されない限り、現在のユーザーのフレームは更新されないので、User1 は、ブラウザーウィンドウを使用して操作を続けることができます。ただし、ブラウザーは、すぐに判別できない場合でも、すでに User2 のセッション Cookie 設定を使用して動作しています。

User1 がこのモード（User2 がログインしてセッション Cookie をリセットしたために User1 と User2 がプロセスを共有）で操作を続ける場合、以下の状態になることがあります。

- User1 のセッションは、User2 に割り当てられている権限を使用して継続的に動作します。
- User1 が操作しても User2 のセッションは中断されませんが、User1 のセッションはタイムアウトになる場合があります。
- どちらかのウィンドウがログアウトすると、両方のセッションが終了します。ログアウトしなかったほうのウィンドウでのその次の動作によって、ユーザーは、タイムアウトまたは早期タイムアウトが発生したかのように、ログインページに転送されることがあります。
- 2 番目のセッション（User2）からログアウトすると、次の警告メッセージが表示されます。

  ```
  Logging out: unknown page to display before redirecting the user to the login page.
  ```

- User2 が、ログアウトした後に User3 としてログインしなおすと、User1 は、User3 のセッションを共有します。
- User1 がログインしているときに User2 がログインする場合、User1 は、URL を変更してインデックスページに転送することができます。これにより、User1 は、ログインせずに iLO にアクセスしているかのような状態になります。

これらの動作は、複製ウィンドウが開いている限り継続されます。すべての動作は、最後のセッション Cookie セットを使用して、同じユーザーに帰属させられます。

現在のセッション Cookie の表示

ログイン後に URL ナビゲーションバーに次のように入力すると、ブラウザーに現在のセッション Cookie が表示されます。

```
javascript:alert(document.cookie)
```

表示される最初のフィールドにセッション ID が示されます。異なるブラウザーウィンドウでセッション ID が同じである場合、これらのウィンドウは iLO セッションを共有しています。

F5 キーを押すか、**表示** > **最新の情報に更新**の順に選択するか、**表示の更新**ボタンをクリックすることによって、ブラウザーの表示を更新して、ユーザーの本当の ID を表示することができます。

Cookie に関連する問題を回避するためのベストプラクティス

- ブラウザーのアイコンまたはショートカットをダブルクリックして、ログインごとに新しいブラウザーを起動します。
- ブラウザーウィンドウを閉じる前に iLO セッションをログアウトします。

iLO Web インターフェイスの概要

iLO の Web インターフェイスは、類似の作業をグループ化しており、容易なナビゲーションとワークフローを提供します。インターフェイスは、ナビゲーションツリーにまとめられています。Web インターフェイスを使用するには、ナビゲーションツリーで項目をクリックし、表示するタブの名前をクリックします。

以下のオプションは、サーバータイプや構成でサポートしている場合のみ、ナビゲーションツリーに表示されます。

- ProLiant サーバーブレードがある場合は、**BL c-Class** オプションが表示されます。
- Synergy コンピュートモジュールがある場合は、**Synergy フレーム**オプションが表示されます。
- サポートされているシャーシモデルに ProLiant サーバーブレードが取り付けられている場合は、**シャーシ情報**オプションが表示されます。
- iLO でリモート管理ツールが使用されている場合は、**<リモート管理ツール名>**オプションが表示されます。

iLO 制御のアイコン

iLO の Web インターフェイスにログインすると、iLO 制御を任意の iLO ページから使用できます。iLO 制御のアイコンをクリックして、製品の機能または情報にアクセスできます。

- **電源アイコン** - 仮想電源ボタン機能にアクセスするには、このアイコンを使用します。

  このアイコンの色は、現在の電源ステータスによって異なります。
- **UID アイコン** - UID LED をオンまたはオフに切り替えるには、このアイコンを使用します。

  このアイコンの色は、現在の UID LED ステータスによって異なります。
- **言語** - 現在の iLO Web インターフェイスセッションの言語を選択するには、このアイコンを使用します。

  言語設定を表示または変更するには、**設定**オプションを使用します。

  このアイコンを使用できるのは、1 つまたは複数の言語パックがインストールされている場合だけです。
- **ヘルスアイコン** - システムヘルスのステータスの概要を表示するには、このアイコンを使用します。このアイコンをクリックして、iLO、サーバーのファン、温度センサー、その他の監視対象サブシステムのヘルスステータスを表示できます。

  リスト内のほとんどのヘルスステータス値について、ステータスをクリックして詳細情報を表示できます。

  Agentless Management Service（AMS）の詳細情報は表示できません。

  このアイコンは、概要が表示されているシステムヘルスのステータスによって異なります。
- **セキュリティアイコン** - このアイコンは iLO のセキュリティ状態を示します。これは、**セキュリティダッシュボード**ページからの結合した結果に基づいています。表示される値は、**OK**、**無視**、および**リスク**です。

  このアイコンをクリックして、**セキュリティダッシュボード**ページに移動できます。

  このアイコンの色は、セキュリティ状態によって異なります。
- **ユーザーアイコン** - このアイコンは次の操作をサポートしています。
  - **ログアウト**オプションを使用して、現在の iLO Web インターフェイスセッションからログアウトします。
  - **セッション**オプションを使用して、アクティブな iLO セッションを表示します。
  - **設定**オプションを使用して、**ユーザー管理**ページで iLO ユーザーアカウントを表示または変更します。

    現在のセッションユーザーの名前をクリックして、**ユーザー管理**ページに移動することもできます。

- ?**ヘルプアイコン** - 現在の iLO Web インターフェイスページのオンラインヘルプを表示するには、このアイコンを使用します。

  ヒント: オンラインヘルプで前後に移動するには、**Alt + 左矢印**または **Alt +右矢印**を押します。

- **...詳細アイコン** - ブラウザーウィンドウが小さすぎるため完全なページが表示されない場合は、**ファームウェア& OS ソフトウェア**ページにこのアイコンが表示されます。

  ファームウェアのアップデートオプション、**iLO レポジトリにアップロード**オプション、および**キューに追加**オプションにアクセスするには、このアイコンを使用します。

iLO ナビゲーションペイン

iLO には、表示/非表示を切り替えることができる折りたたみ可能なナビゲーションペインがあります。

- ナビゲーションペインを非表示にするには、✕をクリックします。

  ナビゲーションペインを非表示にすると、cookie に保存されているご使用の優先設定が次の操作を行う際も引き続き使用されます。

  - 別のページの表示
  - ブラウザーウィンドウのサイズ変更または更新
  - ログイン/ログアウト

- 非表示のナビゲーションペインを表示するには、をクリックします。

iLO ナビゲーションペインのリモートコンソールのサムネイル

ナビゲーションペインには、リモートコンソールのサムネイルが表示されます。

- リモートコンソールを起動するには、サムネイルをクリックし、メニューからコンソールオプションを選択します。
- HTML5 IRC を固定モードで実行する場合、スタティックリモートコンソールサムネイルが変わって、アクティブリモートコンソールセッションを表示します。
- モニターを備えたサーバーの場合：リモートコンソールのサムネイルをクリックし、**Wake-Up モニター**を選択することで、モニターのスリープモードを解除することができます。

ログインページからのリモート管理ツールの起動

前提条件

iLO はリモート管理ツールで制御されています。

手順

1. iLO ログインページに移動します。

   iLO がリモート管理ツールの制御下にある場合、iLO Web インターフェイスに次のようなメッセージが表示されます。

   このシステムは以下によって管理されています：<リモート管理ツール名>。
   iLO 内でローカルで変更すると、その変更は、集中管理された設定と同期が取れなくなります。

リモート管理ツールの名前はリンクになっています。

2. リモート管理ツールのリンクをクリックします。

詳しくは

iLO およびリモート管理ツール

ログインページからの言語の変更

言語パックがインストールされている場合は、ログイン画面の言語メニューを使用して、iLO セッション用の言語を選択します。この選択は、将来使用するために、ブラウザーの Cookie に保存されます。

前提条件

言語パックがインストールされていること。

手順

1. iLO **ログイン**ページに移動します。
2. 言語メニューから言語を選択します。

詳しくは

言語パック

iLO 情報およびログの表示

iLO の概要情報の表示

手順

ナビゲーションツリーで**情報**をクリックします。

iLO 概要ページは、サーバーと iLO サブシステムに関する高レベルな詳細情報を表示し、一般に使用される機能へリンクします。

システム情報の詳細

- **サーバー名** - ホストオペレーティングシステムで定義されたサーバー名。

  アクセス設定ページに移動するには、**サーバー名**リンクをクリックします。
- **製品名** - この iLO プロセッサーを統合する製品。
- **UUID** - ソフトウェアがこのホストを識別するために使用する UUID（Universally Unique Identifier）。この値は、システムの製造時に割り当てられます。
- **UUID（論理）** - ホストアプリケーションに提示されるシステム UUID。この値は、他のソフトウェアによって設定された場合にのみ表示されます。この値により、オペレーティングシステムとアプリケーションのライセンスが影響を受ける場合があります。**UUID（論理）**の値は、システムに割り当てられている論理サーバープロファイルの一部として設定されます。論理サーバープロファイルを削除すると、システム **UUID** の値が **UUID（論理）**の値から **UUID** の値に戻ります。**UUID（論理）**の値が設定されていないと、この項目は表示されません。
- **サーバーシリアル番号** - システムの製造時に割り当てられるサーバーシリアル番号。POST 実行時に ROM ベースのシステムユーティリティを使用すると、この値を変更できます。
- **シリアル番号（論理）** - ホストアプリケーションに提示されるシステムシリアル番号。この値は、他のソフトウェアによって設定された場合にのみ表示されます。この値により、オペレーティングシステムとアプリケーションのライセンスが影響を受ける場合があります。**シリアル番号（論理）**の値は、システムに割り当てられている論理サーバープロファイルの一部として設定されます。論理サーバープロファイルを削除すると、シリアル番号の値が**シリアル番号（論理）**の値から**サーバーシリアル番号**の値に戻ります。**シリアル番号（論理）**の値が設定されていないと、この項目は表示されません。
- **シャーシシリアル番号** - サーバーノードを内蔵するシャーシのシリアル番号。この値は HPE Apollo シャーシ内のサーバーノードに対してのみ表示されます。
- **製品 ID** - この値は、同じシリアル番号を持つ異なるシステムを区別します。製品 ID は、システムの製造時に割り当てられます。POST 実行時に ROM ベースのシステムユーティリティを使用すると、この値を変更できます。
- **システム ROM** - アクティブなシステム ROM のバージョン。
- **システム ROM 日付** - アクティブなシステム ROM の日付。
- **冗長化システム ROM** - 冗長化システム ROM のバージョン。冗長化システム ROM は、システム ROM のアップデートに失敗した場合や、システム ROM がロールバックされる場合に使用されます。この値は、システムが冗長化システム ROM をサポートする場合のみ表示されます。
- **統合リモートコンソール** - サーバーコンソールとのリモートアウトオブバンド通信のためにリモートコンソールを開始できます。

アクセス設定ページで**リモートコンソール**オプションが無効な場合、**無効**の値が表示されます。

現在のユーザーがリモートコンソール権限を割り当てられていない場合、**利用不可**の値が表示されます。

iLO 統合リモートコンソールページに移動するには、**統合リモートコンソール**リンクをクリックします。

- **ライセンスタイプ** - ライセンス済み iLO ファームウェア機能のレベル。

  ライセンスページに移動するには、**ライセンスタイプ**リンクをクリックします。

- **iLO ファームウェアバージョン** - インストールされている iLO ファームウェアのバージョンと日付。

  インストールされたファームウェアページに移動するには、**iLO ファームウェアバージョン**リンクをクリックします。

- **IP アドレス** - iLO サブシステムのネットワーク IP アドレス。

- **リンクローカル IPv6 アドレス** - iLO サブシステムの SLAAC リンクローカルアドレス。**ネットワークサマリー**ページに移動するには、**リンクローカル IPv6 アドレス**リンクをクリックします。

- **iLO ホスト名** - iLO サブシステムに割り当てられた完全修飾ネットワーク名。デフォルトで、ホスト名は **ILO**+システムのシリアル番号および現在のドメイン名です。この値はネットワーク名に使用され、一意である必要があります。

  ネットワーク共通設定ページに移動するには、**iLO ホスト名**リンクをクリックします。

詳しくは

概要ページからの HTML5 IRC の起動
概要ページからの.NET IRC の起動
概要ページから Java IRC（Oracle JRE）の起動

システムステータスの詳細

- **システムヘルス** - サーバーヘルスインジケーター。この値は、全体的なステータスや冗長性（障害処理能力）など、監視対象サブシステムの状態を要約します。起動時にいずれかのサブシステムが冗長でなくても、システムヘルスステータスは劣化しません。表示される値は、**OK**、**劣化**、および**クリティカル**です。

  ヘルスサマリーページに移動するには、**システムヘルス**リンクをクリックします。

- **iLO ヘルス** - iLO ヘルスステータス。iLO 診断セルフテストを組み合わせた結果に基づいています。表示される値は、**OK** および**劣化**です。

  診断ページに移動するには、**iLO ヘルス**リンクをクリックします。

- **iLO セキュリティ**— iLO のセキュリティ状態。**セキュリティダッシュボード**ページからの結合した結果に基づいています。表示される値は、**OK**、**無視**、および**リスク**です。

  セキュリティダッシュボードページに移動するには、 **iLO セキュリティ**リンクをクリックします。

- **サーバー電力** - サーバー電力の状態（**オン**または**オフ**）。

  仮想電源ボタン機能にアクセスするには、**サーバー電源**アイコンをクリックします。

  サーバー電源ページに移動するには、**サーバー電源**リンクをクリックします。

- **UID インジケーター** - UID LED の状態。UID LED を使用すると、特に高密度ラック環境でサーバーを特定し、その位置を見つけることができます。状態には、**UID オン**、**UID オフ**、および **UID 点滅**があります。

  iLO サービスポートが使用中の場合は、**UID 点滅**ステータスにサービスポートのステータスが含まれます。表示される可能性がある値は、**UID 点滅（サービスポートビジー）**、**UID 点滅（サービスポートエラー）**、および **UID 点滅（サービスポート完了）**です。

UID LED をオンまたはオフに変更するには、UID インジケーターアイコンをクリックするか、iLO Web インターフェイスの上部にある UID 制御をクリックするか、サーバーの本体にある UID ボタンを使用します。

UID が点滅していた後で点滅が停止すると、ステータスは前回の値（**UID オン**または **UID オフ**）に戻ります。UID LED が点滅している間に新しい状態を選択すると、UID LED が点滅を停止したときに新しい状態が有効になります。

△ **注意:** UID LED は自動的に点滅して、ホストでリモートコンソールのアクセスやファームウェアアップデートのような重大な操作が進行中であることを示します。UID LED の点滅中は、絶対にサーバーの電源を切らないでください。

- **Trusted Platform Module** または **Trusted Module** - TPM または TM のソケットまたはモジュールのステータス。

  表示される可能性のある値は**未サポート**、**未装着**、または**装着: 有効**です。

  Trusted Platform Module および Trusted Module は、プラットフォームの認証に使用される仕掛けを安全に格納するコンピューターチップです。これらの仕掛けには、パスワード、証明書、暗号鍵などが含まれます。また、TPM または TM を使用すると、プラットフォームの測定値を格納してプラットフォームの信頼性を保証することができます。

  サポートされているシステムでは、ROM は TPM または TM レコードを復号化し、構成ステータスを iLO に渡します。

- **モジュールタイプ** - TPM または TM の種類と仕様のバージョン。指定できる値は、**TPM 1.2**、**TPM 2.0**、**TM 1.0**、**未指定**、および**未サポート**です。この値は、サーバーに TPM または TM が存在する場合に表示されます。

- **microSD フラッシュメモリカード** - 内蔵 SD カードのステータス。存在する場合、SD カードの容量が表示されます。

- **アクセスパネルステータス** - アクセスパネルの状態。表示される可能性のある値は、**OK**（アクセスパネルが取り付けられている）および**侵入**（アクセスパネルが開いている）です。この値は、シャーシの侵入検知が構成されているサーバーでのみ表示されます。

- **iLO 日付/時刻** - iLO サブシステムの内蔵クロック。

  SNTP 設定ページに移動するには、**iLO 日付/時刻**リンクをクリックします。

HPE への接続ステータス

このセクションでは、サポートされているサーバーに関するリモートサポート登録ステータスが表示されます。

以下のステータス値が表示されます。

- **リモートサポートに登録済み** - サーバーは登録されています。
- **登録が完了していません** - サーバーは、Insight Online Direct Connect のリモートサポートに登録されていますが、登録プロセスの手順 2 が完了していません。
- **未登録** - サーバーは登録されていません。
- **HPE リモートサポート情報を取得できません** - 登録ステータスが特定できませんでした。
- **リモートサポート登録エラー** - リモートサポートの接続エラーが発生しました。

ステータス値をクリックして、リモートサポート登録ページに移動できます。

詳しくは

HPE 内蔵リモートサポート

ネットワーク詳細

アクティブなネットワークインターフェイス

アクティブなネットワークインターフェイスについて、以下の詳細が表示されます。

- **アクティブなネットワークインターフェイス名** - アクティブな iLO ネットワークインターフェイス（iLO 専用ネットワークポートまたは iLO 共有ネットワークポート）の名前。

  ネットワークの概要ページに移動するには、ネットワークインターフェイス名リンクをクリックします。

- **IP アドレス** - iLO サブシステムの IP アドレス。IPv4 アドレスが構成されていない場合、この値は表示されません。
- **リンクローカル IPv6 アドレス** - iLO サブシステムの SLAAC リンクローカルアドレス。
- **iLO ホスト名** - iLO サブシステムに割り当てられた完全修飾ネットワーク名。デフォルトで、ホスト名は **ILO**+システムのシリアル番号および現在のドメイン名です。この値はネットワーク名に使用され、一意である必要があります。

iLO 仮想 NIC

iLO 仮想 NIC セクションには、仮想 NIC から iLO に接続するときに使用する IP アドレスが表示されます。

この機能を構成できる**アクセス設定**ページに移動するには、**iLO 仮想 NIC** をクリックします。

詳しくは

iLO アクセス設定の構成
ホスト上での iLO の使用

セキュリティダッシュボードの使用

セキュリティダッシュボードページには、重要なセキュリティ機能のステータス、システムの**全体セキュリティステータス**、**セキュリティ状態**および**サーバー構成ロック**機能の現在の構成が表示されます。ダッシュボードを使用して、構成の潜在的なリスクについて評価します。リスクが検知されたら、詳細情報とシステムセキュリティを向上させる方法についてのアドバイスを見ることができます。

前提条件

無視オプションを構成するための iLO 設定の構成権限。

手順

1. ナビゲーションツリーで**情報**をクリックして、**セキュリティダッシュボード**タブをクリックします。
2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

3. セキュリティダッシュボード表で検出されたリスクについて確認します。

セキュリティ機能に**リスク**ステータスが付いて表示されている場合は、ステータスの値をクリックすると詳細情報が表示されます。詳細情報には、リスクと可能な解決策についての情報が含まれています。

4. （オプション）**無視**オプションをセキュリティ機能に構成します。

   - **無視**オプションは、デフォルトでは無効になっています。
   - **無視**オプションをセキュリティ機能に対して有効にすると、iLO が**全体セキュリティステータス**を判定するときその機能のステータスは無視されます。セキュリティ機能のステータスを無視しても、セキュリティダッシュボード表の**ステータス**値は変わりません。

   セキュリティ機能の**無視**値を変更すると、iLO が**全体セキュリティステータス**を再計算します。

セキュリティダッシュボード詳細

全体セキュリティステータス

- **OK**—iLO が監視対象のセキュリティ機能に関連したセキュリティリスクを検出しませんでした。
- **リスク**—iLO が 1 つ以上の監視対象セキュリティ機能に関連した潜在的セキュリティリスクを検出しました。
- **無視**—iLO が 1 つ以上の監視対象セキュリティ機能に関連した潜在的セキュリティリスクを検出しました。影響を受けるすべての機能が**全体セキュリティステータス**から除外されるよう設定されています。

  このステータスは、**概要**ページと iLO のコントロールにも表示されます。

セキュリティ状態

構成されているセキュリティ状態。表示される値は、以下のとおりです。

- **本番稼働**
- **高セキュリティ**
- **FIPS**
- **CNSA**
- **Synergy セキュリティモード**

サーバー構成ロック

構成されるサーバー構成ロックの設定。この機能は、管理者にデバイスの置き換えまたは追加、ハードウェアの取り外し、セキュアブートの変更、ファームウェアのインストールのような作業について警告します。この機能を UEFI システムユーティリティで構成したり、iLO RESTful API を使用して構成することができます。

セキュリティダッシュボードページでサーバー構成ロック情報を表示するには、環境が以下の要件を満たしている必要があります。

- インストールされているシステム ROM/BIOS ファームウェアが、サーバー構成ロック機能をサポートしている。

Intel ベースのサーバーではバージョン 2.00 が必要で、AMD ベースのサーバーではバージョン 1.40 が必要です。

- iLO 5 1.40 以降にアップグレードした後、サーバーを再起動した。
- セキュリティ状態を本番環境からより高いセキュリティ状態に変更した後、サーバーを再起動した。
- サーバー構成ロックを含むライセンスがインストールされている。

セキュリティダッシュボード表

- **セキュリティパラメーター**—監視対象のセキュリティ機能の名前。

  iLO Web インターフェイスで構成できる機能については、この列のリンクをクリックして関連する web インターフェイスページに移動してください。
- **ステータス**—監視対象のセキュリティ機能のセキュリティステータス。
  - **OK**—iLO がこの機能に関連したセキュリティリスクを検出しませんでした。
  - **リスク**—iLO がこの機能に関連した潜在的なセキュリティリスクを検出しました。
- **状態**—監視対象のセキュリティ機能の現在の状態。表示される値は、以下のとおりです。
  - **有効**—機能は有効です。
  - **無効**—機能は無効です。
  - **不十分**—機能は有効ですが、推奨される構成は使用されていません。
  - **オフ**—機能は**オフ**に設定されています。
  - **オン**—機能は**オン**に設定されています。
  - **OK**—機能は iLO のセキュリティ推奨事項に準拠しています。
  - **失敗**—機能は障害を報告しました。
  - **修正済み**—機能は、修正された障害を報告しました。
  - **真**—機能は使用中です。
  - **偽**—機能は使用されていません。
- **無視**—この列に表示されるスイッチを使って、機能を無視するよう設定できます。**無視**設定を有効にすると、監視対象の機能は**全体セキュリティステータス**値に含まれません。

  機能を無視しても、セキュリティダッシュボード表に表示される**ステータス**値は変わりません。

詳しくは

iLO セキュリティ状態

リスク詳細

セキュリティダッシュボードページでセキュリティ機能のリスク詳細を表示すると、以下の情報が利用可能です。

- **説明** - セキュリティ機能が**リスク**ステータスになっている理由の説明。
- **推奨されるアクション** - 推奨される解決策。

  無視オプションが有効になっている場合、この値は表示されません。

- **無視** - **無視**オプションが有効になった日時。
- **以下によって無視** - **無視**オプションを有効にしたユーザーの名前。

セキュリティリスク状態の原因

以下のセキュリティ機能が**セキュリティダッシュボード**ページで監視されます。サーバーでサポートされない機能は表示されません。

アクセスパネルステータス

シャーシの侵入検知コネクターにより、アクセスパネルのステータスが**侵入**になっていることが報告されました。

この機能は、シャーシの侵入検知が構成されているサーバーでのみ使用できます。

Hewlett Packard Enterprise では、IML と iLO イベントログに記録されたイベントを監査し、監視ビデオをチェックしてサーバーへの物理的な侵入活動がないかどうかを確認することをお勧めします。

認証失敗ログ

iLO は、認証の失敗を記録するように構成されていません。

Hewlett Packard Enterprise では、**アクセス設定**ページのこの機能を有効にすることをお勧めします。

デフォルト SSL 証明書が使用中

iLO のデフォルト自己署名証明書が使用中です。

Hewlett Packard Enterprise では、信頼済みの証明書を **SSL 証明書カスタマイズ**ページで構成することをお勧めします。

IPMI/DCMI over LAN

IPMI/DCMI over LAN 機能が有効になっています。これにより、サーバーは既知の IPMI セキュリティ脆弱性にさらされます。

Hewlett Packard Enterprise では、**アクセス設定**ページのこの機能を無効にすることをお勧めします。

最新のファームウェアスキャン結果

最新のファームウェア検証テストが失敗しました。ファームウェアコンポーネントが壊れているか、その整合性が損なわれています。

Hewlett Packard Enterprise では、影響のあるファームウェアコンポーネントを、検証済みのイメージにアップデートすることをお勧めします。

この機能を使用するには、ライセンスをインストールする必要があります。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

最小パスワード長

最小パスワード長が推奨の長さよりも短くなっています。これにより、サーバーは辞書攻撃に対して脆弱になります。

Hewlett Packard Enterprise では、**アクセス設定**ページでこの値を 8（デフォルト）以上に設定することをお勧めします。

パスワードの複雑さ

iLO は、パスワードの複雑さのガイドラインを適用するように構成されていません。これにより、サーバーは辞書攻撃に対して脆弱になります。

アクセス設定ページでこの機能を有効にできます。

ホスト認証が必要

ホスト認証が必要機能は無効になっており、iLO は高セキュリティのセキュリティ状態を使用するように構成されています。この機能が無効になっていると、ホストベースの構成ユーティリティを使用して管理プロセッサーにアクセスするときに、iLO 認証情報は必要ありません。

Hewlett Packard Enterprise では、**アクセス設定**ページのこの機能を有効にすることをお勧めします。

iLO RBSU へのログインが必要

iLO は、UEFI システムユーティリティの iLO 構成オプションへのアクセスにログイン認証情報を要求するようには構成されていません。この構成では、システムブート中に iLO 構成への未認証のアクセスが許可されます。

Hewlett Packard Enterprise では、**アクセス設定**ページのこの機能を有効にすることをお勧めします。

セキュアブート

UEFI セキュアブートオプションが無効になっています。この構成では、UEFI システムファームウェアは、信頼された署名がブートローダー、オプション ROM ファームウェア、およびシステムソフトウェアの実行ファイルにあるかどうかの検証をスキップします。これにより、電源オン時に iLO によって確立された信頼チェーンが壊れます。

Hewlett Packard Enterprise では、この機能を有効にすることをお勧めします。

詳しくは、UEFI システムユーティリティのドキュメントを参照してください。

セキュリティオーバーライドスイッチ

サーバーのセキュリティオーバーライドスイッチ（システムメンテナンススイッチとも呼ばれる）が有効になっています。セキュリティオーバーライドスイッチを有効にすると、ログイン認証が不要なため、この構成は 1 つのリスクです。

Hewlett Packard Enterprise では、この機能を無効にすることをお勧めします。

SNMPv1

SNMPv1 は有効になっています。この構成は、iLO での SNMPv1 要求の受信および SNMPv1 アラートの送信を許可します。SNMPv1 を有効にすると、攻撃に対するシステムの脆弱性が増加します。

Hewlett Packard Enterprise では、**SNMP 設定**ページでこの機能を無効にすることをお勧めします。

詳しくは

ファームウェア検証
iLO アクセス設定の構成
iLO セキュリティを無効にする理由

iLO セッションの管理

前提条件

ユーザーアカウント管理権限

手順

1. **情報**ページに移動し、**セッションリスト**タブをクリックします。

   セッションリストページには、アクティブな iLO セッションの情報が表示されます。

2. （オプション）セッションを切断するには、その横にあるチェックボックスをクリックして、**セッションの切断**をクリックします。

iLO は、選択したセッションの切断を確認するプロンプトを表示します。

3. **はい、切断します**をクリックします。

セッションリスト詳細

iLO で以下の詳細が**現在のセッション**と**セッションリスト**（*アクティブセッションの総数*）の各表に表示されます。

- **ユーザー** - iLO ユーザーアカウント名。

  通常のユーザーアカウントが*ユーザー : ユーザーアカウント名*の形式で表示されます。サービスアカウントが*サービスユーザー : ユーザーアカウント名*の形式で表示されます。

- **IP** - iLO にログインするために使用するコンピューターの IP アドレス。
- **ログイン時間** - iLO セッションが開始した日時。
- **アクセス時刻** - iLO がセッションで最後にアクティブだった日時。
- **失効** - セッションが自動的に終了する日時。
- **ソース** - セッションのソース （たとえば、リモートコンソール、Web インターフェイス、ROM ベースのセットアップユーティリティ、iLO RESTful API、SSH など）。
- **権限のアイコン**（現在のユーザーのみ） - 現在のユーザーアカウントに割り当てられている権限。チェックマークのアイコンは、権限が有効になっていることを示します。X アイコンは権限が無効になっていることを示します。

詳しくは

iLO ユーザーアカウント

iLO イベントログ

イベントログは、iLO ファームウェアが記録した重要なイベントを記録したものです。

ログに記録されるイベントの例には、サーバーの停電やサーバーのリセットなどのサーバーイベントがあります。ログに記録されるその他のイベントには、ログイン、仮想電源イベント、ログのクリア、一部の構成変更などがあります。

iLO により、パスワードの安全な暗号化、すべてのログインのトラッキング、およびログインに失敗したときのすべての記録の管理が可能となります。 **認証失敗ログ**設定により、認証失敗のログ記録条件を設定できます。イベントログは、DHCP 環境での監査機能を向上させるために記録したエントリーごとにクライアント名を取得し、アカウント名、コンピューター名、および IP アドレスを記録します。

イベントログがいっぱいになると、新しいイベントごとにログ内の一番古いイベントが上書きされます。

イベントログに表示される可能性があるエラーのリストについては、ご使用のサーバーのエラーメッセージガイドを参照してください。

イベントログの表示

手順

1. ナビゲーションツリーで**情報**をクリックし、**iLO イベントログ**タブをクリックします。
2. （オプション）ソート、検索、およびフィルター処理機能を使用して、ログのビューをカスタマイズします。

3. （オプション）イベントリストを更新するには、↻をクリックします。
4. （オプション）イベントをクリックして、イベントの詳細ペインを表示します。

イベントログビューのコントロール

イベントのソート

列でログテーブルをソートするには、列見出しをクリックします。

表示を昇順または降順に変更するには、列見出しをもう一度クリックするか、列の横にある矢印アイコンをクリックします。

イベントリストの更新

ログエントリーのリストを更新するには、↻をクリックします。

イベントの検索

日付、イベント ID、または説明テキストに基づいてイベントを検索するには、🔍をクリックしてから、検索ボックスにテキストを入力します。

イベントフィルター

ログフィルターにアクセスするには、▽をクリックします。

- 深刻度によってフィルターを適用するには、**深刻度**メニューから重大度レベルを選択します。
- カテゴリでフィルタリングするには、**カテゴリ**メニューで値を選択します。
- 表示されるイベントの日付と時刻を変更するには、**時刻**メニューで値を選択します。以下から選択します。
  - **デフォルト表示** - UTC 時間を表示します。
  - **ローカル時刻表示** - iLO Web インターフェイスのクライアント時間を表示します。
  - **ISO 時刻表示** - UTC 時間を ISO 8601 形式で表示します。
- 最終アップデート日でフィルタリングするには、**最終アップデート**メニューで値を選択します。
- フィルターをデフォルト値に戻すには、**フィルターのリセット**をクリックします。

イベントログの詳細

イベントログを表示すると、記録されたイベントの合計数が**フィルターログ**アイコンの上に表示されます。

ログフィルターを適用すると、フィルター条件を満たすイベントの数がフィルターアイコンの下に表示されます。

イベントごとに、次の詳細が表示されます。

- **ID** - イベントの ID 番号。イベントは生成された順番で番号付けされます。

  デフォルトでは、ログは ID でソートされ、最新のイベントが先頭になります。工場出荷時設定へのリセットによりカウンターがリセットされます。
- **深刻度** - 検出されたイベントの重要性。
- **説明** - この説明によって、記録されたイベントの特性が提供されます。

iLO ファームウェアが前のバージョンにロールバックされると、より新しいファームウェアによって記録されたイベントについて、「不明なイベントタイプ」という説明が表示される場合があります。この問題は、サポートされる最新バージョンのファームウェアにアップデートするか、ログをクリアすることによって解決できます。

- **最終アップデート** - このタイプの最新のイベントの発生日時。この値は、iLO ファームウェアによって保存された日時に基づきます。

  イベントがアップデートされた日時を iLO ファームウェアが認識しなかった場合は、値が NOT SET と表示されます。

- **回数** - このイベントが発生した回数（サポートされている場合）。

  通常、重大なイベントは発生するたびにログエントリーを生成します。これらのイベントが 1 つのログエントリーにまとめられることはありません。

  重要度が低いイベントが繰り返し発生する場合、これらのイベントは 1 つのログエントリーにまとめられ、iLO によって**回数**および**最終アップデート**の値がアップデートされます。

  各イベントタイプは定義された間隔を備えており、繰り返し発生するイベントの処理（統合するのかそれとも新しいイベントを記録するのか）はこの間隔によって決定されます。

- **カテゴリ** - イベントのカテゴリ。例：管理、構成、セキュリティ。

イベントログのアイコン

- **クリティカル** - イベントはサービスの消失（またはサービスの消失が予期されること）を示しています。すぐに対処する必要があります。
- **警告** - イベントは重大ですが、性能の低下を示してはいません。
- **情報** - イベントは背景情報を提供します。

イベントログイベントペインの詳細

- **初期アップデート** - このタイプの最初のイベントの発生日時。この値は、iLO ファームウェアによって保存された日時に基づきます。

  イベントが最初に発生した日時を iLO が認識しなかった場合は、NOT SET と表示されます。

- **イベントクラス** - イベントクラスの一意識別子。

  この値は 16 進数形式で表示されます。

- **イベントコード** - イベントクラス内のイベントの一意識別子。

  この値は 16 進数形式で表示されます。

- **推奨されるアクション** - 障害状態に対する推奨されるアクションの簡単な説明。

注記: 推奨されるアクションのテキストは静的です。イベントステータスが変更されても、削除またはアップデートされません。修正アクションが完了したら、推奨アクションを無視してかまいません。

CSV ファイルへのイベントログの保存

手順

1. ナビゲーションツリーで**情報**をクリックし、**iLO イベントログ**タブをクリックします。
2. をクリックします。

CSV アウトプットウィンドウが表示されます。

3. **保存**をクリックし、ブラウザーのプロンプトに従ってファイルを保存するか、ファイルを開きます。

イベントログのクリア

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**情報**をクリックし、**iLO イベントログ**タブをクリックします。
2. 🗑をクリックします。

   iLO が要求を確認するように求めます。
3. **はい、クリアします**をクリックします。

   これまで記録されたすべての情報のログがクリアされます。この操作はイベントログに記録されます。

インテグレーテッドマネジメントログ

IML は、サーバーで発生した履歴イベントの記録です。イベントはシステム ROM や、iLO ドライバーなどのサービスによって生成されます。ログに記録されたイベントには、ヘルスおよびステータス情報、ファームウェアアップデート、オペレーティングシステム情報、ROM ベースの POST コードなど、サーバー固有の情報が含まれます。

IML のエントリーが問題の診断や発生する可能性がある問題の特定に役立つ可能性があります。サービスの中断を防止するために、予防的処置が役立つ場合があります。

iLO は IML を管理するので、サーバーが稼働していない場合でも、サポートされているブラウザーを使用して IML を参照できます。サーバーが稼働していない場合にログを表示できるので、リモートホストサーバーの問題のトラブルシューティングに役立ちます。

IML がいっぱいになると、新しいイベントごとにログ内の一番古いイベントが上書きされます。

IML イベントタイプの例

- ファンのアクションとステータス
- 電源のアクションとステータス
- 温度ステータスと自動シャットダウンのアクション
- ドライブ障害
- ファームウェアフラッシュアクション
- Smart Storage Energy Pack ステータス
- ネットワークアクションとステータス

IML の表示

手順

1. ナビゲーションツリーで**情報**をクリックし、**インテグレーテッドマネジメントログ**タブをクリックします。
2. （オプション）ソート、検索、およびフィルター処理機能を使用して、ログのビューをカスタマイズします。
3. （オプション）イベントリストを更新するには、↻をクリックします。
4. （オプション）イベントをクリックして、イベントの詳細ペインを表示します。

IML ビューのコントロール

イベントのソート

列でログテーブルをソートするには、列見出しをクリックします。

表示を昇順または降順に変更するには、列見出しをもう一度クリックするか、列の横にある矢印アイコンをクリックします。

イベントリストの更新

ログエントリーのリストを更新するには、↻をクリックします。

イベントの検索

日付、イベント ID、または説明テキストに基づいてイベントを検索するには、🔍をクリックしてから、検索ボックスにテキストを入力します。

イベントフィルター

ログフィルターにアクセスするには、▽をクリックします。

- 深刻度でフィルタリングするには、**深刻度**リストから重大度レベルを選択します。
- クラスでフィルタリングするには、**クラス**リストからクラスを選択します。
- カテゴリでフィルタリングするには、**カテゴリ**リストで値を選択します。
- 表示されるイベントの日付と時刻を変更するには、**時刻**メニューで値を選択します。以下から選択します。
  - **デフォルト表示** - UTC 時間を表示します。
  - **ローカル時刻表示** - iLO Web インターフェイスのクライアント時間を表示します。
  - **ISO 時刻表示** - UTC 時間を ISO 8601 形式で表示します。
- **最終アップデート**日付でフィルタリングするには、**最終アップデート**メニューで値を選択します。
- フィルターをデフォルト値に戻すには、**フィルターのリセット**をクリックします。

IML の詳細

IML を表示すると、記録されたイベントの合計数が**フィルターログ**アイコンの上に表示されます。

ログフィルターを適用すると、フィルター条件を満たすイベントの数がフィルターアイコンの下に表示されます。

イベントごとに、次の詳細が表示されます。

- **修復可能なイベント** - Web インターフェイスの左側の最初の列には、ステータスがクリティカルまたは警告の各イベントの隣にアクティブなチェックボックスが表示されます。このチェックボックスは、修復済みとしてマークするイベントを選択するために使用されます。
- **ID** - イベントの ID 番号。イベントは生成された順番で番号付けされます。

  デフォルトでは、ログは ID でソートされ、最新のイベントが先頭になります。工場出荷時設定へのリセットによりカウンターがリセットされます。
- **深刻度** - 検出されたイベントの重要性。
- **クラス** - UEFI、環境、またはシステムのリビジョンなど、発生したイベントの種類を特定します。
- **説明** - この説明によって、記録されたイベントの特性が提供されます。

  iLO ファームウェアがロールバックされると、より新しいファームウェアによって記録されたイベントについて、「不明なイベントタイプ」という説明が表示される場合があります。この問題は、サポートされる最新バージョンのファームウェアにアップデートするか、ログをクリアすることによって解決できます。
- **最終アップデート** - このタイプの最新のイベントの発生日時。この値は、iLO ファームウェアによって保存された日時に基づきます。

  イベントがアップデートされた日時を iLO が認識しなかった場合は、値が `NOT SET` と表示されます。
- **回数** - このイベントが発生した回数（サポートされている場合）。

  通常、重大なイベントは発生するたびにログエントリーを生成します。これらのイベントが 1 つのログエントリーにまとめられることはありません。

  重要度が低いイベントが繰り返し発生する場合、これらのイベントは 1 つのログエントリーにまとめられ、iLO によって**回数**および**最終アップデート**の値がアップデートされます。

  各イベントタイプは定義された間隔を備えており、繰り返し発生するイベントの処理（統合するのかそれとも新しいイベントを記録するのか）はこの間隔によって決定されます。
- **カテゴリ** - イベントのカテゴリ。例：ハードウェア、ファームウェア、管理

IML アイコン

- **クリティカル** - イベントはサービスの消失（またはサービスの消失が予期されること）を示しています。すぐに対処する必要があります。
- **警告** - イベントは重大ですが、性能の低下を示してはいません。
- **情報** - イベントは背景情報を提供します。
- **修正済み** - イベントは修正アクションを行いました。

IML イベントペインの詳細

- **初期アップデート** - このタイプの最初のイベントの発生日時。この値は、iLO ファームウェアによって保存された日時に基づきます。

  イベントが最初に発生した日時を iLO が認識しなかった場合は、`NOT SET` と表示されます。
- **イベントクラス** - イベントクラスの一意識別子。

  この値は 16 進数形式で表示されます。
- **イベントコード** - イベントクラス内のイベントの一意識別子。

この値は 16 進数形式で表示されます。

- **さらに詳しくは** - ここに表示されるリンクをクリックすると、サポートされているイベントのトラブルシューティング情報にアクセスできます。
- **推奨されるアクション** - 障害状態に対する推奨されるアクションの簡単な説明。

注記: 推奨されるアクションのテキストは静的です。イベントステータスが変更されても、削除またはアップデートされません。修正アクションが完了するか、イベントに**修正済み**ステータスが表示されたら、推奨アクションを無視してかまいません。

IML エントリーの修正済みへの変更

IML エントリーのステータスを**クリティカル**または**警告**から**修正済み**に変更するには、この機能を使用します。

前提条件

iLO 設定の構成権限

手順

1. 問題を調べて修正します。
2. ナビゲーションツリーで**情報**をクリックし、**インテグレーテッドマネジメントログ**タブをクリックします。
3. ログエントリーを選択します。

   IML エントリーを選択するには、IML テーブルの最初の列のエントリーの横のチェックボックスをクリックします。IML エントリーの横にあるチェックボックスが表示されない場合、エントリーを修復済みとしてマークすることはできません。
4. をクリックします。

   iLO Web インターフェイスが更新され、選択したログエントリーのステータスが**修正済み**に変化します。

IML にメンテナンスノートを追加する

メンテナンスノートを使用して、次のような作業に関するログエントリーを作成します。

- アップグレード
- システムバックアップ
- 定期的なシステムメンテナンス
- ソフトウェアインストール

前提条件

iLO 設定の構成権限

手順

1. ナビゲーションツリーで**情報**をクリックし、**インテグレーテッドマネジメントログ**タブをクリックします。
2. をクリックします。

メンテナンスノートを入力ウィンドウが開きます。

3. ログエントリーとして追加するテキストを入力し、**OK** をクリックします。

   入力できるテキストの最大長さは 227 バイトです。テキストを入力せずにメンテナンスノートを送信することはできません。

   メンテナンスクラスの**情報**ログエントリーが IML に追加されます。

CSV ファイルへの IML の保存

手順

1. ナビゲーションツリーで**情報**をクリックし、**インテグレーテッドマネジメントログ**タブをクリックします。
2. をクリックします。

   CSV アウトプットウィンドウが表示されます。
3. **保存**をクリックし、ブラウザーのプロンプトに従ってファイルを保存するか、ファイルを開きます。

IML のクリア

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**情報**をクリックし、**インテグレーテッドマネジメントログ**タブをクリックします。
2. をクリックします。

   iLO が要求を確認するように求めます。
3. **はい、クリアします**をクリックします。

   これまで記録されたすべての情報のログがクリアされます。この操作は IML に記録されます。

セキュリティログ

セキュリティログは、iLO ファームウェアによって記録されたセキュリティイベントのレコードを提供します。

ログに記録されるイベントの例には、セキュリティ構成の変更や、セキュリティコンプライアンスの問題などがあります。ログに記録されるその他のイベントには、ハードウェアへの侵入、メンテナンス、サービス拒否攻撃などがあります。

セキュリティログは、記録されたすべてのセキュリティイベントの集中的なビューを提供します。いくつかの同じイベントは、iLO イベントログまたは IML にも含まれます。

セキュリティログがいっぱいになると、新しいイベントごとにログ内の一番古いイベントが上書きされます。

セキュリティログの表示

手順

1. ナビゲーションツリーで**情報**をクリックして、**セキュリティログ**タブをクリックします。
2. （オプション）ソート、検索、およびフィルター処理機能を使用して、ログのビューをカスタマイズします。
3. （オプション）イベントリストを更新するには、↻をクリックします。
4. （オプション）イベントをクリックして、イベントの詳細ペインを表示します。

セキュリティログビューのコントロール

イベントのソート

列でログテーブルをソートするには、列見出しをクリックします。

表示を昇順または降順に変更するには、列見出しをもう一度クリックするか、列の横にある矢印アイコンをクリックします。

イベントリストの更新

ログエントリーのリストを更新するには、↻をクリックします。

イベントの検索

日付、イベント ID、または説明テキストに基づいてイベントを検索するには、🔍をクリックしてから、検索ボックスにテキストを入力します。

イベントフィルター

ログフィルターにアクセスするには、▽をクリックします。

- 深刻度でフィルタリングするには、**深刻度**リストから重大度レベルを選択します。
- クラスでフィルタリングするには、**クラス**リストからクラスを選択します。
- カテゴリでフィルタリングするには、**カテゴリ**リストで値を選択します。
- 表示されるイベントの日付と時刻を変更するには、**時刻**メニューで値を選択します。以下から選択します。
  - **デフォルト表示** - UTC 時間を表示します。
  - **ローカル時刻表示** - iLO Web インターフェイスのクライアント時間を表示します。
  - **ISO 時刻表示** - UTC 時間を ISO 8601 形式で表示します。
- **最終アップデート**日付でフィルタリングするには、**最終アップデート**メニューで値を選択します。
- フィルターをデフォルト値に戻すには、**フィルターのリセット**をクリックします。

セキュリティログの詳細

セキュリティログを表示すると、記録されたイベントの合計数が**フィルターログ**アイコンの上に表示されます。

ログフィルターを適用すると、フィルター条件を満たすイベントの数がフィルターアイコンの下に表示されます。

イベントごとに、次の詳細が表示されます。

- **ID** - イベントの ID 番号。イベントは生成された順番で番号付けされます。

  デフォルトでは、ログは ID でソートされ、最新のイベントが先頭になります。工場出荷時設定へのリセットによりカウンターがリセットされます。

- **深刻度** - 検出されたイベントの重要性。
- **クラス** - UEFI、環境、またはシステムのリビジョンなど、発生したイベントの種類を特定します。
- **説明** - この説明によって、記録されたイベントの特性が提供されます。

  iLO ファームウェアがロールバックされると、より新しいファームウェアによって記録されたイベントについて、「不明なイベントタイプ」という説明が表示される場合があります。この問題は、サポートされる最新バージョンのファームウェアにアップデートするか、ログをクリアすることによって解決できます。

- **最終アップデート** - このタイプの最新のイベントの発生日時。この値は、iLO ファームウェアによって保存された日時に基づきます。

  イベントがアップデートされた日時を iLO が認識しなかった場合は、値が `NOT SET` と表示されます。

- **回数** - このイベントが発生した回数（サポートされている場合）。

  通常、重大なイベントは発生するたびにログエントリーを生成します。これらのイベントが 1 つのログエントリーにまとめられることはありません。

  重要度が低いイベントが繰り返し発生する場合、これらのイベントは 1 つのログエントリーにまとめられ、iLO によって**回数**および**最終アップデート**の値がアップデートされます。

  各イベントタイプは定義された間隔を備えており、繰り返し発生するイベントの処理（統合するのかそれとも新しいイベントを記録するのか）はこの間隔によって決定されます。

- **カテゴリ** - イベントのカテゴリ。たとえば、セキュリティ、メンテナンス、または構成。

セキュリティログアイコン

- **クリティカル** - イベントはサービスの消失（またはサービスの消失が予期されること）を示しています。すぐに対処する必要があります。
- **警告** - イベントは重大ですが、性能の低下を示してはいません。
- **情報** - イベントは背景情報を提供します。

セキュリティログイベントペインの詳細

- **初期アップデート** - このタイプの最初のイベントの発生日時。この値は、iLO ファームウェアによって保存された日時に基づきます。

  イベントが最初に発生した日時を iLO が認識しなかった場合は、値が `NOT SET` と表示されます。

- **イベントクラス** - イベントクラスの一意識別子。

  この値は 16 進数形式で表示されます。

- **イベントコード** - イベントクラス内のイベントの一意識別子。

  この値は 16 進数形式で表示されます。

- **推奨されるアクション** - 障害状態に対する推奨されるアクションの簡単な説明。

注記: 推奨されるアクションのテキストは静的です。イベントステータスが変更されても、削除またはアップデートされません。修正アクションが完了したら、推奨アクションを無視してかまいません。

CSV ファイルへのセキュリティログの保存

手順

1. ナビゲーションツリーで**情報**をクリックして、**セキュリティログ**タブをクリックします。
2. をクリックします。

   CSV アウトプットウィンドウが表示されます。
3. **保存**をクリックし、ブラウザーのプロンプトに従ってファイルを保存するか、ファイルを開きます。

セキュリティログのクリア

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**情報**をクリックして、**セキュリティログ**タブをクリックします。
2. をクリックします。

   iLO が要求を確認するように求めます。
3. **はい、クリアします**をクリックします。

   これまで記録されたすべての情報のログがクリアされます。この操作はセキュリティログに記録されます。

Active Health System

Active Health System は、サーバーハードウェアとシステム構成の変化を監視し、記録します。

Active Health System は、以下の機能を提供します。

- 1,600 を超えるシステムパラメーターの継続的なヘルス監視
- すべての構成変更のログの取得
- ヘルスおよびサービス通知の統合（正確なタイムスタンプ付き）
- アプリケーションのパフォーマンスに影響を与えないエージェントレスの監視

Active Health System のデータ収集

Active Health System では、ユーザーの経営、財務、顧客、従業員、またはパートナーに関する情報を収集しません。

収集される情報の例を示します。

- サーバーモデルとシリアル番号
- プロセッサーのモデルと速度
- ストレージの容量と速度
- メモリの容量と速度
- ファームウェア/BIOS およびドライバーのバージョンと設定

Active Health System は、サードパーティのエラーイベントログ活動（たとえば、OS を介して作成し、渡した内容）から OS データを解析したり、変更したりしません。

Active Health System ログ

Active Health System が収集したデータは Active Health System ログに保存されます。データは、安全に記録され、オペレーティングシステムから分離され、しかも顧客データから独立しています。ホストのリソースは、Active Health System データの収集およびロギングで消費されることはありません。

Active Health System ログが満杯になると、ログ内の最も古いデータが新しいデータで上書きされます。

Active Health System ログがダウンロードされ、サポート担当者に送信されて、担当者がお客様の問題の解決をサポートするのにかかる時間は 5 分以内です。

Active Health System データをダウンロードし、Hewlett Packard Enterprise に送信することで、お客様は、分析、技術的な解決、および品質改善のためにデータが使用されることに同意したものと見なされます。収集されるデータは、プライバシーに関する声明（**https://www.hpe.com/info/privacy** に掲載されています）に従って管理されます。

ログを Active Health System Viewer にアップロードすることもできます。詳しくは、Web サイト（**https://www.hpe.com/support/ahsv-docs**）にある Active Health System Viewer のドキュメントを参照してください。

この機能についてのビデオを視聴するには、次のリンクをクリックしてください。**iLO Active Health System and Viewer**

Active Health System ログのダウンロード方法

Active Health System ログをダウンロードするには、次の方法を使用できます。

- **iLO Web インターフェイス**—**Active Health System ログ**ページから日付の範囲のログをダウンロードするか、ログ全体をダウンロードします。
- **iLO サービスポート**—サーバーの前面の iLO サービスポートに USB フラッシュドライブを接続して、ログをダウンロードします。
- **cURL ユーティリティ**—cURL コマンドラインツールを使用して、ログをダウンロードします。
- **Intelligent Provisioning** - 手順については、Intelligent Provisioning ユーザーガイドを参照してください。
- **iLO RESTful API および RESTful インターフェイスツール** - 詳しくは、**https://www.hpe.com/support/restfulinterface/docs** を参照してください。

詳しくは

日付範囲を指定した Active Health System ログのダウンロード
Active Health System ログ全体のダウンロード
cURL を使用した Active Health System ログのダウンロード
iLO サービスポート経由での Active Health System ログのダウンロード
Active Health System ログ（iLOREST）のダウンロード

日付範囲を指定した Active Health System ログのダウンロード

手順

1. ナビゲーションツリーで**情報**をクリックして、**Active Health System ログ**タブをクリックします。

   ダウンロードのログが進行中の場合、Active Health System ログにアクセスできません。

2. ログに含める日付の範囲を入力します。デフォルト値は 7 日間です。

   a. **開始**ボックスをクリックします。

      カレンダーが表示されます。

   b. カレンダーで範囲の開始日を選択します。

   c. **終了**ボックスをクリックします。

      カレンダーが表示されます。

   d. カレンダーで範囲の終了日を選択します。

   デフォルト値の範囲をリセットするには、⮌をクリックします。

3. （オプション）ダウンロードしたファイルに含める以下の情報を入力します。

   - サポートケース番号（最大 14 文字）
   - 連絡先担当者の氏名
   - 電話番号（最大 39 文字）
   - メールアドレス
   - 会社名

   入力した連絡先情報は、Hewlett Packard Enterprise のプライバシーに関する声明に準拠して取り扱われます。この情報は、サーバーに保存されるログデータには記録されません。

4. **ダウンロード**をクリックします。

5. ファイルを保存します。

6. 開いているサポートケースがある場合は、ログファイルをメールで **gsd_csc_case_mngmt@hpe.com** に送信できます。

   メールの件名は、次のように表記してください。CASE: <ケース番号>。

   25 MB を超えるファイルは、圧縮して FTP サイトにアップロードする必要があります。必要に応じて、FTP サイトについて Hewlett Packard Enterprise にお問い合わせください。

7. （オプション）ファイルを Active Health System Viewer にアップロードします。

   詳しくは、**https://www.hpe.com/servers/ahsv** を参照してください。

Active Health System ログ全体のダウンロード

Active Health System ログ全体のダウンロードには、かなり時間がかかる場合があります。技術的な問題のために Active Health System ログをアップロードする必要がある場合、Hewlett Packard Enterprise は、問題が発生した特定の日付範囲のログをダウンロードすることをお勧めします。

手順

1. ナビゲーションツリーで**情報**をクリックして、**Active Health System ログ**タブをクリックします。

   ダウンロードのログが進行中の場合、Active Health System ログにアクセスできません。

2. **アドバンスト設定を表示**をクリックします。
3. （オプション）ダウンロードしたファイルに含める以下の情報を入力します。

   - サポートケース番号（最大 14 文字）
   - 連絡先担当者の氏名
   - 電話番号（最大 39 文字）
   - メールアドレス
   - 会社名

   入力した連絡先情報は、Hewlett Packard Enterprise のプライバシーに関する声明に準拠して取り扱われます。この情報は、サーバーに保存されるログデータには記録されません。

4. **ログ全体をダウンロード**をクリックします。
5. ファイルを保存します。
6. 開いているサポートケースがある場合は、ログファイルをメールで **gsd_csc_case_mngmt@hpe.com** に送信できます。

   メールの件名は、次のように表記してください。CASE: <ケース番号>。

   25 MB を超えるファイルは、圧縮して FTP サイトにアップロードする必要があります。必要に応じて、FTP サイトについて Hewlett Packard Enterprise にお問い合わせください。

7. （オプション）ファイルを Active Health System Viewer にアップロードします。

   詳しくは、**https://www.hpe.com/servers/ahsv** を参照してください。

cURL を使用した Active Health System ログのダウンロード

iLO では、cURL コマンド行ツールを使用した Active Health System ログの抽出がサポートされています。

手順

1. cURL をインストールします。
2. cURL は以下の Web サイトからダウンロードできます。**http://curl.haxx.se/**
3. コマンドウィンドウを開きます。
4. `curl` ディレクトリに変更します。
5. 以下の例に似たコマンドを実行します。

   重要: これらのコマンドを入力するときは、スペースやその他のサポートされていない文字を使用しないでください。

   コマンドライン環境でアンパサンドなどの特殊文字が必要な場合、この文字の前にエスケープ文字を付ける必要があります。詳しくは、このコマンドライン環境のドキュメントを参照してください。

- 日付範囲を指定して Active Health System ログをダウンロードする場合：

```
curl "https://<iLO_IP_address>/ahsdata/ahs.ahs?from=<yyyy-mm-dd>&to=
<yyyy-mm-dd>" -k -v -u <username>:<password> -o <filename>.ahs
```

- 過去 7 日間の Active Health System ログをダウンロードし、Hewlett Packard Enterprise サポートケース番号をログヘッダーに追加する場合：

```
curl "https://<iLO_IP_address>/ahsdata/ahs.ahs?days=<number_of_days>
&case_no=<number>" -k -v -u <username>:<password> -o <filename>.ahs
```

- 過去 7 日間の Active Health System ログをダウンロードし、ケース番号と連絡先情報を含める場合：

```
curl "https://<iLO_IP_address>/ahsdata/ahs.ahs?days=<number_of_days>
&case_no=<number>&contact_name=<name>&phone=<phone_number>&email=
<email_address>&co_name=<company>" -k -v -u <username>:<password>
-o <filename>.ahs
```

- Active Health System ログ全体をダウンロードする場合：

```
curl "https://<iLO_IP_address>/ahsdata/ahs.ahs?downloadAll=1" -k -v
-u <username>:<password> -o <filename>.ahs
```

6. ファイルは指定したパスに保存されます。
7. コマンドウィンドウを閉じます。
8. （オプション）開いているサポートケースがある場合は、ログファイルをメールで **gsd_csc_case_mngmt@hpe.com** に送信できます。

   メールの件名は、次のように表記してください。CASE: <ケース番号>。

   25 MB を超えるファイルは、圧縮して FTP サイトにアップロードする必要があります。必要に応じて、FTP サイトについて Hewlett Packard Enterprise にお問い合わせください。
9. （オプション）ファイルを Active Health System Viewer にアップロードします。

   詳しくは、**https://www.hpe.com/servers/ahsv** を参照してください。

iLO での cURL コマンドの使用法

cURL を使用して Active Health System ログを抽出する場合、コマンドコンポーネントには以下が含まれます。

オプション

<iLO IP address>

iLO IP アドレスを指定します。

from=<yyyy-mm-dd>&to=<yyyy-mm-dd>

ログの開始と終了の日付範囲を示します。`year-month-day` の形式で日付を入力してください。たとえば、2017/07/29 は、2017-07-29 と入力します。

days=<number of days>

今日の日付から過去`<number of days>`日間のログファイルをダウンロードすることを指定します。

downloadAll=1

ログ全体をダウンロードすることを指定します。

-k

HTTPS 警告が無視されるように指定します。これにより、接続が安全でなくなる可能性があります。

-v

指定すると、詳細な出力が表示されます。

-u <username>:<password>

iLO ユーザーアカウント認証情報を指定します。

-o <filename>.ahs

出力ファイルの名前とパスを指定します。

case_no=<HPE support case number>

ログヘッダーに追加する Hewlett Packard Enterprise サポートケース番号を指定します。

ダウンロードしたログに連絡先情報を追加するためのオプション

phone=<phone number>

ログヘッダーに追加する電話番号を指定します。

email=<email address>

ログヘッダーに追加する電子メールアドレスを指定します。

contact_name=<contact name>

ログヘッダーに追加する連絡先の名前を指定します。

co_name=<company name>

ログヘッダーに会社名を挿入します。

Active Health System ログ（iLOREST）のダウンロード

前提条件

- RESTful インターフェイスツールがインストールされている。
- iLO の設定を構成する権限

手順

1. RESTful インターフェイスツールを起動します。
2. **ilorest** と入力します。
3. iLO システムにログインします。

   `iLOrest > login iLO host name or IP address -u iLO user name -p iLO password`

4. 手順 **3** でログインしたサーバーの Active Health System ログをダウンロードします。

- 直近の 7 日間のログをダウンロードするには、次のようなコマンドを入力します。

  `iLOrest > serverlogs --selectlog=AHS --directorypath=`*ディレクトリパス*

- 指定された期間のログをダウンロードするには、次のようなコマンドを入力します。

  `iLOrest > serverlogs --selectlog=AHS --directorypath=`*ディレクトリパス*
  `--customiseAHS="from=`*YYYY-MM-DD*`&&to=`*YYYY-MM-DD*`"`

- すべての Active Health System ログをダウンロードするには、次のようなコマンドを入力します。

  `iLOrest > serverlogs --selectlog=AHS --downloadallahs --directorypath=`*ディレクトリパス*

ログは次のファイル名でダウンロードされます。`HPE_`*サーバーのシリアル番号*`_`*YYYYMMDD*`.ahs`

5. （オプション）開いているサポートケースがある場合は、ログファイルをメールで **gsd_csc_case_mngmt@hpe.com** に送信できます。

   メールの件名は、次のように表記してください。CASE: <ケース番号>。

   25 MB を超えるファイルは、圧縮して FTP サイトにアップロードする必要があります。必要に応じて、FTP サイトについて Hewlett Packard Enterprise にお問い合わせください。

6. （オプション）ファイルを Active Health System Viewer にアップロードします。

   詳しくは、**https://www.hpe.com/servers/ahsv** を参照してください。

iLOREST serverlog コマンドの使用法

`--selectlog=AHS`

Active Health System ログタイプで処理することを指定します。

`--directorypath=`*ディレクトリパス*

出力ファイルのパスを指定します。

`--customiseAHS="from=`*YYYY-MM-DD*`&&to=`*YYYY-MM-DD*`"`

ログの開始と終了の日付範囲を示します。`year-month-day` の形式で日付を入力してください。たとえば、2017/07/29 は、2017-07-29 と入力します。

`--downloadallahs`

ログ全体をダウンロードすることを指定します。

詳しくは、**RESTful インターフェイスツール**のドキュメントを参照してください。

Active Health System ログの消去

ログファイルが壊れた場合、またはログを消去して再開する場合は、Active Health System ログを消去してください。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**情報**をクリックして、**Active Health System ログ**タブをクリックします。

   ダウンロードのログが進行中の場合、Active Health System ログにアクセスできません。

2. **アドバンスト設定を表示**をクリックします。

3. **ログをクリア**セクションまでスクロールしてから、**クリア**をクリックします。
4. 要求を確認するメッセージが表示されたら、**はい、クリアします**をクリックします。

   ログがクリア中であることが iLO によって通知されます。
5. iLO をリセットします。

   一部の Active Health System データは iLO の起動中にのみログに記録されるため、iLO をリセットする必要があります。この手順を行うことにより、データー式が確実にログに記録されます。
6. サーバーを再起動します。

   サーバーの起動時にオペレーティングシステムの名前とバージョンなど、一部の情報がログに記録されるため、サーバーの再起動が必要です。この手順を行うことにより、データー式が確実にログに記録されます。

iLO とシステム診断の使用

iLO セルフテスト結果の表示

iLO セルフテスト結果セクションには、テスト名、ステータス、ノートを含め、内部の iLO 診断テストの結果が表示されます。

どのようなテストが実行されるかは、システムによって異なります。すべてのシステムですべてのテストが実行されるわけではありません。システムで実行されるテストを確認するには、**診断**ページで一覧を参照してください。

テストに関してステータスが報告されていない場合、そのテストは表示されません。

手順

1. ナビゲーションツリーで**情報**をクリックし、**診断**タブをクリックします。
2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

iLO セルフテストの詳細

iLO ヘルス

iLO ヘルスステータス。iLO 診断セルフテストを組み合わせた結果に基づいています。

セルフテスト

テスト済みの機能

ステータス

テストのステータス。

- **パス** - テストが成功しました。
- **劣化** - テストで問題が検出されました。再起動、ファームウェアやソフトウェアのアップデート、またはサービスが必要になる場合があります。

  セルフテストでこのステータスが報告された場合は、IML をチェックして詳細を確認してください。

  サポートケースを開始する場合は、Active Health System ログをダウンロードし、このログを含めます。
- **情報** - テストされたシステムに関する補足データが**注記**列に提供されます。

注記

注記列にテストの補足情報が含まれる場合があります。

テストによっては、他のシステムプログラマブルロジック（システムボード PAL など）またはパワーマネジメントコントローラーのバージョンがこの列に示されます。

iLO セルフテストの種類

どのようなテストが実行されるかは、システムによって異なります。すべてのシステムですべてのテストが実行されるわけではありません。実行される可能性があるテストを次に示します。

- **暗号** - セキュリティ機能をテストします。
- **NVRAM データ** - 不揮発性の構成データ、ログ、および設定を保持するサブシステムをテストします。
- **内蔵フラッシュ** - 構成、プロビジョニング、およびサービス情報を保存できるシステムの状態をテストします。
- **ホスト ROM** - BIOS をチェックし、管理プロセッサーと比較して BIOS のバージョンが古くないかどうかを確認します。
- **サポートされているホスト** - 管理プロセッサーのファームウェアをチェックし、サーバーハードウェアに対してファームウェアのバージョンが古くないかどうかを確認します。
- **パワーマネジメントコントローラー** - 電力測定値、消費電力上限、および電力管理に関連する機能をテストします。
- **CPLD** - サーバーのプログラマブルハードウェアをテストします。
- **EEPROM** - 製造工程で割り当てられた基本 iLO プロパティを保存しているハードウェアをテストします。
- **ASIC Fuses** - iLO チップに組み込まれていることが予想されるデータと既知のデータパターンを比較して、チップが適切に製造され、動作設定が許容範囲を満たしていることを確認します。

iLO の再起動（リセット）

場合によっては、iLO を再起動しなければならないことがあります。たとえば、iLO がブラウザーに応答しない場合などです。

リセットオプションは iLO の再起動を開始します。構成が変更されることはありませんが、iLO ファームウェアへのアクティブな接続がすべて終了します。ファームウェアファイルのアップロードが進行中の場合、アップロードは強制的に終了します。ファームウェアのフラッシュが進行中の場合、このプロセスが終了するまで iLO をリセットできません。

これらのどのリセット方法も利用できないか、予想どおりに機能しない場合は、サーバーの電源を切り、電源装置を切断します。

iLO の再起動（リセット）方法

iLO の Web インターフェイス

診断ページの**リセットボタン**を使用します。

iLO 5 構成ユーティリティ

UEFI システムユーティリティの **iLO 5 構成ユーティリティ**を使用します。

iLO RESTful API

詳しくは、次の Web サイトを参照してください。**https://www.hpe.com/support/restfulinterface/docs**

コマンドラインとスクリプトツール

詳しくは、HPE iLO 5 スクリプティング/コマンドラインガイドを参照してください。

IPMI

詳しくは、HPE iLO 5 IPMI ユーザーガイドを参照してください。

サーバーの UID

サポートされているサーバーのサーバー UID ボタンを使用して、**正常な再起動**または**ハードウェアの再起動**を開始します。

この方法は、他のリセット方法が使用できない、または期待どおりに機能しない場合に使用できます。

Web インターフェイスを使用した iLO プロセッサーの再起動（リセット）

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**情報**をクリックし、**診断**タブをクリックします。
2. **リセット**をクリックします。

   iLO が要求を確認するように求めます。
3. **はい、iLO をリセットします**をクリックします。

   iLO がリセットされ、ブラウザー接続が閉じます。

iLO の iLO 5 構成ユーティリティを使用した再起動（リセット）

前提条件

iLO の設定を構成する権限

手順

1. （オプション）サーバーにリモートアクセスする場合、iLO リモートコンソールセッションを開始します。
2. サーバーを再起動するかまたは電源を入れます。
3. サーバーの POST 画面で **F9** キーを押します。

   UEFI システムユーティリティが起動します。
4. **システムユーティリティ**画面で、**システム構成**、**iLO 5 構成ユーティリティ**の順にクリックします。
5. **iLO をリセット**メニューで**はい**を選択します。

   iLO 5 構成ユーティリティからリセットを確認するように求められます。
6. **OK** をクリックします。
7. iLO がリセットされ、すべてのアクティブな接続が終了します。iLO をリモートで管理している場合は、リモートコンソールセッションが自動的に終了します。

   iLO をリセットすると、次のサーバー再起動まで iLO 5 構成ユーティリティを使用できなくなります。
8. ブートプロセスを再開します。

   a. （オプション）iLO をリモート管理している場合は、iLO のリセットが完了するのを待ってから、iLO リモートコンソールを起動します。

      以前のセッションの UEFI システムユーティリティが開いています。

   b. メインメニューが表示されるまで **Esc** キーを押します。

c. **システムを終了して再起動**をクリックします。

d. 要求の確認を求めるメッセージが表示されたら、**OK** をクリックしてユーティリティを終了し、通常のブートプロセスを再開します。

サーバーの UID ボタンによる正常な iLO の再起動の実行

サポートされているサーバーの UID ボタンを使用して、適切な iLO の再起動を開始できます。

正常な iLO リブートを開始すると、iLO ファームウェアが iLO のリブートを開始します。

正常な iLO のリブートを開始しても構成が変更されることはありませんが、iLO へのすべてのアクティブ接続が終了します。ファームウェアファイルのアップロードが進行中の場合、その処理が終了します。ファームウェアのフラッシュが進行中の場合、このプロセスが終了するまで iLO をリブートできません。

手順

正常な iLO リブートを開始するには、UID ボタンを 5〜9 秒間押し続けます。

UID ボタン/LED が青色で毎秒 4 回点滅し、正常な iLO リブートが実行中であることを示します。

サーバーの UID ボタンによるハードウェア iLO の再起動の実行

サポートされているサーバーの UID ボタンを使用して、iLO ハードウェアの再起動を開始できます。

ハードウェア iLO の再起動を開始すると、サーバーハードウェアによって iLO の再起動が開始されます。

手順

ハードウェア iLO の再起動を開始するには、UID ボタンを 10 秒以上押し続けます。

注意: ハードウェア iLO の再起動を開始しても構成が変更されることはありませんが、iLO へのすべてのアクティブ接続が終了します。ファームウェアのフラッシュが進行中の場合、フラッシュデバイスでデータの破損が発生する可能性があります。フラッシュデバイスでデータの破損が発生した場合は、セキュアリカバリまたは iLO ネットワークのフラッシュエラーリカバリ機能を使用します。ハードウェア iLO の再起動中にデータの損失や NVRAM の破損が発生する可能性があります。

トラブルシューティングの他のオプションが使用可能な場合は、ハードウェアの再起動を開始しないでください。

UID ボタン/LED が青色で毎秒 8 回点滅し、ハードウェア iLO の再起動が実行中であることを示します。

アプライアンスのイメージの再構築

アプライアンスハードウェアに直接アクセスできない場合、iLO を使用して、サポートされているアプライアンス向けにイメージの再構築プロセスを開始することができます。

警告: アプライアンスのイメージの再構築を行うと、イメージの再構築プロセスが完了するまでオフラインになります。

前提条件

- ログイン権限
- リモートコンソール権限

- 仮想電源およびリセット権限
- 仮想メディア権限

手順

1. iLO 仮想メディア機能を使用して、アプライアンスのソフトウェアイメージを含む USB デバイスを接続します。

   イメージには、HPE OneView または HPE イメージストリーマーソフトウェアが含まれている必要があります。

2. ナビゲーションツリーで**情報**をクリックし、**診断**タブをクリックします。
3. **再構築** をクリックします。

   iLO が要求を確認するように求めます。

4. **はい、アプライアンスのイメージを再イメージ**をクリックします。

詳しくは

仮想ドライブ（クライアント PC 上の物理ドライブ）の使用

システム診断

以下のシステム診断機能が利用できます。機能のサポートは、サーバーモデルと iLO のバージョンによって異なります。サーバーでサポートされていない機能は、**診断**ページに表示されません。

- **NMI を生成する**
- **システムセーフモードで起動する**
- **インテリジェント診断モードで起動する**
- **工場デフォルト設定にリストアする**
- **デフォルトシステム設定をリストアする**

重要: 複数のシステム診断操作を同時に開始しないでください。同時に複数の操作を実行すると、予期しない結果が生じる可能性があります。

NMI の生成

NMI を生成機能で、オペレーティングシステムをデバッグのために停止できます。

この機能は、システムが起動せず、OS 前の状態（たとえば、POST 中）でハングする場合に役立ちます。NMI を使用すると、システム ROM 例外ハンドラーが有効になり、問題が発生したコードのトレースをキャプチャできます。

注意: 診断とデバッグのツールとしての NMI の生成は、主にオペレーティングシステムが使用不能になった場合に使用します。通常のサーバーの運用では、NMI を使用しないでください。NMI の生成ではオペレーティングシステムは適切にはシャットダウンされず、オペレーティングシステムがクラッシュします。このため、サービスとデータは失われます。**NMI を生成**ボタンは、OS が正常に動作せず、経験のあるサポート組織が NMI を推奨する極端なケースのみに使用してください。

前提条件

仮想電源およびリセット権限

手順

1. ナビゲーションツリーで**情報**をクリックし、**診断**タブをクリックします。
2. **システム診断を表示**をクリックします。
3. **NMI を生成**をクリックします。

   iLO が要求を確認するように求めます。

   注意: NMI を生成すると、データ損失やデータ破壊の原因となる可能性があります。

4. **はい、続行します**をクリックします。

   iLO は、NMI が送信されたことを確認します。

システムセーフモードでの起動

サポートされているサーバーで、セーフモードでのシングルブートを開始するには、**システムセーフモード**オプションを使用します。この機能により、安全な最小構成でサーバーを起動できます。

前提条件

- ホスト BIOS 構成権限
- 仮想電源およびリセット権限
- iLO の設定を構成する権限
- サーバープラットフォームでこの機能がサポートされている。
- サーバーの電源がオフになっている。

手順

1. ナビゲーションツリーで**情報**をクリックし、**診断**タブをクリックします。
2. **システム診断を表示**をクリックします。
3. **セーフモードで起動**をクリックします。

   iLO が要求を確認するように求めます。

4. **はい、続行します**をクリックします。

   セーフモードでサーバーの起動に成功すると、ブートプロセッサーと 1 つのメモリチャネルが正常に動作していることが示されます。

   このアクションの結果は IML に記録されます。

インテリジェント診断モードで起動

サポートされているシステムでインテリジェント診断モードに入ると、POST 中のブート障害が自動的に診断されます。

前提条件

- ホスト BIOS 構成権限
- 仮想電源およびリセット権限
- iLO の設定を構成する権限

- サーバープラットフォームでこの機能がサポートされている。
- サーバーの電源がオフになっている。

手順

1. ナビゲーションツリーで**情報**をクリックし、**診断**タブをクリックします。
2. **システム診断を表示**をクリックします。
3. **インテリジェント診断モードで起動**をクリックします。

   iLO が要求を確認するように求めます。
4. **はい、続行します**をクリックします。

   システムがインテリジェント診断モードであることが iLO から通知されます。

   ブート障害の原因を特定するために、サーバーは一連の再起動を開始します。原因が識別されると、影響を受けるデバイスが無効化され、ブートプロセスが再開されます。

   注記: このプロセスは、完了までに長時間かかることがあります。ブート障害の原因を特定するために、複数のサーバーの再起動が必要になる場合があります。インテリジェント診断モードに入ったら、プロセスを中断せずに完了させます。

   ステータスを監視するには、サーバーの POST 画面を確認します。

   このアクションの結果は IML に記録されます。
5. 問題が検出された場合は、必要な手順を実行して問題を解決してください。

工場デフォルト設定のリストア

すべての BIOS 構成設定を工場デフォルト値にリセットするには、**工場デフォルト設定のリストア**オプションを使用します。

このプロセスにより、ブート構成、セキュアブートのセキュリティキー（セキュアブートが有効な場合）、構成された日付時刻の設定など、すべての UEFI 不揮発性変数が削除されます。

一部の UEFI 設定を保持するオプションを使用するには、**デフォルトのシステム設定のリストア**オプションを検討してください。

この機能を使用すると、不揮発性メモリに保存された iLO IP アドレスおよび iLO 設定が保持されます。

前提条件

- ホスト BIOS 構成権限
- 仮想電源およびリセット権限
- iLO の設定を構成する権限
- サーバープラットフォームでこの機能がサポートされている。
- サーバーの電源がオフになっている。

手順

1. （オプション）UEFI システムユーティリティで**ユーザーデフォルトの保存**オプションを**はい、保存します。**に設定します。

このオプションを有効にすると、工場デフォルト設定をリストアするときに、現在の BIOS 設定がデフォルト設定として使用されます。

詳しくは、UEFI システムユーティリティのユーザーガイドを参照してください。

2. ナビゲーションツリーで**情報**をクリックし、**診断**タブをクリックします。
3. **システム診断を表示**をクリックします。
4. **工場デフォルト設定のリストア**をクリックします。

   iLO により、要求の確認を求められます。また、セキュアブートの設定など、以前に構成した設定がデフォルト値にリセットされることが警告されます。
5. **はい、続行します**をクリックします。

   UEFI 不揮発性変数がデフォルト値にリセットされ、サーバーが再起動します。

   ステータスを監視するには、サーバーの POST 画面を確認します。

   このアクションの結果は IML に記録されます。

システムデフォルト設定のリストア

システムデフォルト設定のリストアオプションを使用すると、すべての BIOS 構成設定がデフォルト値にリセットされ、サーバーは再起動します。

このオプションを選択すると、以下を除くすべてのプラットフォーム設定をリセットします。

- セキュアブート BIOS 設定
- 日付と時刻の設定
- プライマリおよび冗長の ROM の選択（サポートされる場合）
- オプションカードや iLO などの他のエンティティは、個別にリセットする必要があります。

  この機能を使用すると、不揮発性メモリに保存された iLO IP アドレスおよび iLO 設定が保持されます。

前提条件

- ホスト BIOS 構成権限
- 仮想電源およびリセット権限
- iLO の設定を構成する権限
- サーバープラットフォームでこの機能がサポートされている。
- サーバーの電源がオフになっている。

手順

1. （オプション）UEFI システムユーティリティで**ユーザーデフォルトの保存**オプションを**はい、保存します。**に設定します。

   このオプションを有効にすると、デフォルトのシステム設定をリストアするときに、現在の BIOS 設定がデフォルト設定として使用されます。

   詳しくは、UEFI システムユーティリティのユーザーガイドを参照してください。
2. ナビゲーションツリーで**情報**をクリックし、**診断**タブをクリックします。
3. **システム診断を表示**をクリックします。

4. **システムデフォルト設定のリストア**をクリックします。

   iLO により、要求の確認を求められ、以前に構成した設定がデフォルト値にリセットされることが警告されます。

5. **はい、続行します**をクリックします。

   BIOS 構成設定がデフォルト値にリセットされ、サーバーが再起動します。

   ステータスを監視するには、サーバーの POST 画面を確認します。

   このアクションの結果は IML に記録されます。

全般的なシステム情報の表示

ヘルスサマリー情報の表示

ヘルスサマリーページには、監視対象サブシステムおよびデバイスのステータスが表示されます。このページの情報は、サーバー構成によって異なります。

サーバーの電源が切れている場合、このページのシステムヘルス情報は、最後に電源が切れた時点の情報になります。ヘルス情報は、サーバーの電源が入っており、POST が完了している場合にのみアップデートされます。

手順

1. ナビゲーションツリーで**システム情報**をクリックします。
2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。
3. （オプション）サポートされるサブシステムとデバイスタイプの関連ページに移動するには、**サブシステムおよびデバイス**リストで値の名前をクリックします。

   Agentless Management Service などの一部のサブシステムおよびデバイスタイプには、関連ページがありません。

冗長ステータス

以下の項目に関する冗長ステータスが表示されます。

- **ファンの冗長化**
- **電源**

サブシステムおよびデバイスのステータス

以下の項目に関するステータス情報が表示されます。

- **Agentless Management Service**
- **BIOS/ハードウェアヘルス**
- **ファン**
- **メモリ**
- **ネットワーク**
- **電源装置**（非ブレードサーバーのみ）
- **プロセッサー**
- **ストレージ**
- **温度**
- **Smart Storage Energy Pack**（サポート対象のサーバーのみ）

サブシステムおよびデバイスステータスの値

- **冗長化**—デバイスまたはサブシステム用のバックアップコンポーネントがあります。
- **OK**—デバイスまたはサブシステムは正常に動作しています。
- **非冗長化**—デバイスまたはサブシステム用のバックアップコンポーネントがありません。
- **利用不可能**—コンポーネントは利用できないか、インストールされていません。
- **劣化**—デバイスまたはサブシステムの機能が低下しています。

  iLO では、一致しない電源装置が取り付けられている場合、電源装置のステータスは**劣化**となります。

  非冗長ファンまたは電源装置を備えたサーバーを起動する場合、システムヘルスステータスは **OK** と表示されます。システムの起動時に冗長ファンまたは電源装置で障害が発生すると、ファンまたは電源装置を交換するまでシステムヘルスステータスは**劣化**になります。
- **冗長化障害**—デバイスまたはサブシステムは動作していません。
- **障害**—デバイスまたはサブシステムの 1 つまたは複数のコンポーネントが動作していません。
- **その他** - 詳しくは、このステータスを報告するコンポーネントの**システム情報**ページに移動してください。
- **不明** - iLO ファームウェアがデバイスステータス情報を受信していません。サーバーの電源がオフになっているときに iLO をリセットした後、一部のサブシステムでステータスが**不明**と表示されます。サーバーの電源がオフになっているとき、iLO はこれらのサブシステムのステータスをアップデートできません。
- **未インストール**—サブシステムまたはデバイスがインストールされていません。

プロセッサー情報の表示

プロセッサー情報ページは、空いているプロセッサースロット、各スロットに装着されたプロセッサーの種類、プロセッサーサブシステムの概要を表示します。

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、最後の電源オフ時のものです。ヘルス情報は、サーバーの電源が入っており、POST が完了している場合にのみアップデートされます。

手順

ナビゲーションツリーで**システム情報**をクリックし、**プロセッサー**タブをクリックします。

プロセッサーの詳細

プロセッサーごとに、次の情報が表示されます。

- **プロセッサー名** - プロセッサーの名前。
- **プロセッサーステータス** - プロセッサーのヘルスステータス。
- **プロセッサー速度** - プロセッサーの速度。
- **実行テクノロジー** - プロセッサーのコアおよびスレッドに関する情報。
- **メモリテクノロジー** - プロセッサーのメモリ機能。
- **内部 L1 キャッシュ** - L1 キャッシュサイズ。

- **内部 L2 キャッシュ** - L2 キャッシュサイズ。
- **内部 L3 キャッシュ** - L3 キャッシュサイズ。

メモリ情報の表示

メモリ情報ページには、システムメモリの概要が表示されます。サーバーの電源が入っていない場合は、AMP データが使用できないため、POST 実行時に存在するメモリモジュールのみが表示されます。

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、最後の電源オフ時のものです。ヘルス情報は、サーバーの電源が入っており、POST が完了している場合にのアップデートされます。

手順

1. ナビゲーションツリーで**システム情報**をクリックし、**メモリ**タブをクリックします。

   メモリページには、以下の詳細が表示されます。

   - **アドバンストメモリプロテクション（AMP）**
   - **メモリの概要**
   - **物理メモリ**

2. （オプション）デフォルトでは、**物理メモリ**テーブルに空のメモリソケットは表示されません。空のメモリスロットを表示するには、**空きのメモリスロットを表示**をクリックします。空のメモリスロットが表示されているときにそれらを非表示にするには、**空きのメモリスロットを隠す**をクリックします。

   このオプションは、空のスロットがない場合は表示されません。

3. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

4. （オプション）追加のメモリ詳細を表示するには、メモリモジュールを選択します。

   メモリ詳細ペインが表示されます。

アドバンストメモリプロテクションの詳細

AMP モードステータス

AMP サブシステムのステータスです。

- **不明/その他** - システムが AMP をサポートしていない、またはマネジメントソフトウェアがステータスを判定できません。
- **非保護** - システムは AMP をサポートしていますが、機能が無効になっています。
- **プロテクト済み** - システムは AMP をサポートしています。機能は有効ですが、動作してはいません。
- **劣化** - システムは保護されていましたが、AMP が保留中です。したがって、AMP はもう使用できません。
- **DIMM ECC** - システムは、DIMM ECC のみによって保護されます。
- **ミラーリング** - システムはミラーモードの AMP で保護されています。DIMM の不具合は検出されていません。

- **ミラーリング劣化** - システムはミラーモードの AMP で保護されています。1 つまたは複数の DIMM の不具合が検出されています。
- **オンラインスペア** - システムはホットスペアモードの AMP で保護されています。DIMM の不具合は検出されていません。
- **オンラインスペア劣化** - システムはホットスペアモードの AMP で保護されています。1 つまたは複数の DIMM の不具合が検出されています。
- **RAID-XOR** - システムは XOR メモリモードの AMP で保護されています。DIMM の不具合は検出されていません。
- **RAID-XOR 劣化** - システムは XOR メモリモードの AMP で保護されています。1 つまたは複数の DIMM の不具合が検出されています。
- **アドバンスト ECC** - システムはアドバンスト ECC モードの AMP で保護されています。
- **アドバンスト ECC 劣化** - システムはアドバンスト ECC モードの AMP で保護されています。1 つまたは複数の DIMM の不具合が検出されています。
- **ロックステップ** - システムはロックステップモードの AMP で保護されています。
- **ロックステップ劣化** - システムはロックステップモードの AMP で保護されています。1 つまたは複数の DIMM の不具合が検出されています。
- **A3DC** - システムは A3DC モードの AMP で保護されています。
- **A3DC 劣化** - システムは A3DC モードの AMP で保護されています。1 つまたは複数の DIMM の不具合が検出されています。

構成済み AMP モード

アクティブな AMP モード。以下のモードがサポートされます。

- **なし/不明** - マネジメントソフトウェアが AMP フォールトトレランスを判定できない、またはシステムが AMP 用に構成されていません。
- **オンラインスペア** - 起動時にメモリの単一のスペアバンクが確保されています。多数の ECC エラーが発生すると、スペアメモリがアクティブになり、エラーが発生したメモリは無効になります。
- **ミラーリング** - システムはミラーメモリ用に構成されています。オンラインスペアメモリの場合の 1 つのメモリバンクとは異なり、ミラー化されたメモリではすべてのメモリバンクが二重化されています。多数の ECC エラーが発生すると、スペアメモリがアクティブになり、エラーが発生したメモリは無効になります。
- **RAID-XOR** - システムは、XOR エンジンを使用して AMP 用に構成されています。
- **アドバンスト ECC** - システムはアドバンスト ECC エンジンを使用して AMP 用に構成されています。
- **ロックステップ** - システムは、ロックステップエンジンを使用して AMP 用に構成されています。
- **オンラインスペア（ランクスペアリング）** - システムはオンラインスペアランク AMP 用に構成されています。
- **オンラインスペア（チャネルスペアリング）** - システムはオンラインスペアランク AMP 用に構成されています。
- **インターソケットミラーリング** - システムは 2 つのプロセッサーまたはボードのメモリの間でミラー化された Intersocket AMP 用に構成されています。

- **イントラソケットミラーリング** - システムは 1 つのプロセッサーまたはボードのメモリの間でミラー化された Intrasocket AMP 用に構成されています。
- **A3DC** - システムは、A3DC エンジンを使用して AMP 用に構成されています。

サポートされる AMP モード

- **RAID-XOR** - システムは、XOR エンジンを使用して AMP 用に構成することができます。
- **デュアルボードミラーリング** - システムは、デュアルメモリボード構成で、ミラー化されたアドバンストメモリ保護用に構成することができます。ミラーメモリは、同じメモリボード上のメモリまたは 2 番目のメモリボード上のメモリと交換することができます。
- **シングルボードミラーリング** - システムは、単一のメモリボードで、ミラー化されたアドバンストメモリ保護用に構成することができます。
- **アドバンスト ECC** - システムは、アドバンスト ECC 用に構成することができます。
- **ミラーリング** - システムは、ミラー化された AMP 用に構成することができます。
- **オンラインスペア** - システムは、オンラインスペア AMP 用に構成することができます。
- **ロックステップ** - システムは、ロックステップ AMP 用に構成することができます。
- **オンラインスペア（ランクスペアリング）** - システムはオンラインスペアランク AMP 用に構成できます。
- **オンラインスペア（チャネルスペアリング）** - システムはオンラインスペアランク AMP 用に構成できます。
- **インターソケットミラーリング** - システムは 2 つのプロセッサーまたはボードのメモリの間でミラー化された Intersocket AMP 用に構成できます。
- **イントラソケットミラーリング** - システムは 1 つのプロセッサーまたはボードのメモリの間でミラー化された Intrasocket AMP 用に構成できます。
- **A3DC** - このシステムは A3DC AMP 用に構成できます。
- **なし** - このシステムは、AMP 用に構成することができません。

メモリの概要

メモリの概要セクションには、搭載され、POST 実行時に正常に動作したメモリの概要が表示されます。

位置

メモリボード、カートリッジ、またはライザーが搭載されているスロットまたはプロセッサー。表示される可能性がある値は、以下のとおりです。

- **システムボード** - 個別のメモリボードスロットはありません。すべての DIMM がマザーボードに取り付けられています。
- **ボード<番号>** - 使用できるメモリボードスロットがあります。すべての DIMM がメモリボードに取り付けられています。
- **プロセッサー<番号>** - メモリ DIMM が搭載されているプロセッサー。
- **ライザー<番号>** - メモリ DIMM が搭載されているライザー。

メモリスロットの総数

メモリモジュールスロットの数。

メモリ合計

メモリの容量。これには、オペレーティングシステムが認識するメモリ、およびスペア、ミラー、または XOR 構成に使用されるメモリが含まれます。

動作周波数

メモリが動作する周波数。

物理メモリ詳細

物理メモリセクションには、ホストに搭載され、POST 実行時に正常に動作していた、ホスト上の物理メモリモジュールが表示されます。メモリモジュールが取り付けられていない位置も示されます。各種の耐障害メモリ構成により、実際のメモリインベントリが、POST の実行時に検出されたものから変化する場合があります。システムに多数のメモリモジュールが搭載されている場合は、一部のモジュール位置しか表示されない場合があります。

ソケットロケーター

メモリモジュールが搭載されているスロットまたはプロセッサー。

ステータス

メモリモジュールのステータスおよびモジュールが使用中かどうか。表示される可能性がある値は、以下のとおりです。

- **追加済 未使用** - DIMM が追加されましたが、未使用です。
- **構成エラー** - DIMM に構成エラーがあります。
- **劣化** - DIMM ステータスが低下しています。
- **不一致** - DIMM タイプが一致していません。
- **予想されたが不明** - DIMM は予想されていますが、欠落しています。
- **良好、使用中** - DIMM は正しく機能しており、使用中です。
- **良好、一部使用** - DIMM は正しく機能しており、一部使用中です。
- **マップアウトエラー** - トレーニングに失敗したため、DIMM はマップから解除されています。
- **マップアウト構成** - 構成エラーのため、DIMM がマップから解除されています。
- **未装着** - DIMM が存在しません。
- **未サポート** - DIMM はサポートされていません。
- **その他** - DIMM ステータスは、標準のステータス定義のいずれにも当てはまりません。
- **装着、スペア** - DIMM が存在し、スペアとして使用されています。
- **装着、未使用** - DIMM が存在し、使用されていません。
- **不明** - DIMM ステータスは不明です。
- **更新済 未使用** - DIMM はアップグレードされましたが、使用されていません。

サイズ

メモリモジュールのサイズ。

サポートされる最大周波数

メモリモジュールでサポートされる最大周波数。

テクノロジー

メモリモジュールのテクノロジー。表示される可能性がある値は、以下のとおりです。

- **不明** - メモリのテクノロジーを判定できません。
- **N/A** - メモリモジュールはありません。
- **SDRAM**（シンクロナスダイナミック RAM）
- **RDIMM**（レジスタ付きメモリモジュール）
- **UDIMM**（レジスタなしメモリモジュール）
- **LRDIMM**（負荷低減メモリモジュール）
- **NVDIMM**（不揮発性デュアルインラインメモリモジュール）
- **NVDIMM-N**（フラッシュメモリと従来のメモリの両方を備えた不揮発性デュアルインラインメモリモジュール）
- **R-NVDIMM**（レジスタ付き不揮発性デュアルインラインメモリモジュール）
- **PMM**（不揮発性メモリモジュール）

メモリ詳細ペイン（物理メモリ）

製造元

メモリモジュールの製造元。

HPE Smart メモリ

メモリモジュールが HPE Smart メモリかどうかを示します。HPE Smart メモリの場合は**はい**が表示されます。他のメモリタイプ（Smart メモリではない HPE メモリを含む）の場合は**いいえ**が表示されます。メモリモジュールが存在しない場合、**N/A** の値が表示されます。

部品番号

メモリモジュールの部品番号。

この値は、HPE メモリモジュールについてのみ表示されます。

タイプ

搭載されたメモリのタイプ。表示される可能性がある値は、以下のとおりです。

- **その他** - メモリタイプを判定できません。
- **ボード** - メモリモジュールは（モジュール式でなく）システムボードまたはメモリ拡張ボードに固定されています。
- **DDR4**
- **N/A** - メモリモジュールはありません。

ランク

メモリモジュール内のランクの数。

誤り訂正

メモリモジュールが使用する誤り訂正のタイプ。

データ幅ビット

メモリモジュールのデータ幅（ビット単位）。

バス幅ビット

メモリモジュールのバス幅（ビット単位）。

チャネル

メモリモジュールが接続されているチャネル番号。

メモリコントローラー

メモリコントローラー番号。

CPU ソケット

メモリモジュールのソケット番号。

メモリスロット

メモリモジュールのスロット番号。

状態

メモリの状態。

ベンダー

メモリベンダー名。ベンダー名が不明な場合、値 **N/A** が表示されます。

ベンダー ID

メモリベンダー ID。

Armed

NVDIMM-N の現在のバックアップ準備状態（使用できる場合）。

最後の操作

最後の操作のステータス（NVDIMM のみ）。

メディア寿命

メディアの残りの寿命の割合（NVDIMM のみ）。

ネットワーク情報の表示

サーバーの電源が切れている場合、**NIC 情報**ページのヘルスステータス情報は、最後に電源が切れた時点の情報になります。ヘルス情報は、サーバーの電源が入っており、POST が完了している場合にのみアップデートされます。

このページのすべてのデータセットを表示するには、AMS がインストールされていて実行中であることを確認します。AMS がインストールされ、サーバー上で実行されている場合にのみ、サーバーの IP アドレス、アドインのネットワークアダプター、サーバーの NIC ステータスが表示されます。

このページの情報は、iLO にログインしたときにアップデートされます。データを更新するには、iLO からログアウトしてログインし直します。

手順

1. ナビゲーションツリーで**システム情報**をクリックし、**ネットワーク**タブをクリックします。
2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

3. （オプション）このページで情報を展開するには**すべてを展開**をクリックし、情報を折りたたむには**すべて閉じる**をクリックします。

物理ネットワークアダプター

内蔵と追加の NIC およびファイバーチャネルアダプター

このセクションには、サーバー内の内蔵と追加の NIC およびファイバーチャネルアダプターに関する次の情報が表示されます。

アダプター番号

アダプター番号。たとえば、**アダプター 1**、**アダプター 2** など。

位置

システムボード上のアダプターの位置。

ファームウェア

インストールされているアダプターのファームウェアのバージョン（該当する場合）。この値は、システム NIC（内蔵および直立型）の場合にのみ表示されます。

ステータス

NIC ステータス。

- Windows サーバー：
  - NIC がネットワークに接続され、正しく機能している場合、iLO にはステータス **OK** が表示されます。
  - NIC がネットワークに接続されていなかった場合、iLO はステータスを**不明**と表示します。
  - NIC がネットワークに接続されていた場合、iLO はステータスを**リンクダウン**と表示します。
  - 複数の NIC による構成で、コンポーネントが故障しているがシステムはまだ機能している場合、iLO はステータスを**劣化**と表示します。
  - NIC が障害を報告した場合、iLO によってステータス**クリティカル**が表示されます。
- Linux サーバー：
  - NetworkManager を使用して NIC を管理する場合、デフォルトのステータスは **OK** であり、リンクステータスが iLO に表示されます。
  - Linux のレガシーユーティリティを使用して NIC を管理する場合、iLO は、NIC が管理者によって設定されている場合にのみリンクステータスを表示します。NIC が設定されていない場合、iLO は、ステータスを**不明**と表示します。
  - 複数の NIC による構成で、コンポーネントが故障しているがシステムはまだ機能している場合、iLO はステータスを**劣化**と表示します。
  - NIC が障害を報告した場合、iLO によってステータス**クリティカル**が表示されます。
- VMware サーバー：

- iLO が NIC ポートと通信できない場合、ステータスを**不明**と表示します。
- NIC ドライバーが `link_down` のステータスを報告する場合、iLO はステータスを**ダウン**と表示します。
- NIC ドライバーが `link_up` のステータスを報告する場合、iLO はステータスを **OK** と表示します。
- 複数の NIC による構成で、コンポーネントが故障しているがシステムはまだ機能している場合、iLO はステータスを**劣化**と表示します。
- NIC が障害を報告した場合、iLO によってステータス**クリティカル**が表示されます。

ポート

設定されているネットワークポート。この値は、システム NIC（内蔵および直立型）の場合にのみ表示されます。

MAC アドレス

ポートの MAC アドレス。

IPv4 アドレス

システム NIC（内蔵および直立型）の場合、サーバーの IP アドレス（使用できる場合）。

IPv6 アドレス

システム NIC（内蔵および直立型）の場合、サーバーの IP アドレス（使用できる場合）。

ステータス

ポートのステータス。

表示される可能性がある値は、**OK**、**障害**、**不明**、および**リンクダウン**です。

チーム/ブリッジ

ポートが NIC チーミング用に設定されている場合、論理ネットワークアダプターを形成する物理ポートの間で設定されているリンクの名前。この値は、システム NIC（内蔵および直立型）の場合にのみ表示されます。

ファイバーチャネルホストバスアダプターまたはコンバージドネットワークアダプター

ファイバーチャネルのホストバスアダプターまたはコンバージドネットワークアダプターに関する、次の情報が表示されます。

- **物理ポート** - 物理ネットワークのポート番号。
- **WWNN** - ポートのワールドワイドノード名。
- **WWPN** - ワールドワイドポート名。
- **ステータス** - ポートのステータス。

ブートの進行状況とブートターゲット

DCI 接続が使用可能な場合は、以下の情報が表示されます。

- **ポート** - 設定済み仮想ポート番号。
- **ブート進行中** - ブートの現在のステータス。
- **ブートターゲット**

- **WWPN** - ワールドワイドポート名。
- **LUN ID** - 論理ユニット番号 ID。

論理ネットワークアダプター

このセクションには、NIC チーミングを使用して 1 つの論理ネットワーク接続に 2 つ以上のポートを搭載しているネットワークアダプターに関する以下の情報が表示されます。

- **アダプター名** - 論理ネットワークアダプターを形成する物理ポートの間で設定されているリンクの名前。
- **MAC アドレス** - 論理ネットワークアダプターの MAC アドレス。
- **IP アドレス** - 論理ネットワークアダプターの IP アドレス。
- **ステータス** - 論理ネットワークアダプターのステータス。

各論理ネットワークアダプターを形成するポートに関する、次の情報が表示されます。

- **メンバー** - 論理ネットワークアダプターを形成する各ポートに割り当てられた一連の番号。
- **MAC アドレス** - 物理アダプターポートの MAC アドレス。
- **ステータス** - 物理アダプターポートのステータス。

デバイスインベントリの表示

デバイスインベントリページには、サーバーにインストールされたデバイスに関する情報が表示されます。このページに表示されるデバイスには、たとえば、取り付けられているアダプター、PCI デバイス、SATA コントローラー、Smart ストレージバッテリなどがあります。

サーバーの電源が切れている場合、このページのヘルスステータス情報は、最後に電源が入った時点の情報になります。ヘルス情報は、サーバーの電源が入っており、POST が完了している場合にのみアップデートされます。

業界標準の管理仕様に準拠していない古いアダプターでは、アダプターのファームウェアバージョン、部品番号、シリアル番号、およびステータスを取得するために、Agentless Management Service（AMS）が必要です。

フィールド交換可能ユニット（FRU）EEPROM をサポートしているアダプターでは、iLO が製品名や部品番号などの静的アダプターの詳細を取得します。これらの値は、IPMI プラットフォーム管理 FRU 情報ストレージ定義の仕様に従ってフォーマットされます。

手順

1. ナビゲーションツリーで**システム情報**をクリックし、**デバイスインベントリ**タブをクリックします。
2. （オプション）デフォルトでは、空のスロットが**デバイスインベントリ**テーブルで非表示になっています。空のスロットを表示するには、**空きのスロットを表示**をクリックします。空のスロットが表示されているときにそれらを非表示にするには、**空きのスロットを隠す**をクリックします。

   このオプションは、空のスロットがない場合は表示されません。
3. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。
4. （オプション）追加のスロット詳細を表示するには、テーブル内のデバイスをクリックします。

スロット詳細ペインが表示されます。

詳しくは

Agentless Management と AMS

デバイスインベントリの詳細

- **MCTP 検出** - サーバーについて、この機能が有効になっているか無効になっているか。
- **位置** - デバイスの取り付け位置。
- **製品名** - デバイスの製品名。

  通常、iLO は、FRU EEPROM からこの値を取得します（製品情報領域フォーマット地域、製品名の値）。

  一部のアダプターでは、この値は専用アダプターのインターフェイスを通じて取得されます。
- **製品バージョン** - デバイスの製品バージョン。

  通常、iLO は、FRU EEPROM からこの値を取得します（製品情報地域フォーマット地域、製品バージョンの値）。

  一部のアダプターでは、この値は専用アダプターのインターフェイスを通じて取得されます。
- **ファームウェアバージョン** - インストールされているアダプターのファームウェアバージョン。

  iLO では、複数の方法を使用してこのアダプター固有情報を取得できます。

  UEFI デバイスドライバーインターフェイスをサポートしているアダプターの場合、この値を取得するための基本的な方法は UEFI です。
- **ステータス** - デバイスステータスの値。

  不明という値が表示された場合は、次を意味します。

  - iLO が、デバイスの初期化を完了していない。
  - デバイスでステータスを提供できない（レガシーチップセット SAS/SATA コントローラーなど）。
  - Agentless Management と Agentless Management Service が、このデバイスに関する情報を提供できない。

  ネットワークアダプターの不明なステータスの値について詳しくは、**ネットワーク情報**ページのドキュメントを参照してください。

  ストレージデバイスの不明なステータスの値について詳しくは、**ストレージ情報**ページのドキュメントを参照してください。

詳しくは

MCTP 検出の構成
ネットワーク情報の表示
ストレージ情報の表示

スロットの詳細ペイン

デバイスインベントリテーブルの行をクリックすると、**スロットの詳細**ペインに詳細情報が表示されます。

表示される値は、選択したデバイスタイプによって異なります。リストされた値をすべて表示しないデバイスタイプもあります。

- **製品部品番号** - アダプターベンダーのプライマリ部品番号。

  通常、iLO は、FRU EEPROM からこの値を取得します（製品情報領域フォーマット地域、製品部品/モデル番号の値）。

  部品番号がサーバーモデルごとに異なる内蔵グラフィックスデバイスに依存している場合は、**各種あり**が表示されます。

- **アセンブリ番号** - アダプターベンダーのスペア部品番号（存在する場合）。

  アダプターベンダーのスペア部品番号が存在しない場合、iLO は、FRU EEPROM からこの値を取得します（ボード情報領域フォーマット地域、ボード部品番号の値）。

- **シリアル番号** - アダプターのシリアル番号。

  通常、iLO は、FRU EEPROM からこの値を取得します（製品情報領域フォーマット地域、製品シリアル番号の値）。

  内蔵デバイスに対しては、通常、**N/A** が表示されます。

- **MCTP ステータス** - MCTP 検出が有効または無効かどうかを示します。

- スロットの詳細

  - **タイプ** - スロットタイプ（PCIe、MXM、SATA など）、または別の業界標準のスロットタイプ。
  - **バス幅** - スロットのバス幅。
  - **長さ** - スロットの長さ。
  - **特性** - スロットに関する情報。たとえば、電圧やその他のサポートに関する情報です。

  スロットの詳細の値について詳しくは、System Management BIOS（SMBIOS）参照仕様のシステムスロット（タイプ 9）を参照してください。

- **バス**（PCIe デバイスのみ） - PCI 構成中に BIOS によって割り当てられた PCI バス。その他すべてのデバイスタイプに対しては、**FFh** または **N/A** が表示されます。

- **デバイス**（PCIe デバイスのみ） - PCI 構成中に BIOS によって割り当てられた PCI デバイス。その他すべてのデバイスタイプに対しては、**FFh** または **N/A** が表示されます。

- **関数**（PCIe デバイスのみ） - PCI 構成中に BIOS によって割り当てられた PCI 関数。その他すべてのデバイスタイプに対しては、**FFh** または **N/A** が表示されます。

詳しくは

MCTP 検出の構成

デバイスステータスの値

デバイスインベントリページでは、次のステータスの値を使用します。

- **有効** - デバイスが有効であり、ヘルスステータスは **OK** です。
- **未サポート CPU** - デバイスのスロットをサポートする CPU が取り付けられていません。
- **N/A** - デバイスが取り付けられていません。
- **有効** - デバイスが有効であり、ヘルスステータスは**クリティカル**です。
- **有効** - デバイスが有効であり、ヘルスステータスは**警告**です。
- **不明** - iLO ファームウェアがデバイスステータスに関するデータを受信していません。

MCTP 検出の構成

MCTP は、サーバーにインストールされているオプションに直接通信するために iLO が使用する業界標準テクノロジーです。MCTP 検出は、デフォルトで有効です。サーバーまたは個々のアダプターに対して MCTP 検出を無効にすると、問題のあるオプションをトラブルシューティングできます。たとえば、アダプターが動作しない場合は、MCTP 検出を一時的に無効にすると、サーバーを操作しながら問題を調査できます。無効にした MCTP 検出を再び有効にする唯一の方法は、MCTP 工場出荷時リセットを実行することです。MCTP 工場出荷時リセットを実行すると、サーバースロットおよびすべてのアダプタースロットに対する MCTP 検出が有効になります。

サーバーの MCTP 検出を無効にすると、すべてのアダプタースロットについて自動的に無効になります。

Hewlett Packard Enterprise では、サポート担当者が推奨しない限り、MCTP 検出を無効にしないことをお勧めします。

警告:

- HPE OneView によって管理されているサーバーの MCTP 検出を無効にすると、無効にしたデバイスから HPE OneView にアクセスできなくなります。
- サーバーの MCTP 検出を無効にすると、iLO は、内蔵 NIC、Smart アレイ、Innovation Engine、メモリ、CPU、およびオプションアダプターなどのコンポーネントのステータス情報の監視や表示を行いません。
- MCTP 検出が無効になっている場合は、Innovation Engine ファームウェアをフラッシュできません。
- MCTP 検出が無効になっている場合は、**パフォーマンス設定**、**パフォーマンス監視**、**ワークロードパフォーマンスアドバイザー**の各ページは使用できません。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**システム情報**をクリックし、**デバイスインベントリ**タブをクリックします。
2. **検出**をクリックします。

   検出設定ページが開きます。
3. サーバースロットおよびすべてのアダプタースロットの MCTP 検出を無効にするには、**MCTP 検出**を無効に設定します。
4. 選択したアダプタースロットの MCTP 検出を無効にするには、**デバイス**テーブルの 1 つまたは複数の **MCTP** オプションを無効に設定します。
5. **適用**をクリックします。

   iLO によって、MCTP 検出を再度有効にするには MCTP の出荷時リセットが必要であることが通知されます。
6. **OK** をクリックします。

MCTP 工場出荷時リセットの開始

MCTP 検出がサーバーまたはサーバーのアダプタースロットに対して無効になっている場合、これを再度有効にする唯一の方法は、MCTP 工場出荷時リセットを実行することです。この手順を実行しても、iLO またはサーバーはリセットされません。

前提条件

iLO 設定の構成権限

手順

1. ナビゲーションツリーで**システム情報**をクリックし、**デバイスインベントリ**タブをクリックします。
2. **検出**をクリックします。

   検出設定ページが開きます。
3. **MCTP 工場出荷時リセット**をクリックします。

   iLO によって、MCTP 工場出荷時リセットを行うとすべてのデバイスで MCTP が有効になるという警告が表示され、要求を確認するように求められます。
4. **はい**をクリックします。

   MCTP 工場出荷時リセットが開始されます。

   プロセスが完了すると、MCTP 検出がすべてのデバイスで有効になります。

ストレージ情報の表示

サーバーの電源がオフの場合、**ストレージ情報**ページのシステムヘルス情報は、最後の電源オフ時のものです。ヘルス情報は、サーバーの電源が入っており、POST が完了している場合にのみアップデートされます。

ストレージ情報ページのすべてのデータセットを表示するには、AMS がインストールされていて実行中であることを確認します。AMS がインストールされ、サーバー上で実行されている場合にのみ、SAS/SATA コントローラーの情報が表示されます。

このページに表示される情報は、ご使用のストレージ構成によって異なります。一部のストレージ構成では、各カテゴリの情報は表示されません。

このページには、ファイバーチャネルアダプターの一覧は表示されません。ファイバーチャネルアダプターに関する情報を表示するには、ナビゲーションツリーで**システム情報**をクリックし、**ネットワーク**タブをクリックします。

手順

1. ナビゲーションツリーで**システム情報**をクリックし、**ストレージ**タブをクリックします。
2. （オプション）すべてのデータを展開するには**すべてを展開** ↙↗をクリックし、すべてのデータを折りたたむには**すべて閉じる** ↗↙をクリックします。
3. （オプション）コンポーネントの詳細を展開または折りたたむには、次のアイコンをクリックします。 ›または⌄.
4. （オプション）コンポーネントの詳細を表示するには、リストされているコンポーネントをクリックします。

   詳細ペインが開き、追加情報が表示されます。
5. （オプション）NVMe ドライブの物理ドライブインジケーター LED ステータスを変更するには、物理ドライブインジケーター LED アイコン⊙をクリックします。

   この機能を使用するには、iLO の設定を構成する権限が必要です。

   LED ステータスをオンまたはオフに変更できます。
6. （オプション）NVMe ドライブの電源をオンまたはオフにするには、**ドライブ電源ボタン**機能を使用します。

この機能を使用するには、iLO の設定を構成する権限が必要です。

詳しくは

ネットワーク情報の表示

サポート対象のストレージコンポーネント

ストレージ情報ページには、以下のストレージコンポーネントに関する次の情報が表示されます。

- Smart アレイコントローラー、ドライブエンクロージャー、接続されている論理ドライブ、および論理ドライブを構成する物理ドライブ。

  iLO では、合計 256 の物理ドライブと合計 256 の論理ドライブを監視できます。

- 直接接続ストレージを管理する Hewlett Packard Enterprise およびサードパーティ製のストレージコントローラー、および接続された物理ドライブ。

  直接接続ストレージのタイプ、SATA、NVMe、および RDE 対応デバイスがサポートされています。表示される情報は、ストレージタイプによって異なります。

サポートされるストレージ製品

- HPE ML/DL サーバー M.2 SSD 対応キット
- HPE 12G SAS エキスパンダー
- HPE デュアル 8 GB MicroSD EM USB キット（Windows のみ）
- NVMe ドライブ

ストレージ詳細

ストレージ情報ページには、Smart アレイおよび直接接続ストレージに関する以下の詳細が表示されます。

注記: 表示される情報は、ストレージタイプによって異なります。一部のストレージタイプでは、リストされている一部プロパティが含まれないことがあります。

コントローラー

コントローラーセクションには、各コントローラーに関する次の詳細が表示されます。

- **コントローラー名**
- **位置** - サーバー内のコントローラーの位置。
- **ステータス** - コントローラーのハードウェアステータスと、コントローラーに関連付けられているコンポーネントのステータスの組み合わせ。コントローラーハードウェアステータスが **OK** であり、関連付けられたいずれかのハードウェアに障害がある場合、最上位のコントローラーステータスは**クリティカル**または**警告**に変化します。コントローラーハードウェアのステータスが**クリティカル**の場合、最上位のコントローラーステータスは**クリティカル**です。
- **モデル**

コントローラーを選択すると、 **コントローラー詳細**ペインが開き、詳細情報が表示されます。

コントローラー詳細ペイン

コントローラー詳細ペインには、選択したコントローラーに関する次の詳細が表示されます。

- **コントローラーハードウェアステータス** - 表示される可能性のある値は **OK** と**クリティカル**です。
- **シリアル番号**
- **ファームウェアバージョン**
- **コントローラータイプ**
- **キャッシュモジュールのステータス**
- **キャッシュモジュールのシリアル番号**
- **キャッシュモジュールメモリ**
- **暗号化ステータス** - コントローラーで暗号化が有効になっているかどうかを示します。

  Smart Storage Administrator ソフトウェアを使用して、Smart アレイコントローラーの暗号化設定を構成できます。

  表示される値は、以下のとおりです。

  - **有効**
  - **有効ではありません**
  - **有効 - ローカルモード** - リモートのキー管理サーバーを使用しない場合は、この値が表示されます。

- **暗号化 ASIC ステータス** - コントローラーの ASIC 暗号化自己診断が成功したか失敗したかどうかを示します。「失敗」ステータスは、コントローラーが暗号化されていないことを示します。
- **暗号化クリティカルセキュリティパラメーター NVRAM ステータス** - コントローラーが正常に重要なセキュリティパラメーター NVRAM を検出したかどうかを示します。「失敗」ステータスは、コントローラーが暗号化されていないことを意味します。

論理ドライブ

論理ドライブセクションには、各論理ドライブについて次の詳細が表示されます。

- **ドライブ名**
- **ステータス**
- **容量**
- **論理ドライブのタイプ**

論理ドライブは、Smart Storage Administrator ソフトウェアで構成しないと、このページに表示されません。

論理ドライブを選択すると、 **論理ドライブ詳細**ペインが開き、詳細情報が表示されます。

論理ドライブの詳細ペイン

論理ドライブ詳細ペインには、選択した論理ドライブに関する次の詳細が表示されます。

- **インターフェイスタイプ**
- **フォールトトレランス**
- **暗号化ステータス**

物理ドライブ

物理ドライブセクションには、各物理ドライブについて次の詳細が表示されます。

- **位置** - 物理ドライブのポート、ボックス、およびベイ番号
- **ステータス**

  物理ドライブが**障害**ステータスにある場合、このステータスは全体的なストレージのヘルスステータスには影響しません。ストレージのヘルスステータスに影響するのは、論理ドライブだけです。
- **容量**
- **メディアタイプ**

物理ドライブを選択すると、物理ドライブ詳細ペインが開き、詳細情報が表示されます。

物理ドライブ詳細ペイン

物理ドライブ詳細ペインには、選択した物理ドライブに関する次の詳細が表示されます。

- **インジケーター LED** - LED ステータス（オンまたはオフ）。LED アイコン⊙をクリックして、ステータスを変更できます。この機能は、NVMe ドライブでのみ使用できます。

  この機能を使用するには、iLO の設定を構成する権限が必要です。
- **ファームウェアバージョン**
- **シリアル番号**
- **モデル**
- **ドライブの構成**
- **暗号化ステータス**
- **電源投入時間** - ドライブの電源がオンになってる時間。
- **現在のワークロードに基づいた推定される残り寿命** - 推定されたドライブの残り寿命。

  残り寿命が 100%のときは 100%の値が表示されます。**残り寿命**が 100%より少ないときは、推定値（日数）が表示されます。
- **残り寿命** - 残っているドライブ寿命のパーセント値です。この値は、ドライブから読み取られたデータに基づきます。
- **障害予告** - 障害がすぐに発生すると予測されるかどうかを示します。指定できる値は、**Yes** および **No** です。
- **PCIe タイプは使用中です**
- **PCIe レーンは使用中です**
- **最大 PCIe タイプがサポートされています**
- **最大 PCIe レーンがサポートされています**
- **ドライブ電源** - 現在のドライブの電源の状態（オン、オフ、または開始中）。

電源オンまたは**電源オフ**ボタンを使用して、NVMe ドライブのドライブ電源を制御できます。

ドライブエンクロージャー（Smart アレイのみ）

ドライブエンクロージャーセクションには、各エンクロージャーに関する次の詳細が表示されます。

- **位置** - エンクロージャーのポート番号とボックス番号。
- **ステータス**
- **ドライブベイ** - ドライブベイの数。

一部のエンクロージャーでは表示されるプロパティの一部しか含まれておらず、一部のストレージ構成ではドライブエンクロージャーが含まれていません。

エンクロージャーを選択すると、**ドライブエンクロージャー詳細**ペインが開き、詳細情報が表示されます。

ドライブエンクロージャー詳細ペイン

ドライブエンクロージャー詳細ペインには次の詳細が表示されます。

- **シリアル番号**
- **モデル番号**
- **ファームウェアバージョン**

NVMe ドライブの電源の管理

NVMe ドライブを選択すると、 **物理ドライブ詳細**ペインの**ドライブ電源ボタン**のセクションに、現在の NVMe ドライブの電源状態が表示されます。表示される可能性のある値は**オン**、 **オフ**、および**開始中**です。

ドライブ電源ボタンオプションを使用して、ドライブの電源をオンまたはオフにすることができます。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**システム情報**をクリックし、**ストレージ**タブをクリックします。
2. NVMe ドライブを選択します。

   NVMe ドライブ詳細ペインが開きます。
3. **電源オン**または**電源オフ**ボタンをクリックします。
4. 要求を確認するメッセージが表示されたら、**OK** をクリックします。

NVMe ドライブの仮想電源ボタンのオプション

- **電源オン** - すぐにドライブの電源を入れます。
- **電源オフ** - すぐにドライブの電源を切ります。このオプションを使用すると、強制的にシャットダウンされます。

ファームウェアおよびソフトウェアの表示および管理

ファームウェアのアップデート

ファームウェアのアップデートでは、新機能、改良、およびセキュリティアップデートによりサーバーと iLO 機能が向上します。

オンライン方式またはオフライン方式によりファームウェアをアップデートすることができます。

オンラインでのファームウェアアップデート

オンライン方式を使用してファームウェアをアップデートする場合、サーバーオペレーティングシステムをシャットダウンせずにアップデートを実行できます。オンラインでのファームウェアアップデートは、インバンドまたはアウトオブバンドで実行できます。

インバンド

ファームウェアは、サーバーホストオペレーティングシステムから iLO に送信されます。

インバンドのファームウェアアップデートには iLO ドライバーが必要です。

iLO が製品セキュリティ状態に設定されている場合、ホストベースのファームウェアアップデートでは、ユーザーの認証情報または権限は確認されません。ホストベースのユーティリティでは、ルート（Linux および VMware）または管理者（Windows）ログインが必要です。

iLO が、高セキュリティ、FIPS、または CNSA のセキュリティ状態を使用するように構成されている場合、ユーザー認証情報が必要になります。

アウトオブバンド

ファームウェアは、ネットワーク接続経由で iLO に送信されます。iLO 設定の構成権限を持つユーザーは、アウトオブバンド方式を使用してファームウェアをアップデートできます。

製品セキュリティ状態を使用するシステムの iLO のセキュリティが無効になるように、システムメンテナンススイッチが設定されている場合、すべてのユーザーは、アウトオブバンド方式でファームウェアをアップデートできます。システムが、高度なセキュリティ状態を使用するように構成されている場合、ユーザー認証情報が必要になります。

インバンドのファームウェアアップデート方法

オンライン ROM フラッシュコンポーネント

サーバーの稼動中に実行可能ファイルを使用してファームウェアをアップデートします。実行可能ファイルには、インストーラーとファームウェアパッケージが含まれています。

このオプションは、iLO が製品セキュリティ状態を使用して構成されている場合にサポートされます。

HPONCFG

このユーティリティを使用し、XML スクリプトを使用してファームウェアをアップデートします。iLO またはサーバーのファームウェアイメージと `Update_Firmware.xml` サンプルスクリプトをダウンロードします。セットアップの詳細でサンプルスクリプトを編集し、スクリプトを実行します。

iLO 5 1.20 以降と共に HPONCFG 5.2.0 以降を使用する場合に必要なユーザーの権限を持っていないと、エラーメッセージが表示されます。

アウトオブバンドのファームウェアアップデート方法

iLO Web インターフェイス

iLO Web インターフェイスを使用してサポートされるファームウェアファイルをダウンロードし、インストールします。単一のサーバーまたは iLO 連携グループのファームウェアをアップデートできます。

iLO RESTful API

iLO RESTful API および RESTful インターフェイスツールなどの REST クライアントを使用して、ファームウェアをアップデートします。

HPQLOCFG

このユーティリティを使用し、XML スクリプトを使用してファームウェアをアップデートします。iLO またはサーバーのファームウェアイメージと `Update_Firmware.xml` サンプルスクリプトをダウンロードします。セットアップの詳細でサンプルスクリプトを編集し、スクリプトを実行します。

HPLOMIG（ProLiant 管理プロセッサー用のディレクトリサポートとも呼ばれる）

HPLOMIG のファームウェアアップデート機能を使用するためにディレクトリ統合を使用する必要はありません。HPLOMIG を使用すると、複数の iLO プロセッサーを検出し、そのファームウェアを一度にアップデートすることができます。

SMASH CLP

SSH ポートを通じて SMASH CLP にアクセスし、標準のコマンドを使用してファームウェア情報を表示し、ファームウェアをアップデートします。

LOCFG.PL

Perl サンプルを使用して RIBCL スクリプトを iLO にネットワーク経由で送信してください。

オフラインでのファームウェアアップデート

ファームウェアのアップデートにオフラインの方法を使用する場合は、オフラインユーティリティを使用してサーバーを再起動する必要があります。

オフラインでのファームウェアアップデート方法

SPP

ファームウェアアップデートをダウンロードし、インストールする

SUM

SUM を使用してサポートされるサーバーおよびその他のノードのファームウェア、ドライバー、およびソフトウェアメンテナンスを実行してください。

iLO と一緒に SUM を使用して、iLO レポジトリにアクセスし、インストールセットとインストールキューを管理できます。

Scripting Toolkit

Scripting Toolkit を使用して、サーバー内で複数の設定を構成したり、ファームウェアをアップデートしたりします。この方法は、複数のサーバーを展開する場合に便利です。

iLO ファームウェアとソフトウェアの管理

iLO Web インターフェイスでは、以下のファームウェアおよびソフトウェア管理機能がサポートされています。

- **インストールされているファームウェア**を表示する。
- 冗長なシステム ROM でアクティブなシステム ROM を**交換する**
- **ファームウェアのアップデート**制御を使用して、ローカルの管理対象サーバーにファームウェアをインストールする。

  ファームウェアのアップデート制御を使用して、iLO **言語パック**をインストールすることもできます。
- **インストールされているソフトウェア**を表示する。
- **メンテナンスウィンドウ**を管理する。インストールキューに追加するタスクにメンテナンスウィンドウを適用できます。
- **グループファームウェアアップデート**機能を使用して、iLO 連携グループ内の複数のサーバーにファームウェアをインストールする。
- Smart Update 機能が統合されている iLO にアクセスする。このバージョンの iLO では、次の操作がサポートされます。
  - **iLO レポジトリ**でコンポーネントを表示および管理する。
  - iLO レポジトリからインストールキューに**コンポーネントを追加する**。
  - **インストールセット**の表示と削除、およびインストールキューへの追加を行う。

    インストールセットを構成するには、SUM を使用します。詳しくは、SUM ドキュメントを参照してください。
  - **システムリカバリセット**を表示するか、iLO RESTful API を使用して**システムリカバリセットを作成する**。
  - **インストールキュー**でタスクを表示および管理する。

    インストールキューの管理には SUM を使用することをお勧めします。詳しくは、SUM ドキュメントを参照してください。

ファームウェアのアップデート、**iLO レポジトリへのアップロード**、**キューに追加**制御には、**ファームウェア & OS ソフトウェア**ページのすべてのタブからアクセスできます。

詳しくは、**ファームウェアのアップデート**のビデオを参照してください。

インストール済みファームウェア情報の表示

手順

1. ナビゲーションツリーで**ファームウェア& OS ソフトウェア**をクリックします。

   インストールされたファームウェアページには、さまざまなサーバーコンポーネントのファームウェア情報が表示されます。サーバーの電源が切れている場合、このページの情報は、最後に電源が切れた時点の情報になります。ファームウェア情報は、サーバーの電源が入っており、POST が完了している場合にのみアップデートされます。
2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

ファームウェアの種類

インストールされたファームウェアページに表示されるファームウェアタイプは、サーバーモデルおよびサーバーの構成によって変化します。

ほとんどのサーバーでは、システム ROM および iLO ファームウェアが表示されます。他の可能なファームウェアオプションは、次のとおりです。

- パワーマネジメントコントローラー
- サーバープラットフォームサービスファームウェア
- Smart アレイ
- Intelligent Platform 抽象化データ
- Smart Storage Energy Pack
- TPM または TM ファームウェア
- SAS プログラマブルロジックデバイス
- システムプログラマブルロジックデバイス
- Intelligent Provisioning
- ネットワークアダプター
- NVMe バックプレーンファームウェア
- Innovation Engine (IE) ファームウェア
- ドライブファームウェア
- 電源装置ファームウェア
- 内蔵ビデオコントローラー
- 言語パック
- HPE Persistent Memory

ファームウェアの詳細

インストールされたファームウェアページでは、リストされているファームウェアのタイプごとに以下の情報が表示されます。

- **ファームウェア名** - ファームウェアの名前。
- **ファームウェアバージョン** - ファームウェアのバージョン。
- **位置** - 表示されたファームウェアを使用するコンポーネントの位置。

冗長なシステム ROM でアクティブなシステム ROM を交換

前提条件

- ホスト BIOS 構成権限
- サーバーは冗長なシステム ROM をサポートしています。

手順

1. ナビゲーションツリーで**ファームウェア& OS ソフトウェア**をクリックします。
2. **インストール済みファームウェア**ページで、🔄（**冗長化システム ROM** の詳細の横）をクリックします。

   iLO が要求を確認するように求めます。
3. **OK** をクリックします。

   変更は、次のサーバー再起動後に有効になります。

   iLO から開始されるサーバーの再起動には、仮想電源およびリセットの権限が必要です。

フラッシュファームウェア機能を使用した iLO またはサーバーのファームウェアのアップデート

iLO Web インターフェイスを使用して、任意のネットワーククライアントからファームウェアをアップデートできます。署名済みファイルが必要です。

前提条件

- iLO レポジトリにファームウェアをフラッシュし、コンポーネントを格納するには、iLO 設定の構成権限が必要です。
- 正常なファームウェアアップデート後、システムリカバリセットの任意のアップデートを実行するには、リカバリセット権限が必要です。
- **リカバリセットをアップデート**機能を使用する場合、システムリカバリセットが存在し、アップデートするコンポーネントがこれに含まれている必要があります。

手順

1. サーバーファームウェアまたは iLO ファームウェアのファイルを入手します。
2. イノベーションエンジン（IE）またはサーバープラットフォームサービス（SPS）のファームウェアをアップデートする場合は、サーバーの電源を切ってから 30 秒待ちます。
3. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**ファームウェアアップデート**クリックします。

   ファームウェアアップデートオプションが表示されない場合は、iLO Web インターフェイスの右上隅にある省略記号アイコンをクリックし、**ファームウェアアップデート**をクリックします。
4. **ローカルファイル**または**リモートファイル**オプションを選択します。
5. 選択したオプションに応じて、以下のいずれかを実行します。
   - 使用するブラウザーに応じて、**ローカルファイル**ボックスで**参照**または**ファイルを選択**をクリックして、ファームウェアコンポーネントの場所を指定します。
   - **リモートファイル URL** ボックスに、アクセス可能な Web サーバー上のファームウェアコンポーネントの URL を入力します。
6. （オプション）コンポーネントのコピーを iLO レポジトリに保存するには、**同様に、iLO レポジトリに保存**チェックボックスを選択します。

7. （オプション）手順 **5** で選択したコンポーネントのバージョンがシステムリカバリセットに存在する場合は、**リカバリセットをアップデート**チェックボックスを選択して、選択したコンポーネントに既存のコンポーネントを置き換えます。

   このオプションを選択すると、システムリカバリセット内のコンポーネントのバージョンの方が新しい場合でも、コンポーネントが置き換えられます。

   システムリカバリセットが存在しない場合やこの操作に必要な権限が与えられていない場合、このオプションは表示されません。

   このオプションを選択すると、システムリカバリセットが iLO レポジトリに保存されるため、**iLO レポジトリに保存**オプションが自動的に選択されます。

8. TPM または TM がサーバーにインストールされているサーバーでは、TPM または TM の情報を保存するソフトウェアを一時停止またはバックアップしてから、**TPM の上書きを確認してください** チェックボックスを選択します。

   ドライブ暗号化ソフトウェアは、TPM または TM の情報を保存するソフトウェアの例です。

   > **注意:** ドライブ暗号化ソフトウェアを使用している場合は、ファームウェアのアップデートを開始する前に停止してください。この指示に従わない場合、ご使用のデータにアクセスできなくなる可能性があります。

9. **フラッシュ**をクリックして、アップデートプロセスを開始します。

   サーバーの構成に応じて、iLO によって次のことが通知されます。

   - iLO ファームウェアをアップデートすると、iLO は自動的に再起動します。
   - 一部のサーバーファームウェアタイプではサーバーの再起動が必要になりますが、サーバーは自動的には再起動しません。

10. **OK** をクリックします。

    iLO ファームウェアは、ファームウェアイメージを受信、検証、フラッシュします。

    iLO ファームウェアをアップデートすると、iLO が再起動し、ブラウザー接続が終了します。接続が再確立されるまでに、数分かかることがあります。

11. iLO ファームウェアのアップデートのみ：新しいファームウェアを使用するには、ブラウザーのキャッシュをクリアし、iLO にログインします。

12. サーバーファームウェアのアップデートのみ：ファームウェアのタイプによって、新しいファームウェアを有効にするためにシステムリセットやサーバーの再起動が必要になる場合は、適切なアクションを実行します。

13. （オプション）新しいファームウェアがアクティブであることを確認するには、**インストールされたファームウェア**ページでファームウェアバージョンを確認します。

    概要ページで iLO ファームウェアバージョンを確認することもできます。

詳しくは

システムリカバリセット
iLO ファームウェアイメージファイルの入手
サポートされるサーバーファームウェアイメージファイルの入手
フラッシュファームウェア機能で言語パックをインストール
ファームウェアアップデートを有効にするための要件

日次のファームウェアフラッシュ制限

iLO およびサーバーハードウェアを執拗なフラッシュ攻撃から保護するために、iLO では、サポートされている各ファームウェアタイプをフラッシュできる 1 日あたりの回数を制限しています。制限は 20 回です。これには、ファームウェアフラッシュアクティビティの成功と失敗の両方が含まれます。ファームウェアフラッシュカウントは 24 時間ごとに、またはファームウェアのアップデートに成功してから 24 時間後にリセットされます。ファームウェアフラッシュ制限は、どのアプリケーションまたはインターフェイスから開始されたファームウェアアップデートにも適用されます。

ファームウェアフラッシュカウントは不揮発性メモリに保存されます。フラッシュ制限を超えた場合、ファームウェアをフラッシュできず、後で再試行する必要があることがソフトウェアから通知されます。

ファームウェアアップデートが失敗すると、イベントが iLO イベントログに記録されます。

フラッシュ制限プロセスの例

1. 月曜日の午前 10 時に、前の金曜日以降では初めて、BIOS ファームウェアがフラッシュされます。
2. ファームウェアのフラッシュ中、BIOS ファームウェアフラッシュ制限のタイムスタンプが iLO によりチェックされます。

   この例では、最後のファームウェアフラッシュは 24 時間以上前であり、ファームウェアフラッシュカウントは 1 にリセットされます。
3. 月曜日のそれ以降に、BIOS ファームウェアがさらに 19 回フラッシュされます。

   フラッシュアクティビティごとにフラッシュカウントが 1 ずつ増加し、合計 20 になります。
4. 月曜日の終業前に BIOS ファームウェアがもう一度フラッシュされますが、フラッシュ制限のためアップデートは失敗します。

   この失敗は、翌朝 10 時にフラッシュカウントがリセットされるまで続きます。

サポートされるファームウェアタイプ

サーバーのプラットフォームに応じて、さまざまなファームウェアアップデートのタイプがサポートされます。一般的な例には、以下のものがあります。

- iLO
- システム ROM/BIOS
- シャーシ
- パワーマネジメントコントローラー
- システムプログラマブルロジックデバイス（CPLD）
- バックプレーン
- Innovation Engine（IE）
- サーバープラットフォームサービス（SPS）
- 言語パック
- サードパーティファームウェアパッケージ

  Platform Level Data Model（PLDM）ファームウェアパッケージは、**アクセス設定**ページの **3rd パーティーファームウェアアップデートパッケージの受け入れ**オプションが有効にされている場合にサポートされます。

一部のファームウェアタイプは、組み合わせたアップデートとして提供されます。以下に例を示します。

- SAS プログラマブルロジックデバイスのアップデートは、多くの場合、SAS コントローラーのファームウェアアップデートとの組み合わせになります。
- Intelligent Platform Abstraction Data のファームウェアは、多くの場合、システム ROM/BIOS のアップデートとの組み合わせになります。

ファームウェアアップデートを有効にするための要件

アップデートを有効にするには、ファームウェアタイプに応じて、追加のアクションが必要になる場合があります。

- iLO のファームウェアまたは言語パック - これらの種類のファームウェアは、自動起動される iLO リセットの後に有効になります。
- システム ROM（BIOS） - サーバーの再起動が必要です。
- シャーシファームウェア（電力管理）および Edgeline シャーシコントローラーファームウェア - ただちに有効になります。
- システムプログラマブルロジックデバイス（CPLD） - サーバーの再起動が必要です。
- パワーマネジメントコントローラーおよび NVMe バックプレーンファームウェア - サーバーの再起動やシステムのリセットは必要ありません。

  NVMe ファームウェアバージョンは、次のサーバー再起動後に iLO Web インターフェイスに表示されます。
- イノベーションエンジン（IE）およびサーバープラットフォームサービス（SPS） - これらのファームウェアタイプでは、インストールする前にサーバーの電源を切る必要があります。サーバーに電源を入れると、変更が有効になります。

iLO ファームウェアイメージファイルの入手

iLO ファームウェアイメージファイルをダウンロードし、それを使用してグループ内の 1 つのサーバーまたは複数のサーバーをアップデートできます。

ファームウェア書き換えアップデート機能または**グループファームウェアアップデート**機能を使用して iLO ファームウェアをアップデートするには、iLO オンラインフラッシュコンポーネントからの BIN ファイルが必要です。

手順

1. 次の Web サイトに移動します。**https://www.hpe.com/support/hpesc**
2. 画面の指示に従って iLO オンラインフラッシュコンポーネントファイルを探し、ダウンロードします。

   Windows または Linux のコンポーネントをダウンロードします。
3. BIN ファイルを抽出します。
   - Windows コンポーネントの場合：ダウンロードしたファイルをダブルクリックし、**解凍**ボタンをクリックします。ファイルを抽出する位置を選択して、**OK** をクリックします。
   - Linux コンポーネントの場合：ファイル形式によって異なりますが、次のいずれかのコマンドを入力します。

- #./<firmware_file_name>.scexe –unpack=/tmp/
- #rpm2cpio <firmware_file_name>.rpm | cpio -id

iLO ファームウェアイメージファイルの名前は、iLO 5_<yyy>.bin です。ここで、<yyy>はファームウェアバージョンを表します。

サポートされるサーバーファームウェアイメージファイルの入手

手順

1. 次の Web サイトに移動します。**https://www.hpe.com/support/hpesc**
2. 画面の指示に従ってオンラインフラッシュコンポーネントファイルを探し、ダウンロードします。
3. Windows コンポーネントをダウンロードした場合：
   a. ダウンロードしたファイルをダブルクリックし、**解凍**ボタンをクリックします。
   b. ファイルを抽出する位置を選択して、**OK** をクリックします。
4. Linux コンポーネントをダウンロードした場合：
   a. Linux コンポーネントの場合は、ファイルの形式に応じて、次のコマンドのいずれかを入力します。
      - #./<firmware_file_name>.scexe –unpack=/tmp/
      - #rpm2cpio <firmware_file_name>.rpm | cpio -id
   b. （オプション）イノベーションエンジンまたはサーバープラットフォームサービス（SPS）のファームウェアコンポーネントを使用する場合は、<firmware_file_name>.zip ファイルを見つけて、バイナリファイルを抽出します。

サーバーファームウェアのファイルタイプの詳細

- システム ROM をアップデートする場合、署名付きのイメージまたは署名付きの ROMPAQ イメージを使用する必要があります。
  - **署名付きイメージの例**：

    http://<server.example.com:8080>/<wwwroot>/P79_1.00_10_25_2013.signed.flash
  - **署名付き ROMPAQ イメージの例**：

    http://<server.example.com>/<wwwroot>/CPQPJ0612.A48
- パワーマネジメントコントローラー、シャーシファームウェア、および NVMe バックプレーンファイルは、拡張子.hex を使用します。たとえば、ファイル名は ABCD5S95.hex のようになります。
- システムプログラマブルロジックデバイス（CPLD）のファームウェアファイルは、ファイル拡張子.vme を使用します。
- イノベーションエンジン（IE）およびサーバープラットフォームサービス（SPS）ファームウェアファイルは、ファイル拡張子.bin を使用します。
- 言語パックファイルは拡張子.lpk を使用します。

ソフトウェア情報の表示

前提条件

このページのすべてのデータのセットを表示するには、AMS がインストールされている必要があります。

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**ソフトウェア**タブをクリックします。
2. （オプション）ソフトウェア情報のデータをアップデートするには、↻をクリックします。

   このページの情報はブラウザーにキャッシュされ、iLO では最終アップデートの日時が表示されます。ページをアップデートしてから 5 分以上経過した場合は、↻をクリックし、ページを最新情報にアップデートします。
3. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

HPE ソフトウェアの詳細

このセクションでは、管理対象サーバー上のすべての HPE ソフトウェアを一覧表示します。このリストには、手動で、または SPP を使用して追加された、Hewlett Packard Enterprise のソフトウェアおよび Hewlett Packard Enterprise 推奨の他社製ソフトウェアが含まれます。

- **名前** - ソフトウェアの名前。
- **バージョン** - ソフトウェアのバージョン。

  表示されているファームウェアコンポーネントのバージョンは、ローカルのオペレーティングシステムに保存されているファームウェアフラッシュコンポーネントで利用可能なファームウェアバージョンを示しています。表示されるバージョンが、サーバーで実行されているファームウェアと一致しない可能性があります。
- **説明** - ソフトウェアの説明。

実行中のソフトウェアの詳細

このセクションには、管理対象サーバー上で実行されているか、実行可能であるすべてのソフトウェアが表示されます。

- **名前** - ソフトウェアの名前。
- **パス** - ソフトウェアのファイルパス。

インストールされたソフトウェアの詳細

インストールされたソフトウェア - インストールされた各ソフトウェアプログラムの名前が表示されます。

メンテナンスウィンドウ

メンテナンスウィンドウとは、インストールタスクに適用される構成済みの期間のことです。

メンテナンスウィンドウは次のいずれかの方法で作成できます。

- **メンテナンスウィンドウ**タブ上
- タスクをインストールキューに追加するとき

メンテナンスウィンドウの追加

iLO は、最大 8 つのメンテナンスウィンドウをサポートします。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**メンテナンスウィンドウ**をクリックします。
2. ＋をクリックします。

   iLO は、メンテナンスウィンドウ情報を入力するよう求めるメッセージを表示します。
3. **名前**ボックスに名前を入力します。
4. **説明**ボックスに説明を入力します。
5. メンテナンスウィンドウの開始時刻と終了時刻を**開始**および**終了**ボックスに入力します。

   a. 開始ボックスにある🕒をクリックします。

      カレンダーが表示されます。

   b. 開始日時を選択し、**完了**をクリックします。

   c. 終了ボックスにある🕒（**終了**ボックス内）をクリックします。

      カレンダーが表示されます。

   d. 終了日時を選択し、**完了**をクリックします。

   iLO を管理するために使用しているクライアントの現時時間に基づいて日時を入力します。

   入力した日時に相当する UTC が日時の上に表示されます。

   既存のタスクの開始時刻よりも前の**終了**の値を入力した場合、iLO から、別の値を入力するよう求められます。インストールキューは、タスクの先入れ先出しリストです。既存のタスクの実行前に有効期限が切れるメンテナンスウィンドウを作成することはできません。
6. **追加**をクリックします。

   メンテナンスウィンドウが追加されます。

メンテナンスウィンドウの編集

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**メンテナンスウィンドウ**をクリックします。
2. ✎をクリックします。

   iLO に、メンテナンスウィンドウ情報をアップデートするよう求められます。
3. **名前**ボックスでメンテナンスウィンドウ名をアップデートします。
4. **説明**ボックスで説明をアップデートします。
5. **開始**および**終了**ボックスでメンテナンスウィンドウの開始時刻と終了時刻をアップデートします。

   a. ⏲（**開始**ボックス内）をクリックします。

      カレンダーが表示されます。

   b. 開始日時を選択し、**完了**をクリックします。

   c. ⏲（**終了**ボックス内）をクリックします。

      カレンダーが表示されます。

   d. 終了日時を選択し、**完了**をクリックします。

   iLO を管理するために使用しているクライアントの現時時間に基づいて日時を入力します。

   入力した日時に相当する UTC が日時の上に表示されます。

   既存のタスクの開始時刻よりも前の**終了**の値を入力した場合、iLO から、別の値を入力するよう求められます。インストールキューは、タスクの先入れ先出しリストです。既存のタスクの実行前に有効期限が切れるメンテナンスウィンドウを作成することはできません。
6. **OK** をクリックします。

   メンテナンスウィンドウがアップデートされます。

メンテナンスウィンドウの削除

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**メンテナンスウィンドウ**をクリックします。
2. 🗑（削除するメンテナンスウィンドウの横）をクリックします。

   iLO に、メンテナンスウィンドウの削除を確認するプロンプトが表示されます。
3. **はい、削除します**をクリックします。

   メンテナンスウィンドウが削除されます。

   削除されたメンテナンスウィンドウに関連付けられているすべてのタスクが取り消されます。

すべてのメンテナンスウィンドウを削除

前提条件

iLO 設定の構成権限

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**メンテナンスウィンドウ**をクリックします。
2. **すべて削除**をクリックします。

   iLO に、すべてのメンテナンスウィンドウの削除を確認するプロンプトが表示されます。
3. **はい、すべて削除します**をクリックします。

   メンテナンスウィンドウが削除されます。

   削除されたメンテナンス ウィンドウに関連付けられているすべてのタスクが取り消されます。

メンテナンスウィンドウの表示

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**メンテナンスウィンドウ**をクリックします。
2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。
3. （オプション）詳細情報を表示するには、個々のメンテナンスウィンドウをクリックします。

メンテナンスウィンドウのサマリーの詳細

メンテナンスウィンドウタブに **iLO の日時**および構成された各メンテナンスウィンドウに関する次の詳細が表示されます。

- **名前** - メンテナンスウィンドウのユーザー定義名。
- **開始時間** - メンテナンスウィンドウの開始時刻（UTC）。
- **終了時刻** - メンテナンスウィンドウの終了時刻（UTC）。

メンテナンスウィンドウは期限を過ぎてから 24 時間以内に自動的に削除されます。

各メンテナンスウィンドウの詳細

各メンテナンスウィンドウをクリックすると、以下の詳細が表示されます。

- **名前** - メンテナンスウィンドウのユーザー定義名。
- **開始** - メンテナンスウィンドウの開始時刻（UTC）。
- **終了** - メンテナンスウィンドウの終了時刻（UTC）。
- **説明** - メンテナンスウィンドウの説明。

iLO レポジトリ

iLO レポジトリは、システムボードに埋め込まれた不揮発性フラッシュメモリ内の安全なストレージ領域です。不揮発性フラッシュメモリはサイズが 4 ギガバイトで、iLO NAND と呼ばれます。SUM または iLO を使用して、iLO レポジトリ内の署名済みソフトウェアおよびファームウェアコンポーネントを管理します。

iLO、UEFI BIOS、SUM および他のクライアントソフトウェアは、これらのコンポーネントを取得し、サポートされているサーバーに適用できます。SUM を使用して、インストールセットに保存するコンポーネントを整理し、SUM または iLO を使用してインストールキューを管理します。

iLO、SUM、および BIOS ソフトウェアがどのように連携してソフトウェアとファームウェアを管理するかについて詳しくは、**SUM のドキュメント**を参照してください。

iLO レポジトリへのコンポーネントの追加

iLO レポジトリにアップロードペインを使用して、iLO レポジトリにコンポーネントを追加します。**iLO レポジトリにアップロード**ペインは、**ファームウェア & OS ソフトウェア**ページのタブからアクセスできます。

前提条件

- iLO レポジトリにファイルをアップロードするには、iLO 設定の構成権限が必要です。
- iLO レポジトリへのファイルのアップロード後、システムリカバリセットの任意のアップデートを実行するには、リカバリセット権限が必要です。
- **リカバリセットをアップデート**機能を使用する場合、システムリカバリセットが存在し、アップデートするコンポーネントがこれに含まれている必要があります。

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックして、**iLO レポジトリにアップロード**をクリックします。

   ブラウザーウィンドウのサイズが小さいために、**iLO レポジトリにアップロード**オプションが表示されない場合は、iLO Web インターフェイスの右上隅の省略符号アイコンをクリックしてから、**iLO レポジトリにアップロード**をクリックします。

2. **ローカルファイル**または**リモートファイル**オプションを選択します。
3. 選択したオプションに応じて、以下のいずれかを実行します。
   - **ローカルファイル**ボックスで、（使用するブラウザーに応じて）**参照**または**ファイルを選択**をクリックして、ファームウェアコンポーネントの場所を指定します。
   - **リモートファイル URL** ボックスに、アクセス可能な Web サーバー上のファームウェアコンポーネントの URL を入力します。
4. 複数ファイルのみで指定されたファームウェアコンポーネントの場合：**コンポーネントの署名ファイルを持っています**チェックボックスを選択します。
5. 手順 **4** でチェックボックスを選択した場合は、以下のいずれかを実行します。
   - **ローカル署名ファイル**ボックスで、（使用するブラウザーに応じて）**参照**または**ファイルを選択**をクリックしてから、コンポーネント署名ファイルの場所を指定します。
   - **リモート署名ファイル URL** ボックスに、アクセス可能な Web サーバー上のコンポーネント署名ファイルの URL を入力します。

6. （オプション）手順 **3** で選択したコンポーネントのバージョンがシステムリカバリセットに存在する場合は、**リカバリセットをアップデート**チェックボックスを選択して、選択したコンポーネントに既存のコンポーネントを置き換えます。

   このオプションを選択すると、システムリカバリセット内のコンポーネントのバージョンの方が新しい場合でも、コンポーネントが置き換えられます。

   システムリカバリセットが存在しない場合やこの操作に必要な権限が与えられていない場合、このオプションは表示されません。

7. **アップロード**をクリックします。

   iLO により、既存のコンポーネントと同じ名前を持つコンポーネントをアップロードすると既存のコンポーネントが置換されることが通知されます。

8. **OK** をクリックします。

   アップロードが開始されます。アップロードステータスは iLO Web インターフェイスの上部に表示されます。

詳しくは

システムリカバリセット
iLO ファームウェアイメージファイルの入手
サポートされるサーバーファームウェアイメージファイルの入手

iLO レポジトリからコンポーネントをインストールする

iLO レポジトリページからインストールキューにコンポーネントを追加できます。

コンポーネントをインストールキューに追加すると、タスクがキューの末尾に追加されます。キューに入れられた他のタスクが完了した後、コンポーネントタイプのアップデートを開始するソフトウェアがインストール要求を検出したときに、追加されたコンポーネントがインストールされます。アップデートを開始できるソフトウェアについては、**iLO レポジトリ**ページと**インストールキュー**ページでコンポーネントの詳細を確認してください。

前にキューに入れられたタスクが開始または終了を待機している場合、新しいタスクは無期限に遅延する場合があります。たとえば、キューに入れられたコンポーネントが UEFI BIOS によってインストール可能な場合、インストールを開始する前にサーバーの再起動が必要です。サーバーが再起動されない場合、これよりも後のキュー内のタスクは無期限に遅延します。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**iLO レポジトリ**をクリックします。

2. （インストールするコンポーネントの横）をクリックします。

   インストールコンポーネントペインが開き、要求の確認を求められます。

3. （オプション）インストールのスケジュールを指定するには、**スケジュールウィンドウをセット**チェックボックスを選択します。

   a. スケジュールを定義する方法を選択します。

      - **メンテナンスウィンドウを使用**（デフォルト）を選択し、**メンテナンスウィンドウ**ページで構成したメンテナンスウィンドウを選択します。

メンテナンスウィンドウを追加するには、**新規**をクリックして**メンテナンスウィンドウ**ページに移動します。メンテナンスウィンドウを作成してから、この手順を再開します。

- **時間枠を指定してください**を選択し、スケジュールをその場で入力します。

b. 選択した方法によって、以下のいずれかを実行します。

- **メンテナンスウィンドウを使用**を選択した場合は、**メンテナンスウィンドウ**リストで値を選択します。
- **時間枠を指定してください**を選択した場合は、**スケジュールの詳細を入力します**。

4. はい、キューの最後に追加をクリックします。

インストールキューが空で、iLO がコンポーネントのインストールを開始できる場合、ボタンに、**はい、今インストール**というラベルが付けられます。

キューに入れられた既存のタスクが終了し、選択されたコンポーネントタイプのインストールを開始するソフトウェアが保留中のインストールを検出すると、アップデートが開始されます。

インストールキューが空で、iLO がアップデートを開始できる場合、すぐにアップデートが開始されます。

詳しくは

日次のファームウェアフラッシュ制限
iLO レポジトリへのコンポーネントの追加
iLO レポジトリの概要とコンポーネントの詳細の表示
インストールキューの表示
iLO ファームウェアイメージファイルの入手
サポートされるサーバーファームウェアイメージファイルの入手

コンポーネントのインストール時に時間枠の詳細を入力する

時間枠を指定してくださいが選択されているときは、以下の手順を使用してスケジュールを入力します。

前提条件

iLO の設定を構成する権限

手順

1. ◷（**開始**ボックス内）をクリックします。

カレンダーが表示されます。

2. 開始日時を選択し、**完了**をクリックします。

選択した日時は**開始**ボックスに表示されます。

3. ◷（**終了**ボックス内）をクリックします。

カレンダーが表示されます。

4. 終了日時を選択し、**完了**をクリックします。

この値によって、インストールセット内のタスクの有効期限（日付時刻）が設定されます。

選択した日時は**終了**ボックスに表示されます。

iLO レポジトリからのコンポーネントの削除

前提条件

- iLO の設定を構成する権限
- コンポーネントがインストールセットに含まれていない。
- コンポーネントがキューに入れられたタスクの一部ではない。

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**iLO レポジトリ**タブをクリックします。
2. 🗑をクリックします。

   iLO が要求を確認するように求めます。
3. **はい、削除します**をクリックします。

   コンポーネントが削除されます。

iLO レポジトリからすべてのコンポーネントを削除する

前提条件

- iLO 設定の構成権限
- コンポーネントがインストールセットに含まれていない。
- コンポーネントがキューに入れられたタスクの一部ではない。

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**iLO レポジトリ**タブをクリックします。
2. **すべて削除**をクリックします。

   iLO が要求を確認するように求めます。
3. **はい、すべて削除します**をクリックします。

   コンポーネントが削除されます。

iLO レポジトリの概要とコンポーネントの詳細の表示

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**iLO レポジトリ**タブをクリックします。
2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

3. （オプション）コンポーネントの詳細な情報を表示するには、個々のコンポーネントをクリックします。

iLO レポジトリのストレージの詳細

iLO レポジトリページの**概要**セクションには、iLO レポジトリのストレージの使用状況に関する以下の詳細が表示されます。

- **容量** - iLO レポジトリの総ストレージ容量
- **使用中** - 使用されているストレージ
- **空き容量** - iLO レポジトリの使用可能なストレージ
- **コンポーネント** - iLO レポジトリに保存されているコンポーネントの数

iLO レポジトリの内容

iLO レポジトリページの**コンテンツ**セクションには、ソフトウェアコンポーネントまたは各ファームウェアに関する以下の詳細が表示されます。

- **名前**
- **バージョン**

iLO レポジトリの個々のコンポーネントの詳細

個々のコンポーネントをクリックすると、以下の詳細が表示されます。

- **名前** - コンポーネント名
- **バージョン** - コンポーネントのバージョン
- **ファイル名** - コンポーネントのファイル名
- **サイズ** - コンポーネントのサイズ
- **アップロード** - アップロードの日時
- **インストール元** - コンポーネントのアップデートを開始できるソフトウェア
- **インストールセットまたはタスクで使用中ですか?** - コンポーネントがインストールセットまたはキューに入れられたタスクの一部かどうか

  コンポーネントがインストールセットまたはキューに入れられたタスクの一部である場合、インストールセットまたはタスク名のリンクをクリックして、インストールセットの詳細またはキューに入れられたタスクの詳細を表示できます。

インストールセット

インストールセットは、1 つのコマンドでサポートされるサーバーに適用できるコンポーネントのグループです。SUM は、サーバーに何をインストールするかを決定し、iLO にコピーするインストールセットを作成します。既存のインストールセットは、iLO Web インターフェイスの**インストールセット**ページで確認できます。

SUM から展開するときにインストールセットを保存すると、iLO システム上のすべてのコンポーネントが後で使用できるように保持されます。たとえば、元の SPP が見つからなくても、保存したコンポーネントを使用してコンポーネントバージョンをリストアまたはロールバックすることができます。

iLO、SUM、および BIOS ソフトウェアがどのように連携してソフトウェアとファームウェアを管理するかについて詳しくは、**SUM のドキュメント**を参照してください。

インストールセットのインストール

インストールセットページからインストールセットをインストールキューに追加できます。

インストールセットをインストールキューに追加すると、iLO は、インストールセット内のコンポーネントまたはコマンドごとにタスクを追加します。新しいタスクはキューの末尾に追加されます。

キュー内のコンポーネントは、キューに入れられた他のタスクが完了した後、コンポーネントタイプのアップデートを開始するソフトウェアがインストール要求を検出したときにインストールされます。アップデートを開始できるソフトウェアについては、**iLO レポジトリ**ページと**インストールキュー**ページでコンポーネントの詳細を確認してください。

前にキューに入れられたコンポーネントが開始または終了を待機している場合、新しいタスクは無期限に遅延する場合があります。たとえば、キューに入れられたコンポーネントが UEFI BIOS によってインストール可能な場合、インストールを開始する前にサーバーの再起動が必要です。サーバーが再起動されない場合、これよりも後のキュー内のタスクは無期限に遅延します。

前提条件

- iLO の設定を構成する権限
- インストールセット内のコンポーネントが別のインストールタスクの一部としてキューに入れられることはありません。

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**インストールセット**タブをクリックします。
2. （インストールするインストールセットの横）をクリックします。

   インストールコンポーネントペインが開き、要求の確認を求められます。
3. （オプション）インストールのスケジュールを指定する場合は、**スケジュールウィンドウをセット**チェックボックスを選択します。

   a. スケジュールを定義する方法を選択します。

      - **メンテナンスウィンドウを使用**（デフォルト）を選択し、**メンテナンスウィンドウ**ページで構成したメンテナンスウィンドウを選択します。

        メンテナンスウィンドウを追加するには、**新規**をクリックして**メンテナンスウィンドウ**ページに移動します。メンテナンスウィンドウを作成してから、この手順を再開します。
      - **時間枠を指定してください**を選択し、スケジュールをその場で入力します。

   b. 選択した方法によって、以下のいずれかを実行します。

      - **メンテナンスウィンドウを使用**を選択した場合は、**メンテナンスウィンドウ**リストで値を選択します。
      - **時間枠を指定してください**を選択した場合は、**スケジュールの詳細を入力します**。

4. （オプション）キューに入れられた既存のタスクがあり、それらを削除する場合は、**インストールキューをクリア**チェックボックスを選択します。

   既存のタスクがある場合、iLO は、キューに入っているタスクの数を表示し、インストールセットの内容がキューの末尾に追加されることを通知します。

   キューが空で、iLO がインストールセットでアップデートを開始できる場合、このチェックボックスは表示されません。

   キューが空で、iLO がインストールセットでアップデートを開始できない場合、このチェックボックスは無効になっています。

5. **はい、キューの最後に追加**をクリックします。

   手順 **4** でチェックボックスを選択しているか、キューがすでに空のときに、iLO がインストールセットでアップデートを開始できる場合は、ボタンラベルが**はい、今インストール**になります。

   キューに入れられた既存のタスクが終了し、選択されたコンポーネントタイプのインストールを開始するソフトウェアが保留中のインストールを検出すると、アップデートが開始されます。

   インストールキューが空で、iLO が要求されたアップデートを開始できる場合、すぐにアップデートが開始されます。

詳しくは

インストールキューの表示

インストールセットのインストール時に時間枠の詳細を入力する

時間枠を指定してくださいが選択されているときは、以下の手順を使用してスケジュールを入力します。

前提条件

iLO の設定を構成する権限

手順

1. （**開始**ボックス内）をクリックします。

   カレンダーが表示されます。

2. 開始日時を選択し、**完了**をクリックします。

   選択した日時は**開始**ボックスに表示されます。

3. （**終了**ボックス内）をクリックします。

   カレンダーが表示されます。

4. 終了日時を選択し、**完了**をクリックします。

   この値によって、インストールセット内のタスクの有効期限（日付時刻）が設定されます。

   選択した日時は**終了**ボックスに表示されます。

インストールセットを削除する

前提条件

- 保護されていないインストールセットの iLO 設定の構成権限。
- 保護されたインストールセットを削除するための iLO 設定の構成権限とリカバリセット権限。

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**インストールセット**タブをクリックします。
2. 削除するインストールセットの横にある🗑をクリックします。

   iLO が要求を確認するように求めます。
3. **はい、削除します**をクリックします。

   インストールセットが削除されます。

すべてのインストールセットを削除する

前提条件

- iLO の設定を構成する権限
- すべてのインストールセットを削除する要求にシステムリカバリセットを含めるには、リカバリセット権限が必要です。

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**インストールセット**タブをクリックします。
2. **すべて削除**をクリックします。

   iLO が要求を確認するように求めます。
3. （オプション）システムリカバリセットが存在する場合、リカバリセットを削除するには、**保護されたリカバリセットも削除**チェックボックスを選択します。

   ユーザーアカウントにリカバリセット権限が割り当てられていない場合、このオプションは表示されません。
4. **はい、すべて削除**をクリックします。

   インストールセットが削除されます。

インストールセットを表示する

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**インストールセット**タブをクリックします。
2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。
3. （オプション）インストールセットをクリックして詳細情報を表示します。

インストールセットの概要の詳細

インストールセットタブには、各インストールセットに関する以下の詳細が表示されます。

- **名前** - インストールセットの名前。
- **コンポーネント/コマンド** - インストールセット内のコンポーネントとコマンド。バージョン情報はすべてのコンポーネントに含まれます。

インストールセットアイコンを使用して、インストールセットをインストールキューに追加したり、インストールセットを削除したりできます。保護されたインストールセットは、ロックアイコン付きで表示されます。

詳しくは

インストールセットのインストール
インストールセットを削除する

個々のインストールセットの詳細

個々のインストールセットをクリックすると、以下の詳細が表示されます。

- **名前** - インストールセットの名前。
- **作成済み** - 作成日時。
- **説明** - インストールセットの説明。
- **コンポーネント/コマンド** - インストールセット内のコンポーネントとコマンド。バージョン情報はすべてのコンポーネントに含まれます。

  インストールセットにコンポーネントが含まれている場合、コンポーネント名のリンクをクリックすると、コンポーネントの詳細を iLO レポジトリに表示することができます。
- **システムリカバリセット**-インストールセットがシステムリカバリセットとして指定されているかどうかを示します。

  システムリカバリセットは、ランタイムのファームウェアリカバリ操作で使用されます。システムリカバリセットは同時に 1 つのみ存在できます。

システムリカバリセット

デフォルトでは、システムリカバリセットがすべてのサーバーに付属します。 **リカバリセット**権限を持つユーザーアカウントは、このインストールセットを構成できます。 システムリカバリセットは同時に 1 つのみ存在できます。

インテルサーバー用のデフォルトのシステムリカバリセットには、以下のファームウェアコンポーネントが含まれます。

- システム ROM（BIOS）
- iLO ファームウェア
- システムプログラマブルロジックデバイス（CPLD）
- Innovation Engine
- サーバープラットフォームサービス（SPS）ファームウェア

AMD サーバー用のデフォルトのシステムリカバリセットには、以下のファームウェアコンポーネントが含まれます。

- システム ROM（BIOS）
- iLO ファームウェア
- システムプログラマブルロジックデバイス（CPLD）

デフォルトのシステムリカバリセットが削除されている場合

- **リカバリセット**権限を所有しているユーザーは、iLO RESTful API および RESTful インターフェイスツールを使用して iLO レポジトリに保存されているコンポーネントからシステムリカバリセットを作成することができます。
- **リカバリセット**権限を持つユーザーは、SUM を使用してインストールセットを作成し、iLO RESTful API を使用してそれをシステムリカバリセットとして指定できます。

  手順については、オプションキットの **SUM ドキュメントを参照**してください。

詳しくは

システムリカバリセットの作成

システムリカバリセットの作成

システムリカバリセットが削除された場合、iLO RESTful API および RESTful インターフェイスツールを使用して、iLO レポジトリに保存されているコンポーネントから新しいセットを作成できます。

注記: 既存のシステムリカバリセットにある個々のコンポーネントを交換するには、iLO レポジトリにコンポーネントを追加して、**リカバリセットをアップデート**チェックボックスを選択します。

前提条件

- リカバリセット権限
- システムのリカバリのセットは、サーバー上に存在しません。
- RESTful インターフェイスツールがインストールされている。

  詳しくは、**https://www.hpe.com/info/redfish** を参照してください。

手順

1. システムリカバリセットに含めるファームウェアコンポーネントをダウンロードします。

   通常、システムリカバリセットには、以下のコンポーネントが含まれます。

   - iLO ファームウェア
   - システム ROM/BIOS
   - システムプログラマブルロジックデバイス（CPLD）
   - Innovation Engine（IE）
   - サーバープラットフォームサービス（SPS）

2. ダウンロードされたコンポーネントから必要なファイルを抽出します。
3. iLO レポジトリにファームウェアコンポーネントを追加します。
4. テキストエディターを開き、システムリカバリセットを定義するファイルを作成します。

このファイルには、名前と説明が含まれ、`IsRecovery` プロパティを割り当て、追加するコンポーネントを一覧表示します。インストールセットを使用する際に、インストールされる順番でコンポーネントを追加します。

テンプレートとして、次の例を使用します。内容は、ダウンロードしたコンポーネントのバージョンによって異なる場合があります。

```
{
    "Description": "Essential system firmware components",
    "IsRecovery": true,
    "Name": "System Recovery Set",
    "Sequence": [
        {
            "Command": "ApplyUpdate",
            "Filename": "ilo5_130.bin",
            "Name": "System Recovery Set item (iLO 5)",
            "UpdatableBy": [
                "Bmc"
            ]
        },
        {
            "Command": "ApplyUpdate",
            "Filename": "U32_1.32_02_01_2018.signed.flash",
            "Name": "System Recovery Set item (System ROM)",
            "UpdatableBy": [
                "Bmc"
            ]
        },
        {
            "Command": "ApplyUpdate",
            "Filename": "CPLD_DL360_DL380_Gen10_VP1_v2A2A_full_signed.vme",
            "Name": "System Recovery Set item (System Programmable Logic Device)",
            "UpdatableBy": [
                "Bmc"
            ]
        },
        {
            "Command": "ApplyUpdate",
            "Filename": "IEGen10_0.1.5.2.signed.bin",
            "Name": "System Recovery Set item (Innovation Engine)",
            "UpdatableBy": [
                "Bmc"
            ]
        },
        {
            "Command": "ApplyUpdate",
            "Filename": "SPSGen10_04.00.04.288.signed.bin",
            "Name": "System Recovery Set item (Server Platform Services)",
            "UpdatableBy": [
                "Bmc"
            ]
         }
    ]
}
```

5. ファイルを JSON ファイルとして保存します。たとえば、**system_recovery_set.json** と名付けます。
6. RESTful インターフェイスツールを起動します。

   インストール設定の作業に関するヘルプを表示するには、`ilorest installset -help` と入力します。

詳しくは、次の Web サイトを参照してください。**https://www.hpe.com/support/restfulinterface/docs**

7. システムリカバリセットを作成するためのコマンドを入力します。

   ```
   C:\WINDOWS\system32 > ilorest installset add < JSON ファイルの場所 > \ < JSON ファイル名 >
   -u < iLO のログイン名 >-p < iLO パスワード > --url = < iLO ホスト名または IP アドレス >
   ```

8. （オプション）インストール設定を表示するには、次のコマンドを入力します。

   ```
   ilorest installset-u < iLO のログイン名 >-p < iLO パスワード > - url = < iLO ホスト名または IP アドレス >
   ```

   サーバー上のインストールセットは、含まれるコンポーネントと一緒に表示されます。

詳しくは

iLO ファームウェアイメージファイルの入手
サポートされるサーバーファームウェアイメージファイルの入手
iLO レポジトリへのコンポーネントの追加

インストールキュー

インストールキューは、キューに個別に、またはインストールセットの一部として追加されたコンポーネントおよびコマンドの順序付けされたリストです。タスクは、次の方法を使用してキューに追加できます。

- iLO の**キューに追加**ペインを使用する。
- ＋（**インストールキュー**ページ）をクリックする。
- （iLO レポジトリページ）をクリックする。
- SUM を使用する。

詳しくは

インストールキューへのタスクの追加
iLO レポジトリからコンポーネントをインストールする

インストールキューへのタスクの追加

前提条件

- インストールキューにタスクを追加するには、iLO 設定の構成権限が必要です。
- キューに入れられたアップデートが正常に完了した後に、システムリカバリセットの任意のアップデートを実行するには、リカバリセット権限が必要です。
- **リカバリセットをアップデート**機能を使用する場合、システムリカバリセットが存在し、アップデートするコンポーネントがこれに含まれている必要があります。

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**インストールキュー**タブをクリックします。
2. ＋をクリックするか、**キューに追加**をクリックします。

キューに追加ペインは、**ファームウェア & OS ソフトウェア**ページのタブで使用できます。ブラウザーウィンドウのサイズが小さいために、**キューに追加**オプションが表示されない場合は、iLO Web インターフェイスの右上隅にある省略記号アイコンをクリックして、**キューに追加**をクリックします。

iLO は、タスク情報を追加するよう求めるメッセージを表示します。

3. **タスク名**ボックスにタスク名（最大 64 文字）を入力します。
4. **コンポーネント/コマンド**ボックスで値を選択します。

   このリストには、以下のものが含まれます。

   - iLO レポジトリに保存されているコンポーネント。
   - **待機**および **iLO をリセット**コマンド。

5. **待機**コマンドを選択した場合、待機時間を**待機時間（秒）**ボックスに入力します。

   有効な値は 1～3600 秒です。

6. （オプション）インストールのスケジュールを指定するには、**スケジュールウィンドウをセット**チェックボックスを選択します。

   a. スケジュールを定義する方法を選択します。

      - **メンテナンスウィンドウを使用**（デフォルト）を選択し、**メンテナンスウィンドウ**ページで構成したメンテナンスウィンドウを選択します。

        メンテナンスウィンドウを追加するには、**新規**をクリックして**メンテナンスウィンドウ**ページに移動します。メンテナンスウィンドウを作成してから、この手順を再開します。

      - **時間枠を指定してください**を選択し、スケジュールをその場で入力します。

   b. 選択した方法によって、以下のいずれかを実行します。

      - **メンテナンスウィンドウを使用**を選択した場合は、**メンテナンスウィンドウ**リストで値を選択します。
      - **時間枠を指定してください**を選択した場合は、スケジュールの詳細を入力します。

7. （オプション）手順 **4** でコンポーネントを選択し、そのコンポーネントがシステムリカバリセットに存在する場合は、**リカバリセットをアップデート**チェックボックスを選択して、選択したコンポーネントに既存のコンポーネントを置き換えます。

   このオプションを選択すると、システムリカバリセット内のコンポーネントのバージョンの方が新しい場合でも、コンポーネントが置き換えられます。

   次の場合、このオプションは表示されません。

   - コマンドが選択されている。
   - システムリカバリセットがない。
   - 必要な権限がユーザーアカウントに割り当てられていない。

8. サーバーに TPM または TM が存在する場合は、TPM または TM の情報を保存するソフトウェアを一時停止またはバックアップしてから、**TPM の上書きを確認してください**チェックボックスを選択します。

   ドライブ暗号化ソフトウェアは、TPM または TM の情報を保存するソフトウェアの例です。

注意: ドライブ暗号化ソフトウェアを使用している場合は、ファームウェアのアップデートを開始する前に停止してください。この指示に従わない場合、ご使用のデータにアクセスできなくなる可能性があります。

9. **キューに追加**をクリックします。

   iLO によって、タスクがインストールキューの最後に追加されたことが通知されます。このイベントは iLO イベントログに記録されます。

   タスクの有効期限が、キューでそのタスクに先行する既存のタスクの開始時刻より前に切れる場合、iLO はタスクを保存できないことを通知します。インストールキューは、タスクの先入れ先出しリストです。既存のタスクの実行前に有効期限が切れるタスクを作成することはできません。

   リカバリセットをアップデートチェックボックスを選択した場合は、タスクが開始され、正常に完了した後に、コンポーネントがアップデートされます。

詳しくは

システムリカバリセット
メンテナンスウィンドウの追加
タスクをキューに入れるときに時間枠の詳細を入力する
インストールキューに追加できるコマンド
インストールキュー内のタスクの処理方法

インストールキューに追加できるコマンド

待機

インストールキューを停止し、構成された時間（秒）待機します。有効な値は 1～3600 秒です。

iLO をリセット

iLO をリセット（再起動）します。

このコマンドを実行しても構成が変更されることはありませんが、iLO ファームウェアへのアクティブな接続がすべて終了します。

タスクをキューに入れるときに時間枠の詳細を入力する

時間枠を指定してくださいが選択されているときは、以下の手順を使用してスケジュールを入力します。

前提条件

iLO の設定を構成する権限

手順

1. （**開始**ボックス内）をクリックします。

   カレンダーが表示されます。

2. 開始日時を選択し、**完了**をクリックします。

   選択した日時は**開始**ボックスに表示されます。

3. （**終了**ボックス内）をクリックします。

   カレンダーが表示されます。

4. 終了日時を選択し、**完了**をクリックします。

   この値によってタスクの有効期限（日付時刻）が設定されます。

選択した日時は**終了**ボックスに表示されます。

インストールキュー内のタスクの処理方法

タスクをインストールキューに追加するとき：

- キューの最後に追加されます。
- コマンドを追加した場合、キューに入れられた既存のタスクが終了した後、タスクが開始されます。
- コンポーネントを追加した場合、タスクは以下の後に開始されます。
  - キューに入れられた既存のタスクが終了した。
  - 選択されたコンポーネントタイプのインストールを開始するソフトウェアが保留中のインストールを検出した。

  インストールキューが空で、iLO がアップデートを開始できる場合、すぐにアップデートが開始されます。

  アップデートを開始できるソフトウェアについては、**iLO レポジトリ**ページと**インストールキュー**ページでコンポーネントの詳細を確認してください。
- 前にキューに入れられたタスクが開始または終了を待機している場合、新しいタスクは無期限に遅延する場合があります。たとえば、サーバー POST 中に UEFI BIOS が検出するまで待機している、キューに入れられたコンポーネントがあるとします。サーバーが再起動されない場合、キュー内のこのタスクに続くタスクは、無期限に保留されたままになります。
- タスクが、インストールキュー内で先行しているタスクの開始時刻より前に期限切れになった場合、iLO はタスクを保存しません。
- 指定された時間枠内にアップデートが開始されない場合、アップデートは有効期限切れになります。アップデートの有効期限が切れた場合は、タスクを削除して再作成するか、タスクを編集します。

詳しくは

iLO レポジトリの概要とコンポーネントの詳細の表示
インストールキューの表示

インストールキューのタスクの編集

前提条件

- インストールキューのタスクを編集するには、iLO 設定の構成権限が必要です。
- キューに入れられたアップデートが正常に完了した後に、システムリカバリセットの任意のアップデートを実行するには、リカバリセット権限が必要です。
- **リカバリセットをアップデート**機能を使用する場合、システムリカバリセットが存在し、アップデートするコンポーネントがこれに含まれている必要があります。
- 編集対象のタスクは**保留**ステータスです。

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**インストールキュー**タブをクリックします。
2. 編集対象のタスクの横にある✎をクリックします。

   iLO から、タスク情報をアップデートするよう求められます。

3. タスク名をアップデートするには、**タスク名**ボックスに新しい名前（最大 64 文字）を入力します。
4. **コンポーネント**ボックスまたは**コマンド**ボックスで値を選択します。
   - 元のタスクがコンポーネントのアップデートの場合、選択できるのは別のコンポーネントだけです。
   - 元のタスクがコマンドの場合、選択できるのは別のコマンドだけです。
5. **待機**コマンドを選択した場合、待機時間を**待機時間（秒）**ボックスに入力するか、アップデートします。

   有効な値は 1～3600 秒です。
6. （オプション）インストールのスケジュールを指定または編集するには、**スケジュールウィンドウをセット**チェックボックスを選択またはクリアします。
   a. **スケジュールウィンドウをセット**チェックボックスが選択されている場合は、スケジュールの定義に使用する方法を選択またはアップデートします。
      - **メンテナンスウィンドウを使用**（デフォルト）を選択し、**メンテナンスウィンドウ**ページで構成したメンテナンスウィンドウを選択します。

        メンテナンスウィンドウを追加するには、**新規**をクリックして**メンテナンスウィンドウ**ページに移動します。メンテナンスウィンドウを作成してから、この手順を再開します。
      - **時間枠を指定してください**を選択し、スケジュールをその場で入力します。

   b. 選択した方法によって、以下のいずれかを実行します。
      - **メンテナンスウィンドウを使用**が選択されている場合は、**メンテナンスウィンドウ**リストで値を選択または変更します。
      - **時間枠を指定してください**が選択されている場合は、スケジュールの詳細を追加またはアップデートします。
7. （オプション）手順 **4** で選択したコンポーネントのバージョンがシステムリカバリセットに存在する場合は、**リカバリセットをアップデート**チェックボックスを選択または選択解除します。

   このオプションが有効になっている場合、システムリカバリセットの既存のコンポーネントは、タスクが完了すると、選択したコンポーネントに置き換えられます。

   このオプションを選択すると、システムリカバリセット内のコンポーネントのバージョンの方が新しい場合でも、コンポーネントが置き換えられます。

   次の場合、このオプションは表示されません。
   - コマンドが選択されている。
   - システムリカバリセットがない。
   - 必要な権限がユーザーアカウントに割り当てられていない。
8. サーバーに TPM または TM が存在する場合は、TPM または TM の情報を保存するソフトウェアを一時停止またはバックアップしてから、**TPM の上書きを確認してください**チェックボックスを選択します。

   ドライブ暗号化ソフトウェアは、TPM または TM の情報を保存するソフトウェアの例です。

注意: ドライブ暗号化ソフトウェアを使用している場合は、ファームウェアのアップデートを開始する前に停止してください。この指示に従わない場合、ご使用のデータにアクセスできなくなる可能性があります。

9. **OK** をクリックします。

   iLO は、タスクがアップデートされたことを通知します。

   タスクの有効期限が、キューでそのタスクに先行するタスクの開始時刻より前に切れる場合、iLO はタスクを保存できないことを通知します。インストールキューは、タスクの先入れ先出しリストです。既存のタスクの実行前に有効期限が切れるタスクを作成することはできません。

   リカバリセットをアップデートチェックボックスを選択した場合は、タスクが開始され、正常に完了した後に、コンポーネントがアップデートされます。

詳しくは

システムリカバリセット
メンテナンスウィンドウの追加
タスクをキューに入れるときに時間枠の詳細を入力する
インストールキューに追加できるコマンド
インストールキュー内のタスクの処理方法

インストールキューからのタスクの削除

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**インストールキュー**タブをクリックします。
2. コンポーネントの削除アイコン🗑をクリックします。

   iLO が要求を確認するように求めます。
3. **はい、削除します**をクリックします。

   コンポーネントが削除されます。

インストールキューからのすべてのタスクの削除

前提条件

- iLO の設定を構成する権限
- コンポーネントがインストールセットに含まれていない。
- コンポーネントがキューに入れられたタスクの一部ではない。

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**インストールキュー**タブをクリックします。
2. **すべて削除**をクリックします。

iLO が要求を確認するように求めます。

3. **はい、削除します**をクリックします。

   タスクが削除されます。

インストールキューの表示

インストールキューページにはキューに入っている各タスクの概要情報が表示されます。個々のタスクをクリックすると、詳細情報が表示されます。現在の **iLO 日付/時間**の値は、ページの上部に表示されます。

手順

1. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**インストールキュー**タブをクリックします。
2. （オプション）詳細な情報を表示するには、個々のタスクをクリックします。

キューに入れられたタスクサマリーの詳細

状態

タスクのステータス。値には、以下のものがあります。

- **待機中** - コンポーネントタイプのアップデートを開始するソフトウェアがインストール要求を検出したときにタスクは実行されます。
- **進行中** - タスクは処理されています。
- **完了** - タスクが正常に完了しました。
- **キャンセル** - タスクがキャンセルされた、または期限切れのメンテナンスウィンドウに関連付けられています。
- **失効** - タスクの期限が切れています。このタスクがキューから削除されるまで、その後のタスクは実行されません。
- **例外** - タスクを完了できませんでした。このタスクがキューから削除されるまで、その後のタスクは実行されません。

名前

タスク名。

開始

タスクの開始日時（UTC）。タスクが他のタスクの完了を待機している場合、値は**前のタスクの実行後**になります。

完了、期限切れ、例外の状態のタスクには、N/A という値が表示されます。

期限切れ

タスクの有効期限（日付と時刻）（UTC）。有効期限の日付を設定しない場合、**なし**という値が表示されます。

個々のタスクの詳細

名前

タスク名。

コマンド

コマンドが選択されている場合、この値はコマンド名です。例：**待機**、**iLO リセット**。

コンポーネントが選択されている場合、**アップデートを適用**の値が表示されます。

コンポーネント名

iLO レポジトリのコンポーネントが選択されている場合は、コンポーネント名。

コンポーネント名のリンクをクリックすると、コンポーネントの詳細を iLO レポジトリに表示することができます。

ファイル名

iLO レポジトリのコンポーネントが選択されている場合は、コンポーネントのファイル名。

状態

タスクのステータス。表示される値は**保留中**、**進行中**、**完了**、**キャンセル**、**失効**、または**例外**です。

待機時間（秒）

タスクが**待機**コマンドの場合は、待機時間（秒）。

結果

タスクの結果（ある場合）。例：**タスクは正常に完了しました**、**アップデートはコンポーネント固有のエラーのために失敗しました。コンポーネントエラーを修正した後にアップデートを再試行してください。**

インストール元

選択したコンポーネントのアップデートを開始できるソフトウェア。例：**iLO**、**Smart Update Manager**、**Smart Update Tool**、**UEFI BIOS**。

メンテナンスウィンドウ

タスクがメンテナンスウィンドウ中に実行されるように構成されている場合のメンテナンスウィンドウ名。

開始時刻

タスクの開始日時（UTC）。

- 時間枠が指定されている場合は、開始時刻がリストされます。
- メンテナンスウィンドウが選択されている場合は、メンテナンスウィンドウの開始時刻がリストされます。
- 開始時刻が指定されておらず、タスクの状態が**完了**、**失効**、または**例外**の場合は、N/A の値が表示されます。
- 開始時刻が指定されておらず、タスクの状態が**進行中**または**保留中**の場合は、次のようになります。
  - タスクがキューの最初にある場合は、**関連するアップデータの確認の後、ただちに**の値が表示されます。
  - タスクがキューの最初にない場合は、**前のタスクの実行後**の値が表示されます。

失効

タスクの有効期限（日付と時刻）（UTC）。

メンテナンスウィンドウが選択されている場合は、メンテナンスウィンドウの終了時刻がリストされます。

リカバリセットをアップデートしますか?

この値が表示されるのは、コンポーネントが選択されている場合だけです。値が**はい**の場合、キューに入れられたコンポーネントは、タスクが開始され、正常に完了した後にシステムリカバリセット内のコンポーネントを置き換えます。

リカバリセット権限を持つユーザーによって作成されましたか?

この値が表示されるのは、コンポーネントが選択されている場合だけです。値が**はい**の場合、タスクはリカバリセット権限を持つユーザーによって作成されました。

キューに入れられたアップデートが正常に完了した後に、システムリカバリセットの任意のアップデートを実行するには、この権限が必要です。

ダウングレードポリシーが**ダウングレードには、'リカバリセット'の権限が必要です。**オプションに設定されている場合、この権限はファームウェアのダウングレードにも必要です。

iLO 連携の構成と使用

iLO 連携

iLO 連携では、iLO Web インターフェイスを使用して、1 つのシステムから複数のサーバーを管理できます。

iLO 連携が構成されている場合、iLO はマルチキャスト検出およびピアツーピア通信を使用して、iLO 連携グループ内のシステム間の通信を可能にします。

iLO 連携ページの 1 つに移動すると、Web インターフェイスを実行する iLO システムからそのピアへ、そしてそれらのピアから他のピアへ、選択した iLO 連携グループのすべてのデータが取得されるまでデータリクエストが送信されます。

iLO は次の機能をサポートします。

- グループのヘルスステータス - サーバーのヘルス情報とモデル情報を表示します。
- グループ仮想メディア - サーバーのグループからアクセスできる URL ベースのメディアに接続します。
- グループ電力制御 - サーバーのグループの電源ステータスを管理します。
- グループ消費電力上限 - サーバーのグループに消費電力上限を動的に設定します。
- グループファームウェアアップデート - サーバーのグループのファームウェアをアップデートします。
- グループライセンスのインストール - ライセンスキーを入力して、サーバーのグループでライセンス済みの iLO 機能を有効にします。
- グループ構成 - 複数の iLO システムに対する iLO 連携グループメンバーシップを追加します。

どのユーザーも iLO 連携ページの情報を表示できますが、次の機能を使用するにはライセンスが必要です。グループ仮想メディア、グループ電源制御、グループ消費電力上限、グループ構成、およびグループファームウェアアップデート。

iLO 連携の構成

iLO 連携機能を使用するための前提条件

手順

- **ネットワーク構成が、iLO 連携の要件を満たしている**。
- **iLO 連携グループに追加される各 iLO システムで、マルチキャストオプションが構成されている**。

  デフォルトのマルチキャストオプションの値を使用する場合、構成は不要です。
- **iLO 連携のグループメンバーシップが構成されている**。

  すべての iLO システムが、自動的に **DEFAULT** グループに追加されます。
- **iLO 連携のエンクロージャーサポート**が Onboard Administrator ソフトウェア（ProLiant サーバーブレードのみ）で構成されている。

この設定は、デフォルトで有効になっています。

iLO 連携のネットワーク要件

- （オプション）iLO 連携は、IPv4 と IPv6 の両方をサポートしています。有効な構成が両方のオプションにある場合、IPv6 ではなく IPv4 を使用するように iLO を構成できます。この設定を構成するには、**IPv6 設定**ページの **iLO クライアントアプリケーションは IPv6 を最初に使用**オプションを無効にします。
- 複数の場所にある iLO システムを管理する場合は、マルチキャストトラフィックを転送するようにネットワークを設定します。
- ネットワーク内のスイッチにマルチキャストトラフィックを有効または無効にするためのオプションが含まれている場合は、有効になっていることを確認します。この構成は、iLO 連携と他の Hewlett Packard Enterprise 製品が、ネットワーク上で iLO システムを検出するために必要です。
- レイヤー 3 スイッチで分断されている iLO システムの場合は、ネットワーク間で SSDP マルチキャストトラフィックを転送するようにスイッチを構成する必要があります。
- iLO システム間のマルチキャストトラフィック（UDP ポート 1900）と直接 HTTP（TCP のデフォルトポート 80）通信を許可するようにネットワークを構成します。
- 複数の VLAN を持つネットワークの場合、VLAN 間でマルチキャストトラフィックを許可するようにスイッチを構成します。
- レイヤー 3 スイッチを使用したネットワーク：
  - IPv4 ネットワークの場合：スイッチの PIM を有効にし、PIM デンスモードに設定します。
  - IPv6 ネットワークの場合：スイッチを MLD スヌーピングに設定します。
- BladeSystem c-Class エンクロージャー内のサーバーブレードを iLO 連携で使用する場合、Onboard Administrator Web インターフェイスで、**エンクロージャー iLO 連携サポートを有効**設定を有効にする必要があります。この設定は、デフォルトで有効になっています。

詳しくは

IPv6 設定の構成
エンクロージャー iLO 連携サポートの設定

iLO 連携マルチキャストオプションの構成

以下の手順を実行して、iLO 連携グループに追加するシステムのマルチキャストオプションを構成します。デフォルト値を使用する場合は、構成の必要はありません。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで **iLO 連携**をクリックします。

   セットアップタブが表示されます。
2. **iLO 連携管理**オプションを有効または無効にします。
3. **マルチキャスト検出**オプションを有効または無効にします。
4. **マルチキャストアナウンスメント間隔（秒/分）**の値を入力します。

5. **IPv6 マルチキャストスコープ**の値を選択します。

   マルチキャスト検出が正しく機能するようにするため、**IPv6 マルチキャストスコープ**に、同じグループ内のすべての iLO システムで同じ値を使用していることを確認してください。

6. **マルチキャスト Time To Live（TTL）**の値を入力します。

   マルチキャスト検出が正しく機能するようにするため、**マルチキャスト Time To Live （TTL）**に、同じグループ内のすべての iLO システムで同じ値を使用していることを確認してください。

7. **適用**をクリックします。

   ネットワークが変更され、このページで行った変更は、次のマルチキャスト通知後に有効となります。

マルチキャストオプション

iLO 連携管理

iLO 連携機能を有効または無効にします。デフォルト設定は、**有効**です。**無効**を選択すると、ローカル iLO システムに対する iLO 連携機能が無効になります。

マルチキャスト検出

マルチキャスト検出を有効または無効にします。デフォルト設定は、**有効**です。**無効**を選択すると、ローカル iLO システムに対する iLO 連携機能が無効になります。

Synergy コンピュートモジュールでは、マルチキャスト検出を無効にすることはできません。Synergy コンピュートモジュールで、ネットワーク上のマルチキャストトラフィックの影響を制限するには、**IPv6 マルチキャストスコープ**および**マルチキャスト Time To Live（TTL）**の設定を調整します。

マルチキャストアナウンスメント間隔（秒/分）

この値は、iLO システムがネットワーク上で通知する頻度を設定します。各マルチキャスト通知は約 300 バイトです。30 秒から 30 分の値を選択します。デフォルト値は 10 分です。**無効**を選択すると、ローカル iLO システムに対する iLO 連携機能が無効になります。

指定可能な値は、以下のとおりです。

- 30、60、120 秒
- 5、10、15、30 分
- 無効

IPv6 マルチキャストスコープ

マルチキャストトラフィックを送受信するネットワークの規模です。有効な値は、**リンク**、**サイト**、および**組織**です。デフォルト値は**サイト**です。

マルチキャスト Time To Live (TTL)

マルチキャスト検出が停止する前に通過できるスイッチの数を指定します。有効な値は 1～255 です。デフォルト値は 5 です。

iLO 連携グループ

iLO 連携グループの特性

- すべての iLO システムは **DEFAULT** グループに自動的に追加され、このグループにはそれぞれのグループメンバーのログイン権限が認められています。**DEFAULT** グループメンバーシップは編集することも削除することもできます。
- iLO 連携グループは、一部共通することも、複数のラックおよびデータセンターにまたがることもできます。また、管理ドメインの作成に使用することもできます。
- 各 iLO システムは最大で 10 の iLO 連携グループのメンバーになることができます。
- グループに指定できる iLO システムの数に制限はありません。
- グループメンバーシップを構成するには、iLO 設定権限が必要です。
- iLO Web インターフェイスを使用して、ローカル iLO システムまたは iLO システムのグループのグループメンバーシップを構成することができます。
- RIBCL XML スクリプトを使用してグループメンバーシップを表示および構成できます。

  詳しくは、iLO 連携ユーザーガイドを参照してください。
- iLO RESTful API を使用してグループメンバーシップを構成できます。

  詳しくは、iLO 連携ユーザーガイドを参照してください。
- Hewlett Packard Enterprise は、同じ iLO 連携グループ内の iLO システムには、同じバージョンの iLO ファームウェアをインストールすることをお勧めします。

ローカル iLO システムに対する iLO 連携グループメンバーシップ

ローカル iLO システムにグループメンバーシップを構成する場合、グループのメンバーがローカルの管理対象サーバーを構成するために所有する権限を指定する必要があります。

たとえば、ローカル iLO システムを **group1** に追加し、「仮想電源およびリセット」権限を割り当てた場合、**group1** の他の iLO システムのユーザーは管理対象サーバーの電力状態を変更できます。

ローカル iLO システムが「仮想電源およびリセット」権限を **group1** に認めていない場合は、**group1** の他の iLO システムのユーザーはグループの電力制御機能を使用して管理対象サーバーの電力状態を変更することはできません。

ローカル iLO システム上で iLO セキュリティを無効にするようシステムメンテナンススイッチが設定されている場合、**group1** の他の iLO システムのユーザーは、割り当てられたグループ権限とは無関係に、管理対象サーバーの状態を変更できます。

ローカル iLO システムに対するグループメンバーシップは、**iLO 連携**ページの**セットアップ**タブで構成します。

ローカル iLO システムに対して、以下のタスクを実行できます。

- グループメンバーシップの表示。
- グループメンバーシップの追加と編集。
- グループメンバーシップの削除。

詳しくは

iLO 連携グループメンバーシップを管理する（ローカル iLO システム）

iLO システムのセットに対する iLO 連携グループメンバーシップ

複数の iLO システムに対するグループメンバーシップを一度に追加する場合、グループのメンバーがグループの他のメンバーを構成するために所有する権限を指定する必要があります。

たとえば、**DEFAULT** グループに基づいて **group2** を構成し、「仮想電源およびリセット」権限を割り当てた場合、**group2** の iLO システムのユーザーはグループ内のすべてのサーバーの電力状態を変更できます。

グループ構成ページで、複数の iLO システムに対してグループメンバーシップを追加できます。

iLO システムのグループに対して、以下のタスクを実行できます。

- 既存のグループとメンバーは同じだが、権限が異なるグループを作成します。
- iLO 連携フィルターを使用して選択したメンバーを含むグループを作成します。

詳しくは

iLO 連携グループメンバーシップの追加（複数の iLO システム）

iLO 連携グループの権限

システムがグループに追加されると、グループに以下の権限を付与することができます。

- **ログイン** - グループのメンバーは、iLO にログインできます。
- **仮想電源およびリセット** - グループメンバーは、ホストシステムの電源再投入やリセットを実行できます。これらの操作はシステムの可用性を中断します。
- **仮想メディア** - グループメンバーは、管理対象サーバーで URL ベースの仮想メディアを使用できます。
- **iLO 設定を構成** - グループのメンバーは、iLO 設定を構成し、リモートでファームウェアをアップデートすることができます。

さらに、グループには以下の権限も付与できます。ただし、現在の iLO 連携機能セットでは、それらを必要とするアクションをサポートしていません。

- **ユーザーアカウント管理** - ユーザーアカウント管理権限を必要とするアクションをサポートします。
- **リモートコンソール** - リモートコンソール権限を必要とするアクションをサポートします。
- **ホスト BIOS** - ホスト BIOS 権限を必要とするアクションをサポートします。
- **ホスト NIC** - ホスト NIC 権限を必要とするアクションをサポートします。
- **ホストストレージ** - ホストストレージ権限を必要とするアクションをサポートします。
- **リカバリセット** - リカバリセット権限を必要とするアクションをサポートします。

iLO 連携グループメンバーシップを管理する（ローカル iLO システム）

iLO 連携グループメンバーシップの追加

前提条件

- iLO の設定を構成する権限
- **アクセス設定**ページの**最小パスワード長**設定が 31 文字以下に設定されている。

手順

1. ナビゲーションツリーで **iLO 連携**をクリックします。

セットアップタブが表示されます。

2. **グループへの参加**をクリックします。
3. **グループ名**を入力します。

   この値は 1～31 文字の長さです。
4. **グループキー**および**グループキーの確認**の値を入力します。

   グループキー（パスワード）は、設定されている最小パスワード長～31 文字で指定できます。

   ローカル iLO システムで**パスワードの複雑さ**が有効になっている場合、グループキーがパスワードの複雑さの要件を満たしている必要があります。
5. グループに割り当てる**権限**を選択します。

   ローカル iLO システムによりグループに付与される権限は、管理対象サーバーで、グループ内の他の iLO システムのユーザーが実行できるタスクを制御します。
6. **グループへの参加**をクリックします。

   既存のグループの名前とキーを入力した場合、ローカル iLO システムがそのグループに追加されます。

   存在しないグループの名前とキーを入力した場合、グループが作成され、ローカル iLO システムがそのグループに追加されます。

詳しくは

ローカル iLO システムに対する iLO 連携グループメンバーシップ
iLO 連携グループの権限
iLO 連携グループの特性

iLO 連携グループメンバーシップの編集

前提条件

- iLO の設定を構成する権限
- グループキーを編集する場合、**アクセス設定**ページの**最小パスワード長**設定が 31 文字以下に設定されている。

手順

1. ナビゲーションツリーで **iLO 連携**をクリックします。

   セットアップタブに、ローカル iLO システムの既存のグループメンバーシップが表示されます。
2. グループメンバーシップを選択して、**編集**をクリックします。
3. グループ名を変更するには、**グループ名**ボックスに新しい名前を入力します。

   グループ名は、1～31 文字で指定できます。
4. グループキーを変更するには、**グループキーの変更**チェックボックスを選択して、**グループキー**および**グループキーの確認**ボックスに新しい値を入力します。

   グループキーは、設定されている最小パスワード長～31 文字で指定できます。

   ローカル iLO システムで**パスワードの複雑さ**が有効になっている場合、グループキーがパスワードの複雑さの要件を満たしている必要があります。
5. アップデートする権限のチェックボックスをオンまたはオフにします。

ローカル iLO システムによりグループに付与される権限は、管理対象サーバーで、グループ内の他の iLO システムのユーザーが実行できるタスクを制御します。

6. **グループのアップデート**をクリックします。
7. グループ名またはグループキーをアップデートした場合は、それらを他のシステムの影響を受けるグループでアップデートします。

詳しくは

ローカル iLO システムに対する iLO 連携グループメンバーシップ
iLO 連携グループの権限
iLO 連携グループの特性

ローカル iLO システムからのグループメンバーシップの削除

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで **iLO 連携**をクリックします。

   セットアップタブに、ローカル iLO システムのグループメンバーシップが表示されます。
2. 削除するグループメンバーシップの横にあるチェックボックスを選択します。
3. **削除**をクリックします。
4. 要求を確認するメッセージが表示されたら、**はい、削除します**をクリックします。

iLO 連携グループメンバーシップの表示（ローカル iLO システム）

手順

ナビゲーションツリーで **iLO 連携**をクリックします。

この iLO のグループメンバーシップテーブルには、ローカル iLO システムを含む各グループの名前と、ローカル iLO システムによってそのグループに与えられている権限が示されます。割り当てられた権限がチェックマークのアイコンで表示され、割り当てられていない権限が X アイコンで表示されます。

詳しくは

iLO 連携グループの権限

iLO 連携グループメンバーシップの追加（複数の iLO システム）

既存のグループに基づくグループの追加

この手順を使用して、既存のグループと同じメンバーで構成されるグループを作成します。たとえば、DEFAULT グループとシステムは同じだが権限が異なるグループを作成できます。

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- 少なくとも 1 つの iLO 連携グループが存在する。

手順

1. ナビゲーションツリーで **iLO 連携**をクリックして、**グループ構成**タブをクリックします。
2. **選択されたグループ**メニューからグループを選択します。

   選択したグループ内のすべてのシステムが、作成したグループに追加されます。
3. **影響を受けるシステム上にグループを作成**をクリックします。

   グループの作成インターフェイスが開きます。
4. **グループ名**を入力します。

   この値は 1～31 文字の長さです。

   存在するグループ名を入力すると、iLO から一意のグループ名の入力が求められます。
5. **グループキー**および**グループキーの確認**の値を入力します。

   グループキー（パスワード）は、設定されている最小パスワード長～31 文字で指定できます。

   既存のグループ内のシステムで**パスワードの複雑さ**が有効になっており、グループキーがパスワードの複雑さの要件を満たしていない場合、それらのシステムは新しいグループに追加できません。
6. （オプション）管理するリモートシステム上で、ユーザーアカウントの**ログイン名**および**パスワード**を入力します。

   選択したグループに、管理するリモートシステム上の iLO の設定を構成する権限が割り当てられていない場合は、この情報が必要です。

   複数のリモートシステムの認証情報を入力するには、ログイン名とパスワードが同じユーザーアカウントを各システムで作成します。
7. グループに割り当てる**権限**を選択します。

   使用できるすべての権限を選択するには、**すべてを選択**チェックボックスをクリックします。
8. **グループの作成**をクリックします。

   グループの作成プロセスには、数分かかります。グループは、**マルチキャストアナウンスメント間隔**に構成された時間内に、完全に実装されます。

詳しくは

iLO システムのセットに対する iLO 連携グループメンバーシップ
iLO 連携グループの権限
iLO 連携グループの特性
選択されたグループのリスト

サーバーのフィルターされたリストからのグループの作成

この手順を使用して、サーバーのフィルターされたリストからグループを作成します。たとえば、特定バージョンの iLO ファームウェアを備えているすべてのサーバーを含むグループを作成する場合があります。

サーバーのフィルターされたリストからグループを作成すると、グループ作成プロセスの間、**影響するシステム**リスト内のサーバーのみがグループに含まれます。グループが作成された後にフィルターの条件に適合するサーバーは、グループに追加されません。

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- 少なくとも 1 つの iLO 連携グループが存在する。

手順

1. **iLO 連携**ページでフィルターを使用して、システムのセットを作成します。
2. ナビゲーションツリーで **iLO 連携**をクリックして、**グループ構成**タブをクリックします。

   アクティブなフィルターは**影響するシステム**リストの上に一覧表示されます。
3. **選択されたグループ**メニューからグループを選択します。

   選択したグループ内の、選択したフィルター条件に適合するすべてのシステムが、新しいグループに追加されます。
4. **影響を受けるシステム上にグループを作成**をクリックします。
5. **グループ名**を入力します。

   この値は 1～31 文字の長さです。

   存在するグループ名を入力すると、iLO から一意のグループ名の入力が求められます。
6. **グループキー**および**グループキーの確認**の値を入力します。

   グループキー（パスワード）は、設定されている最小パスワード長～31 文字で指定できます。

   フィルターされたリスト内に、**パスワードの複雑さ**が有効になっているシステムがあり、グループキーがパスワードの複雑さの要件を満たしていない場合、それらのシステムは新しいグループに追加できません。
7. （オプション）管理するリモートシステム上で、ユーザーアカウントの**ログイン名**および**パスワード**を入力します。

   選択したグループに、管理するリモートシステム上の iLO の設定を構成する権限が割り当てられていない場合は、この情報が必要です。

   複数のリモートシステムの認証情報を入力するには、ログイン名とパスワードが同じユーザーアカウントを各システムで作成します。
8. グループに割り当てる**権限**を選択します。

   使用できるすべての権限を選択するには、**すべてを選択**チェックボックスをクリックします。
9. **グループの作成**をクリックして設定を保存します。

   グループの作成プロセスには、数分かかります。グループは、**マルチキャストアナウンスメント間隔**に構成された時間内に、完全に実装されます。

詳しくは

iLO システムのセットに対する iLO 連携グループメンバーシップ
iLO 連携グループの権限

iLO 連携グループの特性
選択されたグループのリスト

グループメンバーシップの変更によって影響を受けるサーバー

グループ構成ページの**影響するシステム**セクションには、グループメンバーシップの変更によって影響を受けるサーバーについて、次の詳細が表示されます。

- **サーバー名** - ホストオペレーティングシステムで定義されたサーバー名。
- **サーバー電源** - サーバー電源の状態（**オン**または**オフ**）。
- **UID インジケーター** - UID LED の状態。UID LED を使用すると、特に高密度ラック環境でサーバーを特定し、その位置を見つけることができます。状態には、**UID オン**、**UID オフ**、および **UID 点滅**があります。
- **iLO ホスト名** - iLO サブシステムに割り当てられた完全修飾ネットワーク名。サーバーの iLO Web インターフェイスを開くには、**iLO ホスト名**列のリンクをクリックします。
- **IP アドレス** - iLO サブシステムのネットワーク IP アドレス。サーバーの iLO Web インターフェイスを開くには、**IP アドレス**列のリンクをクリックします。

次へまたは**前へ**（使用可能な場合）をクリックして、リストのサーバーをさらに表示します。

詳しくは

iLO 連携情報を CSV ファイルにエクスポートする方法

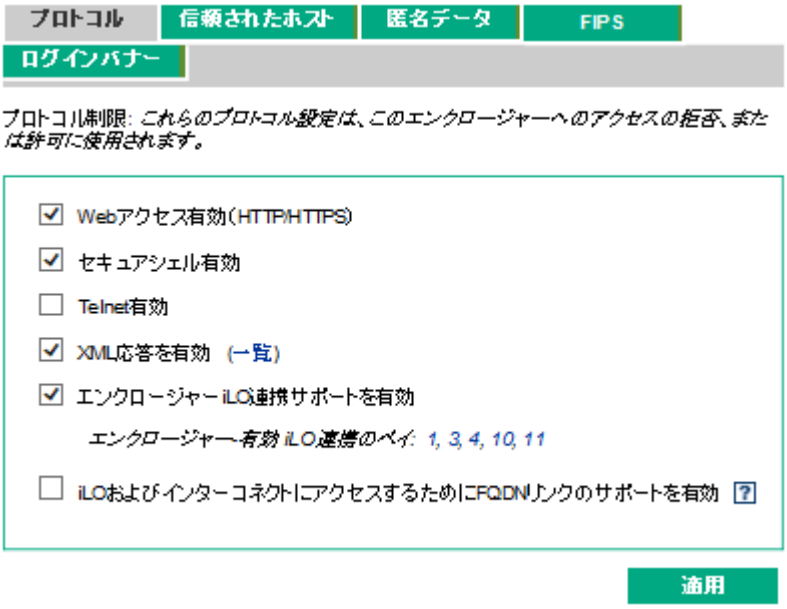
エンクロージャー iLO 連携サポートの設定

iLO 連携で BladeSystem c-Class エンクロージャー内のサーバーブレードを使用する場合、Onboard Administrator ソフトウェアで、**エンクロージャー iLO 連携サポート**オプションを有効にする必要があります。この設定は、エンクロージャー内のサーバーブレード間でピアツーピアの通信を可能にするために必要です。**エンクロージャー iLO 連携サポートを有効**オプションは、デフォルトで有効です。

手順

1. Onboard Administrator の Web インターフェイス（https://<OA のホスト名または IP アドレス>）にログインします。
2. ナビゲーションツリーで、**エンクロージャー情報** > **エンクロージャー設定** > **ネットワークアクセス**を選択します。

   プロトコルタブが表示されます。
3. **エンクロージャーの iLO 連携サポートを有効**チェックボックスを選択し、**適用**をクリックします。



CLI を使用して、**エンクロージャー iLO 連携サポートを有効**オプションを有効または無効にすることもできます。オプションを有効にするには、`ENABLE ENCLOSURE_ILO_FEDERATION_SUPPORT` を入力します。オプションを無効にするには、`DISABLE ENCLOSURE_ILO_FEDERATION_SUPPORT` を入力します。詳しくは、Onboard Administrator CLI ユーザーガイドを参照してください。

iLO 連携に関するサーバーブレードサポートの確認

手順

1. Onboard Administrator の Web インターフェイス（https://<OA のホスト名または IP アドレス>）にログインします。
2. ナビゲーションツリーで**デバイスベイ** > **<デバイス名>** > **iLO** を選択します。
3. **iLO 連携機能**設定が**はい**の値に設定されていることを確認します。

iLO 連携機能の使用

選択されたグループのリスト

セットアップを除くすべての iLO 連携のページには、**選択されたグループ**のリストがあります。

選択されたグループリストからグループを選択する場合：

- **グループ仮想メディア**、**グループ電力**、**グループファームウェアアップデート**、**グループライセンス**、および**グループ構成**ページでの変更の影響を受けるサーバーは、**影響するシステム**の表に表示されます。
- iLO 連携ページに表示される情報は、選択したグループ内のすべてのサーバーに適用されます。
- iLO 連携ページで加えた変更は、選択したグループ内のすべてのサーバーに適用されます。
- 選択されたグループは cookie に保存され、iLO からログアウトする場合でも、維持されます。

グループを選択した後、サーバーの情報を表示するため、またはグループ内のサーバーのサブセットに対して操作を実行するために、リスト内のサーバーをフィルター処理できます。

選択されたグループのリストのフィルター

サーバーのリストを選別する場合：

- iLO 連携ページに表示される情報は、フィルター条件に適合する、選択したグループ内のすべてのサーバーに適用されます。
- iLO 連携ページで加えた変更は、フィルター条件に適合する、選択したグループ内のすべてのサーバーに適用されます。
- フィルターの設定は cookie に保存され、iLO からログアウトする場合でも、維持されます。
- X アイコンまたはフィルター名をクリックすることで、フィルターを削除できます。

選択されたグループのリストのフィルター条件

次の条件を使用して、グループ内のサーバーをフィルタリングすることができます。

- **ヘルスステータス** - ヘルスステータスのリンクをクリックして、特定のヘルスステータスを持つサーバーを選択します。
- **モデル** - サーバーのモデル番号リンクをクリックして、選択したモデルと一致するサーバーを選択します。
- **サーバー名** - 個々のサーバーによってフィルタリングするには、サーバー名をクリックします。
- **ファームウェア情報** - ファームウェアのバージョンまたはフラッシュステータスをクリックし、選択したファームウェアのバージョンまたはステータスに一致するサーバーを選択します。
- **TPM または TM オプション ROM 計測** - オプション ROM 計測ステータスをクリックして、選択したオプション ROM 計測のステータスに一致するサーバーを含めるか、除外します。
- **ライセンスの使用** - ライセンスキーに関連するエラーメッセージが表示される場合は、ライセンスキーをクリックして、そのライセンスキーを使用しているサーバーを選択します。
- **ライセンスタイプ** - ライセンスタイプをクリックして、選択したライセンスタイプがインストールされているサーバーを選択します。
- **ライセンスステータス** - ライセンスステータスをクリックして、選択したステータスに一致するライセンスがインストールされているサーバーを選択します。

iLO 連携情報を CSV ファイルにエクスポートする方法

以下の **iLO 連携**ページで、情報を CSV ファイルにエクスポートできます。

- **マルチシステムビュー** - **クリティカルまたは劣化のステータスのシステム**リストをエクスポートします。
- **マルチシステムマップ** - iLO ピアリストをエクスポートします。
- **グループ仮想メディア** - **影響を受けるシステム**リストをエクスポートします。
- **グループ電力** - **影響を受けるシステム**リストをエクスポートします。
- **グループファームウェアアップデート** - **影響を受けるシステム**リストをエクスポートします。

- **グループライセンス** - **影響を受けるシステム**リストをエクスポートします。
- **グループの構成** - **影響を受けるシステム**リストをエクスポートします。

前提条件

iLO の構成とネットワーク構成が、iLO 連携機能を使用するための前提条件を満たしている。

手順

1. ファイルエクスポート機能をサポートするページに移動します。
2. **表を CSV 形式で表示**をクリックします。
3. **CSV アウトプット**ウィンドウで、**保存**をクリックしてから、ブラウザーのプロンプトに従ってファイルを保存または開きます。

   サーバーが複数のページにまたがってリストされている場合、CSV ファイルには iLO の Web インターフェイスページに現在表示されているサーバーだけが含まれます。

   クエリのエラーが発生した場合、クエリに応答しなかったシステムは、iLO の Web インターフェイスページおよび CSV ファイルから除外されます。

詳しくは

iLO 連携機能を使用するための前提条件

iLO 連携マルチシステムビュー

マルチシステムビューページは、iLO 連携グループ内のサーバーモデル、サーバーのヘルス、およびクリティカルおよび劣化したサーバーに関する概要を提供します。

サーバーヘルスおよびモデル情報の表示

前提条件

iLO の構成とネットワーク構成が、iLO 連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーで **iLO 連携**をクリックして、**マルチシステムビュー**タブをクリックします。
2. **選択されたグループ**メニューからグループを選択します。
3. （オプション）サーバーのリストをフィルタリングするには、ヘルスステータス、サーバーモデル、またはサーバー名のリンクをクリックします。

詳しくは

iLO 連携機能を使用するための前提条件

サーバーヘルスおよびモデルの詳細

- **ヘルス** - 表示された各ヘルスステータスにあるサーバーの数。一覧表示された各ヘルスステータス内のサーバーの総数の%も表示されます。
- **モデル** - モデル番号でグループ化したサーバーのリスト。各モデル番号に対するサーバー総数の割合（%）も表示されます。
- **クリティカルおよび劣化システム** - ステータスがクリティカルまたは劣化であるサーバーのリスト。

詳しくは

サブシステムおよびデバイスステータスの値

クリティカルおよび劣化のステータスを持つサーバーの表示

前提条件

iLO の構成とネットワーク構成が、iLO 連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーで **iLO 連携**をクリックして、**マルチシステムビュー**タブをクリックします。
2. **選択されたグループ**メニューからグループを選択します。
3. （オプション）サーバーのリストをフィルタリングするには、ヘルスステータス、サーバーモデル、またはサーバー名のリンクをクリックします。
4. **次へ**または**前へ**（使用できる場合）をクリックして、**クリティカルおよび劣化システム**リストのサーバーをさらに表示します。

詳しくは

iLO 連携機能を使用するための前提条件

クリティカルおよび劣化のサーバーステータスの詳細

- **サーバー名** - ホストオペレーティングシステムで定義されたサーバー名。
- **システムヘルス** - サーバーのヘルスステータス。
- **サーバーの電源** - サーバーの電源ステータス（**オン**または**オフ**）。
- **UID インジケーター** - サーバー UID LED の状態。UID LED を使用すると、特に高密度ラック環境でサーバーを特定し、その位置を見つけることができます。状態には、**UID オン**、**UID オフ**、および **UID 点滅**があります。
- **システム ROM** - インストールされているシステム ROM バージョン。
- **iLO ホスト名** - iLO サブシステムに割り当てられた完全修飾ネットワーク名。サーバーの iLO Web インターフェイスを開くには、**iLO ホスト名**列のリンクをクリックします。
- **IP アドレス** - iLO サブシステムのネットワーク IP アドレス。サーバーの iLO Web インターフェイスを開くには、**IP アドレス**列のリンクをクリックします。

詳しくは

iLO 連携情報を CSV ファイルにエクスポートする方法
サブシステムおよびデバイスステータスの値

iLO 連携マルチシステムマップの表示

マルチシステムマップページには、ローカル iLO システムのピアに関する情報が表示されます。ローカル iLO システムはマルチキャスト検出を使用してそのピアを識別します。

iLO 連携ページの 1 つに移動すると、Web インターフェイスを実行する iLO システムからそのピアへ、そしてそれらのピアから他のピアへ、選択したグループのすべてのデータが取得されるまでデータリクエストが送信されます。

前提条件

iLO の構成とネットワーク構成が、iLO 連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーで **iLO 連携**をクリックして、**マルチシステムマップ**タブをクリックします。
2. **選択されたグループ**メニューからグループを選択します。

詳しくは

iLO 連携機能を使用するための前提条件

iLO ピアの詳細

- **#** - ピア番号。
- **iLO UUID** - iLO システムの UPnP UUID。
- **最後の参照** - サーバーからの前回の通信のタイムスタンプ。
- **最後のエラー** - 表示されているピアとローカルの iLO システムの間での最新の通信エラーの説明。
- **問い合わせ時間**（秒）- タイムアウトが発生した場合、この値を使用して、迅速に応答していないシステムを識別できます。この値は、最新のクエリに適用されます。
- **ノードカウント** - エラーが発生した場合、この値は、不足している可能性があるデータの量を示していることがあります。値がゼロであることは、直前のクエリがタイムアウトしたことを示します。この値は、最新のクエリに適用されます。
- **URL** - 表示されているピアの iLO Web インターフェイスを起動するための URL。
- **IP** - ピアの IP アドレス。

詳しくは

iLO 連携情報を CSV ファイルにエクスポートする方法

iLO 連携グループ仮想メディア

グループ仮想メディアを使用すると、サーバーのグループからアクセスできる URL ベースのメディアに接続できます。

- URL ベースの仮想メディアは、1.44 MB のフロッピーディスクイメージ（IMG）および CD/DVD-ROM イメージ（ISO）のみをサポートします。イメージは、グループ化された iLO システムと同じネットワーク上の Web サーバーに存在する必要があります。
- 同時に 1 種類のメディアしかグループに接続できません。
- URL ベースのメディアの表示、接続、取り出しや、CD/DVD-ROM ディスクイメージからの起動ができます。URL ベースのメディアを使用する場合は、フロッピーディスクや CD/DVD-ROM のディスクイメージを Web サーバーに保存し、URL を使用してそのディスクイメージに接続します。iLO では HTTP または HTTPS 形式の URL を使用できます。iLO は FTP をサポートしていません。
- 仮想メディア機能を使用する前に、仮想メディアオペレーティングシステムに関する注意事項を確認してください。

詳しくは

仮想メディアを使用するためのオペレーティングシステム要件

グループの URL ベースの仮想メディアの接続

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- 選択した iLO 連携グループの各メンバーが、仮想メディア権限をグループに認めている。
- iLO の構成とネットワーク構成が、iLO 連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーで **iLO 連携**をクリックして、**グループ仮想メディア**タブをクリックします。
2. **選択されたグループ**メニューからグループを選択します。

   接続する URL ベースのメディアは、選択したグループ内のすべてのシステムで利用可能になります。
3. **仮想フロッピーに接続**セクション（IMG ファイル）または **CD/DVD-ROM を接続**セクション（ISO ファイル）の**仮想メディア URL** ボックスにディスクイメージの URL を入力します。
4. 次のサーバー再起動時にのみこのディスクイメージからグループ内のサーバーを起動する場合は、**次回リセット時に起動**チェックボックスを選択します。

   イメージは 2 番目のサーバー再起動時に自動的に取り出されるので、サーバーは一度しかこのイメージから起動しません。

   このチェックボックスを選択しない場合、イメージは手動で取り出すまで接続されたまま残ります。また、サーバーは、システムブートオプションがそのように設定されている場合、以後のすべてのサーバーリセットでイメージから起動します。

   次回のリセット時にブートチェックボックスを有効にしているときにグループ内のサーバーが POST を実行していると、エラーが発生します。POST 中はサーバーブート順序を変更できません。POST が終了するのを待ってから、再試行してください。
5. 仮想フロッピーデバイスのみ：読み取り専用パーミッションを持つ仮想メディアデバイスを接続する場合、**読み取り専用**チェックボックスを選択します。

   読み取り専用チェックボックスはデフォルトで有効になっています。
6. **メディアの挿入**をクリックします。

   iLO はコマンドの結果を表示します。

詳しくは

iLO 連携機能を使用するための前提条件

グループの URL ベースの仮想メディアのステータス表示

前提条件

iLO の構成とネットワーク構成が、iLO 連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーで **iLO 連携**をクリックして、**グループ仮想メディア**タブをクリックします。
2. （オプション）表示される情報をフィルタリングするには、**読み取り専用ステータス**あるいは**イメージ URL** いずれかのリンクをクリックします。

詳しくは

iLO 連携機能を使用するための前提条件

URL ベースの仮想メディアの詳細

URL ベースの仮想メディアを接続すると、以下のセクションに詳細が表示されます。

仮想フロッピー/USB キー/仮想フォルダーステータス

- **挿入されたメディア** - 接続されている仮想メディアの種類。URL ベースのメディアが接続されている場合、**スクリプトメディア**と表示されます。
- **イメージが接続されました** - 仮想メディアデバイスが接続されているかどうかを示します。
- **読み取り専用ステータス** - 仮想メディアデバイスが**読み取り専用**と**読み取り/書き込み**のどちらのアクセス許可で接続されているかを示します。
- **イメージ URL** - 接続されている URL ベースのメディアをポイントする URL。

仮想 CD/DVD-ROM ステータス

- **挿入されたメディア** - 接続されている仮想メディアの種類。URL ベースのメディアが接続されている場合、**スクリプトメディア**と表示されます。
- **イメージが接続されました** - 仮想メディアデバイスが接続されているかどうかを示します。
- **イメージ URL** - 接続されている URL ベースのメディアをポイントする URL。

URL ベースの仮想メディアデバイスの取り出し

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- 選択した iLO 連携グループの各メンバーが、仮想メディア権限をグループに認めている。
- iLO の構成とネットワーク構成が、iLO 連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーで **iLO 連携**をクリックして、**グループ仮想メディア**タブをクリックします。
2. **選択されたグループ**メニューからグループを選択します。

   取り出す URL ベースの仮想メディアデバイスは、選択したグループ内のすべてのシステムから切断されます。
3. **仮想フロッピーステータス**セクションまたは**仮想 CD/DVD-ROM ステータス**セクションの**メディアの取り出し**をクリックします。

詳しくは

iLO 連携機能を使用するための前提条件

グループ仮想メディアの操作の影響を受けるサーバー

影響するシステムセクションには、グループ仮想メディアの操作を開始すると影響を受けるサーバーについて、次の詳細が表示されます。

- **サーバー名** - ホストオペレーティングシステムで定義されたサーバー名。
- **サーバー電力** - サーバー電力の状態（**オン**または**オフ**）。
- **UID インジケーター** - UID LED の状態。UID LED を使用すると、特に高密度ラック環境でサーバーを特定し、その位置を見つけることができます。状態には、**UID オン**、**UID オフ**、および **UID 点滅**があります。
- **iLO ホスト名** - iLO サブシステムに割り当てられた完全修飾ネットワーク名。サーバーの iLO Web インターフェイスを開くには、**iLO ホスト名**列のリンクをクリックします。
- **IP アドレス** - iLO サブシステムのネットワーク IP アドレス。サーバーの iLO Web インターフェイスを開くには、**IP アドレス**列のリンクをクリックします。

次へまたは**前へ**（使用可能な場合）をクリックして、リストのサーバーをさらに表示します。

詳しくは

iLO 連携情報を CSV ファイルにエクスポートする方法

iLO 連携グループ電力

グループ電力機能を使用すると、iLO Web インターフェイスを実行しているシステムから複数のサーバーの電力を管理できます。この機能を使用して、以下を行います。

- **オン**または**リセット**状態にあるサーバーのグループに対して、電源を切る、リセットする、または電源再投入を行う。
- **オフ**状態にあるサーバーのグループに対して電源を入れる。
- **グループ電力**ページの**仮想電源ボタン**セクションでボタンをクリックすると影響を受けるサーバーのリストを表示する。

サーバーグループの電力状態の変更

グループ電力ページの**仮想電源ボタン**セクションには、グループ内のサーバーの現在の電源状態をまとめています。概要情報として、**オン**、**オフ**、または**リセット**状態のサーバーの合計数が含まれます。 **システム電源**概要は、ページが初めて開かれるときのサーバー電源の状態を示します。**システム電源**情報をアップデートするには、ブラウザーの更新機能を使用します。

前提条件

- 仮想電源およびリセット権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- 選択した iLO 連携グループの各メンバーが、仮想電源およびリセット権限をグループに認めている。
- iLO の構成とネットワーク構成が、iLO 連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーで **iLO 連携**をクリックして、**グループ電力**タブをクリックします。
2. **選択されたグループ**メニューからグループを選択します。

   iLO は電力状態別にグループ化されたサーバーを表示し、各状態のサーバーの合計数を示すカウンターも表示します。

3. サーバーのグループの電力状態を変更するには、次のいずれかを実行します。
   - **オン**または**リセット**状態にあるサーバーの場合は、次のいずれかのボタンをクリックします。
     - **瞬間的に押す**
     - **押し続ける**
     - **リセット**
     - **コールドブート**
   - **オフ**状態にあるサーバーの場合は、**瞬間的に押す**ボタンをクリックします。

     オフ状態にあるサーバーでは、**押し続ける**、**リセット**、および**コールドブート**オプションは使用できません。

   iLO が要求を確認するように求めます。
4. **はい、<アクション>**をクリックします。

   たとえば、**リセット**をクリックすると、ボタンのラベルが**はい、リセットします**になります。クリックするボタンの名前は、開始したグループ電力オプションによって異なります。

   仮想電源ボタンの作動に対してグループ化されたサーバーが応答する間、iLO には進行状況バーが表示されます。進行状況バーには、コマンドの実行に成功したサーバーの数が示されます。

   コマンド結果セクションには、電源状態の変更に関連したエラーメッセージなど、コマンドのステータスおよび結果が表示されます。

詳しくは

iLO 連携機能を使用するための前提条件

グループの電力状態オプション

- **瞬間的に押す** - 物理的な電源ボタンを押す場合と同じです。

  一部のオペレーティングシステムは、瞬間的に押した後で適切なシャットダウンを開始するか、またはこのイベントを無視するように構成されている場合があります。Hewlett Packard Enterprise では、仮想電源ボタンを使用してシャットダウンを実行する前に、システムコマンドを使用して正常なオペレーティングシステムのシャットダウンを完了することをお勧めします。
- **押し続ける** - 物理的な電源ボタンを 5 秒間押し続け、離すことと同じです。

  この操作の結果、選択したグループ内のサーバー電源がオフになります。このオプションを使用すると、適切なオペレーティングシステムの終了に影響する場合があります。

  このオプションは、一部のオペレーティングシステムが実装している ACPI 機能を提供します。これらのオペレーティングシステムは、瞬間的に押すと押し続けるによって動作が異なります。
- **コールドブート** - 選択したグループ内のサーバー電源をただちに切ります。プロセッサー、メモリ、および I/O リソースは、メインの電力が失われます。サーバーは、約 6 秒後再起動します。このオプションを使用すると、適切なオペレーティングシステムの終了に影響します。
- **リセット** - 選択したグループ内のサーバーを強制的にウォームブートします。CPU と I/O リソースがリセットされます。このオプションを使用すると、適切なオペレーティングシステムの終了に影響します。

グループの電力状態の変更によって影響を受けるサーバー

影響するシステムリストには、仮想電源ボタンの動作を開始すると影響を受けるサーバーについて、次の詳細が示されます。

- **サーバー名** - ホストオペレーティングシステムで定義されたサーバー名。
- **サーバー電力** - サーバー電力の状態（**オン**または**オフ**）。
- **UID インジケーター** - UID LED の状態。UID LED を使用すると、特に高密度ラック環境でサーバーを特定し、その位置を見つけることができます。状態には、**UID オン**、**UID オフ**、および **UID 点滅**があります。
- **iLO ホスト名** - iLO サブシステムに割り当てられた完全修飾ネットワーク名。サーバーの iLO Web インターフェイスを開くには、**iLO ホスト名**列のリンクをクリックします。
- **IP アドレス** - iLO サブシステムのネットワーク IP アドレス。サーバーの iLO Web インターフェイスを開くには、**IP アドレス**列のリンクをクリックします。

次へまたは**前へ**（使用可能な場合）をクリックして、リストのサーバーをさらに表示します。

詳しくは

iLO 連携情報を CSV ファイルにエクスポートする方法

グループ消費電力上限の構成

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- 選択した iLO 連携グループの各メンバーが、iLO 設定権限をグループに認めている。
- iLO の構成とネットワーク構成が、iLO 連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーで **iLO 連携**をクリックして、**グループ電力設定**タブをクリックします。
2. **選択されたグループ**メニューからグループを選択します。

   このページで行った変更は、選択したグループ内のすべてのシステムに影響します。
3. **手動の電力消費上限を有効**オプションを有効に設定します。
4. **消費電力上限値**をワット数、BTU/時、または割合（%）で入力します。

   %は、最大電力値と最小電力値の差です。消費電力上限値は、サーバー最小電力値より下には設定できません。
5. （オプション）値がワット単位で表示されている場合、BTU/時単位での表示に変更するには**電力単位**メニューの **BTU/時**を選択します。値が BTU/時で表示されている場合、ワット単位での表示に変更するには**ワット**を選択します。
6. **適用**をクリックします。

詳しくは

iLO 連携機能を使用するための前提条件

グループ消費電力上限の注意事項

グループ消費電力上限機能では、iLO Web インターフェイスを実行するシステムから、複数のサーバーの消費電力上限を動的に設定することができます。

- グループ消費電力上限を設定している場合、グループ化されたサーバーは、消費電力上限を超えないように電力を共有します。電力はビジー状態のサーバーにより多く割り当てられ、アイドル状態のサーバーにはより少ない電力が割り当てられます。
- グループに対して設定した消費電力上限は、個々のサーバーの**電力設定**ページで設定できる消費電力上限とともに動作します。
- エンクロージャーまたは個々のサーバーレベルで構成されている消費電力上限や、別の iLO 連携グループによって構成されている消費電力上限がサーバーに影響を与える場合は、他のグループの消費電力上限によりそのサーバーに割り当てられる電力が少なくなる可能性があります。
- 消費電力上限が設定されている場合、グループ化されたサーバーの平均電力測定値は、消費電力上限値以下である必要があります。
- POST 実行中、ROM は最大電力測定値と最小電力測定値を決定する 2 つの電力テストを実行します。

  消費電力上限の設定を決定するときは、**HPE 自動グループ消費電力上限の設定**の表の値を考慮してください。

  - **最大利用可能電力** - グループ内のすべてのサーバーの総電源容量。この値は、**最大消費電力上限値**のしきい値でもあります。設定できる最高の消費電力上限です。
  - **サーバー最大電力** - グループ内のすべてのサーバーの最大電力測定値。この値は、**最小ハイパフォーマンス上限**のしきい値でもあります。グループ内のサーバーのパフォーマンスに影響を与えずに設定できる最小の消費電力上限値です。
  - **サーバー最小電力** - グループ内のすべてのサーバーの最小電力測定値。この値は、**最小消費電力上限**のしきい値でもあります。グループ内のサーバーが使用する最小電力を表します。この値に設定されている消費電力上限は、サーバーの電力使用量を最小化するため、その結果サーバーのパフォーマンスが低下します。

- 消費電力上限は、一部のサーバーではサポートされていません。詳しくは、サーバーの仕様書を参照してください。
- 一部のサーバーでは、iLO Web インターフェイスの外部で消費電力上限設定を管理する必要があります。次のようなツールを使用できます。

  - HPE Advanced Power Manager

  サーバーでサポートされる電力管理機能について詳しくは、**https://www.hpe.com/info/qs** でサーバーの仕様書を参照してください。

グループ消費電力上限情報の表示

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- iLO の構成とネットワーク構成が、iLO 連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーで **iLO 連携**をクリックして、**グループ電力設定**タブをクリックします。
2. **選択されたグループ**メニューからグループを選択します。
3. （オプション）値がワット単位で表示されている場合、BTU/時単位での表示に変更するには**値を BTU/時で表示**をクリックします。値が BTU/時で表示されている場合、表示を W に変更するには**値をワットで表示**をクリックします。

詳しくは

iLO 連携機能を使用するための前提条件

消費電力上限の詳細

HPE 自動グループ消費電力上限の設定

このセクションの内容は、次のとおりです。

- **計測された電力値** - 最大利用可能電力、サーバー最大電力、およびサーバー最小電力。
- **電力消費上限値** - 電力消費上限値（設定されている場合）。

現在の状態

このセクションでは、以下の内容について説明します。

- **現在の電力測定値** - 選択されたグループの現在の電力測定値。
- **現在の消費電力上限値** - 選択したグループに割り当てられている電力の合計量。消費電力上限が設定されていない場合、この値はゼロです。

このシステムへのグループの電力割り当て

ローカル iLO システムに影響を及ぼすグループ消費電力上限と、各グループ消費電力上限によってローカル iLO システムに割り当てられる電力の量。消費電力上限が設定されていない場合、割り当て電力値はゼロです。

iLO 連携グループファームウェアアップデート

グループファームウェアアップデート機能では、ファームウェア情報を表示し、1 つの iLO Web インターフェイスを実行するシステムから、複数のサーバーのファームウェアをアップデートすることができます。

グループのファームウェアアップデート機能は、次のファームウェアタイプをサポートします。これらのファームウェアタイプは、サーバーと環境がサポートしている場合にのみアップデートできます。

- iLO ファームウェア
- システム ROM（BIOS）
- シャーシファームウェア（パワーマネジメント）
- パワーマネジメントコントローラー
- システムプログラマブルロジックデバイス（CPLD）
- NVMe バックプレーンファームウェア
- Innovation Engine（IE）
- サーバープラットフォームサービス（SPS）

- 言語パック
- サードパーティファームウェアパッケージ

  Platform Level Data Model（PLDM）ファームウェアパッケージは、**アクセス設定**ページの **3rd パーティーファームウェアアップデートパッケージの受け入れ**オプションが有効にされている場合にサポートされます。

一部のファームウェアタイプは、組み合わせたアップデートとして提供されます。以下に例を示します。

- SAS プログラマブルロジックデバイスのアップデートは、多くの場合、SAS コントローラーのファームウェアアップデートとの組み合わせになります。
- Intelligent Platform Abstraction Data のファームウェアは、多くの場合、システム ROM/BIOS のアップデートとの組み合わせになります。

複数のサーバーのファームウェアのアップデート

前提条件

- iLO の設定を構成する権限
- 選択した iLO 連携グループの各メンバーが、iLO 設定権限をグループに認めている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- iLO の構成とネットワーク構成が、iLO 連携機能を使用するための前提条件を満たしている。

手順

1. サポートされているファームウェアを、Hewlett Packard Enterprise サポートセンター（**https://www.hpe.com/support/hpesc**）からダウンロードしてください。
2. Web サーバーにファームウェアファイルを保存します。
3. ナビゲーションツリーで **iLO 連携**をクリックして、**グループファームウェアアップデート**タブをクリックします。
4. **選択されたグループ**メニューからグループを選択します。

   このページでファームウェアアップデートを開始すると、選択したグループ内のすべてのシステムが影響を受けます。
5. （オプション）ファームウェアのバージョン、フラッシュステータス、または TPM または TM オプション ROM 計測ステータスリンクをクリックして、影響を受けたシステムのリストをフィルタリングします。

   注意: TPM または TM がインストールされているサーバーでシステム ROM または iLO ファームウェアのアップデートを実行しようとすると、iLO は、TPM または TM に情報を保存しているソフトウェアを一時停止またはバックアップするように求めます。たとえば、ドライブ暗号化ソフトウェアを使用している場合は、ファームウェアのアップデートを開始する前に停止してください。この指示に従わない場合、ご使用のデータにアクセスできなくなる可能性があります。
6. （オプション）Innovation Engine（IE）またはサーバープラットフォームサービス（SPS）のファームウェアをアップデートする場合は、アップデートしたいサーバーの電源を切ってから 30 秒待ちます。
7. **ファームウェアアップデート**セクションで、Web サーバーのファームウェアファイルへの URL を入力し、**ファームウェアのアップデート**をクリックします。

入力する URL は、`http://<server.example.com>/<subdir>/iLO 5_<yyy>.bin` です。ここで、`<yyy>`はファームウェアバージョンを表します。

iLO が要求を確認するように求めます。

8. **はい、アップデートします**をクリックします。

   選択した各システムがファームウェアイメージをダウンロードし、それをフラッシュしようと試みます。

   フラッシュステータスセクションアップデートされ、iLO はアップデートが進行中であることを通知します。アップデートが完了すると、**ファームウェア情報**セクションがアップデートされます。

   ファームウェアイメージがシステムに対して無効か、署名が不適切またはない場合、iLO はイメージを拒否し、**フラッシュステータス**セクションに、影響を受けるシステムのエラーが表示されます。

   ファームウェアアップデートの種類によっては、新しいファームウェアを有効にするために、システムのリセット、iLO のリセット、またはサーバーの再起動が必要になる場合があります。

詳しくは

iLO ファームウェアイメージファイルの入手
サポートされるサーバーファームウェアイメージファイルの入手
iLO 連携機能を使用するための前提条件
選択されたグループのリスト

グループのファームウェアアップデートの影響を受けるサーバー

影響するシステムリストには、グループのファームウェアアップデートによって影響を受けるサーバーについて、次の詳細が示されます。

- **サーバー名** - ホストオペレーティングシステムで定義されたサーバー名。
- **システム ROM** - インストールされているシステム ROM（BIOS）。
- **iLO ファームウェアバージョン** - インストールされている iLO ファームウェアバージョン。
- **iLO ホスト名** - iLO サブシステムに割り当てられた完全修飾ネットワーク名。サーバーの iLO Web インターフェイスを開くには、**iLO ホスト名**列のリンクをクリックします。
- **IP アドレス** - iLO サブシステムのネットワーク IP アドレス。サーバーの iLO Web インターフェイスを開くには、**IP アドレス**列のリンクをクリックします。

次へまたは**前へ**（使用可能な場合）をクリックして、リストのサーバーをさらに表示します。

詳しくは

iLO 連携情報を CSV ファイルにエクスポートする方法

グループファームウェア情報の表示

前提条件

iLO の構成とネットワーク構成が、iLO 連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーで **iLO 連携**をクリックして、**グループファームウェアアップデート**タブをクリックします。
2. **選択されたグループ**メニューからグループを選択します。
3. （オプション）ファームウェアのバージョン、フラッシュステータス、または TPM または TM オプション ROM 計測ステータスリンクをクリックして、表示されるシステムのリストをフィルタリングします。

詳しくは

iLO 連携機能を使用するための前提条件
選択されたグループのリスト

ファームウェアの詳細

ファームウェア情報セクションには、以下の情報が表示されます。

- サポート対象の iLO ファームウェアバージョンのサーバー数。リストされているファームウェアのバージョンを搭載するサーバーの総数の割合（%）も表示されます。
- グループ化されたサーバーのフラッシュステータス。一覧表示されたステータスのサーバーの総数の%も表示されます。
- グループ化されたサーバーの TPM または TM オプション ROM 計測ステータス。一覧表示されたステータスのサーバーの総数の%も表示されます。
- システム ROM のバージョンごとのサーバーの数。一覧表示されたシステム ROM バージョンを搭載するサーバーの総数の%も表示されます。

ライセンスキーのインストール（iLO 連携グループ）

グループライセンスページには、選択した iLO 連携グループのメンバーのライセンスステータスが表示されます。以下の手順を使用して、キーを入力して、ライセンス済みの iLO 機能を有効にします。

前提条件

- iLO の設定を構成する権限
- iLO 連携グループの各メンバーが、iLO 設定の構成権限をグループに認めている。
- iLO ライセンスが、選択したサーバーでサポートされている。
- 選択したサーバーの数に対して認証されている iLO ライセンスアクティベーションキーを取得している。
- iLO の構成とネットワーク構成が、iLO 連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーで **iLO 連携**をクリックして、**グループライセンス**タブをクリックします。
2. （オプション）影響を受けたシステムのリストをフィルタリングするには、ライセンスのタイプまたはステータスリンクをクリックします。

   以下に例を示します。すでにキーがインストールされているサーバー上でライセンスキーをインストールした場合、現在のキーは新しいキーに置き換えられます。既存のライセンスを置き換えたくな

い場合は、**ステータス**セクションの **Unlicensed** をクリックして、ライセンスが適用されていないサーバーにのみラインセンスをインストールします。

3. **アクティブ化キー**ボックスにライセンスキーを入力します。

   アクティベーションキーボックスで、セグメント間でカーソルを移動するには、**Tab** キーを押す、またはボックスのセグメントの内側をクリックします。 **アクティベーションキー**ボックスのセグメントにデータを入力すると、カーソルは自動的に次に進みます。

   ライセンスキーをインストールすると、iLO に最後の 5 桁のみが表示されます。Hewlett Packard Enterprise では、後で必要になる場合に備えて、ライセンスキー情報を記録して保存することをお勧めします。

4. **インストール**をクリックします。

   エンドユーザー使用許諾契約を読み、合意したことを確認するプロンプトが iLO で表示されます。

   エンドユーザー使用許諾契約の詳細は、ライセンスパックオプションキットに記載されています。

5. **同意する**をクリックします。

   ライセンスがインストールされた後、**ライセンス情報**セクションがアップデートされ、選択したグループ用の新しいライセンスの詳細を表示します。

詳しくは

iLO 連携機能を使用するための前提条件
iLO ライセンス
選択されたグループのリスト

ライセンスインストールの影響を受けるサーバー

影響するシステムセクションには、ライセンスキーをインストールする場合に影響を受けるサーバーに関する、次の詳細が表示されます。

- **サーバー名** - ホストオペレーティングシステムで定義されたサーバー名。
- **ライセンス** - インストールされているライセンスタイプ。
- **iLO ファームウェアバージョン** - インストールされている iLO ファームウェアバージョン。
- **iLO ホスト名** - iLO サブシステムに割り当てられた完全修飾ネットワーク名。サーバーの iLO Web インターフェイスを開くには、**iLO ホスト名**列のリンクをクリックします。
- **IP アドレス** - iLO サブシステムのネットワーク IP アドレス。サーバーの iLO Web インターフェイスを開くには、**IP アドレス**列のリンクをクリックします。

次へまたは**前へ**（使用可能な場合）をクリックして、リストのサーバーをさらに表示します。

詳しくは

iLO 連携情報を CSV ファイルにエクスポートする方法

iLO 連携グループライセンス情報の表示

前提条件

iLO の構成とネットワーク構成が、iLO 連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーで **iLO 連携**をクリックして、**グループライセンス**タブをクリックします。
2. **選択されたグループ**メニューからグループを選択します。
3. （オプション）サーバーのリストをフィルタリングするには、**ライセンス情報**セクションのライセンスタイプまたはステータスリンクをクリックします。

詳しくは

iLO 連携機能を使用するための前提条件
選択されたグループのリストのフィルター
選択されたグループのリストのフィルター条件

iLO 連携グループのライセンスの詳細

- **タイプ** - 一覧表示されている各ライセンスタイプのあるサーバーの数。一覧表示されている各ライセンスタイプを持つサーバーの総数の%も表示されます。
- **ステータス** - 一覧表示されている各ライセンスステータスのあるサーバーの数。各ライセンスステータスのあるサーバーの総数の%も表示されます。以下のステータス値が表示されます。
  - **Evaluation** - 有効な評価ライセンスをインストールします。
  - **Expired** - 期限切れの評価ライセンスがインストールされています。
  - **Perpetual** - 有効な iLO ライセンスがインストールされています。このライセンスに有効期限はありません。
  - **Unlicensed** - 工場出荷時のデフォルト（iLO Standard）機能が有効になっています。

iLO リモートコンソール

iLO リモートコンソールを使用すると、ホストサーバーのグラフィックディスプレイ、キーボード、およびマウスにリモートにアクセスできます。リモートコンソールを使用すると、リモートファイルシステムやネットワークドライブにアクセスできます。

リモートコンソールでアクセスすれば､サーバーが起動するときの POST メッセージを確認することができ、ROM ベースのセットアップアクティビティを開始してサーバーハードウェアを構成することができます。OS をリモートでインストールする場合、リモートコンソールにより、インストールプロセス全体をホストサーバーのモニターに表示して、制御することができます。

統合リモートコンソール（IRC）のアクセスオプション

iLO Web インターフェイスから、以下の統合リモートコンソールオプションにアクセスできます。

- **HTML5 統合リモートコンソール** - サポートされているブラウザーを使用しているクライアント用。
- **.NET 統合リモートコンソール** - サポートされているバージョンの Windows .NET Framework を使用している Windows クライアント用。このコンソールを使用するには、使用しているブラウザーで、ClickOnce を使用した.NET アプリケーションの起動をサポートしている必要があります。
- **Java 統合リモートコンソール（Web Start）** - Oracle JRE を使用している Windows クライアントまたは Linux クライアント用。
- **Java 統合リモートコンソール（アプレット）** - Java プラグインを使用している Windows クライアントまたは Linux クライアント用。

  OpenJDK の Linux システムでは､Java プラグインをサポートするブラウザーを採用してアプレットオプションを使用する必要があります。

ブレードサーバーでは、統合リモートコンソールは常に有効です。

ブレード以外のサーバーで、OS の起動後に統合リモートコンソールを使用するには、ライセンスをインストールする必要があります。

その他のリモートコンソールのアクセスオプション

iLO Web インターフェイスの外部から、以下のリモートコンソールオプションを使用できます。

- **HTML5 スタンドアロンリモートコンソール** - iLO Web インターフェイスを使用せずに､サポートされているブラウザーから HTML5 リモートコンソールにアクセスできます。
- **スタンドアロンのリモートコンソール（HPLOCONS）** - iLO の Web インターフェイスを経由せずに、Windows デスクトップからリモートコンソールに直接アクセスできます。

  HPLOCONS の機能と要件は、.NET 統合リモートコンソールと同じです。HPLOCONS は、Web サイト **https://www.hpe.com/support/ilo5** からダウンロードしてください。
- **iOS デバイスおよび Android デバイス用の iLO モバイルアプリケーション** - サポートされる携帯電話やタブレットからリモートコンソールにアクセスする機能を提供します。

  モバイルアプリケーションの機能とその使用方法については、Web サイト（**https://www.hpe.com/support/ilo-docs**）のモバイルアプリケーションのドキュメントを参照してください。

リモートコンソールの使用に関する留意事項

- 統合リモートコンソールは、遅延が大きい（モデム）接続に適しています。
- 同じサーバー上のホストオペレーティングシステムから統合リモートコンソールを実行しないでください。

- リモートコンソールを通じてサーバーにログインするとき、Hewlett Packard Enterprise では、コンソールを閉じる前にログアウトすることを推奨します。
- リモートコンソールの使用が完了したら、ウィンドウを閉じるか、ブラウザーの**閉じる**ボタン（X）をクリックして終了します。
- リモートコンソールセッションがアクティブの場合、UID LED が点滅します。
- **アイドル接続タイムアウト**では、ユーザーの操作がないまま経過し、リモートコンソールセッションが自動的に終了するまでの時間を指定します。仮想メディアデバイスが接続されている場合、この値はリモートコンソールセッションに影響を与えません。
- リモートコンソールウィンドウ上にマウスが置かれている場合、コンソールウィンドウにフォーカスがあるかどうかに関係なく、コンソールはすべてのキーストロークをキャプチャーします。
- **アクセス設定**ページで**リモートコンソール**機能を有効および無効にできます。
- HTML5 リモートコンソールをスタンドアロンモードまたは新規ウィンドウモードで使用すると、リモートコンソールは最初に iLO Web UI セッションで稼動します。リモートコンソールビデオが開始すると、専用のリモートコンソールセッションが開始します。Web UI セッションが終了すると、HTML5 コンソールへの接続が終了するため、リモートコンソールに再接続する必要があります。

詳しくは

iLO アクセス設定の構成

リモートコンソールのアクセス設定の表示

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブでは、リモートコンソールのアクセス設定が**一般情報**セクションに表示されます。

2. （オプション）これらの設定を構成できる**アクセス設定**ページに移動するには、**リモートコンソールステータス**リンクまたは**リモートコンソールポート**リンクをクリックします。

リモートコンソールのアクセス設定の詳細

リモートコンソールステータス

現在のリモートコンソールのアクセス設定（有効または無効）。

リモートコンソールが無効になっている場合：

- グラフィカルリモートコンソールまたはテキストベースのリモートコンソールにアクセスできません。
- ポートスキャナーを使用して、セキュリティの脆弱性をスキャンするセキュリティ監査で、設定されているリモートコンソールポートが検出されません。

アクセス設定ページでこの設定を表示するには、**リモートコンソールステータス**リンクをクリックします。

リモートコンソールポート

設定されているリモートコンソールポート。デフォルト値は 17990 です。

アクセス設定ページでこの設定を表示するには、**リモートコンソールポート**リンクをクリックします。

統合リモートコンソールの起動

HTML5 IRC の起動

サポートされているブラウザーでリモートコンソールにアクセスするには、以下の手順を使用します。

前提条件

- リモートコンソール権限
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- Microsoft Internet Explorer の場合のみ：ホスト名または IPv4 アドレスを使用して、iLO Web インターフェイスに接続している。

  HTML5 IRC は、Microsoft Internet Explorer による IPv6 接続でサポートされていません。Microsoft WebSocket 実装では、標準以外の IPv6 リテラルアドレスが必要です。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. 次のいずれかを実行して、HTML5 IRC を起動します。
   - **HTML5 コンソール**ボタンをクリックします。

     このオプションは、iLO Web インターフェイスと同じブラウザウィンドウにコンソールを開きます。コンソールをブラウザーウィンドウから移動することはできません。
   - **新規ウィンドウ**ボタンをクリックします。

     このオプションは、新しいウィンドウにコンソールを開きます。ウィンドウを別の位置やモニターに移動したり、最小化したりできます。

   HTML5 IRC が起動します。
3. リモートコンソール機能を使用します。
4. （オプション）HTML5 リモートコンソールのオンラインヘルプを表示するには、**メニュー**アイコンをクリックし、**ヘルプ**を選択します。

詳しくは

iLO アクセス設定の構成
HTML5 リモートコンソールのコントロール

概要ページからの HTML5 IRC の起動

サポートされているブラウザーでリモートコンソールにアクセスするには、以下の手順を使用します。

前提条件

- リモートコンソール権限
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。

- Microsoft Internet Explorer の場合のみ：ホスト名または IPv4 アドレスを使用して、iLO Web インターフェイスに接続している。

  HTML5 IRC は、Microsoft Internet Explorer による IPv6 接続でサポートされていません。Microsoft WebSocket 実装では、標準以外の IPv6 リテラルアドレスが必要です。

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**情報**をクリックし、**概要**タブをクリックします。
2. 次のいずれかを実行して、HTML5 IRC を起動します。
   - **HTML5** リンクをクリックします。

     このオプションは、iLO Web インターフェイスと同じブラウザウィンドウにコンソールを開きます。コンソールをブラウザーウィンドウから移動することはできません。
   - をクリックします。

     このオプションは、新しいウィンドウにコンソールを開きます。ウィンドウを別の位置やモニターに移動したり、最小化したりできます。

   HTML5 IRC が起動します。
3. リモートコンソール機能を使用します。
4. （オプション）HTML5 リモートコンソールのオンラインヘルプを表示するには、**メニュー**アイコンをクリックし、**ヘルプ**を選択します。

詳しくは

iLO アクセス設定の構成
HTML5 リモートコンソールのコントロール

HTML5 スタンドアロンリモートコンソールの起動

最初に iLO Web インターフェイスにログインせずに、HTML5 リモートコンソールにアクセスするには、この手順を使用します。

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。

手順

1. ブラウザーウィンドウを開き、次の Web ページに移動します。**`https://<iLO ホスト名または IP アドレス>/irc.html`**

   Microsoft Internet Explorer の場合のみ：ホスト名または IPv4 アドレスを使用します。

HTML5 リモートコンソールは、Microsoft Internet Explorer による IPv6 接続でサポートされていません。Microsoft WebSocket 実装では、標準以外の IPv6 リテラルアドレスが必要です。

iLO HTML5 リモートコンソールログインページが開きます。

- ログインセキュリティバナーが構成されている場合は、バナーテキストが**通知**セクションに表示されます。
- iLO ヘルスステータスが**劣化**で**匿名データ**アクセスオプションが有効な場合は、ヘルスステータスと問題の説明が iLO のログインページに表示されます。セキュリティ侵害の可能性があるセルフテスト障害は、説明には表示されません。

2. ディレクトリまたはローカルアカウントログイン名とパスワードを入力して、**ログイン**をクリックします。

   iLO が Kerberos ネットワーク認証用に設定されている場合は、**ログイン**ボタンの下に **Zero サインイン**ボタンが表示されます。**Zero サインイン**ボタンを使用して、ユーザー名とパスワードを入力せずにログインできます。

   iLO が CAC Smartcard 認証用に設定されている場合は、**ログイン**ボタンの下に **Smartcard でログイン**ボタンが表示されます。スマートカードを接続して、**Smartcard でログイン**ボタンをクリックすることができます。CAC Smartcard 認証を使用する場合、ログイン名とパスワードを入力しないでください。

3. リモートコンソール機能を使用します。
4. （オプション）HTML5 リモートコンソールのオンラインヘルプを表示するには、**メニュー**アイコンをクリックし、**ヘルプ**を選択します。

HTML5 リモートコンソールモード

HTML5 リモートコンソールには、利用可能ないくつかの表示モードがあります。コンソールを使用しているときに、ある表示モードからサポートされている別のモードに切り替えることができます。サポートされている表示モードは、コンソールの起動に使用する方法によって異なります。

ウィンドウモード

リモートコンソールは、iLO Web インターフェイスと同じブラウザーウィンドウのセカンダリウィンドウに表示されます。コンソールをブラウザーウィンドウから移動することはできません。

このモードは、次の方法を使用してコンソールを起動するときに使用できます。

- **iLO 概要**ページの **HTML5** をクリックします。
- **iLO 内蔵リモートコンソール**ページの **HTML5 コンソール**をクリックします。
- iLO ナビゲーションペインのリモートコンソールサムネイルをクリックし、次に **HTML5 コンソール**を選択します。

このモードからドッキングモードまたはフルスクリーンモードに切り替えることができます。

新規ウィンドウモード

リモートコンソールは、別の位置やモニターに移動できるウィンドウに表示されます。ブラウザーのタブとして追加したり、ウィンドウを最小化したりすることもできます。

このモードは、次の方法を使用してコンソールを起動するときに使用できます。

- （**iLO 概要**ページ）をクリックします。
- **iLO 内蔵リモートコンソール**ページの**新規ウィンドウ**をクリックします。

このモードからフルスクリーンモードに切り替えることができます。

ドッキングモード

リモートコンソールは、ナビゲーションペインサムネイルに表示されます。

このモードは、次の方法を使用してコンソールを起動するときに使用できます。

- **iLO 概要**ページの **HTML5** をクリックします。
- **iLO 内蔵リモートコンソール**ページの **HTML5 コンソール**をクリックします。
- iLO ナビゲーションペインのリモートコンソールサムネイルをクリックし、次に **HTML5 コンソール**を選択します。

このモードからウィンドウモードまたはフルスクリーンモードに切り替えることができます。

フルスクリーンモード

リモートコンソールはモニターのフルサイズで表示されます。リモートコンソールメニューを表示するには、カーソルを画面の一番上に移動します。メニューのデフォルト位置は左上です。クリックしてドラッグすると、メニューを別の位置に移動できます。メニューの位置を変更すると、変更は現在のリモートコンソールセッションに対して維持されます。

このモードは、すべてのコンソールモードで使用できます。

スタンドアロンモード

スタンドアロンモードの使用時は、リモートコンソールがブラウザータブに表示されます。

このモードは、次の方法を使用してコンソールを起動するときに使用できます。

次の Web ページに移動して、ログインします。**`https://<iLO` ホスト名または `IP` アドレス`>/irc.html`**

このモードからフルスクリーンモードに切り替えることができます。

HTML5 リモートコンソールのコントロール

リモートコンソールウィンドウの上には、以下のコントロールがあります（左から右の順）。コントロールアイコンの上にカーソルを移動すると、ツールヒントの説明が表示されます。

メニュー

このアイコンでは、以下を行うことができます。

- iLO 仮想電源ボタン機能にアクセスします。
- **環境設定**メニューを使用して、リモートコンソールのステータスバーを表示または非表示にします。
- iLO ホスト名とサーバー名を表示するには、**情報**メニューを使用します。
- HTML5 コンソールのオンラインヘルプを表示するには、**ヘルプ**メニューを使用します。

このアイコンは、ドッキングモードでは使用できません。

仮想キーボード

このアイコンでは、以下を行うことができます。

- リモートサーバーに送信できる次のキーボードショートカットにアクセスする：**CTRL+ALT+DEL**
- リモートコンソールの以下の仮想キーにアクセスする：
  - **CTRL**-コントロール
  - **ESC**-エスケープ
  - **CAPS**-CapsLock
  - **NUM**-NumLock
  - **L OS**-左 OS 固有のキー
  - **L ALT**-左 ALT キー
  - **R ALT**-右 ALT キー
  - **R OS**-右 OS 固有のキー
- HTML5 リモートコンソールキーボードレイアウトを表示または変更します。

仮想メディア⊙

このアイコンから、仮想メディア機能にアクセスできます。

リモートコンソールを閉じる╳

リモートコンソールセッションを閉じるには、このアイコンを使用します。

リモートコンソールディスプレイおよびモードコントロール

次のコントロールを使用して、リモートコンソールの表示を変更したり、別の表示モードに切り替えたりします。

利用可能なコントロールは、アクティブな**コンソールモード**によって異なります。アクティブなコンソールモードでコントロールがサポートされていない場合、そのコントロールは表示されません。

最大化□およびリストア ⧉

最大化アイコンは、リモートコンソールウィンドウをブラウザーウィンドウ内で最大化します。

リストアアイコンは、ウィンドウを元のサイズにリセットします。

これらの機能はウィンドウモードで使用できます。

全画面に切り替え↙↗

この機能はすべてのモードで使用できます。

ドッキングモード⊡

このアイコンを使用して、ウィンドウモードからドッキングモードに変更できます。

この機能はウィンドウモードでは使用できません

全画面を終了↙↗

フルスクリーンモードを終了し、以前に選択したモードに戻るには、このアイコンを使用します。

Esc キーを押してフルスクリーンモードを終了することもできます。

ウィンドウモード🖵

このアイコンを使用して、ドッキングモードからセカンダリウィンドウに変更できます。

この機能はドッキングモードでは使用できません。

ピンアイコン

画面の上部にあるツールバーを固定または固定解除するには、このアイコンを使用します。この設定は現在のリモートコンソールセッションに対して維持されます。

この機能はフルスクリーンモードで使用できます。

.NET IRC の起動

Windows クライアント上のサポートされているブラウザーでリモートコンソールにアクセスするには、以下の手順を使用します。

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- サポート対象のバージョンの Microsoft .NET Framework がインストールされている。
- 使用しているブラウザーで、ClickOnce を使用した.NET アプリケーションの起動をサポートしている。

  Microsoft Edge での.NET IRC の使用については、HPE iLO 5 トラブルシューティングガイドを参照してください。
- ポップアップブロッカーが無効になっている。

  場合によっては、**.NET コンソール**ボタンを **Ctrl を押したままクリックする**ことでポップアップブロッカーをバイパスできることがあります。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. **.NET コンソール**ボタンをクリックします。

   リモートコンソールが、別のウィンドウで起動します。
3. リモートコンソール機能を使用します。

詳しくは

iLO アクセス設定の構成
.NET IRC 要件

概要ページからの.NET IRC の起動

Windows クライアント上のサポートされているブラウザーでリモートコンソールにアクセスするには、以下の手順を使用します。

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- サポート対象のバージョンの Microsoft .NET Framework がインストールされている。
- 使用しているブラウザーで、ClickOnce を使用した.NET アプリケーションの起動をサポートしている。

  Microsoft Edge での.NET IRC の使用については、HPE iLO 5 トラブルシューティングガイドを参照してください。
- ポップアップブロッカーが無効になっている。

  場合によっては、**.NET コンソール**ボタンを **Ctrl を押したままクリックする**ことでポップアップブロッカーをバイパスできることがあります。

手順

1. ナビゲーションツリーで**情報**をクリックし、**概要**タブをクリックします。
2. **.NET** リンクをクリックします。
3. リモートコンソール機能を使用します。

詳しくは

iLO アクセス設定の構成
.NET IRC 要件

.NET IRC 要件

Microsoft .NET Framework

.NET IRC には、Microsoft .NET Framework バージョン 4.5.1 以降が必要です。

Windows 7、8、8.1、および 10 では、サポートされる.NET Framework バージョンは、オペレーティングシステムに含まれています。.NET Framework は、Microsoft ダウンロードセンター（**http://www.microsoft.com/download**）でも入手できます。

Internet Explorer ユーザーのみ：**iLO 統合リモートコンソール**ページは、サポートされているバージョンの.NET Framework がインストールされているかどうかを示します。Internet Explorer がユーザーエージェント文字列を非表示にするように設定されている場合、この情報は表示されません。

Microsoft Edge ブラウザーでは、インストールされている.NET Framework のバージョンに関する情報は表示されません。

Microsoft ClickOnce

.NET IRC は、.NET Framework の一部である Microsoft ClickOnce を使用して起動します。ClickOnce では、SSL 接続からインストールされるすべてのアプリケーションが信頼できるソースからのものでなければなりません。ブラウザーが iLO システムを信頼するように設定されていないときに **IRC は iLO 内の信頼された証明書を要求します**の設定が**有効**に設定されている場合、ClickOnce に次のエラーメッセージが表示されます。

アプリケーションを起動できません。アプリケーションのダウンロードは成功しませんでした。

.NET アプリケーションを起動するための ClickOnce 拡張機能をサポートしていないため、.NET IRC は Google Chrome または Mozilla Firefox ではサポートされていません。回避策として、別のリモートコンソールを選択するか、別のブラウザーを使用します。

新しい Microsoft Edge ブラウザーでの ClickOnce の使用については、HPE iLO 5 トラブルシューティングガイドを参照してください。

Java IRC の起動（Oracle JRE）

この手順を使用して、Windows または Linux と Oracle JRE の環境で Java IRC を起動します。Oracle JRE をサポートする Java IRC のバージョンは、Java Web Start アプリケーションです。

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- ご使用の環境は Java Web Start をサポートしており、最新バージョンの Java 8 がインストールされています。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. **Web Start** ボタンをクリックします。

   ブラウザーが、Hewlett Packard Enterprise JNLP ファイルを保存して開くように要求します。

3. JNLP ファイルを保存して開くには、ブラウザーの指示に従います。
4. **セキュリティ警告**ダイアログボックスが表示された場合は、**続行**をクリックします。

   続行をクリックしないと、Java IRC は起動しません。

5. アプリケーションの実行を確認するプロンプトが表示されたら、**実行**をクリックします。

   実行をクリックしないと、Java IRC は起動しません。

   Java Web Start アプリケーションは、Web ブラウザーの外部にある別のウィンドウで実行されます。起動時に空白のセカンダリウィンドウが開きます。Java IRC がロードされた後は、このウィンドウを閉じないでください。

6. **リモートコンソール機能**を使用します。

詳しくは

iLO アクセス設定の構成

概要ページから Java IRC（Oracle JRE）の起動

この手順を使用して、Windows または Linux と Oracle JRE の環境で Java IRC を起動します。Oracle JRE をサポートする Java IRC のバージョンは、Java Web Start アプリケーションです。

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- ご使用の環境は Java Web Start をサポートしており、最新バージョンの Java 8 がインストールされています。

手順

1. ナビゲーションツリーで**情報**をクリックし、**概要**タブをクリックします。
2. **Java Web Start** リンクをクリックします。

   ブラウザーが、Hewlett Packard Enterprise JNLP ファイルを保存して開くように要求します。
3. JNLP ファイルを保存して開くには、ブラウザーの指示に従います。
4. **セキュリティ警告**ダイアログボックスが表示された場合は、**続行**をクリックします。

   続行をクリックしないと、Java IRC は起動しません。
5. アプリケーションの実行を確認するプロンプトが表示されたら、**実行**をクリックします。

   実行をクリックしないと、Java IRC は起動しません。

   Java Web Start アプリケーションは、Web ブラウザーの外部にある別のウィンドウで実行されます。起動時に空白のセカンダリウィンドウが開きます。Java IRC がロードされた後は、このウィンドウを閉じないでください。
6. リモートコンソール機能を使用します。

詳しくは

iLO アクセス設定の構成

Java IRC の起動（OpenJDK JRE）

Linux と OpenJDK JRE の環境で Java IRC を起動するには、この手順を使用します。OpenJDK JRE をサポートする Java IRC のバージョンは、Java アプレットです。

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- OpenJDK JRE がインストールされている。
- ポップアップブロッカーが無効になっている。

  場合によっては、リモートコンソール起動ボタンを **Ctrl を押したままクリック**することでポップアップブロックをバイパスできることがあります。
- クライアントのブラウザーに、Java プラグインがインストールされている。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

起動タブにリモートコンソールの起動オプションが表示されます。

2. **アプレット**ボタンをクリックします。
3. **セキュリティ警告**ダイアログボックスまたは確認ダイアログボックスが表示された場合は、画面の指示に従って続行します。
4. アプリケーションの実行を確認するプロンプトが表示されたら、**実行**をクリックします。

   実行をクリックしないと、Java IRC は起動しません。

   Java アプレットは、別のウィンドウで実行されます。
5. リモートコンソール機能を使用します。

詳しくは

iLO アクセス設定の構成

リモートコンソールの取得

別のユーザーがリモートコンソールで作業している場合、そのユーザーからリモートコンソールを取得することができます。

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. 使用するリモートコンソールのボタンをクリックします。

   別のユーザーがリモートコンソールで作業していることが iLO から通知されます。
3. リモートコンソールを取得する要求を送信するには、画面の指示に従います。

   他のユーザーは、要求を承認するか拒否するように求められます。

   他のユーザーが承認するか、10 秒以内に応答しない場合、許可が与えられます。リモートコンソールが起動します。

詳しくは

iLO アクセス設定の構成

共有リモートコンソールセッションへの参加（.NET IRC 専用）

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. **.NET コンソール**ボタンをクリックします。

   .NET リモートコンソールが使用中であることを通知するメッセージが表示されます。

3. Share (共有) をクリックします。

   セッションリーダーは、共有リモートコンソールセッションへの参加要求を受信します。

   セッションリーダーが**はい**をクリックすると、ユーザーはセッションへのアクセスを許可され、キーボードやマウスを使えるようになります。

詳しくは

iLO アクセス設定の構成

共有リモートコンソール（.NET IRC 専用）

共有リモートコンソール機能を使用すると、複数のユーザーが同じリモートコンソールセッションに接続できます。この機能は、トレーニングやトラブルシューティングのような活動に使用できます。

通常、リモートコンソールセッションを開始する最初のユーザーがサーバーに接続し、セッションリーダーに指名されます。リモートコンソールアクセスを要求する以後のユーザーは、サテライトクライアント接続のアクセス要求を開始します。セッションリーダーのデスクトップで、各アクセス要求のダイアログボックスが開きます。要求には、要求元のユーザー名と DNS 名または IP アドレスが含まれています。セッションリーダーは、アクセスを許可または拒否するよう求められます。応答がない場合、アクセスは拒否されます。

セッションリーダーの指名を別のユーザーに譲渡することはサポートされていません。

接続障害が発生した場合、再接続はサポートされていません。接続障害後にユーザーアクセスを許可するには、リモートコンソールセッションを再起動する必要があります。

共有リモートコンソールセッション中、セッションリーダーはすべてのリモートコンソール機能にアクセスできます。他のユーザーはキーボードとマウスにアクセスできるだけです。

iLO は、最初にクライアントを認証し、セッションリーダーが新しい接続を許可するかどうかを決定して共有リモートコンソールセッションを暗号化します。

リモートコンソールのステータスバーの表示

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. リモートコンソールを起動します。

   リモートコンソールウィンドウが開き、ステータスバーが表示されます。

3. （オプション）ステータスバーのオンとオフを切り替えるには、**メニュー**アイコンをクリックして、**環境設定** > **ステータスバーを表示**を選択します。

   HTML5 IRC のみがこの機能をサポートしています。

詳しくは

iLO アクセス設定の構成

リモートコンソールのステータスバーの詳細

解像度

リモートコンソールウィンドウの解像度。

POST コード

POST 実行中の POST コードは、ステータスバーの中央に表示されます。

コンソールの取得（.NET IRC 専用）

これらのコントロールを使用して、コンソールウィンドウに表示されるアクティビティを記録および再生できます。

スクリーンキャプチャー

HTML5 IRC でカメラアイコンをクリックして、コンソールウィンドウに表示されるアクティビティのスクリーンキャプチャーを作成できます。

.NET IRC のステータスバーをダブルクリックして、画面をキャプチャーし、スクリーンキャプチャーを画像エディターに貼り付けることができます。

暗号化

リモートコンソールと iLO の間の接続のステータスおよび暗号化タイプ。

ヘルスステータス

サーバーヘルスインジケーター。この値は、全体的なステータスや冗長性（障害処理能力）など、監視対象サブシステムの状態を要約します。起動時にいずれかのサブシステムが冗長でなくても、システムヘルスステータスは劣化しません。表示される値は、**OK**、**劣化**、および**クリティカル**です。

アクティビティ LED

リモートコンソールを介して接続されているローカルの仮想メディアデバイスのためのアクティビティインジケーター。この機能は URL ベースの仮想メディアデバイスについてはアクティブではありません。

電源ステータス

電源 - サーバーの電源状態（**オン**または**オフ**）。

統合リモートコンソールの機能

統合リモートコンソール（IRC）は、以下の機能をサポートします。

- **IRC を使用したキーボード操作**
- **仮想電源 IRC の機能**
- **仮想メディア IRC の機能**
- **コンソールのキャプチャー（.NET IRC）**
- **IRC を使用したスクリーンキャプチャー**

IRC を使用したキーボード操作

HTML5 IRC を使用したキーボード操作の送信

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. HTML5 IRC を起動します。
3. 次のいずれかを実行します。
   - クライアントのキーボードを使用して、目的のキーを押します。
   - **Ctrl+Alt+Del** 操作を送信するには、**仮想キーボード**アイコン⌨をクリックして、**CTRL+ALT+DEL** キーボードショートカットをクリックします。
   - Caps Lock または Num Lock 設定を無効にするには、次のいずれかの操作を行います。
     - クライアントキーボードの **NumLock** または **CapsLock** キーを押します。
     - **仮想キーボード**アイコン⌨をクリックして、**CAPS** または **NUM** キーボードショートカットをクリックします。

詳しくは

iLO アクセス設定の構成

.NET IRC または Java IRC を使用したキーボード操作の送信

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. リモートコンソールを起動します。
3. 次のいずれかを実行します。
   - クライアントのキーボードを使用して、目的のキーを押します。
   - **Ctrl+Alt+Del** 操作を送信するには、**キーボード** > **CTRL-ALT-DEL** を選択します。
   - Caps Lock または Num Lock 設定を無効にするには、次のいずれかの操作を行います。
     - クライアントキーボードの **NumLock** または **CapsLock** キーを押します。
     - **キーボード** > **Caps Lock** または**キーボード** > **Num Lock** を選択します。

詳しくは

iLO アクセス設定の構成

リモートコンソールのホットキーの送信

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- **ホットキー**ページでリモートコンソールのホットキーが構成されている。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

起動タブにリモートコンソールの起動オプションが表示されます。

2. リモートコンソールを起動します。
3. ご使用のクライアントのキーボードで、構成されているリモートコンソールホットキーのキーの組み合わせを押します。

詳しくは

リモートコンソールのホットキー
iLO アクセス設定の構成
リモートコンソールのホットキーの作成

HTML5 IRC のキーボードレイアウトを変更する

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- サーバー OS が、使用するキーボードレイアウトをサポートするように構成されている。
- iLO へのブラウズに使用するクライアントが、使用するキーボードレイアウトをサポートするように構成されている。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. HTML5 IRC を起動します。
3. **仮想キーボード**アイコン⌨をクリックします。
4. **キーボードレイアウト** > ***キーボードレイアウト名***を選択します。

   iLO では、EN 101 および JP 106/109 のキーボードレイアウトをサポートします。

   この設定は cookie に保存され、同じブラウザーでリモートコンソールを使用する際に永続的に残ります。

詳しくは

iLO アクセス設定の構成

仮想電源 IRC の機能

HTML5 IRC でリモートコンソールの仮想電源スイッチを使用する

前提条件

- リモートコンソール権限
- 仮想電源およびリセット権限

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. HTML5 IRC を起動します。
3. **メニュー**アイコンをクリックして、**電源**メニューからオプションを選択します。

   サーバーの電源が入っていない場合、**押し続ける**、**リセット**、および**コールドブート**オプションは使用できません。

   iLO が要求を確認するように求めます。
4. **OK** をクリックします。

詳しくは

iLO アクセス設定の構成

.NET IRC または Java IRC でリモートコンソールの仮想電源スイッチを使用する

前提条件

- リモートコンソール権限
- 仮想電源およびリセット権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. .NET IRC または Java IRC を起動します。
3. リモートコンソールの**電源スイッチ**メニューからオプションを選択します。

   サーバーの電源が入っていない場合、**押し続ける**、**リセット**、および**コールドブート**オプションは使用できません。

   iLO が要求を確認するように求めます。
4. **OK** をクリックします。

詳しくは

iLO アクセス設定の構成

仮想電源ボタンのオプション

- **瞬間的に押す** - 物理的な電源ボタンを押す場合と同じです。サーバーの電源が切れている場合は、瞬間的に押すを押すとサーバーに電源が投入されます。

  一部のオペレーティングシステムは、瞬間的に押した後で適切なシャットダウンを開始するか、またはこのイベントを無視するように構成されている場合があります。Hewlett Packard Enterprise では、仮想電源ボタンを使用してシャットダウンを実行する前に、システムコマンドを使用して正常なオペレーティングシステムのシャットダウンを完了することをお勧めします。

- **押し続ける** - 物理的な電源ボタンを 5 秒間押し続け、離すことと同じです。

  サーバーはこの操作の結果、電源がオフになります。このオプションは、オペレーティングシステムの正常なシャットダウン機能に影響する場合があります。

  このオプションは、一部のオペレーティングシステムが実装している ACPI 機能を提供します。これらのオペレーティングシステムは、瞬間的に押すと押し続けるによって動作が異なります。

- **リセット** - サーバーを強制的にウォームブートします。CPU と I/O リソースがリセットされます。このオプションは、オペレーティングシステムの正常なシャットダウン機能に影響する場合があります。

- **コールドブート** - サーバーからただちに電源を切断します。プロセッサー、メモリ、および I/O リソースは、メインの電力が失われます。サーバーは、約 8 秒後に再起動します。このオプションは、オペレーティングシステムの正常なシャットダウン機能に影響する場合があります。

仮想メディア IRC の機能

統合リモートコンソール（IRC）を使用すると、次の作業を実行できます。

- 以下を含む仮想ドライブの接続と切断：
  - クライアント PC の物理ドライブ（フロッピーディスク、CD/DVD-ROM、USB キー）
  - ローカルの IMG または ISO ファイル
  - URL ベースのメディア（IMG または ISO）
  - 仮想フォルダー

  使用するコンソールが仮想メディアタイプをサポートしていることを確認するには、そのメディアタイプの使用に関する説明を確認してください。

- メディアイメージの作成（Java IRC のみ）

詳しくは

iLO Web インターフェイスの仮想メディアオプション

仮想ドライブ（クライアント PC 上の物理ドライブ）の使用

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。

- **仮想メディア機能**が**アクセス設定**ページで有効になっている。
- Windows でリモートコンソールを使用する場合は、物理ドライブをマウントするために必要な Windows 管理者権限を有している。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. この機能をサポートしているリモートコンソールを起動します。

   このリリースでは、.NET IRC および Java IRC がこの機能をサポートしています。

3. **仮想ドライブ**メニューをクリックし、クライアント PC 上のフロッピーディスク、CD-ROM/DVD、または USB キードライブのドライブ文字を選択します。

   仮想ドライブのアクティビティ LED は、仮想ドライブのアクティビティを表示します。

詳しくは

iLO アクセス設定の構成
仮想メディアに関する留意事項

HTML5 IRC でのローカル IMG または ISO ファイルの使用

前提条件

- リモートコンソール権限
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- **仮想メディア機能**が**アクセス設定**ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. HTML5 IRC を起動します。

3. **仮想メディア**アイコン ⊙ をクリックして、**フロッピー** > **ローカル*.img ファイル**、または **CD/DVD** > **ローカル*.iso ファイル**を選択します。

   リモートコンソールによってファイルを選択するよう求められます。

4. **ファイル名**テキストボックスに、イメージファイルのパスまたはファイル名を入力します。

   ファイルの場所を参照して、**開く**をクリックすることもできます。

   仮想ドライブのアクティビティ LED は、仮想ドライブのアクティビティを表示します。

詳しくは

iLO アクセス設定の構成
仮想メディアに関する留意事項

.NET IRC または Java IRC でのローカル IMG または ISO ファイルの使用

前提条件

- リモートコンソール権限
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- **仮想メディア機能**が**アクセス設定**ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. .NET IRC または Java IRC を起動します。
3. **仮想メディア**メニューをクリックし、**イメージファイルリムーバルメディア**（IMG）または**イメージファイル CD-ROM/DVD**（ISO）を選択します。

   IRC によってファイルを選択するよう求められます。
4. **ファイル名**テキストボックスに、イメージファイルのパスまたはファイル名を入力します。

   ファイルの場所を参照して、**開く**をクリックすることもできます。

   仮想ドライブのアクティビティ LED は、仮想ドライブのアクティビティを表示します。

詳しくは

iLO アクセス設定の構成
仮想メディアに関する留意事項

仮想ドライブを使用して OS のインストールと必要なドライバーの指定を行う

リモートコンソールの仮想ドライブ機能を使用して、オペレーティングシステムをインストールできます。インストール中に、ストレージコントローラードライバーなどの必要なドライバーへのアクセスを提供するようにプロンプトが表示されることがあります。

前提条件

- リモートコンソール権限
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- **仮想メディア機能**が**アクセス設定**ページで有効になっている。
- オペレーティングシステムの ISO ファイルは、リモートコンソールを実行するのに使用するクライアント上で利用可能です。
- オペレーティングシステムを NVMe ドライブにインストールする場合は、**ブートモード**が **Unified Extensible Firmware Interface (UEFI)**に設定されます。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. 必要なドライバーをダウンロードして展開してください。

   SPP からドライバーを入手するか、Web サイト（**https://www.hpe.com/support/hpesc**）からダウンロードできます。

2. ドライバーを USB キーまたはクライアント上のフォルダーにコピーし、そこからリモートコンソールにアクセスします。

3. リモートコンソールを起動します。

   - USB キーを使用して必要なドライバーを提供する場合は、.NET IRC または Java IRC を選択します。
   - 仮想フォルダーを使用して必要なドライバーを提供する場合は、.NET IRC を選択します。

4. オペレーティングシステムの ISO をマウントします。

   a. **仮想ドライブ** > **イメージファイル CD-ROM/DVD** を選択します。

      リモートコンソールによってファイルを選択するよう求められます。

   b. **ファイル名**テキストボックスに、イメージファイルのパスまたはファイル名を入力します。

      ファイルの場所を参照して、**開く**をクリックすることもできます。

5. USB キー上で必要なドライバーを指定する場合、以下の操作を実行します。

   a. USB キーを iLO の管理に使用しているクライアントに接続します。

   b. リモートコンソールで、**仮想ドライブ**メニューをクリックし、クライアント PC 上の USB キーのドライブ文字を選択します。

6. iLO の管理に使用しているクライアント上のフォルダーで必要なドライバーを指定する場合、以下の操作を実行します。

   a. **仮想ドライブ** > **フォルダー**の順に選択します。

   b. **フォルダーの参照**ウィンドウで、ドライバーファイルを格納しているフォルダーを選択します。

7. オペレーティングシステムの ISO を起動します。

8. オペレーティングシステムのインストーラーによってドライバーのパスを入力するプロンプトが表示されるまで、画面の指示に従います。

9. ドライバーの場所を指定するプロンプトが表示されたら、ドライバーを格納した USB キーまたは仮想フォルダーのパスを入力します。

10. 画面の説明に従って、オペレーティングシステムのインストールを完了します。

11. 必要なデバイスドライバーがほかにある場合は、それをインストールします。

    デバイスドライバーは SPP から入手できます。

詳しくは

iLO アクセス設定の構成
サーバーブートモードの設定
.NET IRC または Java IRC でのローカル IMG または ISO ファイルの使用
仮想フォルダーの使用（.NET IRC 専用）
仮想メディアに関する留意事項

HTML5 IRC で URL ベースのイメージファイルを使用する

以下の種類の URL ベースのメディアを接続できます。1.44 MB のフロッピーディスクイメージ（IMG）および CD/DVD-ROM イメージ（ISO）。

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- **仮想メディア機能**が**アクセス設定**ページで有効になっている。
- 使用するイメージファイルが、iLO と同じネットワーク上の Web サーバーにある。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. HTML5 IRC を起動します。
3. **仮想メディア**アイコン ⊙ をクリックして、**フロッピー** > **仮想メディア URL**、または **CD/DVD** > **仮想メディア URL** を選択します。

   リモートコンソールで、イメージファイル URL の入力を求められます。

4. 仮想ドライブとしてマウントしたいイメージファイルの URL を入力して、**適用**をクリックします。

   仮想ドライブのアクティビティ LED は、URL でマウントされた仮想メディアのドライブのアクティビティを表示しません。

詳しくは

iLO アクセス設定の構成
スクリプト仮想メディア用 IIS のセットアップ

.NET IRC または Java IRC で URL ベースのイメージファイルを使用する

以下の種類の URL ベースのメディアを接続できます。1.44 MB のフロッピーディスクイメージ（IMG）および CD/DVD-ROM イメージ（ISO）。

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- **仮想メディア機能**が**アクセス設定**ページで有効になっている。
- 使用するイメージファイルが、iLO と同じネットワーク上の Web サーバーにある。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. .NET IRC または Java IRC を起動します。

3. **仮想ドライブ** > **URL リムーバブルメディア**（IMG ファイル）または**仮想ドライブ** > **URL CD-ROM/DVD**（ISO ファイル）を選択します。

   iLO がイメージファイルの URL を入力するように求めます。

4. 仮想ドライブとしてマウントしたいイメージファイルの URL を入力して、**接続**をクリックします。

   仮想ドライブのアクティビティ LED は、URL でマウントされた仮想メディアのドライブのアクティビティを表示しません。

詳しくは

iLO アクセス設定の構成
スクリプト仮想メディア用 IIS のセットアップ

仮想フォルダーの使用（.NET IRC 専用）

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- **仮想メディア機能**が**アクセス設定**ページで有効になっている。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. .NET IRC を起動します。

3. **仮想メディア** > **フォルダー**の順に選択します。

4. **フォルダーの参照**ウィンドウで、使用するフォルダーを選択し、**OK** をクリックします。

   仮想フォルダーが、**iLO フォルダー**という名前でサーバーにマウントされます。

詳しくは

iLO アクセス設定の構成
仮想メディアに関する留意事項

仮想フォルダー

仮想フォルダーを使用すると、ファイルにアクセスし、ファイルを参照し、クライアントから管理対象サーバーにファイルを転送できます。ローカルディレクトリまたはクライアント経由でアクセスできるネットワーク接続されたディレクトリのマウントとアンマウントを行うことができます。フォルダーまたはディレクトリの仮想イメージが作成された後、サーバーはそのイメージに USB ストレージデバイス

として接続します。ユーザーはサーバーにアクセスし、仮想イメージからサーバーにファイルを転送できます。2 ギガバイトまでのサイズの仮想フォルダーがサポートされます。

仮想フォルダーは読み取り専用であり、ここからは起動できません。マウントされたフォルダーは静的です。クライアントフォルダーに行った変更は、マウントされたフォルダーに複製されません。クライアントフォルダーを変更した後で仮想フォルダーの表示をアップデートしたければ、仮想フォルダーを切り離して再接続するだけで十分です。

メディアイメージの作成機能（Java IRC のみ）

仮想メディアを使用するときは、物理ディスクの代わりにイメージファイルを使用すると、パフォーマンスが向上します。DD などの業界標準ツールを使用して、イメージファイルの作成や、ディスクイメージファイルから物理ディスクへのデータコピーを行えます。Java IRC を使用してこれらのタスクを実行することもできます。

ディスクイメージファイルの作成（Java IRC）

メディアイメージの作成機能では、ファイルまたは物理ディスク上のデータからディスクイメージファイルを作成することができます。ISO-9660 ディスクイメージファイル（IMG または ISO）を作成できます。

前提条件

- リモートコンソール権限
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- **仮想メディア機能**が**アクセス設定**ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. Java IRC を起動します。
3. **仮想メディア** > **ディスクイメージの作成**の順に選択します。

   メディアイメージの作成ダイアログボックスが開きます。

4. **ディスク>>イメージ**ボタンが表示されることを確認します。ボタンラベルが**イメージ>>ディスク**の場合は、このボタンをクリックして**ディスク>>イメージ**に変更します。
5. 次のいずれかを実行します。
   - ファイルを使用する場合は、**メディアファイル**を選択して、**参照**をクリックし、使用するファイルの位置に移動します。
   - 物理メディアを使用する場合は、**メディアドライブ**を選択し、フロッピーディスク、USB キー、または CD のドライブ文字を**メディアドライブ**メニューで選択します。
6. **イメージファイル**テキストボックスに、イメージファイルのパスおよびファイル名を入力します。
7. **作成**をクリックします。

   イメージの作成が完了すると、iLO によって通知されます。

8. **閉じる**をクリックします。
9. 指定した場所にイメージが作成されていることを確認します。

詳しくは

iLO アクセス設定の構成

イメージファイルから物理ディスクへのデータのコピー（Java IRC）

メディアイメージの作成機能では、ディスクイメージファイルからフロッピーディスクまたは USB キーにデータをコピーすることができます。ディスクイメージ（IMG）ファイルのみがサポートされます。CD へのデータのコピーはサポートされていません。

ディスクイメージデータをフロッピーディスクまたは USB キーにコピーできます。

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- **仮想メディア機能**が**アクセス設定**ページで有効になっている。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. Java IRC を起動します。
3. **仮想メディア** > **ディスクイメージの作成**の順に選択します。

   メディアイメージの作成ダイアログボックスが開きます。
4. **メディアイメージの作成**ウィンドウで、**ディスク>>イメージ**をクリックします。

   メディアイメージの作成は**イメージ>>ディスク**オプションに変わります。
5. **メディアドライブ**メニューで、フロッピーディスクまたは USB キーのドライブ文字を選択します。
6. **イメージファイル**テキストボックスに、既存のイメージファイルのパスおよびファイル名を入力します。

   操作が完了すると、iLO によって通知されます。
7. **閉じる**をクリックします。
8. 指定した場所にファイルがコピーされたことを確認します。

詳しくは

iLO アクセス設定の構成

コンソールのキャプチャー（.NET IRC）

コンソールのキャプチャーを使用すると、起動、ASR イベント、および検出されたオペレーティングシステムの不具合のようなイベントのビデオストリームを記録し、再生することができます。iLO が、サー

バー起動シーケンスとサーバー事前障害シーケンスを自動的にキャプチャーします。コンソールビデオの録画を手動で開始および停止することもできます。

- サーバー起動シーケンスとサーバー事前障害シーケンスは、ファームウェアのアップデート中またはリモートコンソールの使用中には自動的にキャプチャーされません。
- サーバー起動シーケンスとサーバー事前障害シーケンスは、自動的に iLO メモリに保存されます。ファームウェアのアップデート中、iLO のリセット時、および電源の消失時には失われます。.NET IRC を使用すると、キャプチャーしたビデオをローカルドライブに保存できます。
- サーバー起動ファイルは、サーバーの起動が検出されると、情報のキャプチャーを開始します。ファイルの領域がなくなると停止します。このファイルは、サーバーが起動するたびに上書きされます。
- サーバー事前障害ファイルは、サーバー起動ファイルがいっぱいになると、情報のキャプチャーを開始します。iLO が ASR イベントを検出すると停止します。サーバー事前障害ファイルは、iLO が ASR イベントを検出したときにロックされます。ファイルのロックが解除され、.NET IRC を介してダウンロードした後でファイルが上書き可能になります。
- コンソールのキャプチャーのコントロールボタンは、.NET IRC セッションウィンドウの下部にあります。

コンソールキャプチャーコントロール

左から右に、以下のコンソールキャプチャーコントロールがあります。

- **スタートにスキップ** - ファイルの最初から再生を再開します。
- **一時停止** - 再生を一時停止します。
- **再生** - 現在選択されているファイルが再生されていなかったり一時停止されている場合は、再生を開始します。
- **録画** - .NET IRC セッションを記録します。
- **進行状況バー** - ビデオセッションの進行状況が示されます。

サーバー起動シーケンスとサーバー事前障害シーケンスの表示

前提条件

- リモートコンソール権限
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. .NET IRC を起動します。
3. **再生**ボタンをクリックします。

再生ボタンは緑色の三角形のアイコンで示され、リモートコンソールウィンドウの下部にあるツールバーにあります。

再生ソースダイアログボックスが表示されます。

4. **サーバースタートアップ**または**サーバー事前障害**を選択します。
5. **開始**をクリックします。

詳しくは

iLO アクセス設定の構成
コンソールのキャプチャー（.NET IRC）

サーバー起動ビデオファイルとサーバー事前障害ビデオファイルの保存

前提条件

- リモートコンソール権限
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. .NET IRC を起動します。
3. **再生**ボタンをクリックします。

   再生ボタンは緑色の三角形のアイコンで示され、リモートコンソールウィンドウの下部にあるツールバーにあります。
4. **サーバースタートアップ**または**サーバー事前障害**を選択します。
5. **開始**をクリックします。
6. **再生**ボタンを再びクリックして、再生を停止します。

   iLO によって、記録が書き込み保護されなくなったことが通知され、保存するように求められます。
7. **はい**をクリックします。
8. 保存場所を選択し、ファイル名を入力して、**保存**をクリックします。
9. （オプション） **ビデオファイルを再生します**。

詳しくは

iLO アクセス設定の構成
コンソールのキャプチャー（.NET IRC）

リモートコンソールを使用したビデオファイルのキャプチャー

この手順を使用して、サーバー起動およびサーバー事前障害以外のシーケンスのビデオファイルを手動でキャプチャーします。

前提条件

- リモートコンソール権限
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. .NET IRC を起動します。
3. **録画**ボタンをクリックします。

   録画ボタンは赤い円のアイコンで示され、リモートコンソールウィンドウの下部にあるツールバーにあります。

   ビデオの保存ダイアログボックスが開きます。
4. ファイル名と保存位置を入力し、**保存**をクリックします。
5. 録画が終了したら、もう一度**録画**ボタンを押して録画を停止します。
6. （オプション） **ビデオファイルを再生します**。

詳しくは

iLO アクセス設定の構成
コンソールのキャプチャー（.NET IRC）

リモートコンソールを使用した保存済みビデオファイルの表示

前提条件

- リモートコンソール権限
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. .NET IRC を起動します。
3. **再生**ボタンをクリックします。

   再生ボタンは緑色の三角形のアイコンで示され、リモートコンソールウィンドウの下部にあるツールバーにあります。

   再生ソースダイアログボックスが表示されます。

4. **ファイルから**ボックスの横にある虫眼鏡アイコンをクリックします。
5. ビデオファイルに移動し、**開く**をクリックします。

   リモートコンソールでキャプチャーしたビデオファイルは、iLO ファイルタイプを使用します。
6. **開始**をクリックします。

詳しくは

iLO アクセス設定の構成
コンソールのキャプチャー（.NET IRC）

IRC を使用したスクリーンキャプチャー

サーバーアクティビティのスクリーンキャプチャーを保存する必要がある場合は、リモートコンソールのスクリーンキャプチャー機能を使用します。たとえば、リモートコンソール画面に表示された POST コードのキャプチャーが必要な場合があります。

IRC スクリーンキャプチャー機能を使用する場合、キャプチャーイメージにリモートコンソールのステータスバーは含まれません。ステータスバーを含むスクリーンキャプチャーが必要な場合、別のスクリーンキャプチャー方法を使用してください。

HTML5 リモートコンソール画面のキャプチャー

前提条件

- リモートコンソール権限
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. HTML5 リモートコンソールを起動します。
3. ステータスバーのカメラアイコン をクリックします。

   新しいブラウザータブでスクリーンキャプチャーが開きます。
4. （オプション）スクリーンキャプチャーを保存します。

詳しくは

iLO アクセス設定の構成

.NET IRC 画面のキャプチャー

前提条件

- リモートコンソール権限
- リモートコンソール機能が**アクセス設定**ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. .NET IRC を起動します。
3. ステータスバーをダブルクリックします。

   スクリーンキャプチャーはクリップボードに保存されます。
4. （オプション）スクリーンキャプチャーをイメージエディターに貼り付けます。

詳しくは

iLO アクセス設定の構成

リモートコンソールのホットキー

ホットキーページを使用すると、リモートコンソールセッション中に使用する最大 6 つのホットキーを定義できます。各ホットキーは、最大 5 つのキーの組み合わせを表します。ホットキーが押されると、キーの組み合わせがホストサーバーに送信されます。ホットキーは、統合リモートコンソールおよびテキストベースのリモートコンソールを使用するリモートコンソールセッション中アクティブです。

ホットキーが設定されていない場合、たとえば、**Ctrl+V** は **NONE**、**NONE**、**NONE**、**NONE**、**NONE** に設定され、このホットキーは無効になります。サーバーオペレーティングシステムは、**Ctrl+V** を通常のように解釈します（この例では「貼り付け」）。別のキーの組み合わせを使用するように **Ctrl+V** を設定すると、サーバーオペレーティングシステムは iLO に設定されたキーの組み合わせを使用します（貼り付け機能がなくなります）。

例 1: Alt+F4 をリモートサーバーに送信したいが、このキーの組み合わせを押すとブラウザーが閉じる場合は、**Alt+F4** のキーの組み合わせをリモートサーバーに送信するようにホットキー **Ctrl+X** を構成することができます。ホットキーの設定後は、リモートサーバーに **Alt+F4** を送信したいとき、リモートコンソールウィンドウで **Ctrl+X** を押します。

例 2 : 国際キーボードの **AltGR** キーをリモートサーバーに送信してホットキーを作成したい場合は、キーリストの **R_ALT** を使用します。

注記: リモートコンソールセッションでの入力が多いと、場合によっては、**Ctrl + X** および **Ctrl + V** ショートカットを使用するホットキーの割当てを避ける必要があります。これらのショートカットは、通常、カットアンドペースト機能に割り当てられます。

リモートコンソールのホットキーの作成

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックして、**ホットキー**タブをクリックします。
2. 作成するホットキーごとに、リモートサーバーに送信するキーの組み合わせを選択します。

   ホットキーを構成して国際キーボードからのキーシーケンスを生成するには、国際キーボード上のキーと同じ位置にある US キーボードのキーを選択します。**リモートコンソールコンピューターのロックキーおよびホットキーを構成するキー**はホットキーを設定するときに使用できるキーを示します。
3. **ホットキーを保存**をクリックします。

   iLO は、ホットキーの設定が正常にアップデートされたことを確認します。

詳しくは

リモートコンソールのホットキーの送信
リモートコンソールコンピューターのロックキーおよびホットキーを構成するキー

リモートコンソールコンピューターのロックキーおよびホットキーを構成するキー

ESC	SCRL LCK	0	f
L_ALT	SYS RQ	1	g
R_ALT	PRINT SCREEN	2	h
L_SHIFT	F1	3	I
R_SHIFT	F2	4	j
L_CTRL	F3	5	k
R_CTRL	F4	6	l
L_GUI	F5	7	m
R_GUI	F6	8	n
INS	F7	9	o
DEL	F8	;	p
HOME	F9	=	q
END	F10	[	r
PG UP	F11	\	s

表は続く

PG DN	F12	]	t
ENTER	SPACE	`	u
TAB	'	a	v
BREAK	,	b	w
BACKSPACE	-	c	x
NUM PLUS	.	d	y
NUM MINUS	/	e	z

ホットキーのリセット

ホットキーをリセットすると、現在のすべてのホットキー割り当てがクリアされます。

前提条件

iLO 設定の構成権限

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックして、**ホットキー**タブをクリックします。
2. **ホットキーをリセット**をクリックします。

   iLO が要求を確認するように求めます。
3. 要求を確認するメッセージが表示されたら、**はい、ホットキーをリセットします**をクリックします。

   ホットキーがリセットされたことが iLO によって通知されます。

リモートコンソールの構成済みホットキーの表示（Java IRC）

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **リモートコンソール**機能が**アクセス設定**ページで有効になっている。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックします。

起動タブにリモートコンソールの起動オプションが表示されます。

2. Java IRC を起動します。
3. **キーボード** > **ホットキーを参照**を選択します。

詳しくは

iLO アクセス設定の構成

リモートコンソールセキュリティの設定

リモートコンソールのコンピューターロック設定を構成する

この機能により、リモートコンソールセッションが終了したり iLO へのネットワークリンクが失われると、OS がロックされるかユーザーがログアウトされます。この機能が有効になっているときにリモートコンソールウィンドウを開いた場合、ウィンドウを閉じるときに OS がロックされます。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックして、**セキュリティ**タブをクリックします。
2. 以下の**リモートコンソールコンピューターロック**設定から選択します。**Windows**、**カスタム**、および**無効**。
3. **カスタム**を選択した場合は、コンピューターのロックキーシーケンスを選択します。
4. 変更を保存するには、**適用**をクリックします。

詳しくは

リモートコンソールのコンピューターロックオプション
リモートコンソールコンピューターのロックキーおよびホットキーを構成するキー

リモートコンソールのコンピューターロックオプション

- **Windows** - Windows オペレーティングシステムを実行している管理対象サーバーをロックするように iLO を構成します。リモートコンソールセッションが終了した場合や iLO ネットワークリンクが失われた場合は、サーバーに**コンピューターロック**ダイアログボックスが自動的に表示されます。
- **カスタム** - カスタムキーシーケンスを使用して管理対象サーバーをロックしたりサーバーにログインしているユーザーをログアウトさせたりするように iLO を構成します。最大で 5 つのキーをリストから選択できます。リモートコンソールセッションが終了した場合や iLO ネットワークリンクが失われた場合は、選択されたキーシーケンスがサーバーの OS に自動的に送信されます。
- **無効**（デフォルト） - リモートコンソールのコンピューターロック機能を無効にします。リモートコンソールセッションが終了したり、iLO ネットワークリンクが失われた場合でも、管理対象サーバー上の OS はロックされません。

詳しくは

リモートコンソールのコンピューターロックオプション
リモートコンソールコンピューターのロックキーおよびホットキーを構成するキー

リモートコンソールの信頼設定の構成（.NET IRC）

.NET IRC は、Microsoft .NET Framework の一部である Microsoft ClickOnce を介して起動します。ClickOnce では、SSL 接続からインストールされるすべてのアプリケーションが信頼できるソースからのものでなければなりません。ブラウザーが iLO プロセッサーを信頼するように設定されていないときにこの設定が有効に設定されている場合、ClickOnce は、アプリケーションを起動できないことを通知します。

Hewlett Packard Enterprise では、信頼された SSL 証明書をインストールして、**IRC は iLO 内の信頼された証明書を要求します**設定を有効にすることをおすすめします。この構成では、.NET IRC は HTTPS 接続を使用することにより起動します。**IRC は iLO 内の信頼された証明書を要求します**設定が無効の場合、.NET IRC は SSL 以外の接続を使用することで起動し、.NET IRC が暗号化キーの交換を開始した後で SSL が使用されます。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックして、**セキュリティ**タブをクリックします。
2. **IRC は iLO 内の信頼された証明書を要求します**設定の有効と無効を切り替えるには、切り替えスイッチをクリックします。
3. 変更を保存するには、**適用**をクリックします。

詳しくは

SSL 証明書の管理
.NET IRC 要件

テキストベースのリモートコンソールの使用

iLO は、テキストベースのリモートコンソールをサポートします。サーバーからビデオ情報が取得され、ビデオメモリの内容が iLO マネジメントプロセッサーへ送信され、圧縮され、暗号化され、管理クライアントアプリケーションに転送されます。iLO は画面フレームバッファーを使用して、テキストベースのクライアントアプリケーションに（画面上の位置情報とともに）文字を送信します。この方法により、標準的なテキストベースクライアントとの互換性、良好な性能、および単純さが確保されます。ただし、ASCII 以外の文字やグラフィカル情報は表示できず、表示される文字の画面上の位置の送信順序が前後にずれる場合があります。

iLO は、ビデオアダプターの DVO ポートを使用して、ビデオメモリに直接アクセスします。この方法により、iLO の性能が大幅に向上します。ただし、デジタルビデオストリームには有用なテキストデータが含まれず、テキストベースのクライアントアプリケーション（SSH など）では、このデータを表示できません。

以下の各項で説明するように、テキストベースのコンソールオプションには 2 つのタイプがあります。

- **iLO 仮想シリアルポート**
- **テキストベースのリモートコンソール（Textcons）**

iLO 仮想シリアルポート

標準ライセンスと仮想シリアルポートを使用すると、iLO からテキストベースのコンソールにアクセスできます。

仮想シリアルポートにより、サーバーのシリアルポートと双方向データフローが提供されます。リモートコンソールを使用すると、リモートサーバーシリアルポート上に物理シリアル接続が存在するかのように操作できます。

仮想シリアルポートはテキストベースのコンソールとして表示されますが、その情報はグラフィカルビデオデータを通じて描画されます。iLO では、サーバーがプレオペレーティングシステム状態であるときに、この情報が SSH クライアント経由で表示されます。この機能を使用すると、iLO 標準システムで POST 中のサーバーを監視および操作できます。

仮想シリアルポートを使用すると、リモートユーザーは以下の操作を実行できます。

- サーバーの POST シーケンスおよびオペレーティングシステムの起動シーケンスの操作

  UEFI システムユーティリティを起動するには、仮想シリアルポートセッション中に、**ESC + Shift 9** キーまたは **Esc + (**キーの組み合わせを入力します。
- オペレーティングシステムとのログインセッションの確立、オペレーティングシステムの操作、およびオペレーティングシステム上のアプリケーションの実行と操作
- グラフィックフォーマットで Linux を実行する iLO システムの場合は、サーバーのシリアルポートで `getty()` を構成し、仮想シリアルポートを使用して Linux OS へのログインセッションを表示できます。
- 仮想シリアルポートからの EMS コンソールの使用。EMS は、Windows の起動の問題とカーネルレベルの問題をデバッグする場合に便利です。

iLO 仮想シリアルポートの使用

手順

1. **UEFI システムユーティリティで iLO 仮想シリアルポートを構成します**。
2. iLO 仮想シリアルポートを使用するようにオペレーティングシステムを設定します。
   - サポートされる Linux オペレーティングシステムについては、**iLO 仮想シリアルポートを使用するための Linux の設定**を参照してください。
   - サポートされる Windows オペレーティングシステムについては、**iLO 仮想シリアルポート搭載の Windows EMS コンソール**を参照してください。
3. **iLO 仮想シリアルポートセッションを開始します**。
4. （オプション）**iLO 仮想シリアルポートログを表示します**。

UEFI システムユーティリティでの iLO 仮想シリアルポートの構成

次の手順は、iLO 仮想シリアルポートを使用する前に必要な設定です。この手順は Windows システムと Linux システムの両方で必要です。

手順

1. UEFI システムユーティリティにアクセスします。
   a. （オプション）サーバーにリモートアクセスする場合、iLO リモートコンソールセッションを開始します。
   b. サーバーを再起動するかまたは電源を入れます。
   c. サーバーの POST 画面で **F9** キーを押します。

      UEFI システムユーティリティが起動します。
2. 仮想シリアルポートの COM ポートを設定します。
   a. **システム構成**をクリックし、**BIOS/プラットフォーム構成（RBSU）**をクリックします。
   b. **システムオプション**をクリックし、**シリアルポートオプション**をクリックします。
   c. **仮想シリアルポート**メニューで、使用する COM ポートを選択します。
3. BIOS シリアルコンソールおよび EMS プロパティを設定します。
   a. **シリアルポートオプション**ページの上部で、**BIOS シリアルコンソールおよび EMS** を選択します。
   b. **BIOS シリアルコンソールポート**メニューで、使用する COM ポートを選択します。
   c. **BIOS シリアルコンソールボーレート**メニューで、**115200** を選択します。

      注記: iLO 仮想シリアルポートは物理 UART を使用しません。**BIOS シリアルコンソールボーレート**の値は、iLO 仮想シリアルポートがデータを送受信するのに使用する速度には影響しません。
   d. Windows ユーザーの場合のみ : **EMS コンソール**メニューで、**仮想シリアルポート**で選択した COM ポートに一致する COM ポートを選択します。
4. 変更を保存して終了するには、**F12** キーを押します。

5. 要求を確認するメッセージが表示されたら、**はい - 変更を保存します**をクリックします。

   UEFI システムユーティリティによって、システムの再起動が必要であることが通知されます。

6. **再起動**をクリックします。

iLO 仮想シリアルポートを使用するための Linux の設定

コンソールリダイレクションを使用して、Linux サーバーをリモートから管理できます。コンソールリダイレクションを使用するように Linux を設定するには、Linux ブートローダー（GRUB）を設定する必要があります。サーバーのシステム ROM が POST を完了すると、ブート可能デバイスからブートローダーアプリケーションがロードされます。シリアルインターフェイスをデフォルトのインターフェイスに定義して、10 秒（デフォルトタイムアウト値）以内にローカルキーボードから入力がなければ、システムは出力先をシリアルインターフェイス（iLO 仮想シリアルポート）に変更します。

iLO 仮想シリアルポートを使用するための Red Hat Enterprise Linux 7 の構成

手順

1. テキストエディターで`/etc/sysconfig/grub` を開きます。

   この設定例では、`ttys0` を使用します。

   - `GRUB_CMDLINE_LINUX` 行の最後に、**`console=ttys0`** を入力します。
   - `rhgb quiet` を削除します。
   - 次のパラメーターを入力します。

```
GRUB_TIMEOUT=5
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap console=ttyS0,115200n8"
GRUB_DISABLE_RECOVERY="true"
```

2. 次のコマンドを入力して `grub.cfg` ファイルを作成します。

```
grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

3. シリアルポートに対して `getty` ログインサービスを有効にします。

   以下に例を示します。

```
systemctl enable serial-getty@ttyS0.service
```

4. シリアルポートで `getty` をリッスンします。

   以下に例を示します。

```
systemctl start getty@ttyS0.service
```

5. 構成したシリアルポートでシェルセッションを開始するには、システムブート中に自動的にログインプロセスを開始するように`/etc/inittab` ファイルに次の行を追加します。

   次の例は、`/dev/ttyS0` でログインコンソールを開始します。

```
S0:2345:respawn:/sbin/agetty 115200 ttyS0 vt100
```

6. SSH を使用して iLO に接続し、CLP コマンド `start /system1/oemhpe_vsp1` を使用して、Linux オペレーティングシステムへのログインセッションを表示します。

iLO 仮想シリアルポートを使用するための Red Hat Enterprise Linux 8 の構成

手順

1. grub2-env コマンドを使用して、kernelopts パラメーターを確認します。

   以下に例を示します。

   ```
   # grub2-editenv - list | grep kernelopts
   kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhel-swap
   rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap
   ```

2. list コマンドの結果をコピーします。

   以下に例を示します。

   ```
   kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhel-swap
   rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap
   ```

3. カーネルオプションを設定します。

   手順 **2** でコピーした既存のカーネルオプションを含め、最後にシリアルコンソールオプションを追加します。

   以下に例を示します。

   ```
   # grub2-editenv - set
   "kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhel-swap
   rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap console=ttyS0,115200 console=tty0"
   ```

4. （オプション）パラメーターが正しく設定されたことを確認するには、list コマンドを再度実行します。

   以下に例を示します。

   ```
   # grub2-editenv - list | grep kernelopts
   kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhel-swap
   rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap console=ttyS0,115200 console=tty0
   ```

5. サーバーを再起動します。

シリアルコンソールを使用するための GRUB の構成（Red Hat Enterprise Linux 8）

VGA コンソールの代わりにシリアルコンソールを使用するように GRUB を構成できます。この機能を使用すると、別のカーネルを選択するために起動プロセスを中断するタスクや、シングルユーザーモードでの起動タスク用のカーネルパラメーターを追加するタスクなどを実行できます。

手順

シリアルコンソールを使用するように GRUB を構成するには、スプラッシュイメージをコメントアウトして、grub.conf ファイルに serial オプションと terminal オプションを追加します。

以下に例を示します。

```
[root@localhost ~]# cat /boot/grub/grub.conf
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
#splashimage=(hd0,0)/grub/splash.xpm.gz
```

```
serial --unit=0 --speed=115200
terminal --timeout=5 serial console
title Red Hat Enterprise Linux AS (2.4.21-27.0.2.ELsmp)
root (hd0,0)
        kernel /vmlinuz-2.4.21-27.0.2.ELsmp ro root=LABEL=/ console=ttyS0,115200 console=tty0
        initrd /initrd-2.4.21-27.0.2.ELsmp.img
```

変更は、次のシステム再起動後に有効になります。

iLO 仮想シリアルポートを使用するための SUSE Linux Enterprise Server の構成

手順

1. テキストエディターで`/etc/default/grub` を開きます。

   この設定例では、`ttys0` を使用します。

   `GRUB_CMDLINE_LINUX_DEFAULT` 行の最後に、**"console=tty0 console=ttyS0,115200n8"**を入力します。

2. `grub.cfg` ファイルをアップデートするには、次のいずれかのコマンドを入力します。

   UEFI ブートモードを使用しているサーバーの場合：

   ```
   grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

   レガシー BIOS ブートモードを使用しているサーバーの場合：

   ```
   grub-mkconfig -o /boot/efi/EFI/sles/grub.cfg
   ```

3. `systemctl` を使用して、`getty` を`/dev/ttyS0` 上でリッスンするように構成します。

   ```
   systemctl start getty@ttyS0.service
   ```

4. `getty` をすべてのブートで`/dev/ttyS0` をリッスンするように構成するには、その特定のポートに対してサービスを有効にします。

   以下に例を示します。

   ```
   systemctl enable serial-getty@ttyS0.service
   ```

5. 構成したシリアルポートでシェルセッションを開始するには、システムブート中に自動的にログインプロセスを開始するように`/etc/inittab` ファイルに次の行を追加します。

   次の例は、`/dev/ttyS0` でログインコンソールを開始します。

   ```
   S0:2345:respawn:/sbin/agetty 115200 ttyS0 vt100
   ```

6. SSH を使用して iLO に接続し、iLO の CLP コマンド `start /system1/oemhpe_vsp1` を使用して、Linux オペレーティングシステムへのログインセッションを表示します。

iLO 仮想シリアルポート搭載の Windows EMS コンソール

iLO を使用すると、Windows EMS コンソールをネットワーク経由で Web ブラウザーを介して使用できます。EMS を使用すると、ビデオ、デバイスドライバーなど OS 機能が原因で通常の動作や通常の修正処置が実行できない場合に、Emergency Management Services（EMS）を実行できます。

iLO で Windows EMS コンソールを使用する場合：

- 仮想シリアルポートを使用する前に、OS に Windows EMS コンソールを構成する必要があります。EMS コンソールを有効化する方法については、OS のドキュメントを参照してください。EMS コン

ソールが OS で有効になっていない場合は、仮想シリアルポートにアクセスしようとしたときに、iLO がエラーメッセージを表示します。

- Windows EMS シリアルポートは、UEFI システムユーティリティから有効にする必要があります。構成オプションでは、EMS ポートを有効または無効にすることや COM ポートを選択することができます。iLO は、EMS ポートの有効/無効を自動的に検出し、COM ポートの選択を検出します。
- Windows EMS コンソールは、リモートコンソールと同時に使用できます。
- `SAC>`プロンプトを表示するには、仮想シリアルポートコンソールを介して接続した後で、**Enter** を押す必要があります。

iLO 仮想シリアルポートを使用するための Windows の構成

これらの手順を実行するときの構文ヘルプについては、**`bcdedit /?`**を入力します。

手順

1. コマンドウィンドウを開きます。
2. 起動構成データを編集するには、次のコマンドを入力します。

   ```
   bcdedit /ems on
   ```

3. 次のコマンドを入力して、EMSPORT および EMSBAUDRATE の値を構成します。

   ```
   bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
   ```

   注記: EMSPORT:1 が COM1 で、EMSPORT:2 が COM2 です。

4. ブートアプリケーションに対して緊急管理サービスを有効または無効にするには、次のコマンドを入力します。

   ```
   bcdedit /bootems on
   ```

5. オペレーティングシステムを再起動します。

iLO 仮想シリアルポートセッションの開始

前提条件

- 仮想シリアルポート設定は、UEFI システムユーティリティで構成されます。
- Windows または Linux オペレーティングシステムは、仮想シリアルポートを使用するように構成されます。

手順

1. SSH セッションを開始します。
   たとえば、**`ssh Administrator@<iLO IP`** アドレス**>**を入力するか、または `putty.exe` をポート 22 で接続します。
2. プロンプトが表示されたら、iLO アカウントの認証情報を入力します。
3. `</>hpiLO->`プロンプトで、**`VSP`** と入力し、**Enter** キーを押します。
4. （Windows システムの場合のみ）`<SAC>`プロンプトで **`cmd`** と入力して、コマンドプロンプトチャネルを作成します。

5. （Windows システムの場合のみ）チャネル番号で指定されたチャネルに切り替えるには、**ch - si <#>**と入力します。

6. プロンプトが表示されたら、OS のログイン認証情報を入力します。

詳しくは

iLO 仮想シリアルポートの使用

iLO 仮想シリアルポートログの表示

仮想シリアルポートログが有効な場合、`vsp log` コマンドを使用して仮想シリアルポートの動作を表示できます。

仮想シリアルポートの動作が iLO メモリにある 150 ページの循環バッファーに記録され、CLI コマンド `vsp log` を使用して表示できます。仮想シリアルポートのバッファーサイズは 128 KB です。

前提条件

この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. **セキュリティ - アクセス設定**ページの**セキュアシェル（SSH）**および**仮想シリアルポートログ**を有効にします。
2. SSH 経由で CLI に接続します。
3. **vsp** コマンドを使用して、仮想シリアルポートの動作を表示します。
4. **ESC** を入力して、終了します。
5. 仮想シリアルポートログを表示するには、**vsp log** を入力します。

詳しくは

iLO アクセス設定の構成

テキストベースのリモートコンソール（Textcons）

ライセンスが適用された iLO システムと SSH を使用してテキストベースのリモートコンソール（Textcons）にアクセスできます。SSH を使用すると、SSH クライアントと iLO が使用する暗号化方法によって、認証情報を含むデータストリームが保護されます。

この機能は、レガシー BIOS ブートモードを使用するように構成されたサーバーでのみサポートされます。このブートモードはフレームバッファーコンソールを使用しません。この機能は、UEFI ブートモードを使用するように構成されたサーバーではサポートされません。

Textcons を使用する場合、色、文字、および画面制御の表示は、SSH クライアントによって異なります。iLO と互換性のあるすべての標準 SSH クライアントを使用できます。

機能およびサポートは、以下のとおりです。

- 以下を含む 80×25 のテキストモード画面の表示（標準のカラー構成）:
  - システム起動プロセス（POST）
  - 標準オプション ROM

- テキストブートローダー（フレームバッファーのないブートローダー）
- VGA 80×25 モードの Linux オペレーティングシステム
- DOS
- その他のテキストベースのオペレーティングシステム

- 国際言語キーボード（サーバーおよびクライアントシステムが同様に設定されている場合）
- クライアントアプリケーションで適切なフォントとコードページが選択されている場合の線画文字

テキストベースのリモートコンソールの使用

前提条件

サーバーはレガシー BIOS ブートモードを使用するように構成されています。

手順

1. SSH を使用して、iLO に接続します。

   ターミナルアプリケーションの文字エンコード方法が **Western（ISO-8859-1）**に設定されていることを確認します。

2. iLO にログインします。
3. プロンプトで、`textcons` と入力します。

   メッセージが表示され、テキストベースのリモートコンソールが起動中であることを示します。

4. テキストベースのリモートコンソールを終了し、CLI セッションに戻るには、**ESC+Shift+9** キーを押します。

詳しくは

ブート順序

テキストベースのリモートコンソールと組み合わせた Linux

シリアルポートに端末セッションを提示するように設定された Linux システムで、テキストベースのリモートコンソールを実行することができます。この機能は、リモートログサービスの使用を可能にします。シリアルポートにリモートでログオンして、出力をログファイルにリダイレクトできます。シリアルポートに転送されたシステムメッセージは、リモートでログ記録されます。

Linux でテキストモードで必要になる一部のキーの組み合わせは、テキストベースのリモートコンソールに渡されない可能性があります。たとえば、**Alt キーと Tab キー**の組み合わせはクライアントによって阻止される場合があります。

テキストベースのリモートコンソールのカスタマイズ

`textcons` コマンドのオプションと引数を使用してテキストベースリモートコンソールの表示をカスタマイズできます。一般に、このオプションを変更する必要はありません。

サンプリングレートの制御

`textcons speed` オプションを使用して、サンプリング間隔をミリ秒で表示します。このサンプリング間隔で、iLO ファームウェアが画面の変更を調べ、テキストベースのリモートコンソールをアップデートします。速度の調整により、長いまたは短いネットワークリンク上の不要なトラフィック、帯域幅使用、

および iLO CPU 時間を削減することができます。Hewlett Packard Enterprise は、1～5,000（1 ミリ秒～5 秒）の値を指定することをおすすめします。次に例を示します。

```
textcons speed 500
```

スムージングの制御

iLO は、画面上で変更され、変更が止まったときにのみ、データを送信します。iLO が変更をサンプリングする間隔よりも速いタイミングでテキスト画面の行が変更される場合、行は、変更が止まるまで送信されません。

テキストベースのリモートコンソールがアクティブのときは、データの表示が速く、判読できません。iLO がネットワーク経由でこの判読不能なデータを送信すると、帯域幅が消費されます。デフォルトの動作はスムージング（遅延 0）です。つまり、画面での変更が止まったときにのみデータが送信されます。遅延オプションを使用してスムージングを制御または無効化することができます。以下に例を示します。

```
textcons speed 500 delay 10
```

文字マッピングの設定

ASCII 文字セットでは、制御文字（32 未満の ASCII 文字）は印刷不能文字で、表示されません。これらの文字は、矢印、星、丸などの記号を表示するために使用される場合があります。これらの文字のいくつかは、同等の ASCII 表現にマッピングされます。次の表は、サポートされる同等表現のリストです。

表 1: 文字の同等表現

文字値	説明	マッピングされる同等表現
0x07	小さな点	·
0x0F	太陽	☉
0x10	右向きのポインター	>
0x11	左向きのポインター	<
0x18	上向きの矢印	^
0x19	下向きの矢印	v
0x1A	左向きの矢印	<
0x1B	右向きの矢印	>
0x1E	上向きのポインター	^
0x1F	下向きのポインター	v
0xFF	影付きブロック	空白スペース

ホスト上での iLO の使用

仮想 NIC 機能により、ホストオペレーティングシステムから直接 iLO に安全に接続できます。この機能をホストサーバーで直接使用するか、リモートコンソール接続経由で使用します。iLO との対話は、Web インターフェイス、SSH、または iLORESTful API を使用して行うことができます。

仮想 NIC 機能は、以下を行う場合に役立ちます。

- ネットワーク構成により管理ネットワーク経由で接続できない場合に iLO にアクセスするとき。たとえば、本番環境ネットワークにアクセスできるが iLO 専用管理ネットワークにアクセスできない場合、仮想 NIC の接続を使用します。
- ホストまたは iLO に NIC ケーブルが接続されていない場合に iLO にアクセスするとき。

工場出荷時のデフォルトの**仮想 NIC** 設定は、iLO のほとんどのバージョンで無効になっています。iLO 5 v2.10 では、この設定はデフォルトで有効になっています。iLO を工場出荷時のデフォルト設定にリセットすると、**仮想 NIC** 設定は、iLO のインストールされているバージョンのデフォルト設定に戻ります。ファームウェアのアップグレードまたはダウングレードでは、この設定は変更されません。

仮想 NIC についてのオペレーティングシステムのサポート

仮想 NIC 機能は、iLO 5 および次のオペレーティングシステムを有するサーバーが要件を満たします。

- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- SUSE Linux Enterprise Server 12
- SUSE Linux Enterprise Server 15
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 8

この機能は、CDC EEM ドライバーが含まれている、要件を満たさない他のオペレーティングシステムで動作することが予想されます。

仮想 NIC を使用するための前提条件

- **ホストサーバー OS が仮想 NIC をサポートしている**。
- USB CDC-EEM ドライバーがホストサーバー OS にインストールされている。

  このドライバーは、この機能をサポートするオペレーティングシステムについてのオペレーティングシステムのインストールの一部です。
- **仮想 NIC 機能がアクセス設定ページで有効になっている**。
- iLO への接続に使用するインターフェイスが**アクセス設定**ページで有効になっている。

  たとえば、iLO Web インターフェイスに接続する場合、**iLO Web インターフェイス**オプションが有効になっている。
- ホストサーバーが、iLO への接続に使用するインターフェイス用のポートをブロックするように構成されていない。

たとえば、デフォルトの iLO 構成で iLO Web インターフェイスを使用するとき、ホストサーバーがポート 443 をブロックしないようにしてください。

- 仮想 NIC インターフェイスが、いずれのホスト NIC ともチーミングまたはブリッジされていない。この構成では、仮想 NIC が使用できなくなったり安全でなくなる可能性があります。
- iLO のホスト名と仮想 NIC IP アドレスは、仮想 NIC へのアクセスに使用するクライアントシステム上の `hosts` ファイル内にあります。iLO のホスト名を使用して仮想 NIC で iLO に接続するには、この構成で名前解決が機能し、SSL 接続が正しく検証される必要があります。

詳しくは

iLO アクセス設定の構成
仮想 NIC についてのオペレーティングシステムのサポート

仮想 NIC 機能の構成

前提条件

iLO の設定を構成する権限

手順

1. 仮想 NIC 機能が有効になっていることを確認します。
   a. ナビゲーションツリーで**セキュリティ**をクリックします。

      アクセス設定ページが表示されます。
   b. **iLO** セクションで**仮想 NIC** が**有効**に設定されていることを確認します。
2. **仮想 NIC** が**有効**に設定されていない場合は、有効にします。
   a. ✎（**iLO** カテゴリの隣にある）をクリックします。

      iLO 設定の編集ページが表示されます。
   b. **仮想 NIC** チェックボックスを選択して、**OK** をクリックします。

      iLO が、保留中の変更を有効にするにはリセットを必要であることを通知します。
   c. アクセス設定のアップデートが完了している場合は、**iLO のリセット**をクリックします。

      iLO が要求を確認するように求めます。
   d. **はい、iLO をリセットします**をクリックします。

      接続が再確立されるまでに、数分かかることがあります。

      リセットが完了したら、仮想 NIC 機能が有効になり、ホストサーバーの OS によって検出されます。
3. （オプション）DHCP 用の新しいネットワークインターフェイスを自動的に構成しない Linux ディストリビューションの場合 : 仮想 NIC インターフェイスのネットワーク構成を静的から DHCP に変更します。

   詳しくは、以下を参照してください。

- **仮想 NIC インターフェイスを静的から DHCP に変更する（ネットワークマネージャー）**
- **仮想 NIC インターフェイスを静的から DHCP に変更する（CLI）**

4. ホストオペレーティングシステムで仮想 NIC が使用できることを確認します。

a. リモートコンソールセッションを開始するか、物理ホストシステムにアクセスします。

b. 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す。

c. 次のいずれかを実行します。

- Windows システムの場合：`ipconfig` を実行し、IP アドレスが 16.1.15.2、サブネットマスクが 255.255.255.252 の **Ethernet adapter Ethernet** という名前のアダプターを探します。
- Linux システムの場合：ネットワークインターフェイス名を特定し、`ifconfig` を実行します。アダプターの IP アドレスは 16.1.15.2、サブネットマスクは 255.255.255.252 です。

警告: ホストのアダプター IP アドレスは変更しないでください。IP アドレスを 16.1.15.2 から他の値に変更すると、仮想 NIC にアクセスできなくなります。

詳しくは

iLO アクセス設定の構成

仮想 NIC インターフェイスを静的から DHCP に変更する（ネットワークマネージャー）

Linux ディストリビューションが DHCP の新しいネットワークインターフェイスを自動的に構成しない場合、仮想 NIC インターフェイスのネットワーク構成を静的から DHCP に変更します。

手順

1. ネットワークマネージャーを開きます。

2. **仮想 NIC** インターフェイスを探します。

3. DHCP を使用するように**仮想 NIC** インターフェイスを構成します。

仮想 NIC インターフェイスを静的から DHCP に変更する（CLI）

Linux ディストリビューションが DHCP の新しいネットワークインターフェイスを自動的に構成しない場合、仮想 NIC インターフェイスのネットワーク構成を静的から DHCP に変更します。

手順

1. `/sys/bus/usb/devices` 内のデバイスを特定します。

以下に例を示します。

- `cat /sys/bus/usb/devices/1-4/idVendor` は値 `03f0` を表示します。
- `cat /sys/bus/usb/devices/1-4/idProduct` は値 `2927` を表示します。

2. 仮想 NIC ネットワークインターフェイス名を特定します。

以下に例を示します。

```
/sys/bus/usb/devices/1-4/1-4:1.0/net/usb0
```

3. DHCP を使用するよう仮想 NIC インターフェイスを構成するネットワーク構成スクリプトを記述します。

   たとえば、構成スクリプトに次のエントリーを含む`/etc/sysconfig/network/ifcfg-usb0` を作成します。`BOOTPROTO='dhcp'`.

4. 仮想 NIC インターフェイスにアクセスするか、ネットワークサービスを再起動します。

iLO Web インターフェイスにアクセスするための仮想 NIC の使用

前提条件

- ご使用の環境が仮想 NIC 機能を使用するための一般的な前提条件を満たしていること。
- プロキシサーバーを使用するようにブラウザーが構成されていないこと。

手順

1. リモートコンソールセッションを開始するか、物理ホストシステムにアクセスします。
2. 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す。
3. サポートされているブラウザーを開きます。
4. 次の URL を入力します。**`https://16.1.15.1`**

   iLO のホスト名と仮想 NIC の IP アドレスがクライアントシステムの hosts ファイルにある場合は、iLO ホスト名を使用して接続することもできます。

   `https://`*`iLO hostname`*

   Web サイト証明書に関連するセキュリティ警告が表示されます。

5. ブラウザーに応じて、以下のいずれかを行います。

   - **Internet Explorer - Web ページへ移動（推奨されません）**をクリックします。
   - **Microsoft Edge - 詳細**をクリックしてから、**Web ページへ移動**をクリックします。
   - **Google Chrome - 詳細**をクリックしてから、**<iLO ホスト名または IP アドレス>にアクセスする（安全ではありません）**をクリックします。
   - **Mozilla Firefox - 詳細**をクリックしてから、**危険性を承知で続行**をクリックします。

   ローカルシステムの iLO ログイン画面が表示されます。

6. iLO にログインします。

   IP アドレスが **16.1.15.2** のセッションが**セッションリスト**ページに表示されます。

7. iLO Web インターフェイスを使用してサーバーまたは iLO 構成を表示またはアップデートします。

詳しくは

iLO Web インターフェイスへのログイン

仮想 NIC を使用するための前提条件
サポートされているブラウザー

ホスト上での iLOREST の使用

前提条件

- ご使用の環境が仮想 NIC 機能を使用するための一般的な前提条件を満たしていること。
- ホストサーバーオペレーティングシステムに RESTful インターフェイスツールがインストールされていること。

手順

1. リモートコンソールセッションを開始するか、物理ホストシステムにアクセスします。
2. ホストサーバー OS にログインします。
3. iLOREST を開始します。
4. iLO システムにログインします。

   ```
   iLOrest > login 16.1.15.1 -u iLO user name -p iLO password
   ```

   iLO のホスト名と仮想 NIC の IP アドレスがクライアントシステムの hosts ファイルにある場合は、iLO ホスト名を使用して接続することもできます。

   ```
   iLOrest > login iLO hostname -u iLO user name -p iLO password
   ```

5. iLOREST コマンドを使用してサーバーまたは iLO 構成を表示またはアップデートします。

詳しくは

仮想 NIC を使用するための前提条件

仮想 NIC での SSH 接続の使用

前提条件

- ご使用の環境が仮想 NIC 機能を使用するための一般的な前提条件を満たしていること。
- Windows オペレーティングシステムの場合のみ：PuTTy または OpenSSH がインストールされていること。

手順

1. リモートコンソールセッションを開始するか、物理ホストシステムにアクセスします。
2. 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す。
3. インストールされているオペレーティングシステムに応じて、コマンドプロンプトまたは PuTTY ターミナルプロンプトを開きます。
4. iLO システムにログインします。

   ```
   ssh iLO user name@16.1.15.1
   ```

iLO のホスト名と仮想 NIC の IP アドレスがクライアントシステムの hosts ファイルにある場合は、iLO ホスト名を使用して接続することもできます。

```
ssh iLO user name@iLO hostname
```

5. SSH クライアントを使用してサーバーまたは iLO 構成を表示またはアップデートします。

詳しくは

仮想 NIC を使用するための前提条件

iLO 仮想メディアの使用

仮想メディアに関する留意事項

iLO 仮想メディアは、ネットワークウェブの任意の位置で標準のメディアからリモートホストサーバーを起動するために使用できる仮想デバイスを提供します。仮想メディアデバイスは、ホストシステムの起動時に使用できます。仮想メディアデバイスは、USB テクノロジーを使用してホストサーバーに接続します。

仮想メディアを使用する場合、以下の点に注意してください。

- 同時に 1 種類の仮想メディアしか接続できません。
- 仮想メディア機能は、最大 8 TB の ISO イメージをサポートしています。ISO イメージの最大ファイルサイズは、ISO イメージが保存されているファイルシステムの 1 つのファイルサイズの制限や、サーバーの OS がサポートする SCSI コマンドなどの要因に依存します。
- OS では、仮想フロッピー/USB キーまたは仮想 CD/DVD-ROM は、通常のドライブのように見えます。仮想メディアを初めて使用する場合、ホスト OS が、新しいハードウェアの検出ウィザードを実行するよう指示する場合があります。
- 仮想デバイスが接続されてから接続を切断するまで、ホストサーバーは仮想デバイスを使用できます。仮想メディアデバイスの使用を終了して仮想メディアを切断するときに、ホスト OS から「unsafe device removal」という警告メッセージを受け取る場合があります。デバイスを切断する前に、デバイスを停止するための OS 機能を使用することにより、この警告を避けることができます。
- iLO 仮想 CD/DVD-ROM は、サポートされるオペレーティングシステムで、サーバーの起動時に使用できます。仮想 CD/DVD-ROM から起動することにより、ネットワークドライブからの OS の展開、障害の発生したオペレーティングシステムのディザスタリカバリなどの作業を実行できます。
- ホストサーバーの OS が USB の大容量記憶装置または SD デバイスをサポートする場合、ホストサーバーの OS をロードした後で、iLO 仮想フロッピー/USB キーを使用できます。
  - ホストサーバーの OS の実行中に、仮想フロッピー/USB キーは、ドライバーのアップグレード、緊急時修復ディスクの作成などの作業に使用できます。
  - サーバーの実行時に仮想フロッピー/USB キーを使用できるようにしておくと、NIC ドライバーを診断し、修復する必要がある場合に役立てることができます。
  - 仮想フロッピー/USB キーは、Web ブラウザーが動作している物理フロッピーディスク、USB キー、または SD ドライブである場合があります。または、ローカルのハードディスクドライブまたはネットワークドライブに保存されているイメージファイルの場合もあります。
  - 最適な性能を得るために、Hewlett Packard Enterprise はクライアント PC のハードディスクドライブまたは高速ネットワークリンクを介してアクセスできるネットワークドライブに格納されているイメージファイルを使用することを推奨します。
- ホストサーバーの OS が USB の大容量記憶装置をサポートする場合、ホストサーバーの OS をロードした後にも、iLO 仮想 CD/DVD-ROM を使用できます。
  - ホストサーバーの OS の実行中に、仮想 CD/DVD-ROM を使用して、デバイスドライバーのアップグレード、ソフトウェアのインストールなどの作業を行うことができます。
  - サーバーの実行時に仮想 CD/DVD-ROM を使用できるようにしておくと、NIC ドライバーを診断し、修復する必要がある場合に役立てることができます。

- 仮想 CD/DVD-ROM は、Web ブラウザーを実行しているマシン上の物理 CD/DVD-ROM ドライブである場合があります。また、仮想 CD/DVD-ROM は、ローカルのハードディスクドライブまたはネットワークドライブに保存されているイメージファイルの場合もあります。
- 最適な性能を得るために、Hewlett Packard Enterprise はクライアント PC のハードディスクドライブまたは高速ネットワークリンクを介してアクセスできるネットワークドライブに格納されているイメージファイルを使用することを推奨します。

・ 仮想フロッピー/USB キーまたは仮想 CD/DVD-ROM 機能が使用されている場合、通常、クライアント OS からはフロッピードライブまたは CD/DVD-ROM ドライブにアクセスできません。

△ **注意:** ファイルやデータが壊れることを防止するために、ローカルメディアを仮想メディアデバイスとして使用しているときは、ローカルメディアへのアクセスを試行しないでください。

・ OpenJDK を使用する HTML5 IRC および Java IRC のみ：iLO の Web インターフェイスウィンドウを更新するか閉じると、リモートコンソール接続は終了します。

リモートコンソール接続が終了すると、URL ベースの仮想メディアを使用して接続されていたデバイスを除き、リモートコンソールを通じて接続されていた仮想メディアデバイスにアクセスできなくなります。

仮想メディアを使用するためのオペレーティングシステム要件

ここでは、iLO 仮想メディア機能を使用する場合に注意する必要があるオペレーティングシステム要件について説明します。

オペレーティングシステムの USB 要件

仮想メディアデバイスを使用するには、オペレーティングシステムが USB 大容量記憶装置を含む USB デバイスをサポートする必要があります。詳しくは、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。

システムのブート中に、ROM BIOS が USB サポートを適用し、オペレーティングシステムがロードされます。MS-DOS は、BIOS を使用してストレージデバイスと通信しているので、DOS を起動するユーティリティディスケットも仮想メディアとして機能します。

オペレーティングシステムに関する注意事項：仮想ディスケット/USB キー

Windows Server 2008 以降

仮想ディスケット/USB キードライブは、Windows が USB デバイスを認識した後に自動的に表示されます。仮想デバイスを、ローカル接続されたデバイスと同じように使用してください。

Windows のインストール中に仮想ディスケットをドライバーディスクとして使用するには、ホスト RBSU の内蔵ディスクドライブを無効にします。この操作により、仮想ディスケットが強制的にドライブ A として表示されます。

Windows のインストール中にドライバーディスケットとして仮想 USB キーを使用するには、USB キードライブのブート順序を変更します。Hewlett Packard Enterprise では、USB キードライブのブート順序を最初にすることをお勧めします。

Red Hat Enterprise Linux および SUSE Linux Enterprise Server

Linux は、USB ディスケットとキードライブの使用をサポートしています。

ディスケットの交換

物理 USB ディスクドライブがあるクライアントマシンで、仮想ディスケット/USB キーを使用する場合、ディスク交換操作は認識されません。たとえば、ディスケットディスクからディレクトリリストを取得し

た後、ディスクを交換すると、次のディレクトリリストには、最初のディスケットのディレクトリリストが表示されます。仮想ディスケット/USB キーの使用中にディスクを交換する必要がある場合は、必ず、非 USB のディスクドライブを搭載するクライアントマシンを使用してください。

オペレーティングシステムに関する注意事項：仮想 CD/DVD-ROM

MS-DOS

仮想 CD/DVD-ROM は、MS-DOS ではサポートされていません。

Windows

仮想 CD/DVD-ROM は、Windows がデバイスのマウントを認識した後に自動的に表示されます。これを、ローカル接続された CD/DVD-ROM ドライブと同じように使用してください。

Linux

仮想 CD/DVD-ROM は、Linux GUI では自動的にマウントされます。

Linux コマンドラインで仮想 CD/DVD-ROM をマウントする方法については、**USB 仮想メディア CD/DVD-ROM をマウントする（Linux コマンドライン）**を参照してください。

Linux ディストリビューションによっては、仮想 CD/DVD-ROM は次のいずれかデバイスファイルでアクセスできます。

- `/dev/cdrom`
- `/dev/scd0`
- `/dev/sr0`

ローカルの CD/DVD-ROM デバイスが存在するサーバーでは、仮想 CD/DVD-ROM デバイスは、ローカル DVD デバイスに続くデバイス番号（たとえば、`/dev/cdrom1`）でアクセスできます。

USB 仮想メディア CD/DVD-ROM をマウントする（Linux コマンドライン）

手順

1. iLO Web インターフェイスにログインします。
2. .NET IRC または Java IRC を起動します。
3. **仮想ドライブ**メニューを選択します。
4. CD/DVD-ROM または ISO ファイルを選択します。
5. Linux システム上の iLO 仮想メディアデバイスエントリーを見つけます。

   デバイスエントリーはシステムメッセージログファイルで確認できます。たとえば、次のイメージはデバイスエントリー`/dev/sr0` を示しています。

```
[82693.715699] usb 1-2: new high-speed USB device number 22 using ehci-pci
[82693.831447] usb 1-2: New USB device found, idVendor=03f0, idProduct=2227
[82693.831454] usb 1-2: New USB device strings: Mfr=1, Product=2, SerialNumber=0
[82693.831457] usb 1-2: Product: Virtual CD-ROM
[82693.831461] usb 1-2: Manufacturer: iLO
[82693.832239] usb-storage 1-2:1.0: USB Mass Storage device detected
[82693.832537] scsi host11: usb-storage 1-2:1.0
[82694.932330] scsi 11:0:0:0: CD-ROM            iLO      Virtual DVD-ROM       PQ: 0 ANSI: 0 CCS
[82694.973476] sr 11:0:0:0: [sr0] scsi3-mmc drive: 12x/12x cd/rw tray
[82694.973915] sr 11:0:0:0: Attached scsi CD-ROM sr0
[82694.974139] sr 11:0:0:0: Attached scsi generic sg4 type 5
[82913.362270] ISO 9660 Extensions: RRIP_1991A
```

6. マウントポイントを作成します。

   以下に例を示します。

- Red Hat Enterprise Linux：`mkdir/mnt/cdrom`*X*、ここで X は選択した数字です。
- SUSE Linux Enterprise Server：`mkdir /media/cdrom`*X*、ここで X は選択した数字です。

7. `mount` *`device file mount point`* のようにコマンドを入力して、デバイスをマウントします。

   以下に例を示します。

   - Red Hat Enterprise Linux：`mount /dev/cdrom1 /mnt/cdrom1`
   - SUSE Linux Enterprise Server：`mount /dev/scd0 /media/cdrom1`

オペレーティングシステムに関する注意事項：仮想フォルダー

- **起動プロセスおよび DOS セッション** - 仮想フォルダーデバイスは、標準 BIOS ディスケットドライブ（ドライブ A）として表示されます。このとき、物理的に接続されたディスケットドライブがあっても使用できません。ローカル物理ディスケットドライブと仮想フォルダーを同時に使用することはできません。
- **Windows** - Windows が仮想 USB デバイスのマウントを認識すると、仮想フォルダーは自動的に表示されます。フォルダーは、ローカル接続されたデバイスと同じように使用できます。仮想フォルダーからは起動できません。仮想フォルダーから起動しようとすると、サーバーが起動できない場合があります。
- **Red Hat Enterprise Linux および SuSE Linux Enterprise Server** - Linux は、FAT 16 ファイルシステムフォーマットを使用する仮想フォルダー機能の使用をサポートします。

iLO Web インターフェイスの仮想メディアオプション

アクセス設定ページで**仮想メディア**機能が有効になっている場合、**仮想メディア**ページで次の作業を実行できます。

- 物理ドライブ、ローカルイメージファイル、仮想フォルダーなどのローカルメディアを表示または取り出す。
- URL ベースのメディアから表示、接続、イジェクト、または起動を実行する。URL ベースのメディアとは、URL を使用して Web サーバーに保存されているイメージを接続することを示します。iLO では、HTTP または HTTPS 形式の URL を使用できます。FTP はサポートされません。

詳しくは

仮想メディア IRC の機能

仮想メディアのステータスおよびポート構成の表示

仮想メディア機能の構成を表示するには、**仮想メディア**ページを使用します。これらの設定は、**アクセス設定**ページで構成できます。

手順

1. **リモートコンソール & メディア**ページに移動し、**仮想メディア**タブをクリックします。

   仮想メディアステータスおよび**仮想メディアポート**が表示されます。

2. （オプション）仮想メディア機能のステータスを構成するには、**仮想メディアステータス**リンクをクリックします。

アクセス設定ページが表示されます。

3. （オプション）仮想メディアポートを構成するには、**仮想メディアポート**リンクをクリックします。

   アクセス設定ページが表示されます。

詳しくは

iLO アクセス設定の構成

接続されているローカルメディアの表示

前提条件

- 仮想メディア権限
- **仮想メディア機能**が**アクセス設定**ページで有効になっている。

手順

接続されたローカルメディアデバイスを表示するには、ナビゲーションツリーで**リモートコンソール&メディア**をクリックして、**仮想メディア**タブをクリックします。

詳しくは

iLO アクセス設定の構成

ローカルメディアの詳細

ローカル仮想メディアを接続すると、以下のセクションに詳細が表示されます。

仮想フロッピー/USB キー/仮想フォルダーステータス

- **挿入されたメディア** - 接続されている仮想メディアの種類。

  ローカルメディアが接続されている場合、**ローカルメディア**と表示されます。
- **接続ステータス** - 仮想メディアデバイスが接続されているかどうかを示します。
- **読み取り専用** - 仮想メディアデバイスが読み取り専用パーミッションで接続されているかどうか。

仮想 CD/DVD-ROM ステータス

- **挿入されたメディア** - 接続されている仮想メディアの種類。

  ローカルメディアが接続されている場合、**ローカルメディア**と表示されます。
- **接続ステータス** - 仮想メディアデバイスが接続されているかどうかを示します。

ローカル仮想メディアデバイスの取り出し

前提条件

- 仮想メディア権限
- **仮想メディア機能**が**アクセス設定**ページで有効になっている。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックして、**仮想メディア**タブをクリックします。
2. **仮想フロッピー/USB キー/仮想フォルダーステータス**セクションまたは**仮想 CD/DVD-ROM ステータス**セクションにある**メディアの強制取り出し**ボタンをクリックします。

詳しくは

iLO アクセス設定の構成

URL ベースのメディアの接続

仮想メディアページから URL ベースのメディアを接続できます。 **仮想メディア**ページは、1.44 MB のフロッピーイメージ（IMG）および CD/DVD-ROM イメージ（ISO）の接続をサポートします。イメージは、iLO と同じネットワーク上の Web サーバーに存在している必要があります。

前提条件

- 仮想メディア権限
- **仮想メディア機能**が**アクセス設定**ページで有効になっている。

手順

1. ナビゲーションツリーで**リモートコンソール&メディア**をクリックして、**仮想メディア**タブをクリックします。
2. **仮想フロッピーに接続**セクション（IMG ファイル）または **CD/DVD-ROM を接続**セクション（ISO ファイル）の**仮想メディア URL** ボックスに URL ベースのメディアの URL を入力します。
3. CD/DVD-ROM のみ : 次のサーバー再起動時にサーバーをこのイメージだけから起動したい場合は、**次回リセット時にブート**チェックボックスを選択します。

   イメージは 2 番目のサーバー再起動時に自動的に取り出されるので、サーバーは一度しかこのイメージから起動しません。

   このチェックボックスを選択しない場合、イメージは手動でイジェクトするまで接続されたまま残ります。サーバーは、システムブートオプションがそのように構成されている場合、以後すべてのサーバーリセット時にイメージに対して起動します。

   サーバーが POST を実行している場合に、**次回のリセット時に起動**チェックボックスを有効にしようとすると、エラーが発生します。POST 中はブート順序を変更できません。POST が終了するのを待ってから、再試行してください。
4. 仮想フロッピーのみ : 読み取り専用パーミッションを持つ仮想メディアデバイスを接続する場合、**読み取り専用**チェックボックスを選択します。

   読み取り専用チェックボックスはデフォルトで有効になっています。
5. **メディアの挿入**をクリックします。
6. （オプション）接続されたイメージからいますぐ起動するには、サーバーを再起動します。

詳しくは

iLO アクセス設定の構成
スクリプト仮想メディア用 IIS のセットアップ

接続されている URL ベースのメディアの表示

前提条件

- 仮想メディア権限
- **仮想メディア機能**が**アクセス設定**ページで有効になっている。

手順

ナビゲーションツリーで**リモートコンソール&メディア**をクリックして、**仮想メディア**タブをクリックします。

詳しくは

iLO アクセス設定の構成

URL ベースのメディアの詳細

URL ベースの仮想メディアを接続すると、以下のセクションに詳細が表示されます。

仮想フロッピー/USB キー/仮想フォルダーステータス

- **挿入されたメディア** - 接続されている仮想メディアの種類。

  URL ベースのメディアが接続されている場合、**スクリプトメディア**と表示されます。
- **接続ステータス** - 仮想メディアデバイスが接続されているかどうかを示します。
- **イメージ URL** - 接続されている URL ベースのメディアをポイントする URL。
- **読み取り専用** - 仮想メディアデバイスが読み取り専用パーミッションで接続されているかどうか。

仮想 CD/DVD-ROM ステータス

- **挿入されたメディア** - 接続されている仮想メディアの種類。

  URL ベースのメディアが接続されている場合、**スクリプトメディア**と表示されます。
- **接続ステータス** - 仮想メディアデバイスが接続されているかどうかを示します。
- **イメージ URL** - 接続されている URL ベースのメディアをポイントする URL。

URL ベースの仮想メディアデバイスの取り出し

前提条件

- 仮想メディア権限
- **仮想メディア機能**が**アクセス設定**ページで有効になっている。

手順

1. ナビゲーションツリーで**リモートコンソール & メディア**をクリックして、**仮想メディア**をクリックします。
2. URL ベースのメディアデバイスを取り出すには、**仮想フロッピー/仮想フォルダーステータス**セクションまたは**仮想 CD/DVD-ROM ステータス**セクションにある**メディアの強制取り出し**ボタンをクリックします。

仮想メディアの完全な権限を付与するライセンスがないサーバーブレードでは、URL ベースの仮想メディアイメージで**メディアの強制取り出し**オプションを使用できません。この場合、Onboard Administrator DVD ドライブが接続されている可能性が高く、Onboard Administrator ソフトウェアを介してこの接続を切断する必要があります。iLO をリセットして、接続を切断することもできます。

詳しくは

iLO アクセス設定の構成

スクリプト仮想メディア用 IIS のセットアップ

前提条件

スクリプト仮想メディア用に IIS をセットアップする前に、IIS が動作状態であることを確認してください。IIS を使用して、簡単な Web サイトをセットアップし、そのサイトにアクセスして正しく動作していることを確認します。

IIS の設定

以下の手順に従って、ディスケットまたは ISO-9660 CD イメージの読み取り専用アクセス用に IIS を設定します。

手順

1. ディレクトリを Web サイトに追加し、イメージをディレクトリに置きます。
2. IIS が使用している MIME タイプにアクセスできることを確認します。

   たとえば、ディスケットイメージファイルが拡張子 `.img` を使用している場合は、その拡張子に対して MIME タイプを追加する必要があります。IIS Manager を使用して、自分の Web サイトの**プロパティ**ダイアログボックスにアクセスします。**HTTP ヘッダー**タブで、**MIME の種類**をクリックして MIME タイプを追加します。

   Hewlett Packard Enterprise は、次のタイプを追加することをおすすめします。

   - `.img application/octet-stream`
   - `.iso application/octet-stream`

3. 読み取り専用ディスクイメージを処理するように Web サーバーが構成されていることを確認します。

   a. Web ブラウザーを使用して、ディスクイメージの位置に移動します。

   b. ディスクイメージをクライアントにダウンロードします。

   以下の手順が正常に完了した場合、Web サーバーは正しく設定されます。

読み出し/書き込みアクセス用の IIS の設定

手順

1. Perl（たとえば、ActivePerl）をインストールします。
2. 必要に応じて、仮想メディアヘルパーアプリケーションをカスタマイズします。
3. 仮想メディアヘルパースクリプトの Web サイトにディレクトリを作成し、そのディレクトリにスクリプトをコピーします。

スクリプト例ではディレクトリ名 `cgi-bin` を使用していますが、任意の名前を使用できます。

4. ディレクトリの**プロパティ**ページの**アプリケーションの設定**で**作成**をクリックしてアプリケーションディレクトリを作成します。

   IIS Manager のディレクトリのアイコンがフォルダーアイコンからギアアイコンに変わります。

5. **実行**アクセス許可を**スクリプトのみ**に設定します。

6. Perl がスクリプトインタープリターとしてセットアップされていることを確認します。

   アプリケーションの関連を確認するには、**プロパティ**ページの**構成**をクリックします。Perl が次の例に示すように構成されていることを確認します。

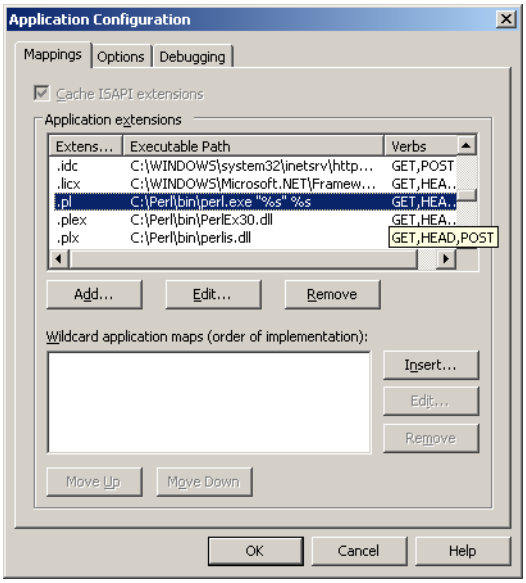


図 3: Perl 設定の例

7. Web Service Extensions が Perl スクリプトの実行を許可していることを確認します。そうでない場合は、**Web Service Extensions** をクリックして **Perl CGI Extension** を **Allowed** に設定します。

8. ヘルパーアプリケーションのプレフィックス変数が正しく設定されていることを確認します。

詳しくは

ヘルパーアプリケーションによる仮想メディアの挿入
仮想メディアヘルパーアプリケーションのサンプル

ヘルパーアプリケーションによる仮想メディアの挿入

`INSERT_VIRTUAL_MEDIA` コマンドでヘルパーアプリケーションを使用する場合、URL の基本形式は次のようになります。

```
protocol://user:password@servername:port/path,helper-script
```

変数は次のとおりです。

- `protocol` - 必須です。HTTP または HTTPS です。
- `user:password` - オプションです。指定された場合は、HTTP 基本認証が使用されます。
- `servername` - 必須です。Web サーバーのホスト名または IP アドレスです。
- `port` - オプションです。Web サーバーの標準でないポートです。

- `path` - 必須です。アクセスしているイメージファイルです。
- `helper-script` - オプションです。IIS Web サーバー上のヘルパースクリプトの位置です。

`INSERT_VIRTUAL_MEDIA` コマンドについて詳しくは、HPE iLO 5 スクリプティング/コマンドラインガイドを参照してください。

仮想メディアヘルパーアプリケーションのサンプル

以下の Perl スクリプトは、部分書き込みの不可能な Web サーバー上でディスケットへの書き込みを可能にする CGI ヘルパーアプリケーションの例です。ヘルパーアプリケーションと `INSERT_VIRTUAL_MEDIA` コマンドを組み合わせて使用すると、書き込み可能なディスクをマウントできます。

ヘルパーアプリケーションを使用する場合、iLO ファームウェアは、以下のパラメーターを使用して、このアプリケーションに要求を提示します。

- `file` パラメーターは、元の URL で提供されるファイルの名前を含みます。
- `range` パラメーターは、データの書き込み先を指定する 16 進数の包含範囲を含みます。
- `data` パラメーターは、書き込まれるデータを示す 16 進数の文字列を含みます。

ヘルパースクリプトは、`file` パラメーターをその作業ディレクトリに対する相対パスに変換する必要があります。この手順では、パラメーターの前に"../,"というプレフィックスを配置するか、またはエイリアス化された URL パスをファイルシステム上の真のパスに変換する必要があります。ヘルパースクリプトは、ターゲットファイルに対する書き込みアクセスを必要とします。ディスケットイメージファイルは、適切なパーミッションを備える必要があります。

例：

```
#!/usr/bin/perl

use CGI;
use Fcntl;

#
# The prefix is used to get from the current working directory to the
# location of the image file that you are trying to write
#
my ($prefix) = "c:/inetpub/wwwroot";
my ($start, $end, $len, $decode);

my $q = new CGI();          # Get CGI data

my $file =  $q->param('file'); # File to be written
my $range = $q->param('range'); # Byte range to be written
my $data =  $q->param('data'); # Data to be written

#
# Change the file name appropriately
#
$file = $prefix . "/" . $file;

#
# Decode the range
#
if ($range =~ m/([0-9A-Fa-f]+)-([0-9A-Fa-f]+)/) {
```

```
$start = hex($1);
$end = hex($2);
$len = $end - $start + 1;
}

#
# Decode the data (a big hexadecimal string)
#
$decode = pack("H*", $data);

#
# Write it to the target file
#
sysopen(F, $file, O_RDWR);
binmode(F);
sysseek(F, $start, SEEK_SET);
syswrite(F, $decode, $len);
close(F);

print "Content-Length:0\r\n";
print "\r\n";
```

電力および温度機能の使用

サーバーの電源オン

セキュアリカバリ

電源がシステムに供給されると、iLO によって独自のファームウェアが検証および起動されます。iLO ファームウェアで検証に失敗すると、リカバリイメージが使用可能な場合は自動的に iLO ファームウェアがフラッシュされます。この機能は、iLO Standard ライセンスでサポートされています。

サーバーの起動時に、システム ROM が検証されます。アクティブなシステム ROM の検証に失敗し、冗長化システム ROM が有効である場合は、冗長化システム ROM がアクティブになります。アクティブシステム ROM と冗長化システム ROM の両方が無効であり、iLO Advanced ライセンスがインストールされている場合は、ファームウェア検証スキャンが開始されます。構成されているファームウェア検証の設定に応じて、システムリカバリセット内のコンポーネントを使用した修復が開始されるか、または障害のログが記録され、手動で修復を完了する必要があります。システム ROM が検証されない場合、サーバーは起動しません。

ファームウェアの検証アクティビティおよびリカバリアクションについて IML をチェックします。

ブレード以外のサーバー

iLO 5 を搭載した Gen10 以降のサーバーで AC 電源が失われた場合は、再びサーバーの電源を入れる前に約 30 秒待つ必要があります。この間に電源ボタンを押すと、電源ボタンが点滅し、要求が保留状態であることを示します。

この遅延は、iLO ファームウェアのロード、認証、およびブートが行われているためです。iLO は、初期化の完了時に保留中の電源ボタン要求を処理します。サーバー電源が切断されていない場合、遅延はありません。30 秒の遅延は、iLO のリセット中のみ発生します。iLO が電源を管理できるようになるまで、電源ボタンは無効になります。

iLO ファームウェアは管理対象電源システムをサポートするために、（たとえば、Hewlett Packard Enterprise 消費電力上限テクノロジーを使用して）電力しきい値を監視し、構成します。iLO が電源を管理できる前にシステムの起動を許可すると、複数のシステムで電圧低下、電圧消失、および温度過負荷が発生する場合があります。AC 電源が失われると電源管理状態が失われるので、電源管理状態を復元し、電源を投入できるように、最初に iLO を起動する必要があります。

C クラスブレードサーバーと Synergy コンピュートモジュール

ProLiant Gen10 以降のブレードサーバーおよび Synergy コンピュートモジュールでは、iLO によってサーバーとエンクロージャーまたはフレームの電源要件が特定され、電源が供給されていることが確認されるまで、サーバーの電源をオンにすることができません。エンクロージャーまたはフレーム内のサーバーに AC 電源が供給されると、わずかな遅延が発生します。ボタンを押してもシステムの電源がオンにならない場合は、詳細について OA（C クラス）または HPE OneView（ProLiant または Synergy）をチェックしてください。問題によってサーバーの電源がオンにならない場合は、イベントが IML に報告されます。

電圧低下からの復旧

電圧低下条件は、動作中のサーバーへの電源が瞬間的に失われるとが発生します。電圧低下の期間およびサーバーハードウェアの構成によっては、電圧低下によりオペレーティングシステムが中断することがありますが、iLO ファームウェアは中断しません。

iLO は、電圧低下を検出し、電圧低下から復旧します。iLO が電圧低下の発生を検出すると、**常に電源オン**が**常に電源をオフのまま**に設定されていない場合、電源オン遅延の後でサーバー電源が復元されます。

電圧低下の復旧後、iLO ファームウェアは、iLO イベントログに `Brown-out recovery` イベントを記録します。

詳しくは

自動電源オン

正常なシャットダウン

iLO のプロセッサーで正常なシャットダウンを実行するには、オペレーティングシステムの協調動作が必要です。正常なシャットダウンを実行するには、Agentless Management Service（AMS）をロードする必要があります。iLO は AMS と通信し、オペレーティングシステムを安全にシャットダウンするための適切な方法を実行して、データの完全性を確保します。

AMS がロードされていない場合、iLO プロセッサーはオペレーティングシステムを使用して、電源ボタンにより正常なシャットダウンを行います。iLO は、オペレーティングシステムを正常にシャットダウンするために、電源ボタンを押す操作（iLO を瞬間的に押す）をエミュレートします。オペレーティングシステムの動作は、オペレーティングシステムの設定と電源ボタンを押す設定によって異なります。

UEFI システムユーティリティのサーマルシャットダウンオプションを使用して、自動シャットダウン機能を無効にできます。この構成では、物理的な損傷が発生する可能性がある極端な条件下の場合を除き、自動シャットダウンを無効にすることができます。

詳しくは

Agentless Management Service

電力効率

iLO を使用すると、高効率モード（HEM）を使用して電力消費を改善できます。HEM は、セカンダリパワーサプライを省電力モードに入れてシステムの電力効率を改善します。セカンダリパワーサプライが省電力モードにある場合は、プライマリパワーサプライがシステムにすべての DC 電力を供給します。各 AC 入力ワット数あたりの DC 出力ワット数が増えるため、パワーサプライがより効率的です。

HEM は、ブレードサーバー以外でのみ使用できます。

システムがプライマリパワーサプライの最大電力出力の 70%を超える電力を使用すると、セカンダリパワーサプライが正常動作に戻ります（省電力モードを終了する）。消費電力がプライマリパワーサプライの 60%未満の容量に低下すると、セカンダリパワーサプライが省電力モードに戻ります。HEM を使用すると、プライマリパワーサプライとセカンダリパワーサプライの最大電力出力に等しい消費電力を実現し、低い消費電力レベルで改善された効率を維持することができます。

HEM は、電源の冗長性に影響しません。プライマリパワーサプライに障害が発生した場合は、セカンダリパワーサプライがただちにシステムへの DC 電力の供給を開始し、停止時間を防止します。

HEM を設定するには、UEFI システムユーティリティを使用します。これらの設定を iLO から行うことはできません。詳しくは、UEFI システムユーティリティユーザーガイドを参照してください。

構成済みの HEM 設定は、**電力情報**ページに表示されます。

詳しくは

電力情報の表示

電源投入時の保護

iLO は、サーバーハードウェアを識別できない場合に、ハードウェアの電源投入を妨げることによって、Synergy コンピュートモジュールの電源投入時の保護を提供します。この状況は、メザニンカードが誤って取り付けられているか、サーバーがハードウェアコンポーネントと通信できない場合に発生する可能性があります。

電源投入時の保護は、自動電源投入および仮想電源ボタンの瞬間的に押す機能と連携して動作します。サーバーの電源がリストアされるか、または瞬間的に押すが要求されたときに、サーバーハードウェアを識別できない場合、サーバーの電源がオンになりません。

電源投入時の保護機能により、サーバーの電源投入が妨げられる場合：

- イベントが IML に記録されます。
- サーバーのヘルスステータスがクリティカルに設定されます。
- HPE OneView がサーバーを管理する場合、SNMP トラップが HPE OneView に送信されます。

詳しくは

自動電源オン
仮想電源ボタンのオプション

電力割り当て（ブレードサーバーおよびコンピュートモジュール）

ブレードサーバーは、エンクロージャーまたはフレームと電力を共有する環境で動作します。サーバーの電源を入れる前に、そのエンクロージャー（ProLiant サーバー）またはフレーム（Synergy コンピュートモジュール）から電力の割り当てを取得する必要があります。

電源投入が妨げられた場合、エラーが IML に記録され、サーバーヘルス LED が変更されます。次のエラーは、電源投入を妨げる場合があります。

- **Electronic Keying または I/O 設定エラー** - サーバーのメザニンデバイスとエンクロージャーの背面のスイッチが一致していません。
- **電力が十分でない** - サーバーに電源を投入するために十分な電力がエンクロージャーで利用できません。
- **冷却が十分でない** - サーバーを冷却するために十分な冷却がエンクロージャーで利用できません。
- **エンクロージャーがビジー状態である** - エンクロージャーがブレードに関する情報を収集中でビジー状態です。サーバーの挿入後にこのエラーが発生し、自動電源投入が有効になっている場合、iLO は許可されるまで電力を要求し続けます。それ以外の場合は、瞬間的に押すボタンをもう一度押してください。
- **Manager プロファイルによる電力保持**（Synergy コンピュートモジュールのみ） - HPE OneView がこのサーバーの電力を保持しました。
- **エンクロージャーエラー**（Synergy コンピュートモジュールのみ） - エンクロージャーエラーが発生しました。

トラブルシューティングについては、ご使用のサーバーのエラーメッセージガイドを参照してください。

サーバー電力の管理

サーバー電力ページの**仮想電源ボタン**セクションは、サーバーの現在の電源状態およびリモートサーバー電源制御オプションを表示します。**システム電源**は、ページが初めて開かれるときのサーバー電源の状態を示します。サーバー電源の状態は、**オン**、**オフ**、または**リセット**のいずれかです。サーバー電源の現在の状態を表示するには、ブラウザーの更新機能を使用します。サーバーは、まれに**リセット**状態に入ることがあります。

前提条件

仮想電源およびリセット権限

手順

1. ナビゲーションツリーで**電力管理**をクリックします。

   サーバー電力タブが選択されたページが開きます。

2. 次のいずれかのボタンをクリックします。

   - **瞬間的に押す**
   - **押し続ける**
   - **リセット**
   - **コールドブート**

   サーバーの電源が入っていない場合、**押し続ける**、**リセット**、および**コールドブート**オプションは使用できません。

3. 要求を確認するメッセージが表示されたら、**OK** をクリックします。

仮想電源ボタンのオプション

- **瞬間的に押す** - 物理的な電源ボタンを押す場合と同じです。サーバーの電源が切れている場合は、瞬間的に押すを押すとサーバーに電源が投入されます。

  一部のオペレーティングシステムは、瞬間的に押した後で適切なシャットダウンを開始するか、またはこのイベントを無視するように構成されている場合があります。Hewlett Packard Enterprise では、仮想電源ボタンを使用してシャットダウンを実行する前に、システムコマンドを使用して正常なオペレーティングシステムのシャットダウンを完了することをお勧めします。

- **押し続ける** - 物理的な電源ボタンを 5 秒間押し続け、離すことと同じです。

  サーバーはこの操作の結果、電源がオフになります。このオプションは、オペレーティングシステムの正常なシャットダウン機能に影響する場合があります。

  このオプションは、一部のオペレーティングシステムが実装している ACPI 機能を提供します。これらのオペレーティングシステムは、瞬間的に押すと押し続けるによって動作が異なります。

- **リセット** - サーバーを強制的にウォームブートします。CPU と I/O リソースがリセットされます。このオプションは、オペレーティングシステムの正常なシャットダウン機能に影響する場合があります。

- **コールドブート** - サーバーからただちに電源を切断します。プロセッサー、メモリ、および I/O リソースは、メインの電力が失われます。サーバーは、約 8 秒後に再起動します。このオプションは、オペレーティングシステムの正常なシャットダウン機能に影響する場合があります。

システム電力リストア設定

システム電源リストア設定セクションでは、電源が喪失した後のシステムの動作を制御できます。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**電力管理**をクリックします。

   ページが開いて**サーバーの電源**タブが選択されています。

2. **サーバーの自動電源オン**の値を選択します。

   サーバーの自動電源オンの値の変更は次回のサーバーの再起動後まで有効にならない場合があります。

3. **電源オン遅延**の値を選択します。

   サーバーの自動電源オンオプションが**常に電源をオフのまま**に設定されている場合、この設定は選択できません。

4. **適用**をクリックします。

自動電源オン

自動電源オン設定は、たとえば、サーバーの電源を接続した場合や、電源障害の後で UPS がアクティブになった場合など、電源のリストア後の iLO の動作を制御します。この設定は、Micro UPS システムではサポートされていません。

次の自動電源オン設定の中から選択します。

- **常に電源オン** - 電源投入の遅延の後でサーバーの電源を入れます。

  このオプションは、サーバーブレードのデフォルト設定です。

- **常に電源をオフのまま** - サーバーは、オンにされるまでオフのまま残ります。

- **最新の電源状態をリストア** - サーバーを、電源が失われたときの電源状態に戻します。サーバーがオン状態だった場合、電源がオンになります。サーバーがオフ状態だった場合、オフのままとなります。

  このオプションは、非ブレードサーバーのデフォルト設定です。

  Synergy コンピュートモジュールがこの設定を使用するように構成されている場合、電源が復旧すると、iLO は以前の電源状態に戻すように試みます。電力不足や冷却不足などの問題が発生した場合、または HPE OneView の電力保持が発生すると、電源状態を戻せない可能性があります。詳しくは、HPE OneView または IML をチェックしてください。

電源オン遅延

電源オン遅延設定は、データセンター内のサーバーの自動電源投入を遅らせます。これは、iLO の起動が完了してからサーバーの電源をオンにするまでの iLO の待機時間を決定します。この設定は、Micro UPS システムではサポートされていません。

サポートされているサーバーで、次の電源オン遅延設定のいずれかを選択します。

- **最小遅延** - iLO の起動が完了した後に電源オンします。
- **15 秒遅延** - 電源投入を 15 秒遅らせます。
- **30 秒遅延** - 電源投入を 30 秒遅らせます。
- **45 秒遅延** - 電源投入を 45 秒遅らせます。
- **60 秒遅延** - 電源投入を 60 秒遅らせます。
- **120 秒までランダム** - 電源投入遅延は変化し、最大 120 秒まで可能です。

15、30、45、60 秒の遅延の値は、c-Class ブレードサーバーまたは Synergy コンピュートモジュールでは使用できません。これらのサーバータイプは、OA、HPE OneView、フレームリンクモジュールのような外部製品によって管理されます。iLO は構成済みの電源オン遅延設定に基づいてサーバーの電源投入を試みますが、実際の起動時間は外部要因の影響を受けることがあります。

サーバー電力使用量の表示

電力メーターグラフは、最新のサーバー電力使用量を表示します。サーバーの電源が切断されているときは、電力履歴情報は収集されません。サーバーの電源が切断されていた期間を含むグラフを表示する場合、グラフには、データが収集されていないことを示すギャップが表示されます。

iLO がリセットされるかサーバーの電源が再投入されると、グラフのデータはクリアされます。たとえば、仮想電源ボタンのリセットまたはコールドブート操作を使用すると、データが消去されます。瞬間的に押したり押し続けたりした場合、データは消去されません。

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- サーバー電源装置とシステム BIOS は、電力読み取りをサポートしています。電力読み取りがサポートされていない場合、このページには次のメッセージが表示されます。`Power Metering is unavailable for this configuration.`（電力メーターは、この構成では利用することができません。）

手順

1. ナビゲーションツリーで**電力および温度**をクリックして、**電力メーター**タブをクリックします。
2. **20 分**または **24 時間**をクリックして、グラフタイプを選択します。

   直近 20 分間または直近 24 時間のグラフを表示できます。
3. （オプション）グラフ表示をカスタマイズするには、以下のチェックボックスを選択またはクリアします。
   - **消費電力上限**
   - **最大**
   - **平均値**
   - **合計 CPU**
   - **合計 GPU**
   - **合計 DIMM**

   サーバーが機能をサポートしていない場合、関連するチェックボックスは表示されません。
4. （オプション）このページでデータを更新する方法を選択します。

   デフォルトで、ページを開いた後にページのデータは自動的に更新されません。
   - 選択したグラフタイプのページデータを更新するには、↻をクリックします。
   - ページデータの自動更新を開始するには、▷をクリックします。選択したグラフのタイプに応じて、□をクリックするか、別のページに移動するまで、ページは自動的に更新されます。

5. （オプション）**ワット**または **BTU/時**をクリックし、iLO 電源単位の優先設定を構成します。

   この値を設定すると、一貫した Web インターフェイス体験が提供されるよう値が cookie に保存されます。電源単位を表示するその他のページにも、これと同じ設定が使用されます。

6. （オプション）グラフ上で特定のポイントのデータを表示するには、グラフの下にあるスライダー〇を目的のポイントに移動します。

   次の方法でスライダーを移動することもできます。

   - スライダートラックをクリックします。
   - スライダーアイコンをクリックし、キーボードの矢印キーを押します。

電力メーターグラフ表示オプション

グラフタイプ

20 分または **24 時間**オプションをクリックし、グラフタイプを選択します。

- **20 分** - 過去 20 分間にわたるサーバーの電力使用量を示します。iLO ファームウェアは、このグラフの電力使用量情報をサーバーから 10 秒ごとに収集します。
- **24 時間** - 過去 24 時間にわたるサーバーの電力使用量を示します。iLO ファームウェアは、このグラフの電力使用量情報を 5 分ごとにアップデートします。

チャートデータ

以下のチェックボックスを使用して、電力メーターグラフに含まれるデータをカスタマイズします。

サーバーが機能をサポートしていない場合、関連するチェックボックスは表示されません。

- **消費電力上限** - サンプル中に設定されている消費電力上限。
  - 消費電力上限は、長期間の平均消費電力を制限します。
  - 消費電力上限は、サーバーの再起動時に維持されないため、起動時に一時的なスパイクが発生します。
  - 消費電力上限を、最大電力とアイドル電力間の指定されたパーセンテージしきい値未満に設定すると、サーバー内の変化によりサーバーにアクセスできなくなることがあります。Hewlett Packard Enterprise は、このしきい値より低い消費電力上限を設定することはお勧めしません。システム構成に対して低すぎる消費電力上限値を構成すると、システムパフォーマンスが低下する可能性があります。
- **最大** - サンプル中の瞬間最高電力。iLO は、秒未満の単位でこの値を記録します。
- **平均** - サンプル中の電力測定値の平均。
- **合計 CPU** - サーバー内のすべての CPU を対象とした電力測定値の合計。

  サーバーがパフォーマンス監視機能をサポートしている場合、この値は、Innovation Engine を使用して取得されるパフォーマンス監視の **CPU 電力**の値と異なる場合があります。
- **合計 GPU** - サーバー内のすべての GPU を対象とした電力測定値の合計。

  この値は次の場合に表示されます。
  - サーバーに 1 つ以上の GPU がインストールされている。
  - OS が実行されている（POST は終了済み）。

- GPU ドライバーが OS にインストールされている。

  Linux および VMware の場合 : NVIDIA オプションカードにはベンダーのドライバーがインストールされ、持続モードが有効になっている必要があります。詳しくは、ベンダーのオプションカードドキュメントを参照してください。

- GPU が電力レポートをサポートしている
- 電力履歴データを利用できる。

· **合計 DIMM** - サーバー内のすべての DIMM を対象とした電力測定値の合計。

電力メーターデータの更新

能力メーターページに移動すると、デフォルトの 20 分のグラフが表示されます。

· 選択したグラフタイプのページデータを更新するには、↻をクリックします。この方法を使用すると、カスタムグラフ設定が保持されます。

· ページデータの自動更新を開始するには、▷をクリックします。選択したグラフのタイプに応じて、□をクリックするか、別のページに移動するまで、ページは自動的に更新されます。

電力単位の表示

ワットまたは **BTU/時**をクリックし、電力読み取り表示をワットまたは BTU/時に変更します。

グラフ上に特定のデータポイントを表示

· グラフ上で特定のポイントのデータを表示するには、グラフの下にあるスライダー○を目的のポイントに移動します。

  次の方法でスライダーを移動することもできます。

  - スライダートラックをクリックします。
  - スライダーアイコンをクリックし、キーボードの矢印キーを押します。

· 自動更新の実行時に、グラフの下にあるスライダー○を動かすと、x 軸方向の特定の履歴ポイントに該当するデータポイントに焦点が当たります。たとえば、20 分のグラフでは、スライダーを-10 分の位置に配置できます。チャートを更新しても、スライダーの位置は 10 分前に設定された値の位置のままになります。

現在の電源状態の表示

前提条件

サーバー電源装置とシステム BIOS は、電力読み取りをサポートしています。電力読み取りがサポートされていない場合、このページには次のメッセージが表示されます。`Power Metering is unavailable for this configuration.`（電力メーターは、この構成では利用することができません。）

手順

ナビゲーションツリーで**電力 & 温度**をクリックして、**電力メーター**タブをクリックします。

電源ステータスセクションに、現在の電源状態の詳細が表示されます。

現在の電源状態の詳細

電力ステータスセクションに表示される情報は、サーバータイプによって変化します。表示される可能性のある値は次のとおりです。

- **現在の電力測定値** - サーバーからの現在の電力測定値。

  この値は、すべてのサーバーについて表示されます。

- **現在の消費電力上限値** - サーバーに対して設定されている消費電力上限。消費電力上限が設定されていない場合、この値は 0 です。

  この値は、ML サーバー、DL サーバー、およびサーバーブレードについて表示されます。消費電力上限をサポートしないサーバーでは表示されません。

- **入力電圧** - サーバーに指定された入力電圧。

  この値は、ML サーバーおよび DL サーバーについて表示されます。

- **パワーレギュレーターモード** - 設定されているモード。設定できる内容については、**電力設定**を参照してください。

  この値は、すべてのサーバーについて表示されます。

- **パワーサプライ容量** - サーバーの電力容量。

  この値は、XL サーバーについて表示されます。

- **ピーク電力測定値** - 最大電力測定値。

  この値は、XL サーバーについて表示されます。

サーバー電力履歴の表示

前提条件

サーバー電源装置とシステム BIOS は、電力読み取りをサポートしています。電力読み取りがサポートされていない場合、このページには次のメッセージが表示されます。`Power Metering is unavailable for this configuration.`（電力メーターは、この構成では利用することができません。）

手順

ナビゲーションツリーで**電力 & 温度**をクリックして、**電力メーター**タブをクリックします。

電力履歴セクションには、サーバーの電力履歴の詳細が表示されます。

電力履歴の詳細

電力の履歴テーブルには、5 分、20 分、24 時間の 3 つの期間で電力測定値を表示します。

- **最大電力** - 指定された期限でのサーバーからの最大電力測定値。サーバーが指定された期限にわたり稼動していない場合は、サーバーの起動時からのすべての測定値の最大値になります。
- **平均電力** - 指定された期限での電力測定値の平均。サーバーが指定された期限にわたり稼動していない場合は、サーバーの起動時からのすべての測定値の平均になります。
- **最小電力** - 指定された期限でのサーバーからの最小電力測定値。サーバーが指定された期限にわたり稼動していない場合は、サーバーの起動時からのすべての測定値の最小値になります。

複数の電源装置がサーバーから同時に削除されると、**電力履歴**セクションまたは**電源メーター**グラフに情報が表示されない短い期間があります。iLO この情報は、搭載されている残りの電源装置に関する情報が収集された後、再度表示されます。iLO

電力設定

電力設定ページを使用すると、サーバーの電力管理機能を表示および制御することができます。このページに表示される電力管理機能は、サーバーの構成によって変化します。

パワーレギュレーターの設定

パワーレギュレーター機能を使用すると、iLO は動作条件に基づいてプロセッサーの周波数レベルと電圧レベルを変更できます。これにより、パフォーマンスへの影響を最小限に抑えながら電力を節約することができます。

注記: パワーレギュレーター機能は、AMD プロセッサーを搭載するサーバーではサポートされません。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**電力管理**をクリックして、**電力設定**タブをクリックします。
2. パワーレギュレーターモードを選択します。
3. **適用**をクリックします。

   サーバーがオフまたは POST 状態の場合、この変更は POST が完了するまで有効になりません。

   ダイナミックパワーセービングモード、 スタティックローパワーモード、およびスタティックハイパフォーマンスモード設定：iLO が、電力レギュレーター設定が変更されたことを通知します。

   OS コントロールモード設定の場合、iLO は、パワーレギュレーター設定の変更を完了するにはサーバーの再起動が必要であることを通知します。

   OS コントロールモードから他のモードに変更すると、サーバーを再起動してパワーレギュレーター設定の変更を完了する必要があります。
4. 変更を完了するために再起動が必要な場合は、サーバーを再起動します。

パワーレギュレーターモード

パワーレギュレーターを設定するときに、以下のモードから選択します。

- **ダイナミックパワーセービングモード** - プロセッサーの利用率に基づいてプロセッサー速度と電力使用量を自動的に変化させます。このオプションにより、パフォーマンスに影響を与えずに全体的な消費電力を減らすことができます。このオプションは、OS のサポートを必要としません。
- **スタティックローパワーモード** - プロセッサー速度を下げ、電力使用量を減らします。このオプションは、システムの最大電力量の値を低く抑えます。パフォーマンスへの影響は、プロセッサーの使用率が高い環境では増大します。

- **スタティックハイパフォーマンスモード** - OS の電力管理ポリシーに関係なく、プロセッサーは常に最大電力および最大パフォーマンスで動作します。
- **OS コントロールモード** - OS が電力管理ポリシーを有効にしない場合、プロセッサーは常に最大電力および最大パフォーマンスで動作します。

消費電力上限の構成

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- サーバーモデルが消費電力上限をサポートしている。

  サポート情報については、サーバーの仕様書を参照してください。

  消費電力上限は、Synergy コンピュートモジュールではサポートされません。
- 消費電力上限値管理機能は、ROM ベースのシステムユーティリティでは有効になっています。

  BIOS 設定をデフォルト値にリセットすると、ROM ベースシステムユーティリティの消費電力上限が無効になります。機能を使用するには、機能を有効にする必要があります。

  ProLiant BL460c サーバーでは、消費電力上限はデフォルトで有効になっています。
- サーバーには、一致しない電源装置の構成はありません。

手順

1. ナビゲーションツリーで**電力管理**をクリックして、**電力設定**タブをクリックします。
2. **手動の電力消費上限を有効**チェックボックスを選択します。
3. **消費電力上限値**をワット数、BTU/時、または割合（%）で入力します。

   %は、最大電力値と最小電力値の差です。

   消費電力上限値は、サーバー最小電力値より下には設定できません。
4. （オプション）値がワット単位で表示されている場合、BTU/時単位での表示に変更するには**値を BTU/時で表示**をクリックします。値が BTU/時で表示されている場合、表示を W に変更するには**値をワットで表示**をクリックします。
5. **適用**をクリックします。

   変更が正常に終了したことが iLO によって通知されます。

消費電力上限の注意事項

- POST 実行中、ROM は最大電力測定値と最小電力測定値を決定する 2 つの電力テストを実行します。

  消費電力上限の構成を決定するときは、**消費電力上限値設定**の表の値を検討してください。
  - **電源定格—最大電力上限**のしきい値（設定可能な最大消費電力上限)。

    サーバーブレードの場合、この値は初期パワーオンリクエスト値です。

ブレード以外のサーバーの場合、この値は電源装置容量です。

- **サーバー最大電力** - サーバーの最大電力測定値。この値は、**最小ハイパフォーマンス上限**のしきい値でもあります。サーバーのパフォーマンスに影響を与えずに設定できる最小の消費電力上限値です。
- **サーバー最小電力** - サーバーの最小電力測定値。この値は、**最小電力上限**のしきい値でもあります。サーバーが使用する最小電力を表します。この値に設定されている消費電力上限は、サーバーの電力使用量を最小化するため、その結果サーバーのパフォーマンスが低下します。

- 消費電力上限を設定した場合は、サーバーの平均電力測定値が、消費電力上限以下にならなければなりません。
- サーバーがエンクロージャー動的消費電力上限に含まれる場合、消費電力上限値設定は無効になっています。

  これらの値は、Onboard Administrator または Insight Control 電力管理を使用して設定と変更を行います。
- 消費電力上限は、一部のサーバーではサポートされていません。詳しくは、サーバーの仕様書を参照してください。
- 一部のサーバーの消費電力上限値設定は、iLO Web インターフェイスの外部で次のようなツールを使用して管理する必要があります。
  - HPE Advanced Power Manager

  サーバーでサポートされる電力管理機能について詳しくは、**https://www.hpe.com/info/qs** でサーバーの仕様書を参照してください。
- 消費電力上限機能は、一致しない電源装置があるサーバーでは無効になります。

バッテリバックアップユニット設定の構成

バッテリバックアップユニットを備えているサーバーに対して電源装置が電源を供給できない場合、サーバーはバッテリバックアップユニットから供給される電源で実行されます。

以下の手順を使用して、サーバーがバッテリバックアップユニットで実行中である場合に iLO が実行する操作を選択します。

注記: システムがスケーラブル永続性メモリ用に構成されている場合、バッテリバックアップユニットの設定は無効になります。

前提条件

iLO 設定の構成権限

手順

1. ナビゲーションツリーで**電力管理**をクリックして、**電力設定**タブをクリックします。
2. **バッテリバックアップユニット設定**セクションで、サーバーがバッテリバックアップユニットで動作している場合に iLO が実行する操作を選択します。
3. **適用**をクリックします。

   変更が正常に終了したことが iLO によって通知されます。

バッテリバックアップユニットのオプション

サーバーがバッテリ電源で動作している場合に、以下のいずれかの操作を実行するように iLO を設定できます。

- **アクションなし**（デフォルト） - サーバーがバッテリ電源で動作しているときは何もしません。電源が回復しない場合、バッテリが消耗するとサーバーの電源は失われます。
- **電源ボタンを一瞬押す** - サーバーがバッテリ電源で 10 秒以上動作していることを iLO が検出した場合、電源ボタンを一瞬押す指示をサーバーに送信します。オペレーティングシステムが電源ボタンの押下に対応するように構成されている場合、オペレーティングシステムはシャットダウンを開始します。

  シャットダウンメッセージを OS に送信 - サーバーがバッテリ電源で 10 秒以上動作していることを iLO が検出した場合、ホストのオペレーティングシステムにシャットダウンメッセージを送信します。必要なサーバー管理ソフトウェアがインストールされている場合、オペレーティングシステムはシャットダウンを開始します。

サーバーがバッテリバックアップユニットをサポートしているかどうかを確認するには、Web サイト（**https://www.hpe.com/info/qs**）でサーバー仕様をご覧ください。

電力しきい値設定超過の SNMP アラートの構成

電力しきい値超過による SNMP アラート機能を使用すると、定義されたしきい値を消費電力が超えたときに SNMP アラートを送信できます。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**電力管理**をクリックして、**電力設定**タブをクリックします。
2. **警告トリガー**リストで値を選択します。
3. **ピーク時消費電力**または**平均消費電力**を選択した場合は、次を入力します。
   - **警告しきい値**
   - **期間**
4. （オプション）**警告しきい値**のワット表示と BTU/時表示を切り替えるには、**値をワットで表示**と**値を BTU/時で表示**のいずれかをクリックします。
5. **適用**をクリックします。

電力しきい値超過による SNMP アラートのオプション

- **警告トリガー** - 警告が、ピーク電力消費量に基づくか、平均電力消費量に基づくか、または無効かを決定します。
- **警告しきい値**—消費電力しきい値を設定します。指定期間にわたって消費電力がこの値を超える場合、SNMP アラートがトリガーされます。
- **持続時間**—SNMP アラートがトリガーされるまでに消費電力が警告しきい値を超えていなければならない時間を分単位で設定します。生成される SNMP アラートは、iLO がサンプリングした電力使用量

のデータに基づいています。**持続時間**の値が変更された正確な日時には基づいていません。5～240分の値を入力します。この値は 5 の倍数でなければなりません。

マウスとキーボードの持続接続の設定

電力設定ページの**その他の設定**セクションを使用すると、キーボードとマウスの持続接続の機能を有効または無効にすることができます。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**電力管理**をクリックして、**電力設定**タブをクリックします。
2. **マウス、キーボードの持続接続**設定を構成します。

   設定が変更されたことが iLO によって通知されます。

その他の設定オプション

マウス、キーボードの持続接続

- **有効** - iLO 仮想キーボードおよびマウスは、iLO UHCI USB コントローラーに常時接続されます。
- **無効**（デフォルト） - iLO 仮想キーボードおよびマウスは、リモートコンソールアプリケーションが開いて iLO に接続したときにのみ、iLO UHCI コントローラーに動的に接続されます。

  この機能を無効にすると、一部のサーバーでは次の場合に 15 ワットの消費電力をさらに節約できます。

  - サーバー OS がアイドル状態である。
  - 仮想 USB キーボードおよびマウスが接続されていない。

  たとえば、24 時間当たりの電力節約は 15 ワット×24 時間、つまり 360 ワット時間（0.36 キロワット時）になります。

電力情報の表示

手順

1. ナビゲーションツリーで**電力管理**をクリックして、**電力**タブをクリックします。

   電力情報ページに表示される情報は、サーバータイプによって変化します。表示される可能性のあるセクションは次のとおりです。

   - **電源装置の概要**
   - **電源装置**
   - **HPE Power Discovery Services**
   - **バッテリバックアップユニット**
   - **Smart Storage Energy Pack**

- **電力測定値**
- **パワーマイクロコントローラー**

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、最後の電源オフ時のものです。ヘルス情報は、サーバーの電源が入っており、POST が完了している場合にのみアップデートされます。

電源装置概要の詳細

このセクションは、ブレード以外のサーバーに対して表示されます。

現在の電力測定値

共有スロット電源装置が取り付けられている場合、サーバーからの最新の電力測定値が表示されます。他の電源装置では、このデータは表示されません。

この値は、通常、すべてのアクティブな電源装置の出力の合計に等しくなりますが、個々の電源装置を読み取るため、変動する場合があります。この値はあくまで参考であり、**電力メーター**ページに表示される値ほど正確ではありません。

パワーマネジメントコントローラーのファームウェアバージョン

パワーマネジメントコントローラーのファームウェアバージョン番号。iLO ファームウェアがこの値を決定するには、サーバーの電源が入っている必要があります。この機能は、一部のサーバーではサポートされません。

電源ステータス

サーバーに供給されている電源の全体的なステータス。

- サーバーの電源装置がインテリジェントタイプではない電源に接続されている場合、このセクションにはサーバー内部の電源装置のステータスが表示されます。
- サーバーの電源装置が iPDU を介して Power Discovery Service に接続されている場合、このセクションにはサーバー内部の電源装置に供給されている電源のステータスが表示されます。

以下の**電源ステータス**値が表示されます。

- **冗長化** - 電源装置に冗長性があることを示します。

  インフラストラクチャに Power Discovery Service が統合されている場合、この値は、内部電源装置に外部から供給されている電源に冗長性があるどうかを示します。
- **非冗長化** - 電源装置または iPDU（Power Discovery Service を使用している場合）の少なくとも 1 つがサーバーに電力を提供していないことを示します。このステータスの最も一般的な原因は、電源装置への入力電力の喪失です。また、同じ iPDU に複数の電源装置が接続されている構成でも、このステータスが発生する場合があります。その場合、個々の電源装置のステータスは**良好、使用中**ですが、**電源ステータス**の値は**非冗長化**です。これは、その iPDU への入力電源が喪失するとサーバーの電源がすべて喪失するからです。
- **冗長化の障害** - 4 つの電源装置をサポートするサーバーでは、このステータスは、サーバーに電力を提供している電源装置の数がサーバーの動作に必要な数よりも少ないことを示します。サーバーは引き続き動作する場合がありますが、この状態では電源問題のリスクが高くなります。電源装置冗長化設定が正しいことを ROM ベースのシステムユーティリティで確認してください。

- **OK** - 共有スロット電源装置は取り付けられていません。インストールされている電源装置は正常に動作しています。
- **N/A** - 電源装置が 1 つのみ搭載されています。この構成では冗長化を適用できません。

Power Discovery Services ステータス

値には、以下のものがあります。

- **冗長化** - サーバーは冗長化 iPDU 構成用に設定されています。
- **非冗長化** - 冗長性をサポートするのに十分な iPDU がないか、またはサーバーの電源装置が同じ iPDU に接続されています。
- **N/A** - iPDU は検出されませんでした。

iLO プロセッサーまたはサーバーがリセットされると、iPDU の検出プロセスの完了に数分間かかる場合があります。

高効率モード

冗長電源装置が構成されている場合に使用される冗長電源装置モード。

値には、以下のものがあります。

- **N/A** - 該当なし。
- **バランスモード** - 取り付けられているすべての電源装置に均一に電力が供給されます。
- **高効率モード（自動）** - 片方の電源装置には完全に電力を供給し、もう一方の電源装置は低い消費電力レベルでスタンバイ状態にします。**自動**オプションではサーバーのシリアル番号に基づいて奇数の電源装置か偶数の電源装置が選ばれるため、ほぼランダムに電力が供給されます。
- **高効率モード（偶数サプライがスタンバイ）** - 奇数番号の電源装置には完全に電力を供給し、偶数番号の電源装置は低い消費電力レベルでスタンバイ状態にします。
- **高効率モード（奇数サプライがスタンバイ）** - 偶数番号の電源装置には完全に電力を供給し、奇数番号の電源装置は低い消費電力レベルでスタンバイ状態にします。
- **サポートされていません** - 取り付けられている電源装置は高性能モードをサポートしていません。

詳しくは

サーバー電力使用量の表示

電源装置のリスト

このリストの一部の値について情報を提供しない電源装置もあります。ある値について電源装置からの情報がない場合は、**N/A** が表示されます。

このセクションは、ブレード以外のサーバー（DL、ML）に対して表示されます。

- **ベイ** - 電源装置のベイ番号。
- **設置** - 電源装置が搭載されているかどうかを示します。指定できる値は、**OK** および**未インストール**です。
- **ステータス** - 電源装置のステータス。表示される値は、ステータスアイコン（**OK**、**劣化**、**障害**、または**その他**）、および詳細情報を提供するテキストを示します。値には、以下のものがあります。

- **不明**
- **良好、使用中**
- **良好、スタンバイ**
- **一般障害**
- **過電圧障害**
- **過電流障害**
- **過熱障害**
- **入力電圧消失**
- **ファン障害**
- **高入力 A/C 警告**
- **低入力 A/C 警告**
- **高出力警告**
- **低出力警告**
- **入口温度警告**
- **内部温度警告**
- **高 Vaux 警告**
- **低 Vaux 警告**
- **電源装置の不一致**

· **PDS** - 搭載された電源装置が Power Discovery Service（電力情報検出機能）用に有効になっているかどうか。

· **ホットプラグ** - 電源装置ベイがサーバーの電源が入った状態での電源装置の交換をサポートするかどうか。この値が**はい**で、電源装置が冗長化の場合は、サーバーの電源がオンのときに電源装置を取り外したり、交換したりすることができます。

· **モデル** - 電源装置のモデル番号。

· **スペア** - スペア電源装置の部品番号。

· **シリアル番号** - 電源装置のシリアル番号。

· **容量** - 電源装置の容量（W）。

· **ファームウェア** - 搭載された電源装置のファームウェアバージョン。

Power Discovery Services iPDU 概要

このセクションは、ブレード以外のサーバーでサーバーの電源装置が iPDU に接続されている場合に表示されます。

iLO をリセットしてから、または iPDU を接続してから、iLO Web インターフェイスに iPDU 概要データが表示されるまで約 2 分かかります。この遅延は、iPDU 検出プロセスによるものです。

ベイ

電源装置のベイ番号。

ステータス

iPDU によって決定される全体的な通信リンクステータスおよびラック入力電源の冗長。表示される可能性がある値は、以下のとおりです。

- **iPDU 冗長化** - この**良好**ステータスは、サーバーが 2 台以上の異なる iPDU に接続されていることを示します。
- **iPDU 非冗長化** - この**警告**ステータスは、サーバーが 2 台以上の異なる iPDU に接続されていないことを示します。このステータスは、次のいずれかの条件が発生すると表示されます。
  - iPDU リンクが、一部の電源装置で確立されていない。
  - 同じ iPDU に 2 台以上の電源装置が接続されている。

    入力電力が同じ iPDU から供給される電源装置について、iPDU の MAC アドレスおよびシリアル番号が同一である。1 台の電源装置が接続の確立を待っている場合、iPDU は**非冗長化**と表示されます。
- **接続を待機中** - この**情報**ステータスは、以下の 1 つまたは複数の条件を示します。
  - 電源装置を iPDU に接続するために正しくない電源コードが使用された。
  - iPDU と iLO プロセッサーが接続プロセス中である。このプロセスには、iLO プロセッサーまたは iPDU をリセットしてから最大 2 分かかります。
  - iPDU モジュールにネットワーク（または IP）アドレスがない。

部品番号

iPDU の製品番号。

シリアル

iPDU のシリアル番号。

MAC アドレス

iPDU ネットワークポートの MAC アドレス。各 iPDU が固有の MAC アドレスを持っているため、この値を参照すると接続されている各 iPDU を特定できます。

iPDU リンク

iPDU の HTTP アドレス（使用できる場合）。インテリジェントモジュラー PDU の Web インターフェイスを開くには、この列のリンクをクリックします。

電力測定値

このセクションは、サーバーブレードと Synergy コンピュートモジュールに対して表示されます。

現在の電力測定値

サーバーからの最新の電力測定値。

この値は、通常、すべてのアクティブな電源装置の出力の合計に等しくなりますが、個々の電源装置を読み取るため、多少変動する場合があります。この値はあくまで参考であり、**電力管理**ページに表示される値ほど正確ではありません。

詳しくは

サーバー電力使用量の表示

パワーマイクロコントローラー

このセクションは、サーバーブレードと Synergy コンピュートモジュールに対して表示されます。

ファームウェアバージョン

パワーマイクロコントローラーのファームウェアのバージョン。

iLO ファームウェアがパワーマイクロコントローラーのファームウェアバージョンを決定するには、サーバーの電源が入っている必要があります。

バッテリバックアップユニットの詳細

バッテリバックアップユニットをサポートするブレード以外のサーバーでは、以下の詳細が表示されます。

- **ベイ** - バッテリバックアップユニットが設置されているベイ。
- **設置** - バッテリバックアップユニットが設置されているかどうか。値には **OK**、**バッテリ障害**、**バッテリ交換**があります。
- **ステータス** - バッテリバックアップユニットのステータス。指定できる値は、**OK**、**劣化**、**障害**、または**その他**です。
- **充電** - バッテリバックアップユニットの充電レベル（%）。充電ステータスの値には、**充電完了**、**放電中**、**充電中**、**低速充電**、**充電していません**があります。
- **シリアル番号** - バッテリバックアップユニットのシリアル番号。
- **容量** - バッテリバックアップユニットの容量（ワット）。
- **ファームウェア** - インストールされているバッテリバックアップユニットのファームウェアバージョン。

Smart Storage Energy Pack のリスト

電力情報ページには、Smart Storage Energy Pack をサポートするサーバーに関する以下の情報が表示されます。

索引

Energy Pack 索引番号です。

装着

Energy Pack の装着状態。表示される値は、**OK** および**未装着**です。

ステータス

Energy Pack のヘルスステータス。表示される値は、**OK**、**劣化**、**障害**、または**その他**です。

モデル

モデル番号。

スペア

スペア Energy Pack の部品番号。

シリアル番号

Energy Pack のシリアル番号。

タイプ

Energy Pack のタイプ。

ファームウェア

インストールされている Energy Pack ファームウェアのバージョン。

電力監視

iLO は、サーバーとオペレーティングシステムの稼動時間が最大になるように、サーバーの電源装置を監視します。電源装置は低電圧などの電気条件による影響を受ける可能性があります。また、不注意で AC コードが外れる場合があります。冗長電源装置が構成されている場合は、これらの条件により冗長性が失われます。冗長電源装置が使用されていない場合は、これらの条件により操作性が失われます。電源装置のハードウェア障害の検出時や、AC 電源コードの切断時には、イベントが IML に記録され、LED インジケーターが使用されます。

iLO プロセッサーは、Power Discovery Service インフラストラクチャの必須コンポーネントです。iLO プロセッサーは、各 Platinum Plus 電源装置に接続されている iPDU と通信して、ラックおよびデータセンターの電源の冗長について判断します。Power Discovery Service インフラストラクチャに iLO プロセッサーが含まれる場合、iLO プロセッサーはサーバーの外部入力電源の冗長化および個々（内部）の電源装置のステータスをインテリジェントに報告します。

詳しくは、次の Web サイトを参照してください。**http://www.hpe.com/jp/info/rackandpower**

高効率モード

高効率モードは、セカンダリ電源装置をスタンバイモードにすることにより、サーバーの電力効率を改善します。セカンダリ電源装置がスタンバイモードにある場合は、プライマリ電源装置がシステムにすべての DC 電力を供給します。電源装置の出力レベルが高いほど電源装置の効率が上がり（AC 入力 W 当たりの DC 出力 W が増加し）、全体的な電力効率が向上します。

高効率モードは、電源の冗長性に影響しません。プライマリ電源装置に障害が発生した場合は、セカンダリ電源装置がただちにシステムへの DC 電力の供給を開始し、停止時間を防止します。冗長電源装置モードは、UEFI システムユーティリティを通じてのみ構成できます。これらの設定を iLO ファームウェアから変更することはできません。

サポートされていないモードを使用するように高効率モードが構成されている場合、電源装置効率が低下する可能性があります。

ファンの構成と表示

最小ファン速度の構成

iLO は、取り付けられたファンが構成された設定よりも遅い速度で動作するのを防ぐ最小ファン速度（パーセンテージ）をサポートしています。サーバーが稼働している場合、ファンは構成された速度以上で動作します。

最小ファン速度が温度構成値より大きい場合、最小ファン速度設定によって、温度構成設定がオーバーライドされます。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**電力管理**をクリックして、**ファン**タブをクリックします。
2. ✎をクリックします。

   ファン設定ページが開きます。
3. 取り付けられているすべてのファンの**最小ファン速度（%）**を入力し、**OK** をクリックします。

温度構成設定の構成

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**電力管理**をクリックして、**ファン**タブをクリックします。
2. ✎をクリックします。

   ファン設定ページが開きます。
3. **温度構成**値を選択します。
4. **OK** をクリックします。

   変更を適用するにはリセットが必要であることが iLO によって通知されます。
5. **はい、適用およびリセット**をクリックします。

   iLO は、変更を保存してリセットします。

   接続が再確立されるまでに、数分かかることがあります。

温度構成設定

最適な冷却

ファンが適切な冷却を行うために必要な最低限の速度に構成されるため、最も効率的な冷却が可能になります。

強化された CPU 冷却

プロセッサーへの冷却を強化することにより、パフォーマンスが向上する可能性があります。

増強した冷却

ファンの速度を上げて動作させます。

最大冷却

システムで使用できる最大の冷却能力を提供します

最小ファン速度が温度構成値より大きい場合、最小ファン速度設定によって、温度構成設定がオーバーライドされます。

ファン情報の表示

ファン情報ページに表示される情報は、サーバー構成によって異なります。

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、最後の電源オフ時のものです。ヘルス情報は、サーバーの電源が入っており、POST が完了している場合にのみアップデートされます。

手順

1. ナビゲーションツリーで**電力管理**をクリックして、**ファン**タブをクリックします。
2. （オプション）冷却ファンの冗長をサポートしているサーバーでは空のファンベイは表示されません。ファンベイを表示するには、**空白のベイを表示**をクリックします。空のファンベイが表示されているときにそれらを非表示にするには、**空白のベイを隠す**をクリックします。

ファン概要の詳細

全体のステータス

取り付けられたファンのヘルスステータスの概要。

冗長性

ファンの冗長性ステータス。

最小ファン速度

取り付けられているすべてのファンの最小速度（0～100%）。サーバーが稼働している場合、ファンは構成された速度以上で動作します。

温度構成

温度構成値。

詳しくは

サブシステムおよびデバイスステータスの値

ファンの詳細

ファンごとに、次の詳細が表示されます。

- **ファン** - ファンの名前。
- **場所** - この値はサーバータイプによって異なります。

  ブレード以外のサーバーの場合、サーバーシャーシ内の場所が表示されます。

  サーバーブレードの場合、位置が**仮想**の仮想ファンが表示されます。
- **冗長化** - ファンのバックアップコンポーネントがあるかどうか。
- **ステータス** - ファンのヘルスステータス。
- **速度** - ファン速度（%）。

詳しくは

サブシステムおよびデバイスステータスの値

ファン

iLO ファームウェアは、ハードウェアとともに、ファンの動作と速度を制御します。ファンはコンポーネントに欠かせない冷却機能によって、信頼性を向上させて動作の継続を維持します。ファンは、システム全体を対象に監視される温度に反応して最小の雑音で十分な冷却機能を提供します。

ファンサブシステムの監視には、十分、冗長化、および非冗長化のファン構成が含まれます。1 つまたは複数のファンが故障しても、サーバーは動作を続けるのに十分な冷却機能を提供します。

ファンの動作ポリシーは、ファンの構成や冷却の需要に応じて、サーバーごとに異なります。ファンの制御はシステムの内部温度を監視し、温度を下げるときはファンの回転速度を上げ、十分に下がったときはファンの回転速度を落とします。ファンの障害が発生した場合、ファンの動作ポリシーによっては、他のファンの回転速度を上げ、イベントを IML に記録したり、LED インジケーターを点灯させたりします。

非冗長化構成または冗長化構成で複数のファンに障害が発生すると、システムの損傷を防ぎ、データの整合性を保証するために十分な冷却機能を提供できなくなる可能性があります。この場合、冷却ポリシーに加えて、オペレーティングシステムとサーバーの適切なシャットダウンが開始される可能性があります。

サーバーブレードには内蔵ファンがないため、エンクロージャーファンを使用して冷却機能を提供します。 **ファン**タブでは、エンクロージャーファンのことを**仮想ファン**と呼んでいます。 **Virtual** ファンの測定値は、サーバーブレードがエンクロージャーに要求している冷却量を表します。サーバーブレードは、各種の温度センサーを調べ、適切なファン速度を計算して、必要な冷却量を計算します。エンクロー

ジャーは、搭載するすべてのサーバーブレードおよびサーバー以外のブレードからの情報を使用して、ファンを調整し、適切なエンクロージャー冷却機能を提供します。

温度情報

温度情報ページには、サーバーシャーシの温度センサーの場所、ステータス、温度、しきい値設定が表示されます。

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、最後の電源オフ時のものです。ヘルス情報は、サーバーの電源が入っており、POST が完了している場合にのみアップデートされます。

温度グラフの表示

手順

1. ナビゲーションツリーで**電力および温度**をクリックして、**温度**タブをクリックします。
2. （オプション）グラフ表示をカスタマイズします。
   - 3 次元グラフを表示するには、**3D** オプションを有効にします。
   - 2 次元グラフを表示するには、**3D** オプションを無効にします。
   - サーバーの前面または背面にあるセンサーを表示するには、**フロントビュー**または**バックビュー**を選択します。
3. （オプション）個々のセンサーの詳細を表示するには、マウスカーソルをグラフ上の円に移動します。

   センサー ID、ステータス、および温度測定値が表示されます。

温度グラフの詳細

温度グラフを表示する場合、グラフ上の円形は、**センサーデータ**テーブルに示されるセンサーに対応します。

グラフ上の色は、温度変化の度合いに当たり、緑色から赤色の範囲で示されます。緑色は温度 0°C、赤色は「クリティカル」しきい値を表します。センサーが測定する温度が上がると、グラフが緑色からオレンジ色に変わり、さらに温度が上がって「クリティカル」しきい値に近づくと赤色になります。

温度センサーデータの表示

手順

1. ナビゲーションツリーで**電力および温度**をクリックして、**温度**タブをクリックします。
2. （オプション）温度が摂氏単位で表示されているときは、**°F** をクリックすると、温度が華氏で表示されます。温度が華氏単位で表示されているときは、**°C** スイッチをクリックすると、温度が摂氏で表示されます。
3. （オプション）デフォルトでは、取り付けられていないセンサーは非表示です。取り付けられていないセンサーを表示するには、**センサーなしの情報を表示**をクリックします。見つからないセンサーが表示されているときにそれらを非表示にするには、**センサーなしの情報を隠す**をクリックします。
4. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

温度センサーの詳細

- **センサー** - 温度センサーの ID。センサーの位置も示します。
- **位置** - 温度が測定されている領域。この列では、**メモリ**は次のものを指します。
  - 物理メモリ DIMM 上の温度センサー。
  - メモリ DIMM の近くにあるが、DIMM 上には置かれていない温度センサー。これらのセンサーは、追加の温度情報を提供するために、DIMM の近くの通気冷却経路をさらに下った場所に配置されています。

  センサー列の温度センサーの ID は、温度センサーの正確な位置を示し、DIMM またはメモリ領域に関する詳細な情報を提供します。
- **X** - 温度センサーの x 座標。
- **Y** - 温度センサーの y 座標。
- **ステータス** - 温度ステータス。
- **読み取り値** - 温度センサーによって記録された温度。温度センサーが取り付けられていない場合、**読み取り値**列には **N/A** という値が表示されます。
- **しきい値** - 過熱状態の警告の温度しきい値です。**警告**と**クリティカル**の 2 つのしきい値が示されます。温度センサーが取り付けられていない場合、**しきい値**列には **N/A** という値が表示されます。

温度の監視

次の温度しきい値が監視されます。

- **警告** - サーバーは、温度を「警告」しきい値未満に維持するように設計されています。

  温度が警告しきい値を超えると、ファンの回転速度が最大になります。

  温度が警告しきい値を 60 秒間超えると、適切なサーバーシャットダウンが試行されます。
- **クリティカル** - 温度が制御不能になった場合または急上昇した場合、高い動作温度によって電子コンポーネント障害が発生する前に、「クリティカル」温度しきい値によりサーバーを物理的にシャットダウンしてシステム障害の発生を防ぎます。

監視ポリシーはサーバーの要件によって異なります。ポリシーには通常、次のものが含まれます。

- ファンの速度を上げて冷却を最大にする。
- IML で温度イベントをログに記録する。
- LED インジケータを使用して、イベントを視覚的に示す。
- データの破損を防ぐために、オペレーティングシステムの正常なシャットダウンを開始する。

温度が高すぎる状態を回避すると、追加のポリシーが実装されます。例：

- ファン速度を標準に戻す。
- イベントを IML に記録する。
- LED インジケータをオフにする。
- 進行中のシャットダウンをキャンセルする（該当する場合）。

注記: Linux および VMware の場合 : メモリ温度センサー付きの NVIDIA オプションカードには、ベンダーのドライバーがインストールされ、持続モードが有効になっている必要があります。詳しくは、ベンダーのオプションカードドキュメントを参照してください。

インレット周囲センサーの事前警告しきい値アラートの構成

`UpperThresholdUser` プロパティを使用すると、インレット周囲センサーの読み取り値がユーザー定義の値以上になったときにトリガーされるアラートを構成できます。このアラートを無効にするには、この値を 0 に設定します。

アラートがトリガーされると、次のイベントが IML に記録されます。

```
Inlet Ambient temperature sensor user defined Pre-Caution threshold exceeded.
```

インレット周囲センサーの読み取り値がユーザー設定値を下回ると、イベントは自動的に修復されます。

手順

1. テキストエディターを開いてファイルを作成し、インレット周囲センサーの事前警告しきい値を定義します。

   テンプレートとして、次の例を使用します。

   ```
   {
   "path":"/redfish/v1/Chassis/1/thermal",
   "body": {"Temperatures": [
                   {
           "UpperThresholdUser": Inlet Ambient Temperature
                                   }
                                   ]
                                  }
   }
   ```

2. ファイルを *ファイル名*.`json` として保存します。
3. RESTful インターフェイスツールを起動します。
4. **`ilorest`** と入力します。
5. iLO システムにログインします。

   ```
   iLOrest > login iLO host name or IP address -u iLO user name -p iLO password
   ```

6. 次のコマンドを入力して、アラートを構成します。

   ```
   rawpatch ファイル名.json
   ```

7. （オプション）構成された設定を表示するには、以下のようにします。

   a. **`Select Thermal`** と入力します。

   b. **`get --refresh Temperatures/UpperThresholdUser`** と入力します。

      以下のような出力が得られます。

      ```
      Temperatures=
                   UpperThresholdUser=Inlet Ambient Temperature
      ```

パフォーマンス管理機能の使用

パフォーマンス管理

選択した HPE Gen10 以降のサーバーでは、以下のサーバーのパフォーマンス管理およびチューニング機能がサポートされています。

- **Workload Matching** - 構成済みのサーバープロファイルを使用して、アプリケーションパフォーマンスを最大化します。
- **Jitter Smoothing** - **プロセッサージッター制御モード**設定を使用して、周波数変動（ジッター）をならしてバランスさせ、低レイテンシを実現します。
- **パフォーマンス監視** - Innovation Engine のサポートによってサーバーでサポートされたセンサーから収集したパフォーマンスデータを表示します。収集したデータに基づいてアラートを構成できます。
- **ワークロードパフォーマンスアドバイザー** - 選択されたサーバーワークロード特性を表示します。監視対象データに基づき、推奨のパフォーマンスチューニング設定を表示したり、構成したりできます。
- **コアブースト** - アクティブなプロセッサーコア間のパフォーマンスを高めるためにこの機能を有効にします。

  この機能は Gen10 サーバーのみでサポートされています。Gen10 Plus サーバーではサポートされていません。

iLO を工場出荷時のデフォルト設定にリセットすると、パフォーマンス管理のすべての設定とデータが削除されます。

iLO のバックアップおよびリストア機能を使用するときは、パフォーマンス管理設定が保持されます。収集されたパフォーマンスデータはバックアップまたはリストアされません。

これらの機能の詳細については、Web サイト **https://www.hpe.com/support/ilo-docs** にある HPE サーバーパフォーマンス管理およびチューニングガイドを参照してください。

Jitter Smoothing 設定の構成

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- 使用する場合、HPE パワーレギュレーターが OS コントロール以外のモードに設定されている。
- サーバーが Innovation Engine をサポートしており、1.2.4 以降のバージョンの Innovation Engine ファームウェアがインストールされている。
- MCTP 検出が有効である。
- 1.20 以降のバージョンのシステム ROM（BIOS）がインストールされている。**プロセッサージッター制御最適化**設定を使用するには、1.40 以降のバージョンが必要です。

- サーバーの電源が入っており、POST が完了している。
- **プロセッサー ジッター コントロール最適化**機能のみの場合：iLO を工場出荷時のデフォルト設定にリセットした場合、サーバー OS が再起動されました。

手順

1. ナビゲーションツリーの**パフォーマンス**をクリックします。

   iLO により**設定**タブが表示されます。
2. **設定**をクリックします。
3. **プロセッサージッター制御モード**を選択します。
4. 該当する場合は、**プロセッサージッター制御周波数（MHz）**を入力します。
5. **プロセッサージッター制御最適化**の値を選択します。
6. **適用**をクリックします。

   iLO に、変更の確認を求めるメッセージが表示されます。
7. **はい**をクリックします。

詳しくは

パワーレギュレーターの設定
インストール済みファームウェア情報の表示

Jitter Smoothing オプション

プロセッサージッター制御モード

この機能は、プロセッサーのジッターを低減または除去します（ジッター平滑化）。使用できる設定は、次のとおりです。

- **自動** - 周波数の変化を監視し、長期的な変動を最小限に抑えるように周波数を自動的に調整します。

  自動を選択した場合、以下の点に注意してください。

  - `intel_idle` ドライバーをロードする特定の Linux ディストリビューションは、C ステートサポートの ACPI レポートを無視します。C ステートサポートの ACPI レポートを無視する Linux ディストリビューションで機能する**自動**モードでは、`intel_idle` ドライバーを無効にする必要があります。

    `intel_idle` ドライバーを無効にするには、カーネルブートコマンドのパラメーターに **`intel_idle.max_cstate=0`** を追加します。
  - **最小プロセッサーアイドル電力パッケージ C ステート**で有効な C ステート値があるときに**自動**を選択した場合、**プロセッサージッター制御周波数（MHz）**は自動的にゼロまで減少し、**プロセッサージッター制御モード**は**無効**に設定されます。C ステート値が有効になっているときは、**自動**値の使用はサポートされません。
- **手動** - プロセッサーを固定周波数で動作させ、ユーザーが低い周波数または高い周波数を静的に選択できるようにします。
- **無効** - **プロセッサージッター制御モード**を無効にします。

ワークロードプロファイルが**仮想化 - 電力効率**に設定されている場合は、このオプションを**自動**にも**手動**にも設定できません。

プロセッサージッター制御周波数（MHz）

プロセッサージッター制御モードが**自動**または**手動**に設定されている場合は、この値を入力します。

- **自動**に構成されている場合は、開始周波数単位を MHz で入力します。許容される最大速度を指定するには、0 を入力します。
- **手動**に構成されている場合は、周波数単位を MHz で入力します。

値は 0～10000 で入力できます。サポートされる周波数範囲はプロセッサーモデルによって異なります。通常は、1,000 MHz～4,000 MHz の範囲内になります。

周波数が MHz 単位で入力され、システムファームウェアにより、プロセッサーで可能な最も近い周波数間隔に切り捨てられます。たとえば、Intel Xeon スケーラブルプロセッサーは、100 MHz の間隔でプログラミングする周波数をサポートしています。ユーザーが 2,050 MHz と入力すると、インストールされているプロセッサーでサポートされている場合は、結果として得られる周波数は 2,000 MHz になります。

プロセッサージッター制御最適化

- **スループットに対して最適化** - しきい値とポーリング率は、スループットが最大になるようにプログラムされます。
- **レイテンシに対して最適化** - しきい値とポーリング率は、低レイテンシになるようにプログラムされます。
- **ゼロレイテンシ** - しきい値とポーリング率は、ゼロレイテンシになるようにプログラムされます。

プロセッサージッター制御モードが**手動**に設定されている場合、この機能は無効です。

iLO を工場出荷時のデフォルト設定にリセットすると、サーバーの OS を再起動するまで**プロセッサージッター制御最適化**は利用できません。

iLO 5 および Always On Intelligent Provisioning を使用したワークロードプロファイルの選択

前提条件

- iLO の設定を構成する権限
- ホスト BIOS 構成権限
- リモートコンソール権限
- 1.20 以降のバージョンのシステム ROM（BIOS）がインストールされている。
- サーバーが Innovation Engine をサポートしている。

  Innovation Engine をサポートしていないサーバーでは、**パフォーマンス**ページは表示されません。Innovation Engine がサポートされているかどうかを確認するには、**インストールされたファームウェア**ページで Innovation Engine ファームウェアを検索します。
- MCTP 検出が有効である。
- サーバーの電源が入っており、POST が完了している。
- 最新バージョンの Intelligent Provisioning がインストールされている。

手順

1. ナビゲーションツリーの**パフォーマンス**をクリックします。

   iLO により**設定**タブが表示されます。

2. **設定**をクリックします。

3. Intelligent Provisioning を開始するには、**Always On で構成**をクリックします。

   Intelligent Provisioning Web インターフェイスが新しいブラウザーウィンドウで起動します。

4. **メンテナンスの実行**をクリックします。

5. **BIOS/プラットフォーム構成**をクリックします。

   BIOS/プラットフォーム構成ページが開きます。

6. **ワークロードプロファイル**リストからプロファイルを選択します。

   注記: ワークロードプロファイルを自動的に選択すると、RBSU の**電力およびパフォーマンスオプション**画面で多くのオプションが構成されます。自分で電力とパフォーマンスのオプションを変更するには、**ワークロードプロファイル**リストから**カスタム**を選択します。

   変更は保留中です。**変更の表示**をクリックすると、古い設定と新しい設定を表示できます。

7. **アップデート**をクリックします。

   Intelligent Provisioning は変更を適用し、変更を有効にするにはサーバーの再起動が必要であることを通知します。

8. サーバーを再起動します。

詳しくは

インストール済みファームウェア情報の表示

ワークロードプロファイル

サーバーのパフォーマンスを向上させるには、以下のシステム生成のワークロードプロファイルを使用できます。

一般的な電力効率のコンピューティング

最も一般的なパフォーマンスと電源管理の設定を適用します。BIOS 設定をチューニングしないでワークロードに一致させるユーザーにお勧めします。

一般的なピーク周波数コンピューティング

個々のコアに可能な最大周波数を達成するパフォーマンスと電力管理設定を適用します。計算時間の短縮による恩恵を受けるワークロードにお勧めします。

一般的なスループットのコンピューティング

最大合計持続スループットを達成するパフォーマンスと電力管理設定を適用します。NUMA（不均一メモリアクセス）の認識をサポートするように最適化されています。

仮想化 - 電力効率

すべての仮想化オプションを有効にするパフォーマンスの設定を適用します。電源設定を管理して、仮想化を妨げないようにします。仮想化環境にお勧めします。

このワークロードプロファイルが選択されていると、**Jitter Smoothing** 設定の**プロセッサージッター制御モード**機能を有効にできません。

仮想化 - 最大パフォーマンス

すべての仮想化オプションを有効にするパフォーマンスの設定を適用します。最適なパフォーマンスを実現する電源設定を無効にします。仮想化環境にお勧めします。

低レイテンシ

速度とスループットの低減を適用し電力管理を無効にして、全体的なコンピューティング遅延を低減します。RTOS（リアルタイムオペレーティングシステム）のワークロード、または遅延の影響を受けやすい他のワークロードにお勧めします。

ミッションクリティカル

高度なメモリ RAS（信頼性、可用性、および保守性）機能を管理します。このプロファイルは、基本的なサーバーのデフォルト値を上回るサーバー信頼性とパフォーマンスの妥協点を探る顧客によって使用されるためのものです。

トランザクションアプリケーション処理

最大周波数とスループットを管理します。バックエンドデータベースを必要とする OLTP（オンライントランザクション処理）アプリケーションを使用する環境を処理する場合にお勧めします。

ハイパフォーマンスコンピューティング（HPC）

持続する使用可能な帯域幅とプロセッサーの演算能力を最適化する電力管理を無効にします。従来の HPC 環境を実行するユーザーにお勧めします。

意思決定サポート

このプロファイルは、データマイニングや OLAP（オンライン分析処理）など、データウェアハウスに対する操作またはアクセスに焦点を合わせたエンタープライズビジネスデータベース（ビジネスインテリジェンス）のワークロードを対象にしています。

グラフィック処理

電力管理と仮想化を無効にして、I/O とメモリ間の帯域幅を最適化します。GPU（グラフィックス処理ユニット）を使用するサーバーで実行するワークロードにお勧めします。

I/O スループット

I/O とメモリ間のリンクに影響を与える電力管理機能を無効にします。I/O とメモリ間の最大帯域幅に依存する構成にお勧めします。

カスタム

ワークロードのプロファイルを無効にします。特定の BIOS オプションを設定するユーザーにお勧めします。

iLO 5 および Always On Intelligent Provisioning を使用したコアブーストの構成

前提条件

- iLO の設定を構成する権限
- ホスト BIOS 構成権限
- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- サーバーがコアブーストプロセッサーで構成されている。

- 1.20 以降のバージョンのシステム ROM（BIOS）がインストールされている。
- サーバーが Innovation Engine をサポートしており、1.2.4 以降のバージョンの Innovation Engine ファームウェアがインストールされている。
- MCTP 検出が有効である。
- サーバーの電源が入っており、POST が完了している。
- 最新バージョンの Intelligent Provisioning がインストールされている。

手順

1. ナビゲーションツリーの**パフォーマンス**をクリックします。

   iLO により**設定**タブが表示されます。
2. **設定**をクリックします。
3. Intelligent Provisioning を開始するには、**Always On で構成**をクリックします。

   Intelligent Provisioning Web インターフェイスが新しいブラウザーウィンドウで起動します。
4. **メンテナンスの実行**をクリックします。
5. **BIOS/プラットフォーム構成**をクリックします。

   BIOS/プラットフォーム構成ページが開きます。
6. **電力およびパフォーマンスオプション**をクリックします。
7. **アドバンストパフォーマンスチューニングオプション**をクリックします
8. **コアブースト**オプションを選択します。

   変更は保留中です。
9. **BIOS/プラットフォーム構成**をクリックして概要ページに戻ります。
10. **アップデート**をクリックします。

    Intelligent Provisioning は変更を適用し、変更を有効にするにはサーバーの再起動が必要であることを通知します。
11. サーバーを再起動します。

詳しくは

インストール済みファームウェア情報の表示

コアブーストのオプション

有効

この機能を有効にすると、サーバーは、コアブーストをサポートするプロセッサーの強化されたパフォーマンス機能を使用できます。

有効化は、コアブーストプロセッサーが搭載されていることをシステムが検出したときのデフォルト値です。

無効

この機能を無効にすると、プロセッサーではターボ周波数プロファイルが制限され、最大電力容量が低下します。

パフォーマンス設定の表示

サーバーが POST 中の場合、このページの情報は、最後に電源が切れた時点の情報になります。**パフォーマンス設定**ページの情報は、サーバーの電源が入っており、POST が完了している場合にのみアップデートされます。

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- サーバーが Innovation Engine をサポートしている。
- MCTP 検出が有効である。
- サーバーの電源が入れられる。

手順

ナビゲーションツリーの**パフォーマンス**をクリックします。

iLO により**設定**タブが表示されます。

プロセッサージッター制御モードが有効のとき、現在の設定と構成済みの設定の両方が**プロセッサージッター制御周波数**設定にリストされます。

詳しくは

インストール済みファームウェア情報の表示

パフォーマンス監視

パフォーマンス - 監視ページには、Innovation Engine のサポートによってサーバーの次のセンサーから収集されたパフォーマンスデータが表示されます。

CPU 使用率

このセンサーは、システムに搭載されているすべてのプロセッサーの使用率を報告します。測定値は、プロセッサーの最大演算能力のパーセンテージに基づいています。作業時のプロセッサーの動作速度が考慮されます。この測定値は、プロセッサーがアイドル状態でない頻度によって計算されることがよくある使用率に関して一部のオペレーティングシステムが報告する値とは異なる場合があります。

メモリバス使用率

このセンサーは、メモリバスの総帯域幅の使用率を報告します。測定値は、構成の最大メモリ帯域幅のパーセンテージに基づいています。この測定値は、使用可能なシステムメモリのうち使用されている部分、または割り当て済みの部分によって計算されることがよくあるメモリ使用率に関して一部のオペレーティングシステムが報告する値とは異なる場合があります。

I/O バス使用率

このセンサーは、I/O バスに接続されているすべてのプロセッサー（PCI-e バス総帯域幅）の使用率を報告します。この測定値は、それらのバスの最大総帯域幅のパーセンテージに基づいています。この測定値は、I/O デバイスのビジー状態の程度を示すものではなく、デバイスが使用している PCI-e 帯域幅の量を示すものです。

CPU インターコネクト使用率

このセンサーは、システム内の複数のプロセッサーソケットを接続するリンクの計算で得られた帯域幅使用率を報告します。これはシステム内のすべてのリンクの集約です。

Jitter カウント

このセンサーは、毎秒発生するプロセッサー周波数の変化または「揺らぎ」の割合を報告します。

平均 CPU 周波数

このセンサーは、全体の平均的なプロセッサー周波数を報告します。ゼロの値は、プロセッサーがアイドル状態であることを意味します。この値は、プロセッサーがアイドル状態でない場合のみ周波数を測定する一部のオペレーティングシステムでよく見られる「実行時の周波数」とは異なります。

CPU 電力

このセンサーは、プロセッサーが消費する電力を報告します。これはプロセッサー内の電力アキュムレータに基づいており、プロセッサーが電力制限の内部調整に使用する値です。

このページの情報は、Innovation Engine を使用せずに取得される**電力メーター**ページの**合計 CPU** 電力データとは異なる場合があります。

パフォーマンスデータの表示

パフォーマンス監視グラフに、Innovation Engine ファームウェアから収集された最新のデータが表示されます。

サーバーが電源オフまたは POST 状態のとき、メッセージが表示され、パフォーマンス測定値に **0** の値が表示されます。サーバーの電源がオンで POST が完了していると、パフォーマンスデータがアップデートされます。リセット後、グラフの値が **0** の場合がありますが、これはサーバーがオフまたは POST のときにデータが収集されていなかったことになります。これらの値がサーバーリセットのためであることを確認するには、IML を調べます。

iLO をリセットすると：

- **10 分**および **1 時間**間隔のパフォーマンスデータがクリアされます。
- **24 時間**および **1 週間**グラフのデータが保存され、リセットが完了した後に表示できます。
- リセットが完了した後で **24 時間**および **1 週間**のグラフを表示すると、毎時データがなくなっている場合があります。

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

  ライセンスがインストールされていない場合、メッセージが表示されて、10 分間のみグラフが表示されます。
- サーバーが Innovation Engine をサポートしており、2.0.11 以降のバージョンの Innovation Engine ファームウェアがインストールされている。
- MCTP 検出が有効である。
- **iLO 日付/時刻**が正しく設定され、有効なパフォーマンステレメトリーサンプルが確実に収集されている。

手順

1. ナビゲーションツリーで**パフォーマンス**をクリックし、**監視**タブをクリックします。
2. **選択されたセンサー**メニューでセンサーを選択します。
3. 次のいずれかのオプションをクリックしてグラフの間隔を選択します。

- **10 分**
- **1 時間**
- **24 時間**
- **1 週間**

グラフには、要求した間隔のデータが表示されます。

4. （オプション）グラフ上で特定のポイントのデータを表示するには、グラフの下にあるスライダー○を目的のポイントに移動します。

   スライダーを動かすと、グラフ上の選択ポイントの詳細がグラフの横に表示されます。

5. （オプション）**CPU 電力**または**平均 CPU 周波数**を選択した場合、グラフの横にある CPU リスト内のチェックボックスをオンまたはオフにします。

   CPU のチェックボックスを選択すると、グラフに表示されます。CPU のチェックボックスをクリアすると、グラフから除去されます。

6. （オプション）このページでデータを更新する方法を選択します。

   デフォルトで、ページを開いた後にページのデータは自動的に更新されません。

   - 選択したグラフタイプのページデータを更新するには、↻をクリックします。
   - ページの自動更新を開始するには、▷をクリックします。選択したグラフのタイプに応じて、ページは 10 秒または 5 分間隔で更新されます。□をクリックするか、別のページに移動するまで、ページは自動的に更新されます。

詳しくは

インストール済みファームウェア情報の表示
MCTP 検出の構成

パフォーマンスデータの詳細

パフォーマンスデータセクションには、次の詳細が表示されます。

センサー

選択したセンサーの名前。

最大

最大の測定値。

最小

最小の測定値。

パフォーマンス監視のグラフ表示オプション

選択されたセンサーメニュー

センサーのパフォーマンスデータを表示するには、**選択されたセンサー**メニューでセンサーを選択します。

グラフタイプ

グラフの期間を指定するには、グラフタイプ名をクリックします。

- **10 分** - 直近の 10 分間のパフォーマンスデータを表示します。iLO ファームウェアは、20 秒ごとにこのグラフのパフォーマンスデータを収集します。グラフに表示されるサンプルの最大数は 30 です。
- **1 時間** - 直近の 1 時間のパフォーマンスデータを表示します。iLO ファームウェアは、20 秒ごとにこのグラフのパフォーマンスデータを収集します。グラフに表示されるサンプルの最大数は 180 です。
- **24 時間** - 直近の 24 時間のパフォーマンスデータを表示します。iLO ファームウェアは、5 分ごとにこのグラフのパフォーマンスデータを収集します。グラフに表示されるサンプルの最大数は 288 です。
- **1 週間** - 先週のパフォーマンスデータを表示します。iLO ファームウェアは、30 分ごとにこのグラフのパフォーマンスデータを収集します。グラフに表示されるサンプルの最大数は 336 です。

パフォーマンスグラフを更新

- 選択したグラフタイプのページデータを更新するには、↻をクリックします。
- ページの自動更新を開始するには、▷をクリックします。

  □をクリックするか、別のページに移動するまで、ページは自動的に更新されます。

グラフ上に特定のデータポイントを表示

- グラフ上で特定のポイントのデータを表示するには、グラフの下にあるスライダー○を目的のポイントに移動します。

  次の方法でスライダーを移動することもできます。

  - スライダートラックをクリックします。
  - スライダーアイコンをクリックし、キーボードの矢印キーを押します。

  スライダーを動かすと、グラフ上の選択ポイントの詳細がグラフの横に表示されます。
- 自動更新の実行時に、グラフの下にあるスライダー○を動かすと、x 軸方向の特定の履歴ポイントに該当するデータポイントに焦点が当たります。

パフォーマンスアラートの構成

構成されたしきい値に達した場合に IML にイベントを POST するパフォーマンスアラートを構成できます。

CPU 使用率、メモリバス使用率、および I/O バス使用率のセンサーで上限と下限のしきい値がサポートされます。

CPU インターコネクト使用率、CPU 電力、および Jitter カウントのセンサーで上限しきい値がサポートされます。

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- サーバーが Innovation Engine をサポートしており、2.0.11 以降のバージョンの Innovation Engine ファームウェアがインストールされている。

- MCTP 検出が有効である。
- **iLO 日付/時刻**が正しく設定され、有効なパフォーマンステレメトリーサンプルが確実に収集されている。

手順

1. ナビゲーションツリーで**パフォーマンス**をクリックし、**監視**タブをクリックします。
2. パフォーマンスアラートをサポートするセンサーを選択します。
3. しきい値設定と滞留時間を入力し、**適用**をクリックします。

   アラートを無効にするには、滞留時間を 0 に設定します。

詳しくは

インストール済みファームウェア情報の表示

パフォーマンスアラートの設定オプション

しきい値下限

イベントが IML にポストされる前にセンサーが報告できる最小値。

使用率のパーセンテージを入力します。

しきい値上限

イベントが IML にポストされる前にセンサーが報告できる最大値。

- 使用率のセンサーの場合は、選択したセンサーの使用率のパーセンテージを入力します。
- CPU 電力の場合は、値をワット単位で入力します。
- Jitter カウントの場合は、しきい値カウントを入力します。

滞留時間

しきい値に違反するまでの、センサーの測定値が構成済みの値を上回るまたは下回る秒数。しきい値に違反すると、イベントが IML にポストされます。

たとえば、しきい値上限を 70%、滞留時間を 40 秒に設定した場合、センサーが 70%を超える測定値を 40 秒を超えて報告するとイベントがポストされます。

- アラートを有効にするには、20～64800（20 秒～18 時間）の範囲で、滞留時間を 20 の倍数の有効な値に設定します。20 の倍数でない値を入力した場合、値は次の 20 の倍数に切り上げられます。
- アラートを無効にするには、滞留時間を 0 に設定します。

ワークロードアドバイザー

iLO は選択したサーバーワークロード特性を監視し、監視対象のデータに基づいてパフォーマンス調整の推奨設定を提供します。

サーバーワークロード詳細の表示

前提条件

- ホスト BIOS 構成権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- サーバーの電源が入っており、POST が完了している。

  監視する時間間隔でサーバーの電源が入れられたことを確認します。たとえば、24 時間間隔のデータは、サーバーの電源が 24 時間入っていないと表示されません。
- サーバーが Innovation Engine をサポートしており、2.0.11 以降のバージョンの Innovation Engine ファームウェアがインストールされている。
- MCTP 検出が有効である。
- **iLO 日付/時刻**が正しく設定され、有効なパフォーマンステレメトリーサンプルが確実に収集されている。

手順

1. ナビゲーションツリーで**パフォーマンス**をクリックし、**ワークロードアドバイザー**タブをクリックします。
2. 詳細を**サーバーワークロード**セクションで確認します。

   iLO がリセットされた場合、**10 分**間隔の情報はサーバーの電源が 10 分入れられた後で、**1 時間**間隔の情報はサーバーの電源が 1 時間入れられた後で表示されます。
3. （オプション）テーブルを最新情報にアップデートするには、↻をクリックします。

詳しくは

MCTP 検出の構成
インストール済みファームウェア情報の表示
iLO SNTP 設定の構成

サーバーワークロードの詳細

ワークロードの特性とは、ワークロードがシステムリソースをどのように使用しているかについての質的評価です。これらはパフォーマンス監視イベントから得た定量的な測定値に基づいており、チューニングの決定を行うときの参考として役立ちます。このように観測された特性が、通常はインテリジェントなチューニング決定を行う際に必要となります。たとえば、特定の BIOS オプションがメリットをもたらすのはワークロードの NUMA 認識が高い場合に限られます。

以下のワークロード特性が表示されます。

- **CPU 使用率**-サーバー内でプロセッサーはどれだけビジーかです。
- **メモリバス使用率**-サーバーにより観測されるメモリトラフィックの量です。
- **I/O バス使用率**-サーバーにより観測される I/O トラフィックの量です。
- **NUMA 認識**-ワークロードがメモリおよび I/O アクセスを複数のプロセッサーにどのように分散しているかです。NUMA 認識が高いということは、I/O およびメモリトラフィックがリモートリソースよりもローカルリソースに向けられていることを意味します。

表示される値は**高**、**中**、**低**です。

10 分および **1 時間**間隔のサーバーワークロードデータは、iLO がリセットされるとクリアされます。

パフォーマンスチューニングオプションの構成

前提条件

- ホスト BIOS 構成権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- サーバーの電源が入っており、POST が完了している。

  監視する時間間隔でサーバーの電源が入れられたことを確認します。たとえば、**24 時間**間隔のデータおよび推奨事項は、サーバーの電源が 24 時間入れられるまで使用できません。
- サーバーが Innovation Engine をサポートしており、2.0.11 以降のバージョンの Innovation Engine ファームウェアがインストールされている。
- MCTP 検出が有効である。
- **iLO 日付/時刻**が正しく設定され、有効なパフォーマンステレメトリーサンプルが確実に収集されている。

手順

1. ナビゲーションツリーで**パフォーマンス**をクリックし、**ワークロードアドバイザー**タブをクリックします。
2. **選択された間隔**メニューで値を選択します。

   10 分、**1 時間**、または **24 時間**間隔で収集されたデータに基づいて推奨設定を確認できます。
3. 推奨事項を**推奨設定**列で確認します。

   iLO がリセットされた場合、**10 分**間隔の情報はサーバーの電源が 10 分入れられた後で、**1 時間**間隔の情報はサーバーの電源が 1 時間入れられた後で表示されます。
4. 1 つまたは複数の設定を変更するには、**設定**をクリックします。
5. 必要に応じて、チューニングオプションを変更し、**適用**をクリックします。

   iLO は、チューニングオプションの変更によって**ワークロードプロファイル**設定が**カスタム**に変更されることを通知します。
6. **はい、適用します**をクリックします。

   iLO は設定を保存し、変更を有効にするにはサーバーの再起動が必要であることを通知します。
7. サーバーを再起動します。

   ステータスバナーのリンクをクリックして、**サーバーの電源**ページに移動できます。

詳しくは

MCTP 検出の構成
インストール済みファームウェア情報の表示
iLO SNTP 設定の構成

パフォーマンスチューニングの設定

Sub-NUMA クラスタリング

このオプションが**有効**に設定されている場合、プロセッサーコア、キャッシュ、およびメモリはこの機能によって複数の NUMA ドメインに分割されます。NUMA に対応し、最適化されているワークロードでは、この機能を有効にするとパフォーマンスが向上する可能性があります。

この機能を有効にした場合、最大 1GB のシステムメモリが使用できなくなる場合があります。

NUMA グループサイズ最適化

このオプションは、NUMA ノードのサイズ（論理プロセッサー数）をシステム BIOS が報告する方法を構成します。これは、アプリケーションの使用法に応じてプロセッサーをグループ化（Kgroups）することに関して OS を支援します。デフォルト値の**クラスター**は、グループが NUMA の境界に沿って最適化されるため、より良いパフォーマンスが提供されます。一部のアプリケーションは、複数のグループにまたがるプロセッサーを利用するように最適化されない場合があります。このような場合、影響を受けるアプリケーションでより多くの論理プロセッサーが使用されるように、**フラット**オプションを選択することが必要になることがあります。

アンコア周波数のスケーリング

このオプションは、プロセッサーの内部バス（アンコア）の周波数のスケーリングを制御します。このオプションを**自動**に設定すると、プロセッサーはワークロードに基づいて周波数を動的に変更できます。**最大**または**最小**の周波数を設定すると、レイテンシおよび消費電力の調整ができます。

メモリリフレッシュレート

このオプションでは、メモリコントローラーのリフレッシュレートを調整できます。サーバーのメモリのパフォーマンスと耐障害性に影響する場合があります。サーバーの他のドキュメントでデフォルト値 （**1x リフレッシュ**）の変更が推奨されない限り、Hewlett Packard Enterprise はデフォルト値の使用をお勧めします。

パワーレギュレーター

このオプションを使用すると、パワーレギュレーターのサポートを構成できます。以下の値を使用できます。

- **ダイナミックパワーセービングモード** - プロセッサーの利用率に基づいてプロセッサー速度と電力使用量を自動的に変化させます。このオプションにより、パフォーマンスに影響を与えずに全体的な消費電力を減らすことができます。このオプションは、OS のサポートを必要としません。
- **スタティックローパワーモード** - プロセッサー速度を下げ、電力使用量を減らします。このオプションは、システムの最大電力量の値を低く抑えます。パフォーマンスへの影響は、プロセッサーの使用率が高い環境では増大します。
- **スタティックハイパフォーマンスモード** - OS の電力管理ポリシーに関係なく、プロセッサーは常に最大電力および最大パフォーマンスで動作します。
- **OS コントロールモード** - OS が電力管理ポリシーを有効にしない場合、プロセッサーは常に最大電力および最大パフォーマンスで動作します。

注記: ワークロードパフォーマンスアドバイザーページに表示されるパワーレギュレーター設定には、ブート時の静的構成が反映されます。これには、システムの電源投入後に適用された、この設定への実行時の変更は反映されません。**ワークロードパフォーマンスアドバイザー**ページの推奨設定の変更を適用すると、この設定のブート時の構成だけが変更されます。変更を有効にするには、システムの再起動が必要です。

最小プロセッサーアイドル電力パッケージ C ステート

このオプションを使用して、オペレーティングシステムが使用するプロセッサーの最小アイドル電力状態（C ステート）を選択します。C ステートを高く設定すればするほど、そのアイドル状態の消費

電力は少なくなります。プロセッサーがサポートする最も低いアイドル電力状態は、**C6 ステート**です。

エネルギー/パフォーマンスバイアス

このオプションを使用して、プロセッサーのパフォーマンスと消費電力を最適化するように複数のプロセッサーサブシステムを構成します。以下の値を使用できます。

- **最大パフォーマンス** - この設定は、最高のパフォーマンスと最低のレイテンシを必要とし、消費電力にこだわらない環境で使用してください。
- **パフォーマンスに最適化** - この設定では、電力効率が最適化されます。Hewlett Packard Enterprise は、ほとんどの環境でこの設定を推奨します。
- **電力に最適化** - サーバーの使用率に基づいて電力効率が最適化されます。
- **パワーセービングモード** - この設定は、消費電力に関する制約が厳しく、パフォーマンスの低下を容認できる環境に適しています。

iLO ネットワーク設定の構成

iLO ネットワーク設定

ネットワーク設定にアクセスするには、ナビゲーションツリーでアクティブな NIC を選択し、次のページでネットワーク設定を表示または編集します。

- **ネットワーク概要**
- **ネットワーク共通設定**
- **IPv4 設定**
- **IPv6 設定**
- **SNTP 設定**

アクティブでない NIC を選択すると、その NIC を使用するように iLO が構成されていないことを通知するメッセージが表示されます。

ネットワーク構成の概要の表示

手順

ネットワーク構成に応じて、ナビゲーションツリーで **iLO 専用ネットワークポート**または **iLO 共有ネットワークポート**をクリックします。

ネットワーク概要タブが表示されます。

ネットワーク情報の概要

- **使用中の NIC** - アクティブな iLO ネットワークインターフェイス（iLO 専用ネットワークポートまたは iLO 共有ネットワークポート）の名前。
- **iLO ホスト名** - iLO サブシステムに割り当てられた完全修飾ネットワーク名。デフォルトで、ホスト名は **ILO**+システムのシリアル番号および現在のドメイン名です。この値はネットワーク名に使用され、一意である必要があります。
- **MAC アドレス** - 選択している iLO ネットワークインターフェイスの MAC アドレス。
- **リンク設定** - 選択した iLO ネットワークインターフェイスのリンク設定。デフォルト値は自動ネゴシエートです。
- **現在のリンク速度** - ネットワークインターフェイスのリンク速度（メガビット/秒）。
- **デュプレックス設定** - 選択している iLO ネットワークインターフェイスのリンクデュプレックス設定。デフォルト値は自動ネゴシエートです。
- **現在のデュプレックスモード** - デュプレックスモード（全二重または半二重）。

iLO ホスト名および NIC 設定は、**ネットワーク共通設定**ページで構成できます。

共有ネットワークポートが有効な場合は、**リンク設定**オプションや**デュプレックス設定**オプションは変更できません。共有ネットワークポート構成では、オペレーティングシステムでリンク設定を管理する必要があります。

IPv4 概要の詳細

- **DHCPv4 ステータス** - IPv4 で DHCP が有効かどうかを示します。
- **アドレス** - 現在使用中の IPv4 アドレス。値が `0.0.0.0` の場合、IPv4 アドレスは設定されていません。
- **サブネットマスク** - 現在使用中の IPv4 アドレスのサブネットマスク。値が `0.0.0.0` の場合、アドレスは構成されていません。
- **デフォルトゲートウェイ** - IPv4 プロトコルで使用されているデフォルトゲートウェイアドレス。値が `0.0.0.0` の場合、ゲートウェイは構成されていません。

IPv6 概要の詳細

DHCPv6 ステータス

IPv6 で DHCP が有効かどうかを示します。表示される値は、以下のとおりです。

- **有効** - ステートレスおよびステートフルな DHCPv6 が有効になっています。
- **有効（ステートレス）** - ステートレスな DHCPv6 のみが有効になっています。
- **無効** - DHCPv6 が無効になっています。

IPv6 ステートレスアドレス自動構成（SLAAC）

IPv6 で SLAAC が有効かどうかを示します。SLAAC が無効の場合でも、iLO の SLAAC リンクローカルアドレスは必要なため構成されます。

IPv6 アドレスリスト

このテーブルには、iLO に対して現在構成されている IPv6 アドレスが表示されます。テーブルには、次の情報が表示されます。

ソース

アドレスのタイプ。

IPv6

IPv6 アドレス。

プレフィックス長

アドレスプレフィックスの長さ。

ステータス

アドレスのステータス。値には、以下のものがあります。

- **アクティブ** - アドレスは iLO によって使用中です。
- **保留** - 重複したアドレスの検出が進行中です。

- **障害** - 重複したアドレスの検出に失敗しました。アドレスは iLO によって使用されていません。
- **無効** - アドレスプレフィックスの RA（Router Advertised）有効存続期間は更新されず、期限が切れました。このアドレスはもう使用されていません。

デフォルトゲートウェイ

使用されているデフォルト IPv6 ゲートウェイアドレス。IPv6 では、iLO は使われる可能性があるデフォルトゲートウェイアドレスのリストを維持します。このリスト内のアドレスは、ルーターアドバタイズメッセージおよび IPv6 **静的デフォルトゲートウェイ**設定を元に生成されます。

静的デフォルトゲートウェイは、IPv6 ページで設定します。

ネットワーク共通設定

iLO 専用ネットワークポートまたは iLO 共有ネットワークポートの**ネットワーク共通設定**ページを使用して、iLO ホスト名と NIC 設定を構成します。

iLO ホスト名の設定

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで **iLO 専用ネットワークポート**または **iLO 共有ネットワークポート**をクリックします。
2. **全般**タブをクリックします。
3. **iLO サブシステム名（ホスト名）**を入力します。

   ホスト名は iLO サブシステムの DNS 名です。この名前は、DHCP と DNS が IP アドレスではなく iLO サブシステム名に接続するよう構成されている場合のみ使用されます。
4. DHCP が構成されていない場合は、iLO **ドメイン名**を入力します。

   静的ドメイン名を使用するには、**IPv4 設定**ページおよび **IPv6 設定**ページで **DHCPv4 が提供するドメイン名を使用**と **DHCPv6 が提供するドメイン名を使用**の設定を無効にします。
5. **適用**をクリックして変更を保存します。

   1 つ以上の保留中の変更を有効にするには iLO のリセットが必要であることが iLO から通知されます。iLO 設定の構成権限がアカウントに割り当てられている場合、**iLO のリセット**ボタンがメッセージに含まれています。

   iLO のリセットが完了するまで、このメッセージはすべての **iLO 専用ネットワークポート**タブまたは **iLO 共有ネットワークポート**タブに表示されます。
6. （オプション）**全般**、**IPv4**、**IPv6**、**SNTP** の各タブで、その他のネットワーク設定を構成します。
7. iLO ネットワーク設定の構成が完了したら、**iLO のリセット**をクリックします。

   接続が再確立されるまでに、数分かかることがあります。

詳しくは

Kerberos 認証用の iLO ホスト名とドメイン名の構成
IPv4 設定の構成
IPv6 設定の構成

iLO ホスト名とドメイン名の制限

iLO ホスト名設定を構成する場合は、以下の点に注意してください。

- **ネームサービスの制限** - サブシステム名は DNS 名の一部として使用します。
  - DNS では、英数字とハイフンが使用できます。
  - ネームサービスの制限は、**ドメイン名**にも適用されます。
- **ネームスペースの問題** - この問題を避けるために、次のガイドラインに従ってください。
  - アンダースコア文字を使用しない
  - サブシステム名を 15 文字までにする

    iLO ではホスト名に最大 49 文字まで使用できますが、より短い名前を使用することで、環境内の他のソフトウェア製品との相互運用性の問題を回避することができます。
  - IP アドレスと DNS/WINS 名で iLO プロセッサーが PING コマンドで応答があることを確認する
  - NSLOOKUP が iLO ネットワークアドレスを正しく解決し、ネームスペースが競合していないことを確認する
  - DNS と WINS の両方を使用している場合は、iLO ネットワークアドレスが正しく解決されることを確認する
  - ネームスペースを変更した場合は DNS 名を更新する
- Kerberos 認証を使用する場合は、ホスト名とドメイン名が Kerberos 使用の前提条件を満たしていることを確認します。

NIC 設定

ネットワーク共通設定タブの **NIC 設定**セクションで iLO 専用ネットワークポートまたは iLO 共有ネットワークポートを有効にして、関連付けられた NIC 設定の構成を行います。

NIC 設定セクションは、C クラスのブレードサーバーと Synergy Compute Module では使用できません。

iLO Web インターフェイスを介した iLO 専用ネットワークポートの有効化

前提条件

- iLO の設定を構成する権限
- デフォルトのサーバー構成でリモート管理をサポートしていない場合、オプションの iLO ネットワーク有効化モジュールがインストールされています。

手順

1. iLO 専用ネットワークポートを、サーバーを管理する LAN に接続します。
2. ナビゲーションツリーで **iLO 専用ネットワークポート**をクリックします。
3. **全般**タブをクリックします。
4. **iLO 専用ネットワークポートを使用**チェックボックスを選択します。
5. **リンク設定**を選択します。
6. 仮想 LAN を使用するには、**仮想 LAN 有効**オプションを有効にします。

7. 仮想 LAN をオプションを有効にした場合は、**仮想 LAN タグ**を入力します。
8. **適用**をクリックして変更を保存します。

   1 つ以上の保留中の変更を有効にするには iLO のリセットが必要であることが iLO から通知されます。iLO 設定の構成権限がアカウントに割り当てられている場合、**iLO のリセット**ボタンがメッセージに含まれています。

   iLO のリセットが完了するまで、このメッセージはすべての **iLO 専用ネットワークポート**タブまたは **iLO 共有ネットワークポート**タブに表示されます。
9. （オプション）**全般**、**IPv4**、**IPv6**、**SNTP** の各タブで、その他のネットワーク設定を構成します。
10. iLO ネットワーク設定の構成が完了したら、**iLO のリセット**をクリックします。

    接続が再確立されるまでに、数分かかることがあります。

詳しくは

iLO ネットワークポートの構成オプション
iLO ネットワーク接続に関する留意事項

専用ネットワークポートの全般設定

リンク設定

この値は、iLO ネットワークトランシーバーの速度とデュプレックス設定を制御します。

以下の値から選択します。

- **自動**（デフォルト） - iLO を有効にして、ネットワークに接続する際に、サポートされる最高リンク速度とデュプレックス設定をネゴシエートします。
- **1000BaseT、全二重** - 全二重を使用した 1 Gb 接続を強制します（サポートされるサーバーのみ）。
- **100BaseT、全二重** - 全二重を使用する 100 Mb 接続を強制します。
- **100BaseT、半二重** - 半二重を使用する 100 Mb 接続を強制します。
- **10BaseT、全二重** - 全二重を使用した 10 Mb 接続を強制します。
- **10BaseT、半二重** - 半二重を使用した 10 Mb 接続を強制します。

この設定は、サーバーブレードでは使用できません。

VLAN 有効

VLAN を有効にすると、iLO 専用ネットワークポートは VLAN の一部になります。物理的に同じ LAN に接続されている場合でも、異なる仮想 LAN タグを持つすべてのネットワークデバイスが、独立した LAN にあるかのように表示されます。

VLAN タグ

相互に通信するネットワークデバイスすべてが、同じ仮想 LAN タグを持つ必要があります。仮想 LAN タグは、1～4094 の任意の番号です。

iLO Web インターフェイスを介した iLO 共有ネットワークポートの有効化

前提条件

- iLO の設定を構成する権限
- デフォルトのサーバー構成でリモート管理をサポートしていない場合、オプションの iLO ネットワーク有効化モジュールがインストールされています。

手順

1. 共有ネットワークポート LOM、FlexibleLOM、または FlexibleLOM/OCP ポートを LAN に接続します。
2. ナビゲーションツリーで **iLO 共有ネットワークポート**をクリックして、**全般**タブをクリックします。
3. **共有ネットワークポートを使用**チェックボックスを選択します。

   このオプションの名前は異なる場合があります。たとえば、サーバーの構成によっては、 **共有ネットワークポートを使用 - FlexibleLOM** または**共有ネットワークポートを使用 - FlexibleLOM/OCP** が表示されることがあります。
4. サーバーの構成に応じて、**LOM**、**FlexibleLOM**、または **FlexibleLOM/OCP** を選択します。

   このオプションは、複数の NIC を備えたサーバーでのみ利用できます。
5. **ポート**メニューから値を選択します。
6. 仮想 LAN を使用するには、**仮想 LAN 有効**オプションを有効にします。
7. 仮想 LAN 機能を有効にした場合は、**VLAN タグ**を入力します。
8. **適用**をクリックして変更を保存します。

   1 つ以上の保留中の変更を有効にするには iLO のリセットが必要であることが iLO から通知されます。iLO 設定の構成権限がアカウントに割り当てられている場合、**iLO のリセット**ボタンがメッセージに含まれています。

   iLO のリセットが完了するまで、このメッセージはすべての **iLO 専用ネットワークポート**タブまたは **iLO 共有ネットワークポート**タブに表示されます。
9. （オプション）**全般**、**IPv4**、**IPv6**、**SNTP** の各タブで、その他のネットワーク設定を構成します。
10. iLO ネットワーク設定の構成が完了したら、**iLO のリセット**をクリックします。

    接続が再確立されるまでに、数分かかることがあります。

    iLO をリセットすると、共有ネットワークポートがアクティブになります。iLO との間のすべてのネットワークトラフィックが共有ネットワークポート LOM、FlexibleLOM、または FlexibleLOM/OCP ポート経由で転送されるようになります。

詳しくは

iLO ネットワークポートの構成オプション
iLO ネットワーク接続に関する留意事項

共有ネットワークポートの全般設定

NIC

サーバーの NIC タイプ。

ポート

1 以外のポート番号の選択は、サーバーおよびネットワークアダプターの両方がこの構成をサポートしている場合にのみ機能します。無効なポート番号を入力すると、ポート 1 が使用されます。

VLAN 有効

VLAN を有効にすると、iLO 共有ネットワークポートが VLAN の一部になります。物理的に同じ LAN に接続されている場合でも、異なる仮想 LAN タグを持つすべてのネットワークデバイスが、独立した LAN にあるかのように表示されます。

VLAN タグ

相互に通信するネットワークデバイスすべてが、同じ仮想 LAN タグを持つ必要があります。仮想 LAN タグは、1～4094 の任意の番号です。

iLO ネットワークポートの構成オプション

iLO サブシステムは、以下のネットワーク接続オプションを提供します。

- **iLO 専用ネットワークポート** - iLO ネットワークトラフィック専用の独立した NIC を使用します。サポートされている場合、このポートはサーバー背面の RJ-45 ジャックを使用します。

  RJ-45 ジャックには **iLO** というラベルが付いています。

  一部のサーバーでは、このオプションはオプションの iLO ネットワーク有効化モジュールのインストールによって提供されます。

- **共有ネットワークポート LOM** - サーバーに内蔵の固定 NIC を使用します。この NIC は通常、サーバーネットワークトラフィックを処理します。共通の RJ-45 コネクター経由で同時に iLO ネットワークトラフィックを処理するように構成できます。

  一部のサーバーでは、このオプションはオプションの iLO ネットワーク有効化モジュールをインストールすることで有効になります。

- **共有ネットワークポート FlexibleLOM** - サーバー上の特別なスロットに挿入するオプション NIC を使用します。この NIC は通常、サーバーネットワークトラフィックを処理します。共通の RJ-45 コネクター経由で同時に iLO ネットワークトラフィックを処理するように構成できます。

- **共有ネットワークポート FlexibleLOM/OCP** - サーバー上の特別なスロットに挿入するオプションのオープンコンピュートプロジェクト NIC を使用します。この NIC は通常、サーバーネットワークトラフィックを処理します。共通の RJ-45 コネクター経由で同時に iLO ネットワークトラフィックを処理するように構成できます。

使用しているサーバーでサポートされる NIC について詳しくは、次の Web サイトにあるサーバー仕様を参照してください。**https://www.hpe.com/info/qs**

iLO ネットワーク接続に関する留意事項

- iLO は 1 つのアクティブな NIC 接続のみをサポートしているため、一度に有効にできるのは専用ネットワークポートオプションまたは共有ネットワークポートオプションのいずれか 1 つのみです。

- デフォルトでは、iLO 共有ネットワークポートはサーバー NIC のポート 1 を使用します。サーバーの構成に応じて、この NIC は LOM、FlexibleLOM、または FlexibleLOM/OCP アダプターになります。ポート番号は NIC 上のラベルに対応します。これは、オペレーティングシステム内の番号付けとは異なる可能性があります。

  サーバーと NIC の両方でポートの選択がサポートされている場合、iLO ファームウェアで別のポート番号を選択することができます。ポート 1 以外のポートが共有ネットワークポート用に選択されていて、その構成がサーバーでサポートされていない場合、iLO は開始時にポート 1 に戻します。

- 専用ネットワークポートが搭載されていないサーバーでは、標準のハードウェア構成の場合、iLO ネットワーク接続は iLO 共有ネットワークポート接続のみを介して提供されます。これらのサーバーでは、iLO ファームウェアはデフォルトで共有ネットワークポートに設定されています。

- サーバーの補助電源には予算制限があるため、iLO 共有ネットワークポート機能で使用される 1 Gb/s 銅線ネットワークアダプターの一部は、サーバーの電源がオフのときに 10/100 の速度でしか動作しない可能性があります。この問題を避けるために、Hewlett Packard Enterprise では、iLO 共有ネットワークポートが接続されるスイッチを自動ネゴシエート用に構成するか、専用ネットワークポートを使用することをお勧めします。ネットワーク接続について詳しくは、Web サイト **https://www.hpe.com/info/qs** にある iLO 仕様書を参照してください。

iLO が接続されているスイッチポートが 1 Gb/s に構成されている場合、一部の銅線 iLO 共有ネットワークポートアダプターで、サーバーの電源がオフのときに接続が切断される可能性があります。サーバーの電源が再投入されれば、接続は復旧します。

- iLO 共有ネットワークポートを無効にしても、システム NIC は完全に無効にはなりません。サーバーネットワークトラフィックは、引き続き NIC ポートを通過できます。iLO 共有ネットワークポートが無効の場合、iLO との間のすべてのデータ通信量は共有ネットワークポートを通過しません。
- 共有ネットワークポートが有効な場合は、リンク設定やデュプレックス設定は変更できません。共有ネットワークポート構成を使用する場合、オペレーティングシステムでこれらの設定を管理する必要があります。
- 一部のサーバーでは、専用管理ネットワーク（デフォルト）または共有ネットワーク接続によるリモート管理のサポートを追加するために、オプションの iLO ネットワーク有効化モジュールが必要です。iLO ネットワーク有効化モジュールがインストールされていない場合、iLO アクセスは、ホストベース（インバンド）のアクセス方式でのみサポートされます。サポートされているホストベースのアクセス方式の例には、iLO RESTful API、UEFI システムユーティリティ、iLO サービスポート（利用可能な場合）、および仮想 NIC が含まれます。

IPv4 設定の構成

これらの IPv4 設定を構成するとき、192.0.2.0/24 などの特殊な用途の IPv4 アドレスは入力しないでください。これらのアドレスはサポートされていません。詳しくは、IETF の Web サイトにある RFC5735 のドキュメントを参照してください。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで **iLO 専用ネットワークポート**または **iLO 共有ネットワークポート**をクリックして、**IPv4** タブをクリックします。
2. **DHCPv4 構成**設定を構成します。
3. **静的 IPv4 アドレス構成**設定を構成します。
4. **DNS 構成**設定を構成します。
5. **WINS 構成**設定を構成します。
6. **静的経路構成**設定を構成します。
7. **開始時にゲートウェイに PING** 設定を構成します。
8. **適用**をクリックして変更を保存します。

   1 つ以上の保留中の変更を有効にするには iLO のリセットが必要であることが iLO から通知されます。iLO 設定の構成権限がアカウントに割り当てられている場合、**iLO のリセット**ボタンがメッセージに含まれています。

   iLO のリセットが完了するまで、このメッセージはすべての **iLO 専用ネットワークポート**タブまたは **iLO 共有ネットワークポート**タブに表示されます。
9. （オプション）**全般**、**IPv4**、**IPv6**、**SNTP** の各タブで、その他のネットワーク設定を構成します。
10. iLO ネットワーク設定の構成が完了したら、**iLO のリセット**をクリックします。

    接続が再確立されるまでに、数分かかることがあります。

DHCPv4 構成設定

DHCPv4 の設定はデフォルトで有効です。

DHCPv4 有効

iLO による DHCP サーバーからの IP アドレス（およびその他の多くの設定）の取得を有効にします。

DHCPv4 が提供するゲートウェイを使用

DHCP サーバーが提供するゲートウェイを iLO が使用するかどうかを指定します。DHCP を使用しない場合は、**ゲートウェイ IPv4 アドレス**ボックスにゲートウェイアドレスを入力します。

DHCPv4 が提供する静的経路を使用

DHCP サーバーが提供する静的経路を iLO が使用するかどうかを指定します。この静的経路を使用しない場合は、**静的経路 #1 設定**、**静的経路 #2 設定**、および**静的経路 #3 設定**の各ボックスに静的経路宛先、マスク、およびゲートウェイアドレスを入力します。

DHCPv4 のドメイン名の使用

DHCP サーバーが提供するドメイン名を iLO が使用するかどうかを指定します。DHCP を使用しない場合は、**ネットワーク共通設定**ページの**ドメイン名**ボックスにドメイン名を入力します。

DHCPv4 の DNS サーバーの使用

DHCP サーバーが提供する DNS サーバーリストを iLO が使用するかどうかを指定します。DNS サーバーリストを使用しない場合は、**プライマリ DNS サーバー**ボックス、**セカンダリ DNS サーバー**ボックス、および**ターシャリ DNS サーバー**ボックスに DNS サーバーアドレスを入力します。

DHCPv4 が提供する時間設定を使用

DHCPv4 が提供する NTP サービスの場所を iLO が使用するかどうかを指定します。

DHCPv4 が提供する WINS サーバーを使用

DHCP サーバーが提供する WINS サーバーリストを iLO が使用するかどうかを指定します。WINS サーバーリストを使用しない場合は、**プライマリ WINS サーバー**ボックスおよび**セカンダリ WINS サーバー**ボックスに WINS サーバーアドレスを入力します。

注記: DHCP サーバーの予約を作成するには、DHCP クライアント識別子（一意の識別子）が必要です。iLO 5 システムの場合、DHCP クライアント識別子は、後ろに 3 バイト（6 文字）の 0 が続くハードウェア MAC アドレスです。たとえば場合、iLO 5 MAC アドレスが 00-53-00-AA-BB-CC の場合、関連する DHCP クライアント識別子は `005300AABBCC000000` になります。

静的 IPv4 アドレス構成設定

IPv4 アドレス

iLO の IP アドレス。DHCP を使用する場合、iLO の IP アドレスは自動的に提供されます。DHCP を使用しない場合、静的 IP アドレスを入力します。

サブネットマスク

iLO IP ネットワークのサブネットマスク。DHCP を使用している場合、サブネットマスクは自動的に提供されます。DHCP を使用しない場合、ネットワークのサブネットマスクを入力します。

ゲートウェイ IPv4 アドレス

iLO ゲートウェイの IP アドレス。DHCP を使用する場合、iLO ゲートウェイの IP アドレスは自動的に提供されます。DHCP を使用しない場合は、iLO ゲートウェイの IP アドレスを入力します。

IPv4 DNS 構成設定

プライマリ DNS サーバー

DHCPv4 が提供する DNS サーバーを使用が有効な場合、この値は自動的に入力されます。有効でない場合は、プライマリ DNS サーバーのアドレスを入力します。

セカンダリ DNS サーバー

DHCPv4 が提供する DNS サーバーを使用が有効な場合、この値は自動的に入力されます。有効でない場合は、セカンダリ DNS サーバーのアドレスを入力します。

ターシャリ DNS サーバー

DHCPv4 が提供する DNS サーバーを使用が有効な場合、この値は自動的に入力されます。有効でない場合は、ターシャリ DNS サーバーのアドレスを入力します。

DDNS サーバー登録を有効

このオプションを有効または無効にして、iLO がその IPv4 アドレスと名前を DNS サーバーに登録するかどうかを指定します。

このオプションは、デフォルトで有効になっています。

IPv4 の WINS 構成設定

プライマリ WINS サーバー

DHCPv4 が提供する WINS サーバーを使用が有効な場合、この値は自動的に入力されます。有効でない場合は、プライマリ WINS サーバーのアドレスを入力します。

セカンダリ WINS サーバー

DHCPv4 が提供する WINS サーバーを使用が有効な場合、この値は自動的に入力されます。有効でない場合は、セカンダリ WINS サーバーのアドレスを入力します。

WINS サーバー登録を有効

このオプションを有効または無効にして、iLO がその名前を WINS サーバーに登録するかどうかを指定します。

このオプションは、デフォルトで有効になっています。

IPv4 の静的経路構成設定

静的経路 #1 設定、静的経路 #2 設定、および静的経路 #3 設定

iLO 静的経路の接続先、マスク、およびゲートウェイのアドレス **DHCPv4 が提供する静的経路を使用**が有効な場合、これらの値は自動的に入力されます。そうでない場合は、静的経路の値を入力してください。

その他の IPv4 設定

開始時にゲートウェイに ping

iLO プロセッサーの初期化時にゲートウェイに 4 つの ICMP エコー要求パケットを iLO が送信するように構成するには、このオプションを有効にします。これにより、iLO との間のパケット転送を行うルーターで、iLO 用の ARP キャッシュエントリーが最新であることを保証できます。

このオプションは、デフォルトで有効になっています。

IPv6 設定の構成

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで **iLO 専用ネットワークポート**または **iLO 共有ネットワークポート**をクリックします。
2. **IPv6** タブをクリックします。
3. **グローバル IPv6 構成**設定を構成します。
4. **DHCPv6 構成**設定を構成します。
5. **DNS 構成**設定を構成します。
6. **静的 IPv6 アドレス構成**設定を構成します。
7. **静的経路構成**設定を構成します。
8. **適用**をクリックして変更を保存します。

   1 つ以上の保留中の変更を有効にするには iLO のリセットが必要であることが iLO から通知されます。iLO 設定の構成権限がアカウントに割り当てられている場合、**iLO のリセット**ボタンがメッセージに含まれています。

   iLO のリセットが完了するまで、このメッセージはすべての **iLO 専用ネットワークポート**タブまたは **iLO 共有ネットワークポート**タブに表示されます。
9. （オプション）**全般**、**IPv4**、**IPv6**、**SNTP** の各タブで、その他のネットワーク設定を構成します。
10. iLO ネットワーク設定の構成が完了したら、**iLO のリセット**をクリックします。

    接続が再確立されるまでに、数分かかることがあります。

グローバル IPv6 構成設定

iLO クライアントアプリケーションは IPv6 を最初に使用

iLO クライアントアプリケーションで IPv4 サービスアドレスも IPv6 サービスアドレスも構成されている場合は、このオプションでクライアントアプリケーションへのアクセスの際に iLO がどちらのプロトコルを先に試すかを指定します。この設定は、FQDN を使用して NTP を設定する場合、名前リゾルバーから受信したアドレスリストにも適用されます。

- iLO で IPv6 を先に使用する場合、このオプションを有効にします。
- iLO で IPv4 を先に使用する場合、このオプションを無効にします。

最初のプロトコルを使用した通信が失敗すると、iLO は自動的に 2 番目のプロトコルを試します。

このオプションは、デフォルトで有効になっています。

ステートレスアドレス自動構成（SLAAC）を有効

iLO がルーター広告メッセージから自身の IPv6 アドレスを作成するように構成するには、このオプションを有効にします。

iLO は、このオプションが有効になっていない場合でも、自身のリンク-ローカルアドレスを作成します。

このオプションは、デフォルトで有効になっています。

DHCPv6 構成設定

ステートフルモード DHCPv6 を有効（アドレス）

このオプションを有効にすると、iLO は、DHCPv6 サーバーから提供される IPv6 アドレスを要求し、構成できます。

このオプションは、デフォルトで有効になっています。

DHCPv6 急速コミットを使用 - このチェックボックスを選択すると、DHCPv6 サーバーで高速コミットメッセージングモードを使用するよう iLO に指示します。このモードは DHCPv6 のネットワークトラフィックを低減しますが、複数の DHCPv6 サーバーが応答およびアドレスを提供できるネットワークで使用すると、問題の原因になることがあります。

このオプションは、デフォルトでは無効になっています。

ステートレスモード DHCPv6 を有効（その他）

NTP および DNS サービスの場所の設定を iLO が DHCPv6 サーバーに要求するように構成するには、このオプションを有効にします。

このオプションは、デフォルトで有効になっています。

- **DHCPv6 が提供するドメイン名を使用** - このチェックボックスで、DHCPv6 サーバーが提供するドメイン名を使用するかどうかを選択します。

  このオプションは、デフォルトで有効になっています。

- **DHCPv6 が提供する DNS サーバーを使用** - このチェックボックスを選択すると、DNS サーバーの場所に、DHCPv6 サーバーによって提供された IPv6 アドレスが使用されます。この設定は、IPv4 の DNS サーバーの位置オプションと同時に有効にできます。

  このオプションは、デフォルトで有効になっています。

- **DHCPv6 が提供する NTP サーバーを使用** - このチェックボックスを選択すると、NTP サーバーの場所に、DHCPv6 サーバーによって提供された IPv6 アドレスが使用されます。この設定は、IPv4 の NTP サーバーの位置オプションと同時に有効にできます。

  このオプションは、デフォルトで有効になっています。

ステートフルモード DHCPv6 を有効（アドレス）を有効にした場合、**ステートレスモード DHCPv6 を有効（その他）**がデフォルトで有効になります。iLO と DHCPv6 サーバー間で必要な DHCPv6 ステートフルメッセージでは、これが暗黙で了解されているためです。

IPv6 DNS 構成設定

プライマリ DNS サーバー、セカンダリ DNS サーバー、およびターシャリ DNS サーバー

DNS サービスの IPv6 アドレスを入力します。

IPv4 と IPv6 の両方のページで DNS サーバーの場所が構成されている場合、両方のソースが使用されます。使用するソースは、**iLO クライアントアプリケーションは IPv6 を最初に使用**構成オプション、プライマリソース、セカンダリリソース、ターシャリリソースの順にこれらの設定に従って選択されます。

DDNS サーバー登録を有効

このオプションを有効または無効にして、iLO がその IPv6 アドレスと名前を DNS サーバーに登録するかどうかを指定します。

このオプションは、デフォルトで有効になっています。

静的 IPv6 アドレス構成設定

静的 IPv6 アドレス 1、静的 IPv6 アドレス 2、静的 IPv6 アドレス 3、および静的 IPv6 アドレス 4

iLO の最大 4 つの静的 IPv6 アドレスとプレフィックス長を入力します。リンク-ローカルアドレスを入力しないでください。

アドレスごとにステータス情報が表示されます。

静的デフォルトゲートウェイ

ネットワーク上にルーター広告メッセージが存在されない場合に対応できるよう、デフォルト IPv6 ゲートウェイアドレスを入力します。

IPv6 の静的経路構成設定

静的経路#1（宛先）、静的経路#2（宛先）、および静的経路#3（宛先）

静的 IPv6 経路の宛先のプレフィックスとゲートウェイアドレスのペアを入力します。宛先のプレフィックス長を指定します。リンク-ローカルアドレスは宛先としては許可されませんが、ゲートウェイとしては許可されます。

静的経路の値ごとにステータス情報が表示されます。

IPv6 をサポートしている iLO の機能

IPv4 アドレスプールが枯渇に向かっている現状に対応するために、IETF が IPv6 を導入しました。IPv6 では、アドレス不足の問題を解消するために、アドレス長が 128 ビットに拡張されています。iLO はデュアルスタック実装を導入することで両方のプロトコルの同時使用に対応しています。

以下の機能が IPv6 の使用をサポートします

- 共有ネットワークポート接続経由の IPv6
- IPv6 静的アドレス割り当て
- IPv6 SLAAC アドレス割り当て
- IPv6 静的ルート割り当て
- IPv6 静的デフォルトゲートウェイエントリー
- DHCPv6 ステートフルアドレス割り当て
- DHCPv6 ステートレス DNS、ドメイン名、および NTP 構成
- 統合リモートコンソール
- Onboard Administrator シングルサインオン
- HPE のシングルサインオン
- Web サーバー
- SSH サーバー
- SNTP クライアント
- DDNS クライアント
- RIBCL over IPv6
- SNMP
- アラートメール
- リモート syslog

- WinDBG サポート
- HPQLOCFG/HPLOMIG over IPv6 接続
- URL ベースの仮想メディア
- CLI/RIBCL キーインポート over IPv6 接続
- LDAP および Kerberos over IPv6 を使用した認証
- iLO 連携
- IPMI
- 内蔵リモートサポート

iLO SNTP 設定の構成

前提条件

- iLO の設定を構成する権限
- 少なくとも 1 台の NTP サーバーが、ご使用の管理ネットワーク上で使用できます。
- DHCPv4 が提供する NTP サービス構成を使用する場合、**IPv4** タブで DHCPv4 が有効になっている。
- DHCPv6 が提供する NTP サービス構成を使用する場合、**IPv6** タブで DHCPv6 ステートレスモードが有効になっている。

手順

1. ナビゲーションツリーで **iLO 専用ネットワークポート**または **iLO 共有ネットワークポート**をクリックします。
2. **SNTP** タブをクリックします。
3. 以下のいずれかを実行します。
   - DHCP が提供する NTP サーバーアドレスを使用するには、**DHCPv4 が提供する時間設定を使用**か **DHCPv6 が提供する時間設定を使用**、あるいは両方を有効にします。
   - **プライマリタイムサーバー**ボックスおよび**セカンダリタイムサーバー**ボックスに NTP サーバーのアドレスを入力します。
4. **DHCPv6 が提供する時間設定を使用**のみを選択したか、プライマリタイムサーバーとセカンダリタイムサーバーを入力した場合は、サーバーのタイムゾーンを**タイムゾーン**リストから選択します。
5. NTP 時間転送設定を構成します。

   ブレードサーバーでは、この設定は **NTP または OA 時間をホストに転送**と呼ばれています。

   ブレード以外のサーバーでは、この設定は **NTP 時間をホストに転送**と呼ばれています。
6. **適用**をクリックして変更を保存します。

   1 つ以上の保留中の変更を有効にするには iLO のリセットが必要であることが iLO から通知されます。iLO 設定の構成権限がアカウントに割り当てられている場合、**iLO のリセット**ボタンがメッセージに含まれています。

   iLO のリセットが完了するまで、このメッセージはすべての **iLO 専用ネットワークポート**タブまたは **iLO 共有ネットワークポート**タブに表示されます。

7. （オプション）**全般**、**IPv4**、**IPv6**、**SNTP** の各タブで、その他のネットワーク設定を構成します。
8. iLO ネットワーク設定の構成が完了したら、**iLO のリセット**をクリックします。

   接続が再確立されるまでに、数分かかることがあります。

詳しくは

iLO のクロック同期
DHCP NTP アドレスの選択
IPv4 設定の構成
IPv6 設定の構成

SNTP オプション

DHCPv4 が提供する時間設定を使用

DHCPv4 が提供する NTP サーバーアドレスを iLO が使用するように構成します。

このオプションは、デフォルトで有効になっています。

DHCPv6 が提供する時間設定を使用

DHCPv6 が提供する NTP サーバーアドレスを iLO が使用するように構成します。

このオプションは、デフォルトで有効になっています。

NTP 時間の伝達設定

この設定の名前は、サーバーの種類によって異なります。

- **NTP 時間をホストに転送** - AC 電源が適用された後、または iLO がデフォルト設定にリセットされた後に初めて POST を実行している間に、サーバー時間を iLO 時間と同期させるかどうかを決定します。
- **NTP または OA 時間をホストに転送** - AC 電源が適用された後、ブレードが取り付けられた後、または iLO がデフォルト設定にリセットされた後に初めて POST を実行している間に、サーバー時間を iLO 時間と同期させるかどうかを決定します。

  この設定が有効であり、NTP が構成されていないか機能していない場合は、サーバー時間は Onboard Administrator 時間と同期されます。

このオプションは、デフォルトでは無効になっています。

プライマリタイムサーバー

指定したアドレスを持つプライマリタイムサーバーを使用するように iLO を構成します。サーバーアドレスは、サーバーの FQDN、IPv4 アドレス、または IPv6 アドレスを使用して入力できます。

セカンダリタイムサーバー

指定したアドレスを持つセカンダリタイムサーバーを使用するように iLO を構成します。サーバーアドレスは、サーバーの FQDN、IPv4 アドレス、または IPv6 アドレスを使用して入力できます。

タイムゾーン

iLO が現地時間を得るために UTC 時を調整する方法と、夏時間（サマータイム）を得るために時間を調整する方法が決まります。iLO ログのエントリーに正しい現地時間を表示するために、ユーザーはサーバーが存在する場所のタイムゾーンを指定する必要があり、ログの表示フィルターで**ローカル時刻表示**を選択する必要があります。

SNTP サーバーが提供する時間を iLO で調整なしで使用する場合は、UTC 時に調整を加えないタイムゾーンを選択します。さらにそのタイムゾーンは、夏時間の調整が適用されないものである必要があります。この要件に合うタイムゾーンはいくつかあります。iLO で選択可能な 1 つの例は

Greenwich（GMT）です。このタイムゾーンを選択すると、iLO Web インターフェイスのページおよびログエントリーには、SNTP サーバーが提供する時間がそのまま表示されます。

注記: NTP サーバーを協定世界時（UTC）を使用するように設定してください。

iLO のクロック同期

SNTP により iLO は、外部の時刻ソースとクロックを同期させることができます。iLO の日付と時刻は以下のソースによって同期を取ることもできるため、SNTP の構成は省略可能です。

- システム ROM（POST の実行中のみ）
- Onboard Administrator（ProLiant、サーバーブレードのみ）
- フレームリンクモジュール（Synergy コンピュートモジュール）

プライマリおよびセカンダリ NTP サーバーアドレスは、手動でまたは DHCP サーバーにより構成できます。プライマリサーバーのアドレスに接続できない場合は、セカンダリアドレスが使用されます。

DHCP NTP アドレスの選択

DHCP サーバーを使用して NTP サーバーアドレスを提供する場合は、**IPv6** ページの **iLO クライアントアプリケーションは IPv6 を最初に使用**設定によって、プライマリおよびセカンダリ NTP の値の選択を制御します。**iLO クライアントアプリケーションは IPv6 を最初に使用**を選択した場合、DHCPv6 提供の NTP サービスアドレス（使用可能な場合）がプライマリ時刻サーバーに使用され、DHCPv4 提供のアドレス（使用可能な場合）がセカンダリ時刻サーバーに使用されます。

プロトコルベースの優先動作を変更して、DHCPv4 を最初に使用するには、**iLO クライアントアプリケーションは IPv6 を最初に使用**チェックボックスをクリアします。

DHCPv6 アドレスがプライマリアドレスにもセカンダリアドレスにも使用できない場合は、DHCPv4 アドレス（使用可能な場合）が使用されます。

iLO NIC 自動選択

iLO NIC 自動選択を使用すると、iLO が iLO 専用ネットワークポートと iLO 共有ネットワークポートを選択できるようになります。起動時に、iLO は使用可能なポートのネットワークアクティビティを検索し、ネットワークアクティビティに基づいて使用するポートを自動的に選択します。

この機能によって、ProLiant Gen10 以降のサーバーに共通の事前構成を使用することができます。たとえば、複数のサーバーがある場合、一部のサーバーを、iLO 専用ネットワークポート経由で iLO に接続するデータセンター内にインストールします。他のサーバーは、共有ネットワークポート経由で iLO に接続するデータセンター内にインストールします。iLO NIC 自動選択を使用すると、どちらのデータセンターにもサーバーを設置できるようになり、iLO は正しいネットワークポートを選択します。

デフォルトでは、NIC 自動選択は無効です。

詳しくは

iLO NIC 自動選択の有効化

NIC 自動選択のサポート

- ProLiant Gen10 以降の非ブレードサーバーは NIC 自動選択をサポートします。
- iLO 5 は、この構成をサポートしているサーバー上で両方の共有ネットワークポートを検索するように設定できます。
- iLO 5 は NIC フェイルオーバーをサポートします。有効にすると、現在の接続が切断されたときに、iLO が自動的に NIC 接続の検索を開始します。この機能を使用するには、NIC 自動選択を有効にする必要があります。

NIC 自動選択が有効になっている場合の iLO 起動時の動作

NIC 自動選択が有効な場合：

- iLO が電源に接続されると、最初に iLO 専用ネットワークポートをテストします。
- iLO がリセットされると、最後に使用した iLO ネットワークポートを最初にテストします。
- ネットワークポートのテスト時に、iLO がネットワークのアクティビティを検出した場合、そのポートを選択して使用します。約 100 秒後までにネットワークアクティビティが検出されない場合は、iLO は反対側のネットワークポートに切り替え、そのポートのテストを開始します。iLO はネットワークアクティビティが検出されるまで、iLO 専用ネットワークポートと iLO 共有ネットワークポートを交互にテストします。iLO がテストのためにネットワークポートを切り替えるたびに、iLO のリセットが発生します。

  注意: 物理 NIC のいずれかがセキュリティ保護されていないネットワークに接続している場合、iLO が iLO ネットワークポート間で交互に切り替えたときに不正アクセスが発生する可能性があります。Hewlett Packard Enterprise では、必ず iLO を次のようなネットワークに接続することを強くおすすめします。

  - iLO へのアクセスに強力なパスワードを使用している。
  - セキュリティ保護されていないネットワークに iLO 専用ネットワークポートを接続しない。
  - iLO 共有ネットワークポートがセキュリティ保護されていないネットワークに接続されている場合、iLO のうち共有 NIC の部分は VLAN タギングを使用し、VLAN が安全なネットワークに接続されていることを確認する。

- iLO がアクティブなネットワークポートを検索するときは、サーバーの UID LED が点灯します。検索中に iLO がリセットされた場合、UID LED が 5 秒間点滅し、その後アクティブなポートが選択されるか、iLO がリセットされるまで点灯します。
- サーバーが iLO への LOM および FlexibleLOM 共有ネットワークポート接続の両方をサポートしている場合、iLO は構成中に選択されたオプションだけをテストします。iLO は LOM および FlexibleLOM オプションを交互にテストしません。
- NIC 自動選択が DHCP アドレスの割り当てアクティビティを検索するよう構成されており、iLO ネットワークポートのうち 1 つだけで DHCP が有効になっている場合、iLO は DHCP 用に構成されていないポートの受信データパケットアクティビティをテストします。

iLO NIC 自動選択の有効化

手順

1. 両方の iLO ネットワークポートを設定します。

NIC の自動選択機能を有効にして使用する前に、両方の iLO ネットワークポートをそれぞれのネットワーク環境に合わせて設定する必要があります。

2. 次のいずれかを実行します。

   - CLI コマンド `oemhpe_nicautosel` を使用して、NIC 自動選択を設定します。
   - NIC 自動選択を有効にするには、MOD_NETWORK_SETTINGS スクリプトに ILO_NIC_AUTO_SELECT タグを追加し、スクリプトを実行します。

     （オプション）オプションの NIC 自動選択機能を設定するには、MOD_NETWORK_SETTINGS スクリプトに ILO_NIC_AUTO_SNP_SCAN および ILO_NIC_AUTO_DELAY タグを追加します。

   詳しくは、HPE iLO 5 スクリプティング/コマンドラインガイドを参照してください。

3. サーバーのケーブルを配線し、iLO をリセットします。

   NIC 自動選択への変更は、iLO がリセットされるまで反映されません。

詳しくは

iLO NIC 自動選択
NIC 自動選択のサポート
NIC 自動選択が有効になっている場合の iLO 起動時の動作

NIC フェイルオーバーの構成

前提条件

NIC 自動選択が有効になっている。

NIC フェイルオーバーを構成するには、次のいずれかのオプションを使用します。詳しくは、HPE iLO 5 スクリプティング/コマンドラインガイドを参照してください。

手順

- CLI コマンド `oemhpe_nicfailover` を使用して、NIC フェイルオーバーを設定します。
- `ILO_NIC_FAIL_OVER` タグを `MOD_NETWORK_SETTINGS` スクリプトに追加し、スクリプトを実行します。

詳しくは

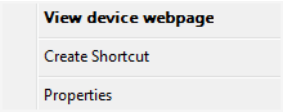
iLO NIC 自動選択の有効化

Windows ネットワークフォルダー内の iLO システムの表示

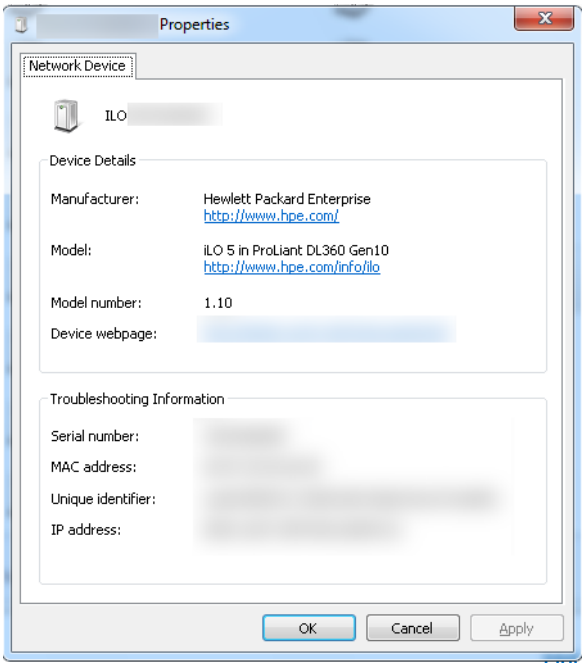
UPnP が構成されている場合、Windows システムと同じネットワーク上の iLO システムが Windows の**ネットワークフォルダー**に表示されます。

手順

- iLO システムの Web インターフェイスを起動するには、Windows の**ネットワーク**フォルダーでアイコンを右クリックし、**デバイスの Web ページの表示**を選択します。



- iLO システムのプロパティを表示するには、Windows の**ネットワーク**フォルダーにあるアイコンを右クリックし、**プロパティ**を選択します。



プロパティウィンドウには、以下の設定があります。

- **デバイスの詳細** - iLO のメーカーとバージョン情報。iLO Web インターフェイスを開始するには、**デバイスの Web ページ**リンクをクリックします。
- **トラブルシューティング情報** - シリアル番号、MAC アドレス、UUID、および IP アドレス。

リモートサポートの管理

HPE 内蔵リモートサポート

HPE iLO 5 には、内蔵リモートサポート機能が含まれており、この機能により、サポートされるサーバーを HPE リモートサポートに登録することができます。

また、iLO を使用してサービスイベントやリモートサポートによるデータ収集を監視することもできます。

Hewlett Packard Enterprise にデバイスを接続することによって、そのデバイスをリモートでサポートします。また、診断、構成、テレメトリー、および連絡先の情報を Hewlett Packard Enterprise に送信できます。その他のビジネス情報は収集されません。またデータはのプライバシー声明に従って管理されます。プライバシーポリシーは、次の Web サイト **https://www.hpe.com/info/privacy** で確認できます。

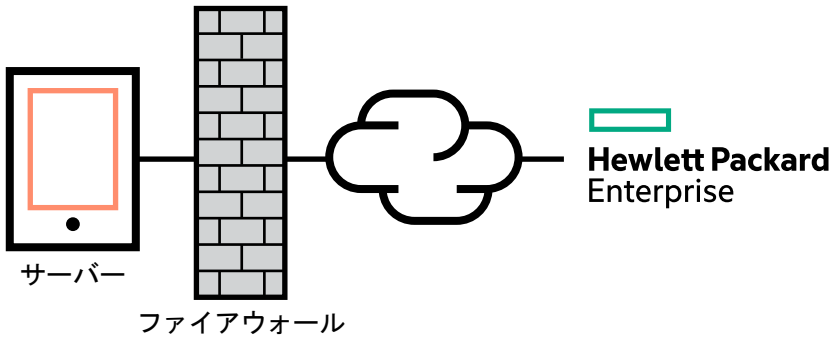
詳しくは、**Remote Settings for HPE ProLiant Gen10 Servers** のビデオをご覧ください。

内蔵リモートサポート機能を使用する場合は、Insight Online Direct Connect と Insight Remote Support Central Connect のどちらかの構成オプションを選択してください。

Insight Online Direct Connect

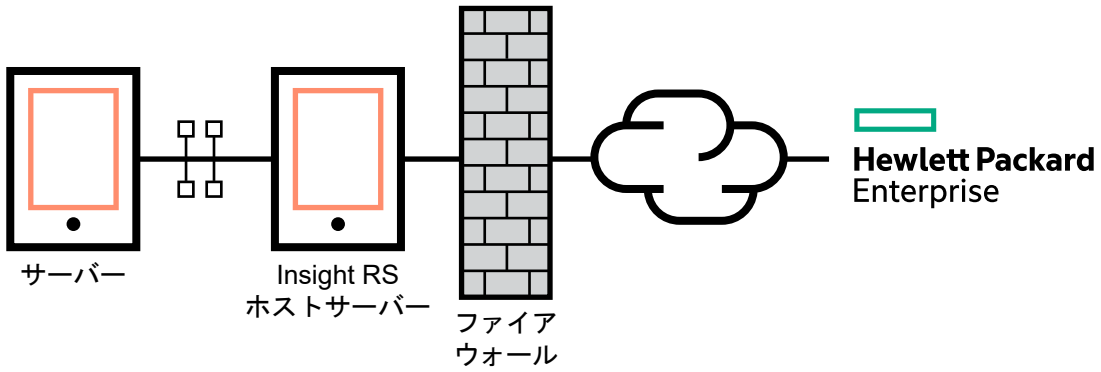
サポート対象のデバイスを Insight Online に直接登録します。ローカル環境に Insight Remote Support の一元化されたホストサーバーをセットアップする必要はありません。Insight Online は、リモートサポート情報のプライマリインターフェイスとなります。

Insight Online は、リモート監視対象のデバイスをいつでもどこでも表示できる、Hewlett Packard Enterprise サポートセンターの機能です。Insight Online は、外出時の監視用モバイルダッシュボードを含む個別化されたダッシュボードを提供し、IT の動作とサポート情報の追跡を簡素化します。



Insight Remote Support Central Connect

ローカル環境にある Insight Remote Support の一元化されたホストサーバーを使用して Hewlett Packard Enterprise にサポート対象のデバイスを登録します。すべての構成およびサービスイベント情報は、ホストサーバーを介してルーティングされます。この情報は、ローカルの Insight RS Console または Insight Online の Web ベースのビュー（Insight RS で有効になっている場合）を使用して表示できます。



デバイスサポート

内蔵リモートサポートの登録は、以下のデバイスタイプをサポートしています。

重要: HPE OneView を使用してご利用の環境を管理する場合は、これを使用してリモートサポートを登録します。詳しくは、HPE OneView のユーザーガイドを参照してください。

Insight Online Direct Connect

- HPE ProLiant Gen10 サーバー
- HPE ProLiant Gen10 Plus サーバー

Insight Remote Support Central Connect

- HPE ProLiant Gen10 サーバー
- HPE ProLiant Gen10 Plus サーバー

HPE リモートサポートにより収集されるデータ

サーバーがリモートサポート対象に登録されている場合、iLO が Active Health System 情報およびサーバー構成情報を収集した後、iLO または Insight RS ホストサーバーが Hewlett Packard Enterprise にこの情報を送信します。Active Health System 情報は 7 日ごとに送信され、設定情報は 30 日ごとに送信されます。以下の情報が含まれます。

登録

サーバーの登録中、iLO は、サーバーハードウェアを一意に識別するためのデータを収集します。登録データには、以下の情報が含まれます。

- サーバーモデル
- シリアル番号
- iLO NIC アドレス

サービスイベント

サービスイベントが記録されると、iLO は、関連ハードウェアコンポーネントを識別するためのデータを収集します。サービスイベントデータには、以下の情報が含まれます。

- サーバーモデル
- シリアル番号
- ハードウェアコンポーネントのパーツ番号
- 説明、場所、およびハードウェアコンポーネントを識別するその他の特徴

構成

データの収集中、iLO は、プロアクティブなアドバイスとコンサルティングを可能にするデータを収集します。構成データには、以下の情報が含まれます。

- サーバーモデル
- シリアル番号
- プロセッサーモデル、速度、および使用率
- ストレージ容量、速度、および使用率
- メモリ容量、速度、および使用率
- ファームウェア/BIOS
- インストールされているドライバー、サービス、およびアプリケーション（AMS がインストールされている場合）

Active Health System

データの収集中、iLO は、サーバーのヘルス、構成、およびランタイムテレメトリーに関するデータを収集します。この情報は、問題のトラブルシューティングおよび、品質分析のための閉じたループで使用されます。

詳しくは

Active Health System
リモートサポートのデータ収集
リモートサポートサービスイベント

HPE プロアクティブケアサービス

HPE プロアクティブケアサービスのお客様は、サーバーをリモートサポート対象に登録して、プロアクティブケア機能（プロアクティブスキャンレポートおよびファームウェアとソフトウェアのバージョンレポート）を受信する必要があります。

Direct Connect と Central Connect リモートサポートオプションには、AMS のインストールが必要です。System Management Assistant を使用する構成はサポートされません。

詳しくは、次の Web サイトを参照してください。**https://www.hpe.com/services/proactivecarecentral**

リモートサポート登録に関する前提条件

手順

1. **リモートサポートソリューションのコンポーネントにログインするときに使用する、サポートされるブラウザーをインストールします**。
2. HPE パスポートのアカウントがない場合は、web サイト **https://www.hpe.com/info/insightonline** でアカウントを作成し、ログイン認証情報を書き留めます。

ほとんどの場合、HPE パスポートのユーザー ID は、HPE パスポートの登録プロセス中に使用したメールアドレスと同じです。Hewlett Packard Enterprise サポートセンターでユーザー ID を変更した場合は、必ず、電子メールアドレスではなくユーザー ID でログインしてください。

3. Web サイト **https://www.hpe.com/support/hpesc** に移動し、リモートサポートに登録する製品に有効な Hewlett Packard Enterprise 保証または契約があることを確認します。
4. 以下の情報を収集します。この情報は、Insight Online Direct Connect の登録手順、または Insight Remote Support Central Connect のホストサーバーの構成手順で使用します。
   - 連絡先情報。Hewlett Packard Enterprise は、サポートケースを作成するときにこの情報を使用します。
   - サイト情報 （サイト名、アドレス、およびタイムゾーン）。Hewlett Packard Enterprise は、サービス担当者または部品をサーバーのある場所に送らなければならないときにこの情報を使用します。
   - Web プロキシ情報（Web プロキシはインターネットにアクセスするために使用されます）。
   - チャネルパートナーがデバイス情報を表示できるようにする場合は、認定サービスプロバイダー、リセラー/ディストリビューター、およびインストーラーのチャネルパートナー ID。インストーラーは Insight Remote Support Central Connect のみに必要です。

     パートナー ID は、パートナー登録プロセス中にチャネルパートナーに割り当てられるロケーション ID です。チャネルパートナー ID がわからない場合は、パートナーにお問い合わせの上、その情報を取得してください。
5. **リモートサポート登録用の ProLiant サーバーをセットアップします**。

   サーバーをセットアップしている場合は、それらがサーバーのセットアップ手順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。
6. iLO のホスト名または IP アドレスとログイン認証情報（ログイン名およびパスワード）を入手します。

   iLO の設定権限を持っているローカルまたはディレクトリベースのユーザーアカウントを使用することができます。
7. Direct Connect のみ：環境が **Insight Online Direct Connect のネットワーク要件**を満たしていることを確認します。
8. Central Connect のみ：**Insight Remote Support Central Connect 環境をセットアップします**。
9. **Insight Online へのアクセスを確認します。**

HPE 組み込みリモートサポートでサポートされるブラウザー

iLO

iLO 5 は、**サポートされるブラウザー**にリストされているブラウザーをサポートします。

Insight RS

- Microsoft Internet Explorer：9x、10x、11x
- Mozilla Firefox：49.x
- Google Chrome：53.x

Insight Online

- Microsoft Internet Explorer：11 以降
- Mozilla Firefox：最新バージョン
- Google Chrome：最新バージョン

リモートサポート登録用の ProLiant サーバーのセットアップ

前提条件

ProLiant サーバーをセットアップまたはアップデートするために必要なファイルがあることを確認します。

構成によっては、**Service Pack for ProLiant** が必要な場合があります。SPP には iLO ファームウェア、iLO 5 Channel Interface ドライバー、および AMS が含まれます。SPP ダウンロードページ **https://www.hpe.com/servers/spp/download** から SPP をダウンロードします。

次の Web サイトで、iLO 5 Channel Interface ドライバー、iLO ファームウェア、および AMS を個別にダウンロードできます。**https://www.hpe.com/support/ilo5**

手順

1. サーバーハードウェアをインストールします。
2. **iLO をネットワークに接続します**。
3. Intelligent Provisioning を使用してサーバーの構成と OS のインストールを実行します。

   詳しくは、Intelligent Provisioning のユーザーガイドを参照してください。
4. （オプション）AMS をまだインストールしていない場合はインストールします。

   Hewlett Packard Enterprise は AMS をインストールすることをお勧めします。

   HPE Proactive Care サービスのカスタマー専用 : プロアクティブケアの機能（プロアクティブスキャンレポートおよびファームウェアとソフトウェアのバージョンレポート）を取得するには、AMS のインストールが 必要です。

   AMS の使用は、iLO がサーバーの名前を取得できる 1 つの方法です。iLO がサーバー名を取得できない場合、Insight Online と Insight RS で表示されているサーバー名は、サーバーのシリアル番号から得られます。
5. AMS をインストールしなかった場合、Insight Online と Insight RS でサーバー名が正しく表示されることを確認するために、以下のいずれかを実行します。

   - Windows システムの場合のみ、オペレーティングシステムを起動します。Insight Online と Insight RS は、サーバーを識別するために、Windows コンピューター名を使用します。
   - iLO Web インターフェイスの**アクセス設定**ページで、**サーバー名**を構成します。

     プライバシーを保護するため、サーバー名に機密情報を使用しないでください。サーバー名は Insight Online および Insight RS に表示されます。
6. Windows サーバー：iLO 5 Channel Interface ドライバーをインストールします。

   Intelligent Provisioning の**自動インストール**インストール方法で Windows をインストールすると、iLO 5 Channel Interface ドライバー for Windows が自動的にインストールされます。

   Red Hat Enterprise Linux および SUSE Linux Enterprise Server の場合、ドライバーは Linux ディストリビューションに含まれています。

7. サポートされるバージョンの iLO ファームウェアがインストールされていることを確認します。

   Insight Remote Support の Central Connect 登録には、iLO 5 1.10 以降が必要です。

   Insight Remote Support の Direct Connect 登録には、iLO 5 1.30 以降が必要です。

8. タイムゾーンが iLO で設定されていることを確認します。

   タイムゾーン値が正しくない場合、Insight Online はイベントおよびデータ収集に不正なタイムスタンプを表示します。

9. DNS サーバーが iLO に構成されていることを確認します。

   デフォルトでは、DHCP を使用して DNS サーバーや他のネットワーク設定を構成するように iLO が設定されています。

   DNS サーバーは、iLO と Insight Online 間の通信に必要です。

10. 登録するサーバーが CNSA セキュリティ状態を使用するように構成されていないことを確認します。

    セキュリティ状態設定は、iLO **暗号化設定**ページに表示できます。

    組み込みリモートサポートは、CNSA セキュリティ状態を使用するように構成されているサーバー上ではサポートされていません。

詳しくは

iLO 暗号化設定
iLO ドライバーのインストール
AMS のインストール
iLO SNTP 設定の構成
ネットワーク構成の概要の表示
インストール済みファームウェア情報の表示
iLO ネットワーク設定の構成

Insight Online Direct Connect のネットワーク要件

Insight Online Direct Connect では、ご使用の環境と Hewlett Packard Enterprise との間の通信を使用してサポートサービスを提供します。ご使用の環境が**図 4: Insight Online Direct Connect のネットワーク要件**に示すポート要件を満たしていることを確認します。

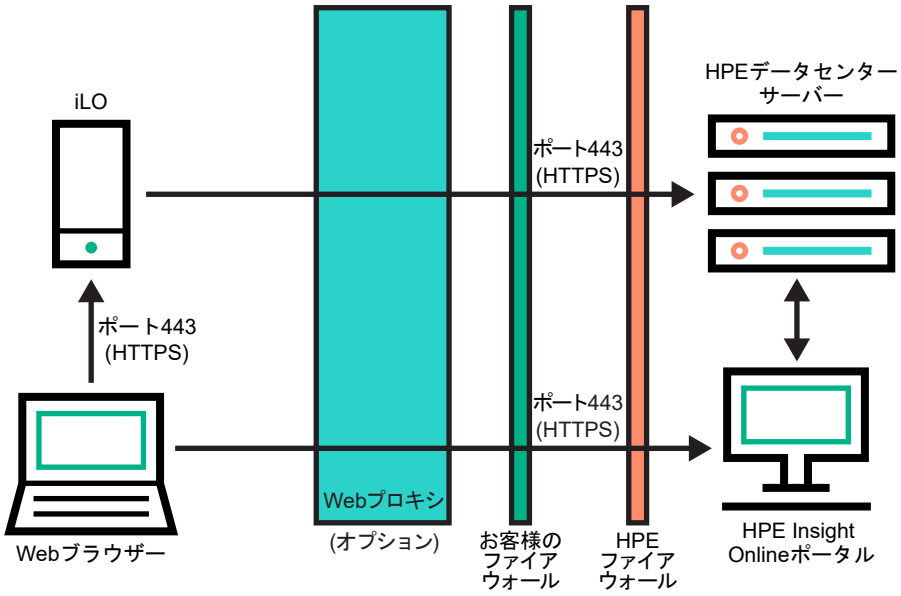


図 4: Insight Online Direct Connect のネットワーク要件

Insight Remote Support Central Connect 環境のセットアップ

Insight Remote Support は、サポートサービスの提供については、ご使用の環境と Hewlett Packard Enterprise の間の通信に依存します。

手順

1. Insight RS ホストサーバーに使用するサーバーが、Insight Remote Support のリリースノートに記載されている要件を満たしていることを確認します。

   Insight RS ソフトウェアでは、ホストサーバーのことを「ホスティングデバイス」と呼んでいます。

2. ご使用の環境が**図 5: Insight Remote Support Central Connect のネットワーク要件**に示すポート要件を満たしていることを確認します。

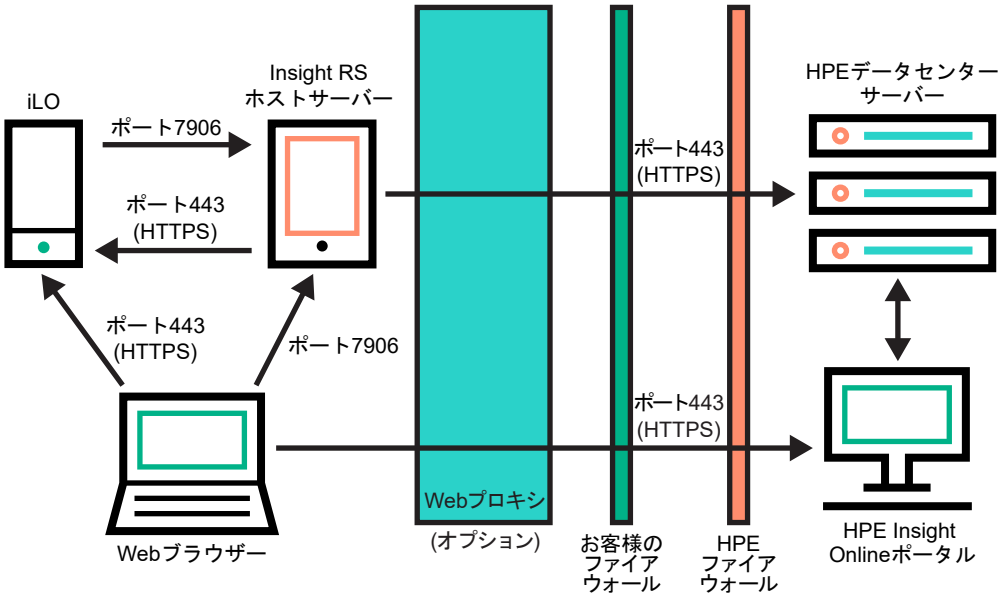


図 5: Insight Remote Support Central Connect のネットワーク要件

3. Insight RS ホストサーバーを設定します。

a. ホストサーバー上の Insight RS ソフトウェアのバージョンが、登録する ProLiant サーバーをサポートしていることを確認します。詳しくは、次の Web サイトを参照してください。**https://www.hpe.com/support/InsightRS-Support-Matrix**

b. Insight RS コンソールを使用して、Insight Remote Support Central Connect に登録する ProLiant サーバーの RIBCL プロトコルを構成します。

c. （オプション）HPE SIM を Insight RS とともに使用する場合は、HPE SIM アダプターを設定します。

詳しくは、Web サイト（**https://www.hpe.com/info/insightremotesupport/docs**）にある Insight Remote Support のインストール/構成ガイドを参照してください。

4. Insight RS ホストサーバーとリモートサポート Web サービスとの間の通信を確認します。

このタスクを完了するには、Insight RS ホストサーバーで Web ブラウザーを起動して、次の Web サイトに移動します。**https://api.support.hpe.com/v1/version/index.html**

サーバーと HPE 間の接続が正しく設定されている場合、Web ブラウザーには、一部のデータセンターコンポーネントのバージョン（たとえば、`19.1.17.470`）が表示されます。

Insight Online へのアクセスの確認

手順

1. 次の Web サイトに移動します。**https://www.hpe.com/info/insightonline**
2. HPE パスポートのユーザー ID とパスワードを入力し、**サインイン**をクリックします。

   HPE パスポートのアカウントをお持ちでない場合は、画面上の手順に従って作成してください。

   Insight Online マイ IT 環境タブが選択されている、Hewlett Packard Enterprise サポートセンターの Web サイトが表示されます。初期セットアップ時には、お客様の IT 環境の**デバイス**、**サービスイベント**、および**契約と標準保証**セクションには何も表示されません。

Insight Online Direct Connect の登録

Insight Online Direct Connect に登録する場合は、iLO の Web インターフェイスと Insight Online ポータルの両方のステップを完了する必要があります。

前提条件

- ご使用の環境が内蔵リモートサポート登録の前提条件を満たしている。
- iLO の設定を構成する権限
- HPE パスポートアカウントがある。詳しくは、**https://www.hpe.com/info/insightonline** を参照してください。

手順

1. **iLO の Web インターフェイスで、Insight Online Direct Connect 登録の手順 1 を完了します。**
2. **Insight Online で、Insight Online Direct Connect 登録の手順 2 を完了します。**

3. **iLO の Web インターフェイスで、登録が完了したことを確認します。**
4. **iLO の Web インターフェイスで、登録後のオプション手順を完了します。**

詳しくは

リモートサポート登録に関する前提条件
Insight Online Direct Connect のホストサーバーとして使用する ProLiant サーバーの登録
サポートされるデバイスの Central Connect から Direct Connect リモートサポートへの変更

Insight Online Direct Connect の登録（手順 1）

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**リモートサポート**をクリックします。

   登録ページが表示されます。
2. **このサーバーを直接 HPE に接続を選択します。**
3. HPE パスポートのユーザー ID とパスワードを入力します。
4. （オプション）サーバーがインターネットへのアクセスに Web プロキシサーバーを使用する場合、次の情報を入力します。

   - **Web プロキシサーバー** - ホスト名または IP アドレスを入力します。
   - **Web プロキシポート**
   - **Web プロキシユーザー名**
   - **Web プロキシパスワード**
5. **以下の条件に同意します**チェックボックスを選択し、ライセンス条件に同意します。

   これらのドキュメントは、次の Web サイトで参照できます。**https://www.hpe.com/software/SWLicensing**
6. **登録**をクリックします。

   iLO は、登録プロセスの手順 1 が完了したことを通知し、手順 2 を完了するよう要求します。

   登録要求が完全に処理されるまで、最大 5 分間待ってください。

Insight Online Direct Connect の登録（手順 2）

手順

1. 次の Web サイトに移動します。**https://www.hpe.com/info/insightonline**
2. HPE パスポートの認証情報を使用してログインします。
3. **Insight Online マイ IT 環境**タブで、**登録が完了していないデバイス**をクリックします。
4. **手順 1：ターゲットデバイスを選択**ページで 1 つまたは複数のデバイスを選択し、**次へ**をクリックします。

選択したデバイスが、サイト、サポートおよびパートナーの情報を共有している場合は、一度に最大 15 個のデバイスを登録できます。

5. **手順 2：サイトとサポートに関する情報を提供します**ページでサイトおよびサポート情報を入力し、**次へ**をクリックします。
6. **手順 3：HPE 認定チャネルパートナー情報の入力**ページで次のいずれかを実行します。
   - Hewlett Packard Enterprise がお客様の IT インフラストラクチャをサポートする場合は、デフォルト設定を受け入れます。
   - Hewlett Packard Enterprise 認定チャネルパートナーがお客様の IT インフラストラクチャをサポートする場合は、認定サービスパートナーおよび認定リセラー/ディストリビューターの**パートナー ID** を入力します。

     ID の確認をクリックして、正しいパートナーを入力したことを確認します。
7. （オプション）Hewlett Packard Enterprise または認定チャネルパートナーがお客様の IT 環境の最適化について連絡することを許可するには、**マイ IT 環境を最適化**チェックボックスを選択します。
8. 続けて**手順 4：確認と送信**ページに進むには、**次へ**をクリックします。
9. 入力した情報を確認し、**登録の完了**をクリックします。

   デバイス登録の完了ウィンドウに登録状況の概要が表示されます。
10. **完了**をクリックします。

登録が完了したことの確認（iLOWeb インターフェイス）

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**リモートサポート**をクリックします。

   登録ページが表示されます。
2. **HPE に接続された製品の登録プロセスが完了したことを確認してください。**チェックボックスを選択して、**適用**をクリックします。

   iLO によって、登録プロセスが終了したことが通知されます。

登録後の手順（オプション）の完了

手順

1. （オプション）iLO と HPE リモートサポート間の接続を確認するために、テストイベントを送信します。
2. （オプション）システムイベントに関する電子メールアラートを受け取るには、アラートメールを構成します。

詳しくは

テストサービスイベントの送信
アラートメールを有効にする

Web プロキシ設定を編集する (Insight Online Direct Connect のみ)

サーバーがリモートサポートに登録した後に Web プロキシ設定が変わった場合、サーバーがデータを Hewlett Packard Enterprise に継続して送信できるように設定をアップデートします。

手順

1. ナビゲーションツリーで**リモートサポート**をクリックします。

   登録ページが表示されます。

2. 必要に応じて、次の設定をアップデートします。

   - **Web プロキシサーバー** - ホスト名または IP アドレスを入力します。
   - **Web プロキシポート**
   - **Web プロキシユーザー名**
   - **Web プロキシパスワード**

3. **適用**をクリックします。

Insight Remote Support Central Connect の登録

前提条件

- ご使用の環境が内蔵リモートサポート登録の前提条件を満たしている。
- iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**リモートサポート**をクリックします。
   登録ページが表示されます。
2. **このサーバーを HPE remote Support ホストサーバーに接続**を選択します。
3. **ホストサーバーのホスト名または IP アドレス**および**ポート**番号を入力します。

   ホスト名、IPv4 アドレス、または IPv6 アドレスを入力できます。

   デフォルトポートは 7906 です。

4. **登録**をクリックします。

   iLO によって、登録プロセスが終了したことが通知されます。

5. （オプション）iLO と HPE リモートサポート間の接続を確認するために、テストイベントを送信します。
6. （オプション）システムイベントに関する電子メールアラートを受け取るには、アラートメールを構成します。

詳しくは

リモートサポート登録に関する前提条件
テストサービスイベントの送信

アラートメールを有効にする
サポートされるデバイスの Direct Connect から Central Connect リモートサポートへの変更

Insight Online Direct Connect からの登録の解除

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**リモートサポート**をクリックします。
2. **登録解除**をクリックします。
3. 要求を確認するメッセージが表示されたら、**はい、削除します**をクリックします。

   iLO によって、サーバーの登録が解除されたことが通知されます。

Insight Remote Support Central Connect の登録解除

手順

1. Insight RS Console にログインします。
2. 次のいずれかを実行します。
   - サーバーの監視を一時的に停止するには、Insight RS Console で、**デバイス** > **Device Summary** タブでサーバーを選択し、**ACTIONS** > **DISABLE SELECTED** を選択します。

     iLO の Web インターフェイスからサーバーの登録を直接解除することは、Insight RS Console でサーバーを一時的に無効にすることと同じです。
   - サーバーの監視を永久に停止するには、Insight RS Console からサーバーを削除します。サーバーを削除するには、**Device Summary** タブでサーバーを選択し、次に **ACTIONS** > **DELETE SELECTED** を選択します。
3. ナビゲーションツリーで**リモートサポート**をクリックします。

   登録ページが表示されます。
4. サーバーが登録されていないことを確認します。

リモートサポートサービスイベント

iLO がハードウェア障害（メモリ DIMM またはファンの問題など）を検出すると、サービスイベントが生成されます。サーバーがリモートサポートに登録されている場合、サービスイベントの詳細がサービスイベントログに記録されます。リモートサポートの構成に応じて、詳細は Insight Online（Direct Connect）または Insight RS ホストサーバー（Central Connect）に送信され、後者の場合、Hewlett Packard Enterprise に転送されます。Hewlett Packard Enterprise がサービスイベントを受信すると、サポートケースが開かれます（保証対象の場合）。計画メンテナンス中にメンテナンスモード機能を有効にすると、計画メンテナンス期間中にサポートケースを開くことができなくなります。

サービスイベントの送信

サービスイベントが発生した場合は、そのイベントに関する情報が Hewlett Packard Enterprise に送信されます。

サービスイベントの送信障害が発生した場合は、さらに 2 回追加で送信が試行されます。3 回の試行後もイベントを送信できない場合は、次が実行されます。

- SNMP トラップ（`cpqSm2IrsCommFailure 9020`）が生成されます。この SNMP トラップは、`cpqsm2.mib` ファイルで定義されています。
- 失敗がサービスイベントログに記録されます。
- 失敗が iLO イベントログに記録されます。
- サービスイベントは Active Health System のログに記録されます。
- 失敗メッセージは、Active Health System のログに記録されます。

メンテナンスモードの設定

サーバーでメンテナンスを実行する場合は、メンテナンスモードを使用します。メンテナンスモードが設定されると、Insight RS または Insight Online に送信される通信には、アクションが不要であることを示すフラグが付けられます。この機能により、Hewlett Packard Enterprise は、サポートケースを開くかどうかを判定できます。

前提条件

- iLO の設定を構成する権限
- サーバーがリモートサポートに登録されています。

手順

1. ナビゲーションツリーで**リモートサポート**をクリックし、**サービスイベント**タブをクリックします。
2. ✎（**メンテナンスモード**セクション内）をクリックします。

   メンテナンスモード設定の編集ページが開きます。
3. **メンテナンスモード**チェックボックスを選択します。
4. **失効**メニューから時間を選択します。
5. **適用**をクリックします。

   iLO によって、メンテナンスモードに設定されたことが通知されます。

   指定した期間を過ぎると、メンテナンスモードは自動的に終了します。必要に応じて、メンテナンスモードを手動でクリアできます。

   メンテナンスモードが設定されるか、期限切れになるか、クリアされると、iLO イベントログにイベントが記録されます。

メンテナンスモードの有効期限の編集

前提条件

- iLO の設定を構成する権限
- サーバーがリモートサポートに登録されています。
- メンテナンスモードが有効になっています。

手順

1. ナビゲーションツリーで**リモートサポート**をクリックし、**サービスイベント**タブをクリックします。

   サービスイベントページには、メンテナンスモードの残り時間が表示されます。

2. ✎（**メンテナンスモード**セクション内）をクリックします。

   メンテナンスモード設定の編集ページが開きます。

3. **失効**メニューで新しい値を選択し、 **適用**をクリックします。

   iLO によって、メンテナンスモードに設定されたことが通知されます。

   指定した期間を過ぎると、メンテナンスモードは自動的に終了します。必要に応じて、メンテナンスモードを手動でクリアできます。

   メンテナンスモードが設定されるか、期限切れになるか、クリアされると、iLO イベントログにイベントが記録されます。

メンテナンスモードのクリア

前提条件

- iLO の設定を構成する権限
- サーバーがリモートサポートに登録されています。

手順

1. ナビゲーションツリーで**リモートサポート**をクリックし、**サービスイベント**タブをクリックします。
2. ✎（**メンテナンスモード**セクション内）をクリックします。

   メンテナンスモード設定の編集ページが開きます。

3. **メンテナンスモード**チェックボックスをクリアして、**適用**をクリックします。

   メンテナンスモードがクリアされ、イベントが iLO イベントログに記録されることが iLO から通知されます。

メンテナンスモードのステータスの表示

前提条件

サーバーがリモートサポートに登録されています。

手順

ナビゲーションツリーで**リモートサポート**をクリックし、**サービスイベント**タブをクリックします。

メンテナンスモードセクションには、現在のメンテナンスモードのステータスが表示されます。

メンテナンスモードが有効になっている場合、残り時間が表示されます。残り時間は、ブラウザーウィンドウを更新するか、テストサービスイベントを送信するとアップデートされます。

テストサービスイベントの送信

リモートサポート設定が正しく機能していることを確認するため、テストイベントを送信できます。

前提条件

- iLO の設定を構成する権限
- サーバーがリモートサポートに登録されています。

手順

1. ナビゲーションツリーで**リモートサポート**をクリックし、**サービスイベント**タブをクリックします。
2. **テストイベントの送信**をクリックします。
3. 要求を確認するメッセージが表示されたら、**はい、送信します**をクリックします。

   送信が完了するとテストイベントは、サービスイベントログ、Insight RS Console（Central Connect のみ）、および Insight Online に表示されます。

   テストが成功すると、サービスイベントログの**送信ステータス**にエラーなしと表示されます。

   サービスイベントログの**生成時刻**列には、構成された iLO タイムゾーンに基づく日時が表示されます。
4. （オプション）リモートサポート構成に応じて、Insight Online または Insight RS Console でテストイベントを表示します。

詳しくは

Insight RS Console を使用したテストサービスイベントの表示
Insight Online を使用したテストサービスイベントの表示

Insight Online を使用したテストサービスイベントの表示

前提条件

リモートサポート用に登録されているサーバーで、テストサービスイベントが送信されました。

手順

1. 次の Web サイトに移動します。**https://www.hpe.com/info/insightonline**
2. HPE パスポートの認証情報を使用してログインします。
3. 記録されたサービスイベントの概要を表示するには、**サービスイベント**をクリックします。

   Insight Online は、サービスイベントの**生成時刻**の値を協定世界時（UTC）に変換します。
4. テストイベントを表示するには、**表示** > **テストイベント**を選択します。

   それ以上の処理は不要であるため、テストイベントは自動的に閉じます。

   Insight Online へのログイン後に発生したアクティビティを表示するには、更新ボタンをクリックします。

Insight RS Console を使用したテストサービスイベントの表示

前提条件

Insight Remote Support Central Connect 用に登録されているサーバーで、テストサービスイベントが送信されました。

手順

1. Insight RS Console にログインします（https://<Insight RS ホストサーバーの IP アドレス>:7906）。
2. **デバイス**ページに移動します。
3. ご使用のサーバーを登録を見つけて、デバイス名をクリックします。
4. **サービスイベント**タブをクリックします。
5. サービスイベントのリストが表示されます。
6. Insight RS は、サービスイベントの**生成時刻**の値を、Insight RS Console へのアクセスに使用するブラウザーのタイムゾーンに変換します。
7. それ以上の処理は不要であるため、テストイベントは自動的に閉じます。

サービスイベントログの表示

前提条件

サーバーがリモートサポートに登録されています。

手順

ナビゲーションツリーで**リモートサポート**をクリックし、**サービスイベント**タブをクリックします。

サービスイベントログの詳細

サービスイベントログには、サービスイベントごとに以下の情報が表示されます。

- **識別子** - サービスイベントを識別する一意の文字列。
- **生成時刻** - サービスイベントが生成された時刻。この列に、構成された iLO タイムゾーンに基づいて日時が表示されます。
- **イベント ID** - サービスイベントタイプの一意の番号。
- **認識された重大度** - イベント表示の重大度（たとえば、5-重度、7-致命的）。
- **送信ステータス** - イベント送信のステータス。イベントが正常に送信されると、ステータスはエラーなしになります。
- **送信先** - Insight Remote Support の Central Connect 構成の場合、サービスイベントを受信した Insight RS ホストサーバーのホスト名または IP アドレスおよびポート。Insight Online Direct Connect 構成の場合、**Insight Online** の値が表示されます。
- **イベントカテゴリ** - メッセージレジストリ内のメッセージ ID の説明に対応するイベントのカテゴリ。

サポートされるサービスイベントタイプ

HPE リモートサポートソリューションでは、以下のサービスイベントタイプがサポートされています。

イベント ID	説明
1	汎用のテストサービスイベント
100	ファン障害サービスイベント
101	システムバッテリ障害サービスイベント
200	電源装置障害サービスイベント
202	電源ヒューズ障害サービスイベント
300	物理ディスクドライブサービスイベント
301	Smart アレイコントローラアクセラレータバッテリ障害イベント
302	Smart アレイコントローラアクセラレータボードステータス変化イベント
303	Smart アレイコントローラステータス変化イベント
304	SAS 物理ドライブステータス変化イベント
305	ATA ディスクドライブステータス変化イベント
306	ファイバーチャネルホストコントローラーのステータス変化イベント
307	NVMe ドライブのステータス変化
308	NVMe ドライブの消耗ステータスの変化
309	SSD ドライブの消耗ステータスの変化
400	メモリモジュール障害または障害予測イベント
401	NVDIMM 障害
500	ストレージシステムのファンステータス変化イベント
501	ストレージシステムの電源装置ステータス変化イベント
600	訂正不能なマシンチェック例外イベント
1000	汎用 IML サービスイベント

サービスイベントログのクリア

前提条件

- iLO の設定を構成する権限
- サーバーがリモートサポートに登録されています。

手順

1. ナビゲーションツリーで**リモートサポート**をクリックし、**サービスイベント**タブをクリックします。
2. **Clear Event Log** をクリックします。

   iLO が要求を確認するように求めます。
3. **はい、クリアします**をクリックします。

   iLO によって、サービスイベントログがクリアされたことが通知されます。

リモートサポートのデータ収集

データ収集ページを使用して、リモートサポートにサーバーを登録するときに Hewlett Packard Enterprise に送信されるデータに関する情報を表示します。デバイス構成が変更されたときに、次にスケジュールされたデータ収集送信まで待てない場合は、このページを使用して Hewlett Packard Enterprise にデータ収集情報を手動で送信することもできます。

データ収集情報の送信

ご使用のリモートサポートの構成に応じて、iLO または Insight RS ホストサーバーが構成情報を Hewlett Packard Enterprise に送信し、お客様の保証およびサービス契約に応じて分析および予防サービスが実行されます。

- **Insight Online Direct Connect** - データは 30 日ごとに送信されます。データ収集スケジュールを編集したり削除したりすることはできません。
- **Insight Remote Support Central Connect** - データ送信の頻度は、Insight RS コンソールで構成します。詳しくは、Insight RS のオンラインヘルプを参照してください。

次にスケジュールされた送信まで待ちたくない場合は、以下の手順を使用してデータ収集を手動で送信します。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**リモートサポート**をクリックし、**データ収集**タブをクリックします。
2. **データ収集の送信**をクリックします。
3. 要求を確認するメッセージが表示されたら、**はい、送信します**をクリックします。

   送信が完了すると、**収集された最新の構成情報送信**および**収集された最新の構成情報送信ステータス**がアップデートされます。この日時は、構成されている iLO タイムゾーンに基づいています。
4. （オプション）Insight Online または Insight RS Console でデータ収集ステータスを表示します。

詳しくは

Insight Online でのデータ収集ステータスの表示
Insight RS Console（Insight Remote Support Central Connect のみ）でのデータ収集ステータスの表示

Active Health System が報告する情報の送信

使用するリモートサポート構成に応じて、iLO または Insight RS ホストサーバーが、サーバーのヘルス、構成、およびランタイムテレメトリーに関する情報を Hewlett Packard Enterprise に送信します。この情報は、問題のトラブルシューティングと閉ループ型の品質解析に使用されます。

- **Insight Online Direct Connect** - データは 7 日ごとに送信されます。Active Health System レポートのスケジュールを編集または削除することはできません。
- **Insight Remote Support Central Connect** - データは 7 日ごとに送信されます。Insight RS Console で Active Health System レポート送信曜日を変更することができます。詳しくは､Insight RS のオンラインヘルプを参照してください。

次にスケジュールされた送信まで待ちたくない場合は、以下の手順を使用して Active Health System レポート情報を手動で送信します。Active Health System 情報を **Active Health System** ページから直接ダウンロードすることもできます。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**リモートサポート**をクリックし、**データ収集**タブをクリックします。
2. **Active Health System レポートの送信**をクリックします。
3. 要求を確認するメッセージが表示されたら、**はい、送信します**をクリックします。

   収集したデータには、最新の 7 日間の Active Health System 情報が含まれます。

   送信が完了すると、**最新の Active Health System レポート送信**および**最新の Active Health System レポート送信のステータス**がアップデートされます。この日時は、構成されている iLO タイムゾーンに基づいています。
4. （オプション）Insight RS Console で **Active Health Service Collection** ステータスを表示します。

詳しくは

Insight RS Console（Insight Remote Support Central Connect のみ）でのデータ収集ステータスの表示

iLO でのデータ収集ステータスの表示

手順

ナビゲーションツリーで**リモートサポート**をクリックし、**データ収集**タブをクリックします。

データ収集の詳細

- **構成情報収集頻度（日数）**（Insight Online Direct Connect のみ） - データが Hewlett Packard Enterprise に送信される頻度。
- **収集された最新の構成情報送信** - 最後にデータが収集された日時。

- **収集された最新の構成情報送信ステータス** - 最後のデータ送信のステータス。
- **次の構成情報収集スケジュール**（Insight Online Direct Connect のみ） - データが次回 Hewlett Packard Enterprise に送信される日時。

iLO での Active Health System レポートステータスの表示

手順

ナビゲーションツリーで**リモートサポート**をクリックし、**データ収集**タブをクリックします。

Active Health System レポートの詳細

- **Active Health System レポート頻度（日数）**（Insight Online Direct Connect のみ） - Active Health System データが Hewlett Packard Enterprise に送信される頻度（日数）。
- **最新の Active Health System レポート送信** - 最後の Active Health System レポートの日時。
- **最新の Active Health System レポート送信のステータス** - 最新データ送信のステータス。
- **次にスケジュールされた Active Health System レポート**（Insight Online Direct Connect のみ） - Active Health System データが次回 Hewlett Packard Enterprise に送信される日時。

Insight Online でのデータ収集ステータスの表示

Insight Online のデバイスの概要ページには、収集された最新の構成情報送信のタイムスタンプが表示されます。

手順

1. Hewlett Packard Enterprise サポートセンター（**https://www.hpe.com/info/insightonline**）にログインします。
2. **デバイス**ページに移動します。
3. デバイスの名前をクリックします。

   概要ページの**設定**セクションに、最後のデータ収集送信の日時が表示されます。

   ヒント: Insight Online にサインインした後に発生したアクティビティを表示するには、更新ボタンをクリックします。

Insight RS Console（Insight Remote Support Central Connect のみ）でのデータ収集ステータスの表示

手順

1. Insight RS Console にログインします（https://<Insight RS ホストサーバーの IP アドレスまたは FQDN>: 7906）。
2. **デバイス**ページに移動します。
3. ご使用のサーバーを登録を見つけて、デバイス名をクリックします。
4. **構成情報収集**タブをクリックします。

収集タブには、構成情報収集および Active Health System レポート情報について、次の名前が表示されます。「**Server Basic Configuration Collection**」と「**Active Health Service Collection**」という名前が使用されます。収集を展開するには、**結果**アイコンの左にあるプラス記号（＋）をクリックします。追加情報を表示する、または収集ファイルをダウンロードするには、**詳細**をクリックします。

Insight RS では、iLO データ送信日時の値が、Insight RS Console へのアクセスに使用されているブラウザーのタイムゾーンに変換されます。

Insight Online Direct Connect のホストサーバーとして使用する ProLiant サーバーの登録

Hewlett Packard Enterprise は、Insight RS ホストサーバーとして使用されている ProLiant サーバーの Insight Online Direct Connect 登録をサポートしていません。Insight Online Direct Connect にアクティブなホストサーバーを登録すると、ホストサーバーによって監視されているすべてのデバイスは、リモートサポートを受けるための Hewlett Packard Enterprise との通信ができなくなります。

ProLiant サーバーをホストサーバーとして使用することを停止し、サーバーを Insight Remote Support Central Connect から登録解除した後、サーバーを Insight Online Direct Connect に登録するには、この手順を使用します。

手順

1. （オプション）Insight RS を使用して、監視対象デバイスのリストを含む一括 CSV ファイルをエクスポートします。

   詳しくは、**Insight RS のドキュメント**を参照してください。

   以前の監視対象デバイスを新しいホストサーバーに追加する場合は、後でこのファイルを使用できます。
2. ProLiant サーバー上の Insight RS ホストサーバーから監視されていたデバイスの登録を解除します。
3. Insight RS から ProLiant ホストサーバーの登録を解除します。
4. ProLiant サーバーから Insight RS をアンインストールします。
5. Insight Online Direct Connect に ProLiant サーバーを登録します。
6. （オプション）Insight RS を異なるサーバーにインストールし、新しいホストサーバーを構成します。
7. （オプション）新しいホストサーバーの Insight RS に一括 CSV ファイルをインポートします。

   詳しくは、**Insight RS のドキュメント**を参照してください。

詳しくは

Insight Remote Support Central Connect の登録解除
Insight Online Direct Connect の登録

サポートされるデバイスのリモートサポート設定の変更

Hewlett Packard Enterprise は、Insight Remote Support Central Connect と Insight Online Direct Connect へのデバイスの同時登録をサポートしていません。両方の構成を使用してデバイスを登録する場合、Hewlett Packard Enterprise と Insight Online に対して 2 つの通信パスを持つことになります。デバイス情報は、データが Hewlett Packard Enterprise に送信されるたびに上書きされます。

サポートされるデバイスの Central Connect から Direct Connect リモートサポートへの変更

手順

1. Insight Remote Support Central Connect からデバイスを登録解除します。
2. デバイスを Insight Online Direct Connect に登録する正しい時刻を決定します。

   iLO と Insight RS ホストサーバーが異なるタイムゾーンを使用していて、iLO が、Insight RS ホストサーバーより早いタイムゾーンを使用している場合は、デバイスをすぐに再登録しないでください。iLO の時刻が、デバイスを登録解除した時刻と同じか、それよりも遅くなるまで待ちます。

   たとえば、Insight RS ホストサーバーをフランスの現地時間に設定し、iLO システムをカリフォルニアの現地時間に設定したとします。フランスで現地時間午後 5 時にデバイスの登録を解除した場合、カリフォルニアでは現地時間午後 5 時まで待ってからデバイスを Insight Online Direct Connect に登録する必要があります。待たない場合、デバイスは Insight Online に表示されません。
3. 該当する場合は、手順 **2** で決められた時刻まで待ちます。
4. Insight Online Direct Connect にデバイスを登録します。

詳しくは

Insight Remote Support Central Connect の登録解除
Insight Online Direct Connect の登録

サポートされるデバイスの Direct Connect から Central Connect リモートサポートへの変更

手順

1. Insight Online Direct Connect からデバイスを登録解除します。
2. デバイスを Insight Remote Support Central Connect に登録する正しい時刻を決定します。

   iLO と Insight RS ホストサーバーが異なるタイムゾーンを使用していて、Insight RS ホストサーバーが、iLO より早いタイムゾーンを使用している場合は、デバイスをすぐに再登録しないでください。Insight RS ホストサーバーの時刻が、デバイスを登録解除した時刻と同じか、それよりも遅くなるまで待ちます。

   たとえば、iLO システムをフランスの現地時間に設定し、ホストサーバーをカリフォルニアの現地時間に設定したとします。フランスで現地時間午後 5 時にデバイスの登録を解除した場合、カリフォルニアでは現地時間午後 5 時まで待ってからデバイスを Insight Remote Support Central Connect に登録する必要があります。待たない場合、デバイスは Insight Online（有効な場合）に表示されません。
3. 該当する場合は、手順 **2** で決められた時刻まで待ちます。
4. Insight Remote Support Central Connect にデバイスを登録します。

詳しくは

Insight Online Direct Connect からの登録の解除
Insight Remote Support Central Connect の登録

iLO の管理機能の使用

iLO ユーザーアカウント

iLO では、セキュアメモリにローカルで保存されているユーザーアカウントを管理できます。

ユーザー指定のログイン名と高度なパスワード暗号化を使用してローカル ユーザー アカウントを最大 12 個作成することができます。権限は各ユーザーの設定を制御し、ユーザーのアクセス要件に合わせてカスタマイズできます。

iLO と連携し、サポートされるアプリケーションにサービスアカウントが必要な場合は、ユーザーアカウントを追加して、このアカウントをサービスアカウントとして指定できます。また、サポートされるアプリケーションまたは iLO RESTful API を使用して、サービスアカウントを追加することもできます。

13 ユーザー以上をサポートするには、ディレクトリサービスを使用してユーザーの認証や権限付与を行うよう iLO を構成します。

詳しくは

iLO のディレクトリの認証と認可設定

ローカルユーザーアカウントの追加

前提条件

ユーザーアカウント管理権限

手順

1. ナビゲーションツリーで**管理**をクリックします。

   ユーザー管理タブが表示されます。

2. **新規**をクリックします。
3. 次の詳細を入力します。

   - **ログイン名**
   - **ユーザー名**
   - **パスワード**と**パスワードの確認**

4. （オプション）事前定義されたユーザー権限セットを選択するには、**役割**メニューで役割を選択します。

   手動で権限を選択する場合は、デフォルトの役割（**カスタム**）を使用します。

5. 手順 **4** で**カスタム**を選択した場合 、次の権限から選択します。

   - **ログイン**
   - **リモートコンソール**
   - **仮想電源およびリセット**
   - **仮想メディア**

- **ホスト BIOS**
- **iLO 設定の構成**
- **ユーザーアカウント管理**
- **ホスト NIC 構成**
- **ホストストレージ構成**
- **リカバリセット**

使用できるすべてのユーザーの権限を選択するには、**すべてを選択**チェックボックスをクリックします。

6. （オプション）アカウントをサポートされているアプリケーションのサービスアカウントとして使用する場合は、**サービスアカウント**チェックボックスを選択します。

   サポートされているアプリケーションには、iLO Amplifier Pack や Onboard Administrator があります。

   サービスアカウントのプロパティは、最初のユーザーアカウントの作成時にのみ構成できます。既存のユーザーアカウントでこの設定を編集することはできません。

7. 新しいユーザーを保存するには、**ユーザーの追加**をクリックします。

   iLO はアカウントが追加されたことを通知します。

詳しくは

iLO ユーザーアカウントオプション
iLO ユーザーアカウントの権限
パスワードに関するガイドライン

ローカルユーザーアカウントの編集

前提条件

ユーザーアカウント管理権限

手順

1. ナビゲーションツリーで**管理**をクリックします。

   ユーザー管理タブが表示されます。

2. ユーザーアカウントを選択し、**編集**をクリックします。
3. 必要に応じて、以下の値をアップデートします。

   - **ログイン名**
   - **ユーザー名**

4. パスワードを変更するには、**パスワードを変更**チェックボックスをクリックし、**パスワード**と**パスワードの確認**の値をアップデートします。
5. （オプション）ユーザーアカウントの権限を変更する場合は、次のいずれかを実行します。

   - 手動で権限を選択するには、**役割**メニューで**カスタム**を選択して、リストから権限を選択します。

使用できるすべてのユーザーの権限を選択するには、**すべてを選択**チェックボックスをクリックします。

- 事前定義されたユーザー権限セットを選択するには、**役割**メニューから **Administrator**、**Operator**、または **ReadOnly** を選択します。

6. ユーザーアカウントの変更を保存するには、**ユーザーのアップデート**をクリックします。

   iLO は、選択したアカウントがアップデートされたことを通知します。

詳しくは

iLO ユーザーアカウントオプション
iLO ユーザーアカウントの権限
パスワードに関するガイドライン

ユーザーアカウントの削除

前提条件

ユーザーアカウント管理権限

手順

1. ナビゲーションツリーで**管理**をクリックします。

   ユーザー管理タブが表示されます。

2. 1 つまたは複数の削除するユーザーアカウントの横にあるチェックボックスを選択します。
3. **削除**をクリックします。
4. 要求を確認するメッセージが表示されたら、**はい、削除します**をクリックします。

   iLO は、選択されたアカウントが削除されたことを通知します。

iLO ユーザーアカウントオプション

- **ログイン名**は、iLO にログインするときに使用する名前です。この名前は、**ユーザー管理**ページのユーザーリスト、**セッションリスト**ページ、ユーザーアイコンをクリックしたときに表示されるメニュー、およびログに表示されます。**ログイン名**は、**ユーザー名**と同じである必要はありません。ログイン名の最大長は 39 文字です。ログイン名には印刷可能な文字を使用する必要があります。
- **ユーザー名**は、**ユーザー管理**ページのユーザーリストに表示されます。**ログイン名**と同じである必要はありません。ユーザー名の最大長は 39 文字です。**ユーザー名**には、印字可能な文字を使用する必要があります。わかりやすいユーザー名を割り当てると、各ログイン名の所有者を識別でき便利です。
- **新しいパスワード**および**パスワードの確認**では、iLO にログインするために使用するパスワードを設定および確認します。
- **役割**では、ユーザーアカウントを追加または編集するときに、事前定義されたユーザー権限セットを選択できます。カスタムオプションを使用して、カスタマイズされた権限セットを定義できます。
- **サービスアカウント**は、アカウントをサービスアカウントとして指定します。サービスアカウントは、iLO で動作するサポート製品で使用されます。

  サポートされているアプリケーションには、iLO Amplifier Pack や Onboard Administrator があります。

  サービスアカウントのプロパティは、最初のユーザーアカウントの作成時にのみ構成できます。既存のユーザーアカウントでこの設定を編集することはできません。

iLO ユーザーアカウントの権限

次の権限は、ユーザーアカウントに適用されます。

- **ログイン** - iLO にログインできます。
- **リモートコンソール** - ビデオ、キーボード、マウスの制御を含めホストシステムのリモートコンソールにアクセスできます。

  この権限を持つユーザーは BIOS にアクセスできるため、ホストベースの BIOS、iLO、ストレージ、およびネットワークタスクを実行できる場合があります。
- **仮想電源およびリセット** - ホストシステムの電源再投入やリセットを実行できます。これらの操作はシステムの可用性を中断します。この権限を持つユーザーは、**システムに NMI を生成**ボタンを使用してシステムを診断できます。
- **仮想メディア** - ホストシステム上の仮想メディア機能を使用できます。
- **ホスト BIOS** - UEFI システムユーティリティを使用してホスト BIOS 設定を構成できます。この権限は、アクティブなシステム ROM を冗長システム ROM で置き換えるために必要です。

  この権限は、ホストベースのユーティリティを使用した構成には影響しません。
- **iLO 設定の構成** - セキュリティ設定を含むほとんどの iLO 設定を構成し、iLO ファームウェアをアップデートすることができます。この権限は、ローカルユーザーアカウント管理を有効にしません。

  iLO を構成したら、すべてのユーザーからこの権限を取り消して、次のインターフェイスからの再構成を防止します。

  - iLO の Web インターフェイス
  - iLO RESTful API
  - CLI
  - HPQLOCFG

  次のインターフェイスにアクセスできるユーザーは、引き続き iLO を再構成できます。

  - UEFI システムユーティリティ
  - HPONCFG

  ユーザーアカウント管理権限を持つユーザーのみが、この権限を有効または無効にすることができます。
- **ユーザーアカウント管理** - ユーザーは、ローカル iLO ユーザーアカウントを追加、編集、および削除できます。この権限を持つユーザーは、すべてのユーザーの権限を変更できます。この権限が割り当てられていないと、本人の設定の表示と本人のパスワードの変更しか実行できません。
- **ホスト NIC 構成** - ホスト NIC 設定を構成できます。

  この権限は、ホストベースのユーティリティを使用した構成には影響しません。
- **ホストストレージ構成** - ホストストレージ設定を構成できます。

  この権限は、ホストベースのユーティリティを使用した構成には影響しません。
- **リカバリセット** - ユーザーがシステムリカバリセットを管理できるようにします。

  デフォルトでは、この権限はデフォルトの管理者アカウントに割り当てられます。この権限を別のアカウントに割り当てるには、すでにこの権限を持つアカウントでログインします。

  システムメンテナンススイッチで iLO セキュリティが無効にされている場合、この権限を使用できません。

次の権限は、CLI または RIBCL スクリプトを介して使用できません。

- ホスト NIC 構成
- ホストストレージ構成
- リカバリセット
- ホスト BIOS
- ログイン

次の権限は、UEFI システムユーティリティの iLO 5 構成ユーティリティから使用できません。

- リカバリセット
- ログイン

iLO ユーザーアカウントロール

Administrator

リカバリセット以外のすべての権限を有効にします。

Operator

iLO 設定の構成、ユーザーアカウントの管理、およびリカバリセット以外のすべての権限を有効にします。

ReadOnly

ログイン権限のみを有効にします。

カスタム（デフォルト）

ユーザーがカスタム権限セットを定義できるようにします。

パスワードに関するガイドライン

Hewlett Packard Enterprise では、ユーザーアカウントを作成およびアップデートする場合に、以下のパスワードに関するガイドラインに従うことをお勧めします。

- パスワードを使用する場合：
  - パスワードをメモまたは記録しないでください。
  - パスワードの共有は避けてください。
  - 辞書に載っている言葉を組み合わせたパスワードを使用しないでください。
  - 推測しやすい単語を含むパスワードを使用しないでください。たとえば、会社名、製品名、ユーザー名、ログイン名などです。
  - パスワードを定期的に変更します。
  - iLO デフォルト認証情報を安全な場所に保管します。
- 強化パスワードには、少なくとも以下の 3 つの特性が必要です。
  - 少なくとも 1 つの大文字 ASCII 文字
  - 少なくとも 1 つの小文字 ASCII 文字

- 少なくとも 1 つの ASCII 数字
- 少なくとも 1 つの他の文字タイプ（記号、特殊文字、句読点など）。

アクセス設定ページの**パスワードの複雑さ**設定を有効にした場合、ユーザーアカウントを作成または編集するときに iLO によってこれらのパスワード特性が強制されます。

- ユーザーアカウントのパスワードの最低文字数は、**アクセス設定**ページで設定します。構成された**最小パスワード長**値によって、パスワードの長さは最小 0 文字（パスワードなし）から最大 39 文字まで可能です。Hewlett Packard Enterprise では、8 文字以上の**最小パスワード長**を使用することをお勧めします。デフォルト値は 8 文字です。

  重要: 保護されたデータセンターの外側に拡大されることのない物理的に安全な管理ネットワークがない場合、**最小パスワード長**を 8 文字未満に設定しないでください。

詳しくは

iLO アクセス設定の構成
セキュリティガイドライン

IPMI/DCMI ユーザー

iLO ファームウェアは、IPMI 2.0 仕様に準拠しています。IPMI/DCMI ユーザーを追加する場合、ログイン名は最長 16 文字、パスワードは最長 20 文字です。

iLO ユーザー権限を選択すると、等価な IPMI/DCMI ユーザー権限が**上記の設定に基づく IPMI/DCMI 権限**ボックスに表示されます。

- **ユーザー** - ユーザーは読み取り専用アクセス権を持っています。ユーザーは、iLO の設定または書き込みやシステムの操作は実行できません。

  IPMI ユーザー権限については、すべての権限を無効にします。Operator レベルを満たさない権限の任意の組み合わせは、IPMI Operator です。

- **Operator** - Operator は、システムの操作を実行できますが、iLO を設定したり、ユーザーアカウントを管理したりすることはできません。

  IPMIOperator 権限については、リモートコンソール、仮想電源およびリセット、および仮想メディアを有効にします。Administrator レベルを満たさない Operator 以上の権限の任意の組み合わせは、IPMI Operator です。

- **Administrator** - Administrator は、すべての機能に対する読み取り/書き込みアクセス権を持っています。

  IPMI Administrator 権限については、すべての権限を有効にします。

ユーザーアカウントの表示

手順

1. ナビゲーションツリーで**管理**をクリックします。

   ユーザー管理ページが表示されます。

   ローカルユーザーテーブルには、各ローカルユーザーのログイン名、ユーザー名、および割り当てられている権限が表示されます。

   割り当てられた権限がチェックマークのアイコンで表示され、割り当てられていない権限が X アイコンで表示されます。

サービスアカウントが構成されている場合、**サービス**テーブルには、各サービスアカウントのログイン名、ユーザー名、および割り当てられている権限が表示されます。サービスアカウントが存在しない場合、このテーブルは表示されません。

2. （オプション）権限の名前を参照するには、カーソルを権限アイコン上に移動します。

詳しくは

iLO ユーザーアカウントオプション
iLO ユーザーアカウントの権限

iLO ディレクトリグループ

iLO ディレクトリグループは、Kerberos 認証とスキーマフリーディレクトリの統合で使用されます。iLO は最大 6 つのディレクトリグループをサポートします。

詳しくは

iLO での Kerberos 認証
スキーマフリーディレクトリ認証

ディレクトリグループの追加

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**管理**をクリックしてから、**ディレクトリグループ**タブをクリックします。
2. **新規**をクリックします。
3. **グループ情報**セクションで、以下の詳細を提供します。
   - **グループ DN**
   - **グループ SID**（Kerberos 認証および Active Directory 統合のみ）
4. 次の権限のいずれかを選択します。
   - **ログイン**
   - **リモートコンソール**
   - **仮想電源およびリセット**
   - **仮想メディア**
   - **ホスト BIOS**
   - **iLO の設定を構成**
   - **ユーザーアカウント管理**

- **ホスト NIC 構成**
- **ホストストレージ構成**
- **リカバリセット**

5. 新しいディレクトリグループを保存するには、**グループの追加**をクリックします。

詳しくは

ディレクトリグループのオプション
ディレクトリグループ権限
Active Directory の入れ子型グループ（スキーマフリー構成のみ）

ディレクトリグループの編集

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**管理**をクリックしてから、**ディレクトリグループ**タブをクリックします。
2. **ディレクトリグループ**セクションでグループを選択し、**編集**をクリックします。
3. **グループ情報**セクションで、以下の詳細を提供します。
   - **グループ DN**
   - **グループ SID**（Kerberos 認証および Active Directory 統合のみ）
4. 次の権限のいずれかを選択します。
   - **ログイン**
   - **リモートコンソール**
   - **仮想電源およびリセット**
   - **仮想メディア**
   - **ホスト BIOS 構成**
   - **iLO の設定を構成**
   - **ユーザーアカウント管理**
   - **ホスト NIC 構成**
   - **ホストストレージ構成**
   - **リカバリセット**
5. ディレクトリグループの変更を保存するには、**グループのアップデート**をクリックします。

詳しくは

ディレクトリグループのオプション
ディレクトリグループ権限
Active Directory の入れ子型グループ（スキーマフリー構成のみ）

ディレクトリグループの削除

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**管理**をクリックしてから、**ディレクトリグループ**タブをクリックします。
2. 削除するディレクトリグループの横にあるチェックボックスを選択します。
3. **削除**をクリックします。
4. 要求を確認するメッセージが表示されたら、**はい、削除します**をクリックします。

   グループが削除されたことが iLO によって通知されます。

ディレクトリグループのオプション

各ディレクトリグループには、DN、SID、およびアカウントの権限が含まれます。Kerberos ログインの場合、グループの SID は、iLO に設定されているディレクトリグループの SID と比較されます。ユーザーが複数のグループのメンバーである場合、そのユーザーアカウントにはすべてのグループの権限が付与されます。

グローバルグループおよびユニバーサルグループを使用して権限を設定できます。ドメインローカルグループは、サポートされていません。

ディレクトリグループを iLO に追加するときは、以下の値を設定します。

- **グループ DN**（セキュリティグループ DN） - このグループのメンバーには、グループに設定された権限が付与されます。ここで指定するグループは、ディレクトリに存在しなければならず、iLO にアクセスする必要があるユーザーは、このグループのメンバーでなければなりません。ディレクトリに存在する DN を入力します（たとえば、CN=Group1, OU=Managed Groups, DC=domain, DC=extension）。

  短縮された DN もサポートされます（たとえば、Group1）。短縮された DN は、一意に一致するものではありません。Hewlett Packard Enterprise では、完全修飾の DN を使用することをおすすめします。
- **グループ SID**（セキュリティ ID） - Microsoft セキュリティ ID（SID）は、Kerberos およびディレクトリグループの権限付与に使用されます。この値は、Kerberos 認証に必要です。必要な形式は、S-1-5-2039349 です。

Active Directory の入れ子型グループ（スキーマフリー構成のみ）

多くの組織では、ユーザーや管理者をグループ分けしています。このように整理すると、グループを 1 つまたは複数の iLO システムに関連付けることができるので便利です。グループメンバーを追加または削除すると、構成をアップデートできます。

Microsoft Active Directory では、あるグループを別のグループ内に配置した入れ子型のグループの作成がサポートされています。

スキーマフリー構成では、間接メンバー（プライマリグループの入れ子型グループであるグループのメンバー）であるユーザーに iLO へのログオンが許可されます。

CAC スマートカード認証を使用する場合は、入れ子型グループがサポートされません。

ディレクトリグループ権限

- **ログイン** - ディレクトリユーザーが iLO にログインできます。
- **リモートコンソール** - ディレクトリユーザーが、ビデオ、キーボード、マウスの制御を含めて、ホストシステムのリモートコンソールにアクセスできます。

  この権限を持つユーザーは BIOS にアクセスできるため、ホストベースの BIOS、iLO、ストレージ、およびネットワーク構成タスクを実行できる場合があります。
- **仮想電源およびリセット** - ディレクトリユーザーがホストシステムの電源再投入やリセットを実行できます。これらの操作はシステムの可用性を中断します。この権限を持つユーザーは、**システムに NMI を生成**ボタンを使用してシステムを診断できます。
- **仮想メディア** - ディレクトリユーザーがホストシステム上の仮想メディア機能を使用できます。
- **ホスト BIOS** - ディレクトリユーザーが UEFI システムユーティリティを使用することでホスト BIOS 設定を構成できます。

  この権限は、ホストベースのユーティリティを使用した設定には影響しません。
- **iLO 設定の構成** - ディレクトリユーザーはセキュリティ設定を含むほとんどの iLO 設定を構成し、iLO ファームウェアをアップデートすることができます。この権限は、ローカルユーザーアカウント管理を有効にしません。

  iLO を構成したら、すべてのユーザーからこの権限を取り消して、iLO Web インターフェイス、iLO RESTful API、HPQLOCFG、または CLI による再構成を防止します。UEFI システムユーティリティまたは HPONCFG にアクセスできるユーザーは、引き続き iLO を再構成することができます。ユーザーアカウント管理権限を持つユーザーのみがこの権限を有効または無効にできます。
- **ユーザーアカウント管理** - ディレクトリユーザーはローカルの iLO ユーザーアカウントを追加、編集、および削除できます。
- **ホスト NIC 構成** - ディレクトリユーザーがホスト NIC 設定を構成できます。

  この権限は、ホストベースのユーティリティを使用した設定には影響しません。
- **ホストストレージ構成** - ディレクトリユーザーがホストストレージ設定を構成できます。

  この権限は、ホストベースのユーティリティを使用した設定には影響しません。
- **リカバリセット** - ディレクトリユーザーがシステムリカバリセットを管理できます。

  デフォルトでは、この権限はデフォルトの管理者アカウントに割り当てられます。この権限を別のアカウントに割り当てるには、すでにこの権限を持つアカウントでログインします。

  セッションを開始したときにシステムメンテナンススイッチが iLO セキュリティを無効にするように設定されている場合、この権限を使用できません。

ディレクトリグループの表示

手順

1. ナビゲーションツリーで**管理**をクリックしてから、**ディレクトリグループ**タブをクリックします。

ディレクトリグループテーブルには、各グループのグループ DN、グループ SID、および割り当てられた権限が表示されます。

割り当てられた権限がチェックマークのアイコンで表示され、割り当てられていない権限が X アイコンで表示されます。

2. （オプション）権限の名前を参照するには、カーソルを権限アイコン上に移動します。

詳しくは

ディレクトリグループのオプション
ディレクトリグループ権限

ブート順序

ブート順序機能を使用すると、サーバーのブートオプションを設定できます。

ブートモード、ブート順序、あるいはワンタイムブートステータスの変更を行うと、サーバーのリセットが必要になります。リセットが必要な場合は、iLO によって通知されます。

サーバーが POST のときにサーバーのブート順序を変更しようとすると、エラーが発生します。POST 中はブート順序を変更できません。このエラーが発生した場合、POST が終了するのを待ってから、再試行してください。

サーバーブートモードの設定

ブートモード設定を使用して、サーバーで OS ブートファームウェアを検索する方法を定義します。UEFI またはレガシー BIOS を選択できます。

ブートモードが**レガシー BIOS** に設定されている場合、統合リモートコンソールと仮想メディアを使用した NVMe ドライブへの OS のインストールはサポートされていません。

前提条件

- iLO の設定を構成する権限
- レガシー BIOS モードを有効にするには、UEFI システムユーティリティでセキュアブート機能を無効にする必要があります。

手順

1. ナビゲーションツリーで**管理**をクリックして、**ブート順序**タブをクリックします。
2. **Unified Extensible Firmware Interface**（**UEFI**）または**レガシー BIOS** を選択し、**適用**をクリックします。

   iLO に、変更の確認を求めるメッセージが表示されます。この設定を変更すると、サーバーをリセットするまで、**ブート順序**のページで変更を追加することはできません。
3. **OK** をクリックします。
4. サーバーをリセットします。

サーバーブート順序の構成

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**管理**をクリックして、**ブート順序**タブをクリックします。

   仮想メディアが接続されると、iLO の Web インターフェイスのページ上部の**仮想フロッピー/USB キー**および**仮想 CD/DVD-ROM** のテキストの横に仮想メディアタイプが表示されます。

2. デバイスのブート順序を上下に移動するには、**サーバーのブート順序**リストでデバイスを選択し、**上へ**または**下へ**をクリックします。

   レガシー BIOS モードでは、以下のデバイスから選択します。

   - **CD/DVD ドライブ**
   - **USB ストレージデバイス**
   - **ハードディスクドライブ**
   - **ネットワークデバイス<番号>**。サーバー Ethernet カードおよび追加の NIC/FlexibleLOM カードはネットワークデバイス 1、2、3 などになります。

   UEFI モードでは、使用可能なブートデバイスのリストからオプションを選択します。

   注記: フロッピードライブはサポートされる iLO 仮想メディアデバイスですが、ブート可能なデバイスとしてはサポートされていません。

3. **適用**をクリックします。

   iLO によって、ブート順序が正常にアップデートされたことが確認されます。

ワンタイムブートステータスの変更

ワンタイムブートステータス機能を使用して、定義済みのブート順序を変更せずに、次回のサーバーリセット時に起動するメディアタイプを設定します。使用する手順は、サーバーがレガシー BIOS モードを使用するか UEFI モードを使用するかによって異なります。

レガシー BIOS モードでのワンタイムブートステータスの変更

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**管理**をクリックして、**ブート順序**タブをクリックします。
2. **ワンタイムブートオプションを選択**リストから、オプションを選択します。
3. **適用**をクリックします。

   iLO は、ワンタイムブートオプションが正常にアップデートされたことを確認します。

   現在のワンタイムブートオプションの値がアップデートされ、選択内容が示されます。

レガシー BIOS モードのワンタイムブートオプション

次のレガシー BIOS モードのワンタイムブートオプションがサポートされています。

注記: フロッピードライブはサポートされる iLO 仮想メディアデバイスですが、ブート可能なデバイスとしてはサポートされていません。

- **ワンタイムブートなし**
- **CD/DVD ドライブ**
- **USB ストレージデバイス**
- **ハードディスクドライブ**
- **ネットワークデバイス** - BIOS は有効なネットワークデバイスをスキャンします。サーバーは、成功するまで、検出されたデバイスを 1 台ずつ起動しようと試みます。
- **Intelligent Provisioning**
- **内蔵 UEFI シェル** - サーバーは、UEFI システムユーティリティから分離した組み込みシェル環境から起動します。

UEFI モードでのワンタイムブートステータスの変更

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**管理**をクリックして、**ブート順序**タブをクリックします。
2. **ワンタイムブートオプションを選択**リストから、オプションを選択します。
3. **ワンタイムブートオプションを選択**リストで **UEFI ターゲット**を選択した場合、**UEFI ターゲットオプションを選択**：リストからブートデバイスを選択します。

   たとえば、2 つのブート可能パーティションがあるハードドライブがある場合、次回のサーバーリセットで使用するパーティションを選択できます。
4. **適用**をクリックします。

   iLO は、ワンタイムブートオプションが正常にアップデートされたことを確認します。

   現在のワンタイムブートオプションの値がアップデートされ、選択内容が示されます。

UEFI モードのワンタイムブートオプション

次の UEFI モードワンタイムブートオプションがサポートされています。

注記: フロッピードライブはサポートされる iLO 仮想メディアデバイスですが、ブート可能なデバイスとしてはサポートされていません。

- **ワンタイムブートなし**
- **CD/DVD ドライブ**
- **USB ストレージデバイス**
- **ハードディスクドライブ**
- **ネットワークデバイス** - BIOS は有効なネットワークデバイスをスキャンします。サーバーは、成功するまで、検出されたデバイスを 1 台ずつ起動しようと試みます。
- **Intelligent Provisioning**
- **HTTP ブート** - ブート可能イメージの URI が ROM ベースのシステムユーティリティで定義されている場合、サーバーは HTTP URI で起動します。

このオプションは、ネットワーク設定の構成に DHCP サーバーを使用する構成でサポートされます。

- **UEFI ターゲット** - このオプションを選択した場合、**UEFI ターゲットオプションを選択**リストの使用可能なブートデバイスの一覧から選択できます。
- **内蔵 UEFI シェル** - サーバーは、UEFI システムユーティリティから分離した組み込みシェル環境から起動します。

ROM ベースユーティリティを次回のリセット時に起動

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**管理**をクリックして、**ブート順序**タブをクリックします。
2. ROM ベースのセットアップユーティリティを次回のサーバーのリセット時に読み込むには、**システムセットアップユーティリティを起動**をクリックします。

ライセンスキーのインストール

前提条件

- iLO の設定を構成する権限
- iLO ライセンスが、そのライセンスをインストールするサーバーでサポートされている。

  詳しくは、HPE iLO ライセンスガイドを参照してください。

手順

1. ナビゲーションツリーで**管理**をクリックし、**ライセンス**タブをクリックします。
2. **アクティブ化キー**ボックスにライセンスキーを入力します。

   アクティベーションキーボックスで、セグメント間でカーソルを移動するには、**Tab** キーを押す、またはボックスのセグメントの内側をクリックします。 **アクティベーションキー**ボックスのセグメントにデータを入力すると、カーソルは自動的に次に進みます。

   すでにキーがインストールされているサーバー上でライセンスキーをインストールした場合、現在のキーは新しいキーに置き換えられます。

   ライセンスキーをインストールすると、iLO に最後の 5 桁のみが表示されます。Hewlett Packard Enterprise では、後で必要になる場合に備えて、ライセンスキー情報を記録して保存することをお勧めします。
3. **インストール**をクリックします。

   エンドユーザー使用許諾契約を読み、合意したことを確認するプロンプトが iLO で表示されます。

   エンドユーザー使用許諾契約の詳細は、ライセンスパックオプションキットに記載されています。
4. **同意する**をクリックします。

   これで、ライセンスキーは有効になります。

ライセンス情報の表示

手順

ナビゲーションツリーで**管理**をクリックし、**ライセンス**タブをクリックします。

ライセンスの詳細

- **ライセンス** - ライセンス名
- **ステータス** - ライセンスのステータス
- **アクティベーションキー** - インストールされているキー

  セキュリティ保護のため、ライセンスキーの下 5 桁のみが表示されます。

iLO ライセンス

iLO 標準機能はすべてのサーバーに搭載され、サーバーのセットアップ、サーバーヘルスの監視、電力および温度制御の監視、およびリモートサーバー管理を簡素化します。

iLO ライセンスは、マルチユーザーコラボレーション用のグラフィカルリモートコンソール、ビデオの録画と再生のような機能や他の多くの機能を有効にします。

- 製品をインストールして使用するサーバーごとに 1 つの iLO ライセンスが必要です。
- ライセンスは譲渡できません。
- iLO Advanced ライセンスは Synergy コンピュートモジュールに自動的に付属します。
- iLO Advanced のライセンスは、2020 年 6 月 1 日以降に出荷された ProLiant e910 サーバーブレードに自動的に含まれています。
- ライセンスキーを失くした場合、HPE iLO ライセンスガイドに記載されている、失くしたライセンスキーに対する手順に従います。
- 詳しくは、**https://www.hpe.com/support/ilo-docs** で HPE iLO ライセンスガイドを参照してください。
  - 無料 iLO トライアルライセンスの入手
  - ライセンスキーの購入、登録、引き換え

iLO のライセンスキーを登録することの利点

ライセンスの登録は重要な手順です。以下のような利点があります。

- Hewlett Packard Enterprise サポートセンターへのアクセス（**https://www.hpe.com/support/hpesc**）。
- My HPE Software Center Web サイトからのソフトウェアアップデートへのアクセス（**https://www.hpe.com/downloads/software**）。
- My HPE Software Center Web サイトから、1 つの便利な場所ですべての Hewlett Packard Enterprise 製品ライセンスを追跡（**https://www.hpe.com/software/hpesoftwarecenter**）。
- 重要な製品アラートの受信。
- 一意の Hewlett Packard Enterprise サポート契約 ID（SAID）のアクティブ化。

Hewlett Packard Enterprise が迅速かつ個々に応じたサポートを提供できるように、SAID はお客様を識別し、お客様の製品を追跡します。

注記: 現時点の My HPE Software Center ポータルでは、SAID 契約を追跡しません。

iLO でのキーマネージャーの使用

iLO 5 でサポートされるキーマネージャーを、HPE の Smart アレイセキュア暗号化と UEFI 管理暗号化と一緒に使用できます。

HPE Smart アレイセキュア暗号化は、HPE Smart アレイコントローラーをサポートし、Hewlett Packard Enterprise サーバーに直接接続したハードディスクドライブまたは SSD ストレージに蓄積データの暗号化を提供します。256 ビットの XTS-AES アルゴリズムを使用することにより、HDD や SSD ボリュームの暗号化に統合ソリューションをもたらします。

UEFI 管理暗号化により、HPE Persistent Memory や NVMe ドライブなど、サポート対象のシステムデバイスで Data-at-rest 暗号化が可能になります。

キーマネージャーは、データ暗号化キーの生成、保存、操作、制御、アクセスの監査を行います。これを使用して、ビジネスクリティカルで機密性のある保存済みデータの暗号化キーへのアクセスを保護し維持することができます。

iLO が、キーマネージャーと他の製品との間のキー交換を管理します。iLO は、キーマネージャーとの通信に、自身の MAC アドレスに基づいた一意のユーザーアカウントを使用します。このアカウントを最初に作成するために、iLO は、管理者権限を持つ、キーマネージャーに以前から存在する展開ユーザーアカウントを使用します。展開ユーザーアカウントについて詳しくは、キーマネージャーのドキュメントを参照してください。

サポートされているキーマネージャー

iLO は以下のキーマネージャーをサポートしています。

- Utimaco Enterprise Secure Key Manager（ESKM）4.0 以降

  FIPS セキュリティ状態が有効になっている場合は、ESKM 5.0 以降が必要です。

  注意: ESKM を使用する場合は、アップデートされたコード署名証明書が含まれているソフトウェアアップデートを必ずインストールしてください。必要なアップデートをインストールしないと、ESKM は 2019 年 1 月 1 日後に再起動するとエラー状態になります。詳しくは、**ESKM のドキュメント**を参照してください。

- SafeNet AT KeySecure G350v 8.6.0
- Gemalto SafeNet KeySecure 150v 8.9.0

注記: CNSA セキュリティ状態を使用するよう iLO が構成されている場合、キーマネージャーの使用はサポートされません。

リモートキー管理の構成

手順

1. キー管理ソフトウェアをキーサーバーにインストールして構成します。

a. ローカルユーザーを作成します。

b. ローカルグループを作成します。

c. マスターキーを作成します。

詳しくは、サポートされているキーマネージャーソフトウェアのドキュメントを参照してください。

2. リモートキー管理をサポートするように iLO を構成します。

   a. **キーマネージャーサーバーを構成します**。

   b. **キーマネージャー構成の詳細を追加します**。

   c. **（オプション）キーマネージャーの構成をテストします**。

3. リモートキー管理モードで動作するように、サポートされているデバイスを構成します。

   - Smart アレイコントローラーについては、Secure Encryption ユーザーガイドを参照してください。
   - HPE Persistent Memory については、HPE Persistent Memory ユーザーガイドまたは UEFI システムユーティリティユーザーガイドを参照してください。
   - NVMe ドライブについては、UEFI システムユーティリティユーザーガイドを参照してください。

   これらのドキュメントは、Web サイト **https://www.hpe.com/support/hpesc** で入手できます。

4. （オプション）Smart アレイコントローラーのみ：iLO の**ストレージ情報**ページで、**暗号化ステータス**が**暗号化済**と表示されていることを確認します。

キーマネージャーサーバーの構成

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- CNSA セキュリティ状態を使用するよう iLO が構成されていない。

手順

1. ナビゲーションツリーで**管理**をクリックして、**キーマネージャー**タブをクリックします。
2. ★✎（**キーマネージャーサーバー**セクション内）をクリックします。

   キーマネージャーサーバー設定を編集ページが開きます。
3. 次の情報を入力します。

   - **プライマリキーサーバーアドレス**
   - **プライマリキーサーバーポート**
   - **セカンダリキーサーバーアドレス**
   - **セカンダリキーサーバーポート**

4. （オプション）プライマリおよびセカンダリキーサーバーを使用した構成でサーバーの冗長化を確認するには、**冗長化が必要**オプションを有効にします。

   Hewlett Packard Enterprise では、このオプションを有効にすることをお勧めします。

5. **OK** をクリックします。

キーマネージャーサーバーのオプション

プライマリキーサーバーアドレス

プライマリキーサーバーのホスト名、IP アドレス、または FQDN。この文字列の最大長は 79 文字です。

プライマリキーサーバーポート

プライマリキーサーバーポート。

セカンダリキーサーバーアドレス

セカンダリキーサーバーのホスト名、IP アドレス、または FQDN。この文字列の最大長は 79 文字です。

セカンダリキーサーバーポート

セカンダリキーサーバーポート。

冗長化が必要

このオプションが有効になっていると、iLO は、構成された両方のキーサーバーに暗号化キーがコピーされていることを確認します。

このオプションが無効になっていると、iLO は、構成された両方のキーサーバーに暗号化キーがコピーされていることを確認しません。

Hewlett Packard Enterprise では、このオプションを有効にすることをおすすめします。

キーマネージャー構成の詳細の追加

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- CNSA セキュリティ状態を使用するよう iLO が構成されていない。
- 少なくとも 1 つのキーマネージャーサーバーが構成されている。

手順

1. ナビゲーションツリーで**管理**をクリックして、**キーマネージャー**タブをクリックします。
2. ★✎（**キーマネージャー構成**セクション内）をクリックします。

   キーマネージャー構成設定を編集ページが開きます。
3. 次の情報を**キーマネージャー上の iLO アカウント**セクションに入力します。

- **アカウントグループ**
- （オプション）**キーマネージャーローカル CA 証明書名**

アカウント名の値は読み取り専用です。

4. 次の情報を**キーマネージャー管理者アカウント**セクションに入力します。
   - **ログイン名**
   - **パスワード**
5. **OK** をクリックします。

   iLO は情報要求をキーマネージャーサーバーに送信します。

   - **ilo-<iLO の MAC アドレス>**というアカウント名が存在しない場合：
     - **キーマネージャー管理者アカウント**セクションで入力したユーザーアカウントが、アカウント名を作成して、キーマネージャーのローカルユーザーとその生成済みパスワードに関連付けます。
     - アカウント名は、手順 **3** で入力したアカウントグループに追加されます。
   - **ilo-<iLO の MAC アドレス>**というアカウント名が存在する場合：
     - **キーマネージャー管理者アカウント**セクションで入力したユーザーアカウントが、キーマネージャーのローカルユーザーにアカウント名を関連付けて、新しいパスワードが生成されます。
     - **キーマネージャー管理者アカウント**セクションで入力したユーザーアカウントが、**ilo-<iLO の MAC アドレス>**アカウントに関連付けられたアカウントグループのメンバーでない場合、そのアカウントがアカウントグループに追加されます。
     - **ilo-<iLO の MAC アドレス>**がすでに、キーマネージャーのローカルグループのメンバーである場合、手順 **3** で入力したグループは無視されます。キーマネージャーでの既存のグループ割り当てが使用され、iLO の Web インターフェイスに表示されます。新しいグループの割り当てが必要な場合は、iLO 設定をアップデートする前にキーマネージャーをアップデートする必要があります。

   手順 **3** で**キーマネージャーローカル CA 証明書名**を入力した場合、**キーマネージャー**ページの**インポートされた証明書の詳細**セクションに証明書情報が一覧表示されます。

キーマネージャー構成の詳細

アカウント名

キーマネージャー上の iLO アカウントに表示されているアカウント名は **ilo-<iLO MAC アドレス>**です。アカウント名は読み取り専用で、iLO がキーマネージャーと通信するときに使用されます。

アカウントグループ

iLO ユーザーアカウントと、iLO がキーマネージャーにインポートしたキーで使用するために、キーマネージャー上に作成されたローカルグループ。キーはインポートされると、自動的に、同じグループに割り当てられたすべてのデバイスで使用可能になります。

グループと、キー管理でのグループの使用について詳しくは、セキュア暗号化インストール/ユーザーガイドを参照してください。

キーマネージャーローカル CA 証明書名

iLO が信頼済みのキーマネージャーサーバーと通信していることを確認するには、ローカル認証機関の証明書の名前をキーマネージャーに入力します。通常は **Local CA** という名前で、キーマネージャーのローカル CA の下に表示されます。iLO は証明書を取得し、それを使用して、今後のすべてのトランザクションでキーマネージャーのサーバーを認証します。

セキュア暗号化では、信頼された第三者認証機関または中間 CA の使用はサポートされません。

ログイン名

キーマネージャーで構成された管理者アクセス権を持つローカルユーザー名。このユーザー名はキーマネージャーデプロイメントユーザーです。

iLO でキーマネージャーの構成詳細を追加する前に、デプロイメントユーザーアカウントを作成する必要があります。

パスワード

キーマネージャーで構成された管理者アクセス権を持つローカルユーザー名に応じたパスワード。

キーマネージャー構成のテスト

構成設定を確認するには、キーマネージャー構成をテストします。以下のテストが試行されます。

- キーマネージャーソフトウェアのバージョンが iLO と互換性があることを確認します。
- TLS を使用してプライマリキーマネージャーサーバー（および構成されている場合はセカンダリキーマネージャーサーバー）に接続します。
- 構成済みの認証情報およびアカウントを使用して、キーマネージャーに認証します。

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- キーマネージャーがセットアップされ、iLO でキーマネージャーの構成が完了している。

手順

1. ナビゲーションツリーで**管理**をクリックして、**キーマネージャー**タブをクリックします。
2. をクリックします。

   テスト結果は、**キーマネージャーイベント**テーブルに表示されます。成功または失敗のメッセージが iLO の Web インターフェイスウィンドウの上部に表示されます。

キーマネージャーイベントの表示

前提条件

この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**管理**をクリックして、**キーマネージャー**タブをクリックします。
2. **キーマネージャーイベント**セクションまでスクロールします。

   各イベントがタイムスタンプと説明とともに一覧表示されます。

キーマネージャーログのクリア

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**管理**をクリックして、**キーマネージャー**タブをクリックします。
2. **キーマネージャーログ**をクリックします。

   iLO が要求を確認するように求めます。
3. **はい、クリアします**をクリックします。

言語パック

言語パックを使用すると、iLO の Web インターフェイスの表示言語を英語から、ユーザーが希望するサポート言語に変更できます。言語パックは、iLO Web インターフェイスと統合リモートコンソールの翻訳を提供します。

言語パックを使用する場合は、以下の点に注意してください。

- 提供されている言語パックは、日本語と簡体字中国語です。
- 英語版はアンインストールできません。
- 複数の言語パックをインストールできます。

  言語パックがインストールされている場合、同じ言語の新しい言語パックをインストールすると、インストールされている言語パックが置き換わります。
- 統合リモートコンソールは、現在の iLO セッションの言語を使用します。
- Windows システムでの Java IRC のローカリゼーションサポートでは、**地域と言語**コントロールパネルで正しい言語を選択する必要があります。
- Linux システムでの Java IRC のローカリゼーションサポートでは、指定した言語用のフォントがインストールされ、そのフォントを JRE が使用できることを確認してください。
- インストールした言語パックのテキスト文字列の翻訳がない場合には、テキストは英語で表示されます。
- iLO ファームウェアをアップデートする場合は、Hewlett Packard Enterprise では言語パックの内容が iLO の Web インターフェイスに対応するように、最新の言語パックをダウンロードすることをおすすめします。

iLO がセッションの言語を決定する方法

iLO は、次のプロセスに基づいて Web インターフェイスセッションの言語を決定します。

1. iLO Web インターフェイスへのログインに使用するコンピューターおよびブラウザーが前回と同じで、ユーザーが Cookie を消去していない場合は、当該の iLO プロセッサーとの最後のセッションの言語設定が使用されます。
2. Cookie がない場合は、現在のブラウザーの言語が使用されます。ただし、その言語が iLO でサポートされ、必要な言語パックがインストールされていなければなりません。
3. Internet Explorer のみ : ブラウザーの言語がサポートされていない場合は、OS の言語が使用されます。ただし、その言語が iLO でサポートされ、必要な言語パックがインストールされていなければなりません。
4. Cookie がなく、ブラウザーの言語も OS の言語もサポートされていない場合、iLO は設定済みのデフォルト言語を使用します。

フラッシュファームウェア機能で言語パックをインストール

前提条件

iLO の設定を構成する権限

手順

1. 次の Web サイトから言語パックをダウンロードします。**https://www.hpe.com/support/ilo5**
2. 言語パックの `LPK` ファイルを抽出します。
   - Windows コンポーネントの場合 : ダウンロードしたファイルをダブルクリックし、**解凍**ボタンをクリックします。ファイルを抽出する位置を選択して、**OK** をクリックします。
   - Linux コンポーネントの場合 : ファイル形式によって異なりますが、次のいずれかのコマンドを入力します。
     - `#./<language_pack_file_name>.scexe -unpack=/tmp/`
     - `#rpm2cpio <language_pack_file_name>.rpm | cpio -id`

   言語パックのファイル名は次のような形式です。`lang_<言語>_<バージョン>.lpk`
3. ナビゲーションツリーで**ファームウェア & OS ソフトウェア**をクリックし、**ファームウェアアップデート**クリックします。

   フラッシュファームウェアコントロールが表示されます。
4. 使用するブラウザーに応じて、**参照**または**ファイルの選択**をクリックします。
5. `lang_<言語>_<バージョン>.lpk` を選択し、**開く**をクリックします。
6. （オプション）言語パックファイルのコピーを iLO レポジトリに保存するには、**同様に、iLO レポジトリに保存**チェックボックスを選択します。
7. **フラッシュ**をクリックします。

   iLO は、インストール要求の確認を求めるメッセージを表示します。
8. **OK** をクリックします。

   iLO によって言語パックがインストールされ、リセットを開始し、ブラウザー接続が終了します。

接続が再確立されるまでに、数分かかることがあります。

詳しくは

ファームウェアおよびソフトウェアの表示および管理

言語パックの選択

次のいずれかの方法を使用して、インストール済みの言語パックを選択します。

手順

- ログインページに移動し、**言語**メニューで言語を選択します。
- iLO の Web インターフェイスページの一番上にある**言語**アイコンをクリックして、言語を選択します。
- ナビゲーションツリーで**管理**をクリックし、**言語**タブをクリックします。**インストールされた言語**リストで言語をクリックします。

デフォルト言語設定の構成

この iLO ファームウェアインスタンスのユーザー用のデフォルト言語を構成するには、以下の手順に従います。

前提条件

- iLO の設定を構成する権限
- 使用する言語の言語パックがインストールされていること。
- 使用する言語がブラウザーにインストールされ、他のインストール済みのブラウザー言語よりもこの言語が優先されるように設定されていること。

手順

1. ナビゲーションツリーで**管理**をクリックして、**言語**タブをクリックします。
2. **デフォルト言語**メニューで値を選択します。

   選択できる言語は英語です。英語以外の言語も言語パックがインストールされていれば選択できます。
3. **適用**をクリックします。

   デフォルト言語が変更されたことが、iLO によって通知されます。

   以降の iLO Web インターフェイスセッションでは、前のセッションからのブラウザーの Cookie がなく、ブラウザーまたは OS の言語をサポートしていない場合、iLO Web インターフェイスに構成済みのデフォルト言語を使用します。

詳しくは

フラッシュファームウェア機能で言語パックをインストール

現在の iLO Web インターフェイスセッション言語の構成

前提条件

使用する言語の言語パックがインストールされていること。

手順

1. ナビゲーションツリーで**管理**をクリックして、**言語**タブをクリックします。
2. **インストールされた言語**リストで言語の名前をクリックします。

   現在のブラウザーセッションの iLO Web インターフェイスが、選択された言語に変更されます。

詳しくは

フラッシュファームウェア機能で言語パックをインストール

言語パックのアンインストール

前提条件

- iLO の設定を構成する権限
- 削除する言語がデフォルト言語として構成されていません。
- 削除する言語が言語パックとしてインストールされました。英語は削除できません。

手順

1. ナビゲーションツリーで**管理**をクリックして、**言語**タブをクリックします。
2. 削除する言語の横にある🗑をクリックします。
3. 要求を確認するメッセージが表示されたら、**はい、削除**をクリックします。

   iLO によって選択した言語パックが削除され、再起動し、ブラウザー接続が終了します。

   接続が再確立されるまでに、数分かかることがあります。

ファームウェア検証

ファームウェア検証機能では、オンデマンドスキャンを実行したり、スケジュールされたスキャンを実施できます。検出された問題に対処するために、iLO を次のように構成できます。

- 結果を記録する。
- 結果を記録し、リカバリインストールセットを使用する修復処置を開始する。

スキャン結果に応じて、情報は Active Health System ログとインテグレーテッドマネジメントログに記録されます。

次のファームウェアタイプがサポートされています。

- iLO ファームウェア
- システム ROM（BIOS）
- システムプログラマブルロジックデバイス（CPLD）
- サーバープラットフォームサービス（SPS）ファームウェア（サポート対象のサーバーのみ）
- イノベーションエンジン（IE）ファームウェア

ファームウェア検証スキャンの実行中は、ファームウェアアップデートをインストールしたり、iLO レポジトリにファームウェアをアップロードしたりすることはできません。

無効な iLO またはシステム ROM（BIOS）のファームウェアが検出された場合は、無効なファイルが iLO レポジトリの隔離領域に保存されます。無効なファイルをダウンロードし、その種類と発生元を調べることができます。隔離されたイメージは **iLO レポジトリ**ページに表示されず、フラッシュファームウェア機能を使用すると選択できません。

サポートされる管理ツールがシステムリカバリイベントをリスンするように構成されている場合は、リカバリイベントをこのページから送信できます。

ファームウェア検証設定の構成

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. **管理**ページに移動し、**ファームウェア検証**タブをクリックします。
2. **スキャン設定**アイコン ☼ をクリックします。
3. **バックグランドスキャンを有効**を有効または無効の状態に設定します。
4. **整合性障害のアクション**を選択します。
5. **スキャン間隔**を日数で設定します。

   有効な値は 1～365 日です。
6. **送信**をクリックします。

ファームウェア検証スキャンオプション

- **バックグランドスキャンを有効** - ファームウェア検証スキャンを有効または無効にします。有効なとき、iLO がサポート対象のインストールファームウェアでファイル破損をスキャンします。
- **整合性障害のアクション** - ファームウェア検証スキャン中に問題が見つかったとき iLO が実行するアクションを決定します。
  - 結果を記録するには、**ログのみ**を選択します。
  - 結果を記録して修復アクションを開始するには、**ログおよび自動的に修復**を選択します。

    サポート対象のファームウェアタイプについて問題が検出された場合、iLO が保護されたインストールセットで影響を受けるファームウェアタイプがあるかを調べます。デフォルトでは、このセットはリカバリセットです。ファームウェアイメージを使用可能な場合、iLO がそのファームウェアイメージをフラッシュして修復を完了します。
- **スキャン間隔（日数）** - バックグランドスキャン頻度（日数）を設定します。有効な値は 1～365 です。

詳しくは

システムリカバリセット

ファームウェア検証スキャンの実行

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. **管理**ページに移動し、**ファームウェア検証**タブをクリックします。
2. **スキャンを実行**をクリックします。

   ファームウェア検証スキャンの実行中は、ファームウェアアップデートをインストールしたり、iLO レポジトリにファームウェアをアップロードしたりすることはできません。

   スキャン結果がページの上部に表示されます。

   障害が発生した場合、**ファームウェア検証**ページのファームウェアの状態が**障害/オフライン**に変わり、システムヘルスのステータスがクリティカルに変わり、イベントが IML に記録されます。ファームウェア検証スキャン機能が**ログおよび自動的に修復**に構成されている場合は、障害が発生したファームウェアはフラッシュされます。成功すると、ファームウェアの状態とシステムヘルスのステータスがアップデートされ、IML イベントは修正済みステータスに変わります。

   自動修復が構成されていない場合は、手動で修復を実行する必要があります。

ファームウェアヘルスステータスの表示

前提条件

この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

管理ページに移動し、**ファームウェア検証**タブをクリックします。

ファームウェアヘルスステータスの詳細

サポートされる各ファームウェアタイプについて、次の情報が表示されます。

ファームウェア名

インストールされているファームウェアの名前。

ファームウェアバージョン

ファームウェアバージョン。

ヘルス

ファームウェアのヘルスステータス。

状態

ファームウェアのステータス。値には、以下のものがあります。

- **有効** - ファームウェアは検証されており、有効です。
- **スキャニング** - ファームウェア検証スキャンが進行中か、起動しようとします。
- **フラッシング**—ファームウェアアップデートが進行中です。
- **障害/オフライン** - ファームウェアは検証できず、修復されませんでした。

リカバリセットバージョン

システムリカバリセットのファームウェアのバージョン。

このファームウェアタイプがシステムリカバリセットにない場合や、システムリカバリセットがない場合は、**未装着**が表示されます。

隔離されたファームウェアの表示

前提条件

この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

管理ページに移動し、**ファームウェア検証**タブをクリックします。

隔離されたファームウェアファイルは、**隔離**セクションに表示されます。

隔離されたファイルがない場合は、「`There are no items under quarantine`（検疫中のアイテムはありません。）」というメッセージが表示されます。

隔離されたファームウェアの詳細

隔離セクションには、無効なファームウェアファイルに関する以下の情報が表示されます。

名前

無効なファームウェアファイルの名前。

作成日

無効なファイルの作成日。

サイズ

無効なファイルサイズ。

個々の隔離されたファイルの詳細

リストのファイルをクリックすると、以下の詳細が表示されます。

- **名前**-隔離されたファイルの名前。
- **作成日**-無効なファイルの作成日。
- **ファイル名**-iLO レポジトリによって使用される名前。
- **イメージの URI**-隔離されたファイルの場所。

- **サイズ**-無効なファイルサイズ。
- **デバイス クラス**-iLO リポジトリのリソースとファームウェアのインベントリデータの間で関係付ける際に使用可能な ID。

隔離されたファームウェアのダウンロード

iLO レポジトリの Quarantine エリアにファイルを保存するかどうか、オフライン分析のためにファイルをダウンロードすることができます。

前提条件

この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. **管理**ページに移動し、**ファームウェア検証**タブをクリックします。
2. **隔離**セクションで、ダウンロードするファイルの横にある⭳をクリックします。

   ステータスメッセージには、ダウンロードの進捗状況が表示されます。
3. ファイルを保存または開くには、ブラウザーの指示に従います。

隔離されたファームウェアの削除

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- リカバリセット権限

手順

1. **管理**ページに移動し、**ファームウェア検証**タブをクリックします。
2. **隔離**セクションで、削除するファイルの横にある🗑をクリックします。

   iLO が要求を確認するように求めます。
3. **はい、削除**をクリックします。

フルシステムリカバリの開始

別の管理ツールを起動してフルシステムリカバリを開始するリカバリイベントを、iLO を使用して生成することができます。リカバリは、サーバーオペレーティングシステムのイメージの再構築に続き、システムリカバリセットのインストールを含めます。

⚠ **注意:** サーバーのイメージの再構築によって、既存のデータが失われる場合があります。

前提条件

- iLO の設定を構成する権限
- 仮想メディア権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- システムリカバリセットが iLO レポジトリに存在する。
- サポートされる管理ツール（iLO Amplifier Pack 1.15 以降など）がサーバーを管理するように構成されている。

手順

1. リカバリプロセスに、サーバーのシャットダウンが必要なコンポーネントが含まれている場合は、サーバーをシャットダウンします。
2. **管理**ページに移動し、**ファームウェア検証**タブをクリックします。
3. **リカバリイベントを送信**をクリックします。
4. **リカバリイベントを送信**ペインで、**はい、リカバリイベントを作成します**チェックボックスを選択して、**リカバリイベントを送信**をクリックします。

   リカバリイベントは、リカバリイベントをリスンするように構成されている管理ツールに送信されます。

   イベントが正常に送信されると、以下の情報イベントが IML に記録されます。

   `Firmware recovery is requested by Administrator.`（管理者がファームウェアリカバリを要求しています。）

詳しくは

システムリカバリセット

iLO のセキュリティ機能の使用

セキュリティガイドライン

iLO をセットアップして使用する場合は、セキュリティを最大化するために、次のガイドラインを考慮してください。

- 専用の管理ネットワーク上に iLO を構成します。

  Hewlett Packard Enterprise では、データネットワークとは別のプライベート管理ネットワークを確立することをお勧めします。管理ネットワークは、管理者のみがアクセスできるように構成します。

  共有ネットワークに iLO デバイスを接続する場合、iLO デバイスを個々のサーバーと考え、それらのデバイスをセキュリティおよびネットワークの監査対象に含まれるようにします。

- iLO は、インターネットに直接接続しないでください。

  iLO プロセッサーは、運用管理ツールであり、インターネットのゲートウェイではありません。ファイアウォール保護を提供する企業 VPN を使用してインターネットに接続します。

  重要: iLO がインターネットに直接接続されている場合、iLO ユーザーアカウントのパスワードをすぐに変更してください。

- 認証機関（CA）によって署名された SSL 証明書をインストールして、デフォルトの自己署名証明書を置き換えてください。

  SSL 証明書情報ページでこのタスクを実行できます。

- LDAP などの外部サービスの証明書をインストールします。
- デフォルトのユーザーアカウントを含め、ユーザーアカウントのパスワードを変更します。

  サーバーの管理者パスワードと同じガイドラインに従って iLO 管理パスワードを変更してください。

  このタスクは、**ユーザー管理**ページからも実行できます。

  重要: ユーザーアカウントを作成およびアップデートする場合、iLO ユーザーアカウントの**パスワードに関するガイドライン**に従います。

- すべての権限を持つユーザーアカウントを作成する代わりに、権限の数が少ないアカウントを複数作成します。
- iLO およびサーバーファームウェアを常に最新の状態に保持します。
- できれば Two-Factor 認証の認証サービス（Active Directory や OpenLDAP など）を使用します。

  この機能により、ネットワーク全体で同じログインプロセスを使用して認証および承認を行うことができます。同時に複数の iLO デバイスを制御する方法を提供します。ディレクトリは、時刻と位置に基づく非常に特殊なロールおよび権限で、iLO へのロールベースのアクセスを提供します。

- Two-Factor 認証を実装します。

  この機能により、さらにセキュリティが強化されます。特に、リモートで、またはローカルネットワークの外で接続できる場合に有効です。

- SNMP トラフィックを保護します。

  管理パスワードと同じガイドラインに従ってコミュニティストリングをリセットします。また、特定の送信元と送信先のアドレスのみを受け入れるようにファイアウォールまたはルーターを設定します。必要ない場合は、サーバーで SNMP を無効にします。

- 使用しないポートおよびプロトコル（**SNMP** や **IPMI/DCMI over LAN** など）を無効にします。

  アクセス設定ページでこのタスクを実行できます。

- .NET リモートコンソールに HTTPS を使用します。

  このオプションを構成するには、認証局（CA）によって署名された信頼できる SSL 証明書をインストールし、**IRC は iLO 内の信頼済みの証明書を要求します**設定を有効にします。

  これらの構成手順は、それぞれ、**セキュリティ**タブの **SSL 証明書情報**ページと**リモートコンソール&メディア**ページで完了することができます。

- 使用しない機能（リモートコンソールなど）を無効にします。

  アクセス設定ページでこのタスクを実行できます。

- サーバー OS コンソールを自動的にロックするようにリモートコンソールを構成します。

  このオプションを構成するには、**リモートコンソール&メディア**ページの**セキュリティ**タブにある、**リモートコンソールのコンピューターロック**設定を構成します。

- **暗号化設定**ページで、より高いセキュリティ状態を構成してください。

- UEFI システムユーティリティで iLO 5 構成ユーティリティを無効にするか、ユーザーがアクセスする場合にログイン認証情報を要求するように iLO を構成します。

  アクセス設定ページでこのタスクを実行できます。

- 認証エラーを記録するよう iLO を構成します。

  アクセス設定ページでこのタスクを実行できます。

- ファームウェア検証スキャンを有効にします。

  このタスクは、**ファームウェア検証**ページで実行できます。

- **セキュリティダッシュボード**ページを使用して、セキュリティリスクと推奨事項を監視します。

- **セキュリティログ**を使用して、セキュリティ関連のイベントを監視します。

- **ホスト認証が必要**機能を有効にします。

  アクセス設定ページでこのタスクを実行できます。

- **ダウングレードポリシー**を、**ダウングレードにはリカバリセットの権限が必要です**に設定します 。

  アクセス設定ページでこのタスクを実行できます。

- リカバリセットを最新の状態に保ちます。

- HTTP 接続経由のアクセスを防ぐように iLO を構成します。

  この動作を構成するには、認証局（CA）によって署名された信頼できる SSL 証明書をインストールし、**IRC は iLO 内の信頼済みの証明書を要求します**設定を有効にします。

  これらの構成手順は、それぞれ、**セキュリティ**タブの **SSL 証明書情報**ページと**リモートコンソール&メディア**ページで完了することができます。

  この構成では、iLO Web インターフェイスにアクセスすると、iLO が応答ヘッダーで HTTP Strict Transport Security（HSTS）フラグを返します。これにより、ブラウザーは HTTP 要求を HTTPS に自動的にリダイレクトできます。

詳しくは、**Top 10 security settings for HPE iLO 5** および **Recommended Security Settings in HPE iLO 5** のビデオをご覧ください。

重要なセキュリティ機能

次の Web インターフェイスページで、iLO セキュリティ機能を設定します。

アクセス設定

- iLO インターフェイスおよび機能を有効または無効にします。
- iLO が使用する TCP/IP ポートをカスタマイズします。
- 認証失敗ログおよび遅延を設定します。
- iLO 5 構成ユーティリティを保護します。

iLO サービスポート

iLO サービスポートの可用性、認証、およびサポートされるデバイスを構成します。

セキュアシェルキー

SSH キーを iLO ユーザーアカウントに追加し、セキュリティを強化します。

証明書マッピングおよび CAC スマートカード

CAC スマートカード認証を設定して、ローカルユーザーのスマートカード証明書を設定します。

SSL 証明書

X.509 CA 署名証明書をインストールして、暗号化通信を有効にします。

ディレクトリ

Kerberos 認証とディレクトリ統合を構成します。

iLO は、ディレクトリサービスを使用してユーザーの認証や権限付与を行えるように設定することができます。この構成により、ユーザーの数の制限がなくなります。また、この構成は、エンタープライズ内の iLO デバイスの数に合わせて、簡単に拡張できます。ディレクトリにより iLO デバイスとユーザーを集中的に管理することもでき、より強力なパスワードポリシーを適用できます。

暗号化

iLO のセキュリティ状態をデフォルト値（製品）から強力な設定に変更して、高度なセキュリティ環境を実装します。

HPE SSO

サポートされているツールで、iLO によるシングルサインオンを設定します。

ログインセキュリティバナー

iLO ログインページにセキュリティ通知を追加します。

iLO の機能によって使用されるポート

ネットワーク設定とポート

表 2: iLO 経由で構成可能なネットワーク設定とポートにリストされている値を、サイトの要件またはセキュリティのイニシアチブに適合するように構成できます。これらの設定は、**iLO アクセス設定**ページで構成できます。

表 2: iLO 経由で構成可能なネットワーク設定とポート

説明	デフォルト設定またはポート	プロトコルタイプ
IPMI/DCMI over LAN ポート	623	UDP
IPMI/DCMI over LAN LAN 経由の iLO との IPMI/DCMI通信を許可するかどうかを指定します。	デフォルトは、無効です。	
リモートコンソールポート	17990	TCP
リモートコンソール iLO リモートコンソール経由のアクセスを有効または無効にすることができます。	初期設定では有効になっています。	
セキュアシェル（SSH）ポート	22	TCP
セキュアシェル（SSH） SSH 機能を有効または無効にすることができます。 SSH は、iLO コマンドラインプロトコル（CLP）に暗号化されたアクセスを提供します。	初期設定では有効になっています。	
SNMP ポート	161	UDP
SNMP Trap Port	SNMP アラートの場合は 162（送信のみ）。	UDP
SNMP iLO が外部の SNMP 要求に応答するかどうかを指定します。	初期設定では有効になっています。	
仮想メディアポート	17988	TCP
仮想メディア 仮想メディアを有効にするか無効にするかを指定できます。	初期設定では有効になっています。	
Web サーバー非 SSL ポート（HTTP）	80	TCP

表は続く

説明	デフォルト設定またはポート	プロトコルタイプ
Web サーバーの SSL ポート（HTTPS）[1]	443	TCP
Web サーバー iLO Web サーバー経由のアクセスを有効または無効にすることができます。	初期設定では有効になっています。	

[1] Direct Connect Remote Support では、この値を 443 に設定する必要があります。

その他の発信ポート

セキュリティ管理者は、**表 3: iLO が使用するその他のポート**にリストされているポートを知っておく必要がある場合があります。これらのポートは、サードパーティの送信サービス用です。

表 3: iLO が使用するその他のポート

説明	既定のポート	プロトコルタイプ	iLO の Web インターフェイスの場所
DNS 解決	53	UDP	該当なし
iLO 連携/SSDP マルチキャスト	1900	UDP	該当なし
DHCPv4	67、68	UDP	該当なし
DHCPv6	547	UDP	該当なし
NTP	123	UDP	該当なし
WINS	42	UDP	該当なし
Kerberos KDC サーバーポート	88	TCP、UDP	**セキュリティ** > **ディレクトリ**
ディレクトリサーバー LDAP SSL ポート	636	TCP	**セキュリティ** > **ディレクトリ**
アラートメール SMTP ポート	25	TCP	**管理** > **アラートメール**
Remote Syslog Port	514	UDP	**管理** > **リモート Syslog**
キーマネージャーのポート	9000	TCP	**管理** > **キーマネージャー**
リモートサポートのポート	7906	TCP	**Remote Support** > **登録**

iLO でサポートされていないポート

iLO は、**表 4: サポートされていないポート**にリストされている一般的に使用されるポートをサポートしていません。

表 4: サポートされていないポート

説明	ポート	プロトコルタイプ	注記
セキュリティ保護されていない LDAP · 接続（TCP） · コネクションレス（UDP）	389	TCP/UDP	iLO は発信 LDAP 接続にセキュアポート 636 を使用します。
グローバルカタログに対してセキュリティ保護されていない LDAP · 接続（TCP） · コネクションレス（UDP）	3268	TCP/UDP	iLO はセキュア LDAP 接続を使用します。

iLO アクセス設定

アクセス設定のデフォルト値は、ほとんどの環境に適しています。**アクセス設定**ページで変更できる値を使用すると、特殊環境向けの iLO 外部アクセス方法をカスタマイズできます。

アクセス設定ページに入力された値は、すべての iLO ユーザーに適用されます。

iLO アクセス設定の構成

この手順は、iLO 機能を除くすべてのアクセス設定を対象とします。iLO 機能を無効にするには、**iLO 機能の無効化**を参照してください。

前提条件

- すべてのアクセス設定の変更に関する前提条件：
  - iLO の設定を構成する権限
- **アップデートサービス**設定の変更に関する前提条件：
  - iLO の設定を構成する権限
  - リカバリセット権限
  - この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**セキュリティ**をクリックします。

   アクセス設定ページが表示されます。

2. アップデートしたいアクセス設定カテゴリの隣にある✎をクリックします。

   以下から選択します。

- **サーバー**
- **アカウントサービス**
- **iLO**
- **アップデートサービス**
- **ネットワーク**

編集*設定タイプ*ページが開きます。

3. 必要に応じて、設定をアップデートし、**OK** をクリックします。

   変更した設定のタイプに応じて、以下が実行される場合があります。

   - iLO が、アップデートが完了したことを通知します。
   - iLO が、保留中の変更を有効にするにはリセットを必要であることを通知します。

     設定によっては、リセットが完了する前に、設定の変更時に即座に影響することがあります。たとえば、リモートコンソールを介したアクセスを無効にした場合、**OK** をクリックするとリモートコンソールセッションを開始できません。構成の変更を完了するには、リセットが必要です。

     リセットが必要なその他の設定では、リセットを行わずに手動で構成を元の状態に戻すことができます。これらの設定の場合は、手動で変更を元に戻して、✕をクリックして、リセットメッセージを無視します。たとえば、仮想 NIC 機能を有効にした場合、保留中の変更にリセットが必要であることが、iLO から通知されます。仮想 NIC オプションを無効にリセットして手動でこの変更を元に戻すと、保留中のリセットメッセージは残され、✕をクリックして、メッセージを無視できます。

     画面またはダイアログボックスで✕をクリックすると、リセットメッセージは破棄されますが、iLO 構成が前の設定に戻されることはありません。変更を元に戻す場合は、手動で変更を元に戻す必要があります。

4. （オプション）**2**～**3** の手順を繰り返して、追加のアクセス設定をアップデートします。
5. リセットが必要な場合、アクセス設定のアップデートが完了したら、**iLO をリセット**をクリックします。

   iLO が要求を確認するように求めます。

6. **はい、iLO をリセットします**をクリックします。

   接続が再確立されるまでに、数分かかることがあります。

詳しくは

iLO 機能の無効化

iLO 機能の無効化

iLO 機能設定は、iLO 機能が使用可能かどうかを制御します。

- この設定が有効（デフォルト）になっている場合、iLO ネットワークを使用でき、オペレーティングシステムドライバーとの通信がアクティブです。
- この設定が無効になっている場合、iLO ネットワークと、オペレーティングシステムドライバーとの通信が切断されます。

  iLO 機能は、ProLiant サーバーブレードまたは Synergy コンピュートモジュールでは無効にできません。

この手順を使用して、iLO 機能の設定を変更します。他の iLO アクセス設定をアップデートするには、**iLO アクセス設定の構成**を参照してください。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**セキュリティ**をクリックします。

   アクセス設定ページが表示されます。

2. ✎（**iLO** セクションの横）をクリックします。

   iLO 設定の編集ページが表示されます。

3. **アドバンスト設定を表示**をクリックします。

4. **iLO 機能**セクションで**無効**をクリックします。

   iLO が要求を確認するように求めます。

5. **iLO の機能の無効の確認**チェックボックスを選択します。

6. **はい、iLO の機能を無効にします**をクリックします。

   > ⚠ **注意:** このボタンをクリックした場合、iLO にはどのインターフェイスからもアクセスできなくなります。iLO の機能をリストアするには、UEFI システムユーティリティを使用できます。

   iLO はセッションを終了します。**iLO 機能**設定を再度有効にするまで、どの iLO インターフェイスからも接続できません。

7. （オプション）**iLO 機能を再度有効にする**には、UEFI システムユーティリティまたはシステムメンテナンススイッチを使用します。

   Hewlett Packard Enterprise では、UEFI システムユーティリティを使用してこの作業を実行することをお勧めします。

詳しくは

iLO アクセス設定の構成
iLO セキュリティを無効にする理由

iLO 機能を有効にする方法

iLO 機能が無効になっている場合、iLO Web インターフェイスから機能を再度有効にすることはできません。UEFI システムユーティリティまたはシステムメンテナンススイッチを使用して、**iLO 機能**を再度有効にすることができます。

UEFI システムユーティリティ

Hewlett Packard Enterprise では、UEFI システムユーティリティを使用して **iLO 機能**を再度有効にすることをお勧めします。

詳しくは、UEFI システムユーティリティドキュメントを参照してください。

システムメンテナンススイッチ

iLO 機能をリストアする別の方法は、システムメンテナンススイッチを使用して iLO セキュリティを無効にするというものです。

iLO セキュリティを無効にすると、iLO のネットワーク構成が工場出荷時のデフォルト設定にリセットされます。工場出荷時のデフォルトネットワークインターフェイスがネットワークに接続されている場合、iLO はネットワーク上で利用可能です。この変更は iLO セキュリティをリストアした後も持続します。

注意: セキュリティを無効にし、iLO が本番環境のセキュリティ状態を使用している場合、どのユーザーも iLO にアクセスして構成を変更することができます。システムメンテナンススイッチを使用してセキュリティを無効にする場合、Hewlett Packard Enterprise では、この構成で iLO を使用する時間をできるだけ短くすることを強くお勧めします。

サーバーアクセス設定オプション

アクセス設定ページの**サーバー**セクションでは、以下の設定を構成できます。

サーバー名

ホストサーバー名を指定することができます。この値を手動で割り当てることができますが、オペレーティングシステムをロードするとホストソフトウェアによって上書きされることがあります。サーバー名は最大 49 バイトまで入力できます。

サーバーの FQDN/IP アドレス

サーバーの FQDN または IP アドレスを指定できます。この値を手動で割り当てることができますが、オペレーティングシステムをロードするとホストソフトウェアによって上書きされることがあります。FQDN または IP アドレスは最大 255 バイトまで入力できます。

アカウントサービスのアクセス設定オプション

アクセス設定ページの**アカウントサービス**セクションでは、以下の設定を構成できます。

遅延前の認証の失敗時

iLO がログイン遅延を課すまでに許容されるログインの失敗数を設定できます。

有効な値は次のとおりです。

- **毎回の失敗時でも遅延なし**—ログイン試行の最初の失敗後、ログイン遅延が発生します。
- **1 回目の失敗時では遅延なし**（デフォルト）—ログイン試行に 2 回失敗するまで、ログイン遅延は発生しません。
- **3 回目の失敗時では遅延なし**—ログイン試行に 4 回失敗するまで、ログイン遅延は発生しません。
- **5 回目の失敗時では遅延なし**—ログイン試行に 6 回失敗するまで、ログイン遅延は発生しません。

認証の失敗時の遅延時間

ログインに失敗した後の iLO ログイン遅延の継続期間を構成できます。有効な値は 2、5、10、および 30 秒です。

デフォルト値は 10 秒です。

認証失敗ログ

認証失敗のログ記録条件を構成できます。以下の設定が有効です。

- **有効-毎回失敗時**— ログインに失敗するたびに、失敗したログインログエントリーが記録されます。
- **有効-2 回の失敗ごと**— ログイン試行に 2 回失敗するごとに、ログインの失敗のログエントリーが記録されます。
- **有効-3 回の失敗ごと**（デフォルト） — ログイン試行に 3 回失敗するごとに、ログインの失敗のログエントリーが記録されます。

- **有効-5 回の失敗ごと**— ログイン試行に 5 回失敗するごとに、ログインの失敗のログエントリーが記録されます。
- **無効**— ログインの失敗のログエントリーは記録されません。

最小パスワード長

ユーザーパスワードの設定または変更の際に許可される文字の最小数を指定します。指定する文字数は、0～39 文字の値でなければなりません。デフォルト値は 8 です。

パスワードの複雑さ設定を有効にした場合、iLO は、最小パスワード長を満たすパスワードを許可しないことがあります。たとえば、最小パスワード長を 1 に設定した場合、1 文字のパスワードはパスワードの複雑さ要件を満たさないため無効になります。

パスワードの複雑さ

ユーザーアカウントおよび iLO 連携グループを作成するときのパスワードの複雑さチェックの動作を制御します。

この設定を有効にすると、新しいまたはアップデートしたユーザーアカウントパスワードには、次の特性のうちの 3 つが含まれる必要があります。

- 少なくとも 1 つの大文字 ASCII 文字
- 少なくとも 1 つの小文字 ASCII 文字
- 少なくとも 1 つの ASCII 数字
- 少なくとも 1 つの他の文字タイプ（記号、特殊文字、句読点など）

この設定を無効（デフォルト）にした場合、これらのパスワード特性は適用されません。

iLO アクセス設定オプション

アクセス設定ページの **iLO** セクションでは、以下の設定を構成できます。

アイドル接続タイムアウト（分）

iLO セッションで、ユーザーの操作がないまま経過し、自動的に終了するまでの時間を指定します。

各接続は別個のセッションであるため、iLO Web インターフェイスおよび.NET IRC および Java IRC は、アイドル時間を別々に追跡します。アイドル接続タイムアウトに達すると、アイドル状態のセッションのみが終了します。

iLO Web インターフェイスと HTML5 コンソールは、1 つの iLO セッションを共有します。アイドル接続タイムアウトに達すると、共有セッションは終了します。

有効な値は次のとおりです。

- **15**、**30**、**60**、**120** 分間 — デフォルト値は 30 分です。
- **無限** - 非アクティブなユーザーはログアウトされません。

異なるサイトにアクセスしたりブラウザーウィンドウを閉じたりすることによって iLO からログアウトしなかった場合も、アイドル接続になります。iLO ファームウェアがサポートする接続数には制限があります。**無限**タイムアウトオプションを乱用すると、他のユーザーが iLO にアクセスできなくなる場合があります。アイドル接続は、期限が切れると再利用されます。

この設定は、ローカル/ディレクトリのユーザーに適用されます。ディレクトリサーバータイムアウト設定は、iLO 設定を優先的に使用する場合があります。

設定を変更しても、現在のユーザーセッションでただちに有効にならない場合がありますが、すべての新しいセッションでただちに強制設定されます。

iLO 機能

この設定については、**iLO 機能の無効化**を参照してください。

iLO RIBCL インターフェイス

iLO と通信するために RIBCL インターフェイスを使用できるかどうかを指定します。この設定はデフォルトで有効になっています。

この機能を無効にすると、HTTP/HTTPS を介した RIBCL、インバンド通信経由の RIBCL、および OA ポート経由の RIBCL は機能しません。

HPE OneView から Insight Remote Support Central Connect またはリモートサポートにサーバーを登録する場合、このオプションを有効にする必要があります。

無効の場合、RIBCL を使用しようとすると次のメッセージが表示されます。

```
<?xml version="1.0"?>
<RIBCL VERSION="2.23">

<RESPONSE
STATUS="0x00FC"
MESSAGE='RIBCL is disabled.'
/>
</RIBCL>
```

この値を変更するときは、iLO をリセットする必要があります。

iLO ROM ベースセットアップユーティリティ

UEFI システムユーティリティの iLO 構成オプションを有効または無効にします。

- この設定が有効（デフォルト）になっている場合、UEFI システムユーティリティへのアクセス時に iLO 構成オプションを使用できます。
- この設定が無効になっている場合、UEFI システムユーティリティへのアクセス時に iLO 構成オプションを使用できません。

システム BIOS でオプション ROM のプロンプトが無効になっている場合、この設定を有効にできません。

iLO Web インターフェイス

iLO と通信するために iLO Web インターフェイスを使用できるかどうかを指定します。この設定はデフォルトで有効になっています。

この値を変更するときは、iLO をリセットする必要があります。リセットの完了後は、UEFI システムユーティリティまたは iLO RESTful API を使用してこの設定を再度有効にするまで、Web ブラウザー経由で iLO インターフェイスにアクセスすることはできません。

リモートコンソールサムネイル

iLO でリモートコンソールのサムネイルイメージの表示を有効または無効にします。

サムネイルを無効にしても、リモートコンソール機能は無効になりません。

この設定を無効にすると、Web インターフェイスがサムネイルの表示を中止するのに約 30 秒かかります。

この設定を有効にする場合は、ブラウザーウィンドウを更新してサムネイルを表示します。iLO からログアウトしてからログインし直して、サムネイルを表示することもできます。

ホスト認証が必要

管理プロセッサーにアクセスするホストベースの構成ユーティリティを使用するために、iLO ユーザー認証情報が必要かどうかを決定します。これらのユーティリティは、管理者または root のホストコンテキストで、ホスト OS のコマンドラインから実行します。

- この設定を有効にすると、すべてのコマンドで有効な資格情報が必要になります。
- この設定を無効にした場合は、有効な認証情報は必要でなく、管理者権限でコマンドは実行します。

  iLO が本番環境または高セキュリティより高いセキュリティ状態を使用するように構成されている場合、この設定は無効にできません。

iLO RBSU へのログイン要求

UEFI システムユーティリティの iLO 構成オプションにユーザーがアクセスしたときに、ユーザー認証情報が必要かどうかを決定します。

- この設定が無効（デフォルト）になっている場合、UEFI システムユーティリティの iLO 構成オプションにユーザーがアクセスするときに、ログインは不要です。

  この設定が無効になっている場合でも、iLO のセキュリティ状態が本番環境または高セキュリティよりも高い場合、UEFI システムユーティリティの iLO 構成オプションにアクセスするには、ユーザー資格情報が必要です。
- この設定が有効になっている場合、UEFI システムユーティリティの iLO 構成オプションにユーザーがアクセスするときに、ログインダイアログボックスが開きます。

シリアルコマンドラインインターフェイス速度

CLI 機能のシリアルポートの速度を変更できます。

以下の速度（ビット/秒）が有効です。

- **9600**（デフォルト）

  Synergy コンピュートモジュールの場合のみ：Synergy コンソールおよび Composer CLI で、この値を 9600 に設定する必要があります。
- **19200**
- **38400** - UEFI システムユーティリティの iLO 構成オプションではこの値はサポートされていません。
- **57600**
- **115200**

正常に動作させるには、シリアルポート構成をパリティなし、データビット 8、ストップビット 1（N/8/1）に設定する必要があります。

この値は、UEFI システムユーティリティで構成されたシリアルポート速度と一致するように設定します。

シリアルコマンドラインインターフェイスステータス

シリアルポート経由での CLI 機能のログインモデルを変更できます。以下の設定が有効です。

- **有効-認証が必要**（デフォルト） - ホストシリアルポートに接続された端末から SMASH CLP にアクセスできます。有効な iLO ユーザー証明書が必要です。
- **有効-認証は不要** - ホストシリアルポートに接続された端末から SMASH CLP にアクセスできます。iLO ユーザー証明書は不要です。
- **無効** - ホストシリアルポートから SMASH CLP へのアクセスを無効にします。物理シリアルデバイスを使用する予定の場合は、このオプションを使用してください。

POST 中に iLO IP を表示

ホストサーバーの POST 中に iLO のネットワーク IP アドレスを表示できます。

- この設定が有効（デフォルト）になっている場合、POST 実行中に iLO の IP アドレスが表示されます。
- この設定が無効になっている場合、POST 実行中に iLO の IP アドレスが表示されません。

外部モニターにサーバーヘルスを表示

外部モニターでサーバーヘルスサマリー画面の表示を有効にします。

- この設定が有効になっている場合は、サーバーの UID ボタンを押して放して、外部モニターにサーバーヘルスサマリー画面を表示できます。
- この設定が無効になっている場合は、サーバーの UID ボタンを押して放しても、サーバーヘルスサマリー画面は開きません。

> **注意:** この機能を使用するには、UID ボタンを押して放します。5 秒以上押し続けると、適切な iLO の再起動またはハードウェア iLO の再起動を開始します。ハードウェア iLO の再起動中にデータの損失や NVRAM の破損が発生する可能性があります。

この機能は、Synergy コンピュートモジュールではサポートされません。

サーバーヘルスサマリー画面について詳しくは、HPE iLO 5 トラブルシューティングガイドを参照してください。

VGA ポート検出オーバーライド

システムのビデオポートに接続されているデバイスの検出方法を制御します。動的検出によってシステムが異常なポート電圧から保護されます。

- この設定が有効になっている場合（デフォルト）、iLO ファームウェアは、ビデオ出力の使用を開始する前に、接続されているデバイスを検出します。
- この設定が無効になっている場合、iLO ハードウェアは、ビデオ出力の使用を開始する前に、接続されているデバイスを検出します。

この設定は、ディスプレイ、KVM コンセントレーター、またはアクティブなドングルへのビデオ出力がない場合のトラブルシューティングで使用できます。

この設定は、Synergy コンピュートモジュールではサポートされません。

仮想 NIC

USB サブシステム経由で仮想 NIC を使用してホストオペレーティングシステムから iLO にアクセスできるかどうかを決定します。

- この設定が有効になっている場合は、以下のことができます。
  - ホスト OS で動作している RESTful インターフェイスツールまたは別のクライアントから iLO RESTful API コマンドを開始する。
  - ホスト OS で動作している SSH クライアントで iLO に接続する。

- ホスト OS で動作しているサポート対象のブラウザーを使用して iLO Web インターフェイスにアクセスする。
- **概要**ページで仮想 NIC の IP アドレスを表示する。

- この設定が無効になっている場合、仮想 NIC を使用して iLO にアクセスすることはできません。

  工場出荷時のデフォルトの**仮想 NIC** 設定は、iLO のほとんどのバージョンで無効になっています。iLO 5 v2.10 では、この設定はデフォルトで有効になっています。iLO を工場出荷時のデフォルト設定にリセットすると、**仮想 NIC** 設定は、iLO のインストールされているバージョンのデフォルト設定に戻ります。ファームウェアのアップグレードまたはダウングレードでは、この設定は変更されません。

サービスアクセス設定オプションのアップデート

ダウングレードポリシー

iLO からアップデートできるファームウェアタイプをダウングレードする要求を iLO がどのようにして処理するかを指定します。

この機能にはライセンスが必要です。この機能をサポートするライセンスがインストールされていない場合、このオプションは表示されません。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

以下の値から選択します。

- **ダウングレードの許可**（デフォルト）-iLO 設定の構成権限を持つすべてのユーザーがファームウェアをダウングレードできます。
- **ダウングレードにはリカバリセットの権限が必要です**-iLO 設定の構成権限とリカバリセット権限を持つユーザーのみがファームウェアをダウングレードできます。
- **ダウングレードを永遠に不許可**-ユーザーはファームウェアをダウングレードできません。

注意: この設定を構成すると iLO に対して永続的な変更が行われます。永遠にダウングレードを禁止するよう iLO を構成した後は、iLO のどのインターフェイスやユーティリティからもこの設定の構成を変更することができなくなります。iLO を出荷時のデフォルト設定に設定しても、この値はリセットされません。

サードパーティーのファームウェアアップデートパッケージの受け入れ

iLO で、デジタル署名されていないサードパーティのファームウェアアップデートパッケージを受け入れるかどうかを指定します。Platform Level Data Model（PLDM）ファームウェアパッケージがサポートされています。この設定は、デフォルトでは無効になっています。

ネットワークアクセス設定オプション

アクセス設定ページの**ネットワーク**セクションでは、iLO の機能を有効および無効にしたり、それらの機能で使用するポートを構成したりできます。

iLO が使用する TCP/IP ポートは構成可能であり、ポート設定に関する任意のサイト要件およびセキュリティのイニシアチブに適合できます。これらの設定は、ホストシステムには影響しません。iLO で有効なポートの値の範囲は 1～65535 です。使用されているポートの番号を入力すると、iLO により別の値を入力するよう求められます。

通常、これらの設定を変更するには、標準の通信と SSL 通信に使用される Web ブラウザーの設定を変更する必要があります。

匿名データ

この設定は、以下を制御します。

- 基本システム情報の匿名要求への応答で iLO が提供する XML オブジェクト。
- `/redfish/v1` に対する Redfish の匿名呼び出しへの応答で提供される情報。

この設定が有効になっている（デフォルト）場合は、次のようになります。

- 他のソフトウェアは、ネットワーク上の iLO システムを検出および特定できます。iLO が提供する XML 応答を表示するには、**XML を表示**をクリックします。
- `/redfish/v1` に対する Redfish の匿名呼び出しには、次のような情報が含まれます。

```
"ManagerFirmwareVersion": "1.40",
"ManagerType": "iLO 5",
"Status": {"Health": "OK"}
```

- iLO のヘルスステータスが**劣化**の場合は、iLO のヘルスステータスと問題の説明がログインページに表示されます。iLO ヘルスステータスは、iLO 診断セルフテストを組み合わせた結果に基づいています。セキュリティ侵害の可能性があるセルフテスト障害は、説明には表示されません。

このオプションが無効になっている場合は、次のようになります。

- iLO は空の XML オブジェクトを使用して要求に応答します。
- iLO のバージョン情報はログインページに表示されません。
- `/redfish/v1` に対する Redfish の匿名呼び出しに次の情報は含まれません。`ManagerFirmwareVersion`、`ManagerType`、および `Status`。

本番環境または高セキュリティより高いセキュリティ状態を有効にすると、この設定は自動的に無効になります。

IPMI/DCMI over LAN

業界標準の IPMI および DCMI コマンドを LAN 経由で送信できます。

この設定は、デフォルトでは無効になっています。

この設定が無効になっていると、iLO は LAN 経由で IPMI/DCMI を無効にします。この機能が無効にされても、サーバー側の IPMI/DCMI アプリケーションは依然として機能します。

この設定が有効になっている場合、iLO では、クライアント側のアプリケーションを使用して LAN 経由で IPMI/DCMI コマンドを送信できます。

IPMI/DCMI over LAN が無効にされている場合、ポートスキャナーを使用して、セキュリティの脆弱性をスキャンするセキュリティ監査で、設定されている **IPMI/DCMI over LAN ポート**が検出されません。

本番環境または高セキュリティより高いセキュリティ状態を有効にすると、この設定は自動的に無効になります。

IPMI/DCMI over LAN ポート

IPMI/DCMI ポート番号を設定します。デフォルト値は UDP 623 です。

リモートコンソール

iLO リモートコンソール経由のアクセスを有効または無効にすることができます。

このオプションを無効にすると、グラフィカルリモートコンソールとテキストベースのリモートコンソールが無効になります。ポートスキャナーを使用して、セキュリティの脆弱性をスキャンするセキュリティ監査で、設定されているリモートコンソールポートが検出されません。

リモートコンソールを無効にしても、リモートコンソールサムネイルは無効になりません。リモートコンソールサムネイルを無効にするには、**iLO のアクセス設定**セクションで**リモートコンソールサムネイル**オプションを編集します。

リモートコンソールポート

リモートコンソールポートを設定します。デフォルト値は TCP 17990 です。

セキュアシェル（SSH）

SSH 機能を有効または無効にすることができます。

SSH は、iLO コマンドラインプロトコル（CLP）に暗号化されたアクセスを提供します。

セキュアシェル（SSH）ポート

SSH ポートを設定します。デフォルト値は TCP 22 です。

SNMP

iLO が外部の SNMP 要求に応答するかどうかを指定します。

SNMP アクセスを無効にすると、iLO はそのまま動作を続行し、iLO Web インターフェイスに表示される情報はアップデートされます。この状態では、警告は生成されず、SNMP アクセスは許可されません。

SNMP アクセスが無効になっている場合、**SNMP 設定**ページのほとんどのボックスは使用できません。

本番環境または高セキュリティより高いセキュリティ状態を有効にすると、この設定は自動的に無効になります。

SNMP ポート

SNMP ポートを設定します。SNMP アクセスのデフォルト値は UDP 161 です。

SNMP ポートの値をカスタマイズすると、標準以外の SNMP ポートの使用をサポートしない一部の SNMP クライアントが、iLO で正しく動作しない場合があります。

SNMP オプションが無効になっている場合、この値をアップデートすることはできません。

SNMP トラップポート

SNMP トラップポートを設定します。SNMP アラート（またはトラップ）のデフォルト値は UDP 162 です。

SNMP トラップポートをカスタマイズすると、標準以外の SNMP トラップポートの使用をサポートしない一部の SNMP 監視アプリケーションが、iLO で正しく動作しない場合があります。

HPE SIM 7.2 以降で SNMP v3 を使用するには、**SNMP トラップポート**の値を 50005 に変更します。

SNMP オプションが無効になっている場合、この値をアップデートすることはできません。

仮想メディア

iLO 仮想メディア機能を有効または無効にすることができます。

このオプションを無効にすると、仮想メディア機能が無効になります。ポートスキャナーを使用してセキュリティの脆弱性をスキャンするセキュリティ監査で、構成されている仮想メディアポートが検出されません。

仮想メディアポート

iLO が着信ローカル仮想メディア接続をリスンするために使用するポート。デフォルト値は TCP 17988 です。

仮想シリアルポートログ

仮想シリアルポートの記録を有効または無効にします。

この設定が有効になっている場合、仮想シリアルポートの動作が iLO メモリ内の 150 ページの循環バッファーに記録されます。CLI コマンド `vsp log` を使用して、記録された情報を表示できます。仮想シリアルポートのバッファーサイズは 128 KB です。

この設定が無効（デフォルト）になっている場合、仮想シリアルポートの動作は記録されません。

Web サーバー

iLO Web サーバー経由のアクセスを有効または無効にすることができます。

注意: この値を無効に設定した場合、iLO は、構成済みの **Web サーバー非 SSL ポート（HTTP）**または **Web サーバー SSL ポート（HTTPS）**での通信をリスンしません。

Web サーバーが無効になっている場合、次の機能は正常に動作しません。

- iLO の Web インターフェイス
- リモートコンソール
- iLO RESTful API
- iLO 連携
- RIBCL

このオプションを無効にすると、ポートスキャナーを使用してセキュリティ脆弱性をスキャンするセキュリティ監査で、構成されている **Web サーバー非 SSL ポート（HTTP）**および **Web サーバー SSL ポート（HTTPS）**が検出されません。

Web サーバー非 SSL ポート（HTTP）

HTTP ポートを設定します。デフォルト値は TCP 80 です。

Web サーバー SSL ポート（HTTPS）

HTTPS ポートを設定します。デフォルト値は TCP 443 です。

SSH クライアントによる iLO ログイン

SSH クライアントで iLO にログインすると、表示されるログインプロンプトの回数は、**認証失敗ログ**オプションの値（無効の場合は 3）に一致します。SSH クライアントはログインが失敗すると実装も遅延するため、SSH クライアント設定は、プロンプトの回数に影響を与える場合があります。

たとえば、デフォルト値（**有効-3 回目の失敗時**）で SSH 認証失敗ログを生成するには、SSH クライアントが、3 回に設定されたパスワードプロンプトで構成されている場合、連続した 3 回のログイン失敗が次のように発生します。

1. SSH クライアントを起動し、正しくないログイン名とパスワードでログインします。

   パスワードプロンプトが 3 回表示されます。正しくないパスワードを 3 回入力すると、接続が終了し、最初のログイン失敗が記録されます。SSH ログイン失敗カウンターが 1 に設定されます。

2. SSH クライアントを起動し、正しくないログイン名とパスワードでログインします。

   パスワードプロンプトが 3 回表示されます。正しくないパスワードを 3 回入力すると、接続が終了し、2 番目のログイン失敗が記録されます。SSH ログイン失敗カウンターが 2 に設定されます。

3. SSH クライアントを起動し、正しくないログイン名とパスワードでログインします。

   パスワードプロンプトが 3 回表示されます。正しくないパスワードを 3 回入力すると、接続が終了し、3 番目のログイン失敗が記録されます。SSH ログイン失敗カウンターが 3 に設定されます。

iLO ファームウェアは、失敗した SSH ログインログエントリーを記録し、SSH ログイン失敗カウンターを 0 に設定します。

iLO サービスポート

サービスポートは、サポートされているサーバーおよびコンピュートモジュールで **iLO** のラベルが付けられている USB ポートです。

お使いのサーバーまたはコンピュートモジュールがこの機能に対応しているか調べるには、次の Web サイト（**https://www.hpe.com/info/qs**）にあるサーバーの仕様ドキュメントを参照してください。

サーバーに物理的にアクセスできる場合、サービスポートを使用して次のことができます。

- サポートされている USB フラッシュドライブに Active Health System ログをダウンロードします。

  この機能を使用する場合、接続されている USB フラッシュドライブにホストオペレーティングシステムはアクセスできません。
- サポートされる USB イーサーネットアダプターにクライアント（ノートパソコンなど）を接続して以下にアクセスします。
  - iLO の Web インターフェイス
  - リモートコンソール
  - iLO RESTful API
  - CLI
  - RIBCL スクリプト

  XL170r など、サーバーによっては、アダプターを使用して USB を iLO サービスポートからイーサーネットアダプターに接続する必要があります。

iLO サービスポートを使用すると、次のようになります。

- 操作が iLO イベントログに記録されます。
- サービスポートのステータスを示すようにサーバーの UID が点滅します。

  REST クライアントと iLO RESTful API を使用してサービスポートのステータスを取得することもできます。
- サービスポートを使用してサーバー内のデバイスまたはサーバー自体を起動することはできません。
- サービスポートに接続してサーバーにアクセスすることはできません。
- 接続されているデバイスにサーバーからアクセスすることはできません。

詳しくは、**HPE ProLiant Gen10 サーバーへの Anywhere アクセス**のビデオをご覧ください。

iLO サービスポート経由での Active Health System ログのダウンロード

前提条件

iLO サービスポートおよび **USB フラッシュドライブ**オプションが **iLO サービスポート**ページで有効になっている。

手順

1. `command.txt` という名前のテキストファイルを作成し、Active Health System ログをダウンロードするための**必須の内容**を記述します。
2. **サポートされている USB フラッシュドライブ**のルートディレクトリにファイルを保存します。
3. USB フラッシュドライブを iLO サービスポート（サーバーの前面にある、**iLO** のラベルが付けられている USB ポート）に接続します。

   ファイルシステムがマウントされ、`command.txt` ファイルが読み込まれて実行されます。

   iLO サービスポートのステータスがビジーに変わり、UID が中速で 4 回点滅してから 1 秒オフを繰り返します。

   コマンドが成功した場合は、iLO サービスポートのステータスが完了に変わり、UID が高速で 1 回点滅してから 3 秒オフを繰り返します。

   コマンドが失敗した場合は、iLO サービスポートのステータスがエラーに変わり、UID が高速で 8 回点滅してから 1 秒オフを繰り返します。

   ファイルシステムがマウント解除されます。
4. USB フラッシュドライブを取り外します。

   iLO サービスポートのステータスが準備完了に変わります。UID は点滅を停止するか、リモートコンソールアクセスやファームウェアアップデートの進行中などの状態を示して点滅します。
5. （オプション）ファイルを Active Health System Viewer にアップロードします。

   詳しくは、**https://www.hpe.com/servers/ahsv** をご覧ください。

詳しくは

iLO サービスポート設定の構成
iLO サービスポートのサポート対象デバイス
iLO サービスポートを通じた Active Health System ログダウンロードのサンプルテキストファイル

iLO サービスポートを通じて iLO にクライアントを接続する

前提条件

- **iLO サービスポート**および **USB イーサネットアダプター**オプションが **iLO サービスポート**ページで有効になっている。
- クライアント NIC がサービスポート機能をサポートするように構成されている。
- サーバーに物理的にアクセスできる。

手順

1. サポートされている USB イーサーネットアダプターを使用して、クライアントをサービスポート（サーバーの前面にある、**iLO** のラベルが付けられている USB ポート）に接続します。

   クライアント NIC にリンクローカルアドレスが割り当てられます。このプロセスには、数秒かかることがあります。
2. IPv4 アドレス **`169.254.1.2`** を使用して、iLO に接続します。

   サービスポートを介してサーバーにクライアントを接続するときは、同じ IP アドレスが使用されます。このアドレスを変更することはできません。

サービスポートのステータスがビジーに変わり、UID が中速で 4 回点滅してから 1 秒オフを繰り返します。

3. 作業を終了したら、クライアントをサービスポートから外します。

   サービスポートのステータスが準備完了に変わります。UID は点滅を停止するか、リモートコンソールアクセスやファームウェアアップデートの進行中などの状態を示して点滅します。

詳しくは

iLO サービスポート設定の構成
iLO サービスポートを通じて接続するクライアントを設定する

iLO サービスポート設定の構成

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**セキュリティ**クリックして、**iLO サービスポート**タブをクリックします。
2. 以下の設定を行います。
   - **iLO サービスポート**
   - **USB フラッシュドライブ**
   - **認証が必要**
   - **USB イーサーネットアダプター**
3. **適用**をクリックします。

   アップデートされた設定はすぐに有効になり、構成変更に関する情報が iLO イベントログに記録されます。

iLO サービスポートオプション

- **iLO サービスポート** - iLO サービスポートを有効または無効にすることができます。デフォルト設定は有効です。この機能を無効にすると、このページの**マスストレージオプション**セクションまたは**ネットワークオプション**セクションの機能を構成することはできません。

  使用中の iLO サービスポートを無効にしないでください。データがコピーされているときにこのポートを無効にすると、データが破損する可能性があります。

- **USB フラッシュドライブ** - USB フラッシュドライブを iLO サービスポートに接続して Active Health System ログをダウンロードできます。デフォルト設定は有効です。

  iLO サービスポートを使用しているときにこの設定を無効にしないでください。データがコピーされているときに USB フラッシュドライブを無効にすると、データが破損する可能性があります。

  この設定が無効のときに USB フラッシュドライブを iLO サービスポートに挿入した場合、デバイスは無視されます。

- **認証が必要** - iLO サービスポートを使用して Active Health System ログをダウンロードするときに iLO ユーザー認証情報を `command.txt` ファイルに入力する必要があります。デフォルト設定は、無効です。

iLO セキュリティを無効にするようシステムメンテナンススイッチが設定されている場合、ユーザー認証情報は不要です。

- **USB イーサーネットアダプター** - USB イーサーネットアダプターを使用してノートパソコンを iLO サービスポートに接続し、統合リモートコンソールにアクセスできます。デフォルト設定は有効です。

  この設定が無効な場合にノートパソコンを接続すると、デバイスは無視されます。

iLO サービスポートを通じて接続するクライアントを設定する

手順

1. IPv4 自動構成アドレスを自動的に取得するクライアント NIC を構成します。

   詳しくは、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。

2. 次のいずれかを実行します。

   - プロキシ例外を追加します。次のいずれかの形式を使用します。
     - Edge、Chrome、Internet Explorer：`169.254.*`
     - Firefox：`169.254.0.0/16`
   - クライアント上で Web プロキシ設定を無効にします。

   プロキシ設定について詳しくは、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。

iLO サービスポートのサポート対象デバイス

大容量ストレージデバイス

iLO サービスポートは、以下の特性を持つ USB キーをサポートします。

- 高速 USB 2.0 準拠。
- FAT32 フォーマット（512 バイトブロックを推奨）。
- 1 つの LUN。
- 最大サイズ 127 GB の 1 つのパーティションと、Active Health System ログをダウンロードするのに十分な空き領域。
- 有効な FAT32 パーティションテーブル。

  USB キーのマウントに失敗した場合、無効なパーティションテーブルがあることが考えられます。Microsoft DiskPart などのユーティリティを使用して、パーティションを削除して再作成してください。
- 読み取り保護されていない。
- ブート可能ではない。

NAND が搭載されていないサーバーでは、大容量ストレージデバイスはサポートされません。

USB イーサーネットアダプター

iLO サービスポートは、ASIX Electronics Corporation の次のいずれかのチップを内蔵した USB イーサーネットアダプターをサポートします。

- AX88772
- AX88772A
- AX88772B
- AX88772C

Hewlett Packard Enterprise は、HPE USB イーサーネットアダプター（部品番号 Q7Y55A）を使用することをお勧めします。

注記: XL170r など、サーバーによっては、アダプターを使用して USB を iLO サービスポートから Ethernet アダプターに接続する必要があります。それらのサーバーについては、Hewlett Packard Enterprise は、HPE Micro USB を使用して USB アダプターに接続することをお勧めします（部品番号 789904-B21）。

iLO サービスポートを通じた Active Health System ログダウンロードのサンプルテキストファイル

iLO サービスポートを使用して Active Health System ログをダウンロードする場合は、`command.txt` というテキストファイルを作成し、**サポートされている USB デバイス**にファイルを保存します。USB デバイスをサーバーに接続すると、`command.txt` ファイルが実行され、ログファイルがダウンロードされます。

command.txt ファイルのファイルテンプレート

`command.txt` ファイルのテンプレートとして、次の例を使用します。

```
{
  "/ahsdata/" : {
    "POST" : {
      "downloadAll"  : "0",
      "from"         : "2016-08-25",
      "to"           : "2016-08-26",
      "case_no"      : "ABC0123XYZ",
      "contact_name" : "My Name",
      "company"      : "My Company, Inc.",
      "phone"        : "281-555-1234",
      "email"        : "my.name@mycompany.com",
      "UserName"     : "my_username",
      "Password"     : "my_password"
    }
  }
}
```

command.txt ファイルのパラメーター

以下の値をカスタマイズできます。

- `downloadAll` - ダウンロード範囲を制御します。日付の範囲のログをダウンロードするには、0 を入力します。ログ全体をダウンロードするには、1 を入力します。
- `from` - 日付範囲に対応するログをダウンロードする場合の開始日。
- `to` - 日付範囲に対応するログをダウンロードする場合の終了日。
- `case_no`（オプション） - 開いている HPE サポートケースのケース番号。この値の最大長は 14 文字です。この値を入力すると、それがダウンロードしたファイルに含まれます。

- `contact_name`（オプション） - このサーバーの連絡担当者。この値を入力すると、それがダウンロードしたファイルに含まれます。この値の最大長は 255 文字です。
- `company`（オプション） - このサーバーを所有する会社。この値を入力すると、それがダウンロードしたファイルに含まれます。この値の最大長は 255 文字です。
- `phone`（オプション） - このサーバーの連絡担当者の電話番号。この値を入力すると、それがダウンロードしたファイルに含まれます。この値の最大長は 39 文字です。
- `email`（オプション） ー このサーバーの連絡担当者のメールアドレス。この値を入力すると、それがダウンロードしたファイルに含まれます。この値の最大長は 255 文字です。
- `UserName` - iLO が大容量ストレージデバイスでの iLO サービスポートのアクションに認証を要求するように構成されている場合は、iLO アカウントのユーザー名を入力します。iLO セキュリティを無効にするようシステムメンテナンススイッチが設定されている場合、ユーザー名は不要です。
- `Password` - iLO が大容量ストレージデバイスでの iLO サービスポートのアクションに認証を要求するように構成されている場合は、入力したユーザー名のパスワードを入力します。iLO セキュリティを無効にするようシステムメンテナンススイッチが設定されている場合、パスワードは不要です。

command.txt ファイルのファイル要件

- ファイルは、有効な JSON 形式でなければなりません。

  Hewlett Packard Enterprise は、オンラインの JSON フォーマッターを使用して、ファイルの構文を確認することをおすすめします。Web サイト **http://www.freeformatter.com/json-formatter.html** で無料のユーティリティを入手できます。
- ファイル内にコメントを含めないでください。
- ファイル内のテキストでは大文字と小文字が区別されます。
- ファイルではプレーンテキストのみサポートされます。追加の書式設定プロパティを埋め込むアプリケーションを使用してファイルを作成しないでください。

SSH キーの管理

Web インターフェイスを使用した新しい SSH キーの認証

前提条件

ユーザーアカウント管理権限

手順

1. `ssh-keygen`、`puttygen.exe`、または別の SSH キーユーティティを使用して、2,048 ビットの DSA キーまたは RSA キーを生成します。

   iLO が CNSA セキュリティ状態を使用するように構成されている場合、NIST P-384 曲線を使用する ECDSA 384 ビットキーが必要です。
2. `key.pub` という名前で公開キーを保存します。
3. `key.pub` ファイルの内容をコピーします。
4. ナビゲーションツリーで**セキュリティ**をクリックして、**セキュアシェルキー**タブをクリックします。
5. SSH キーを追加するユーザーアカウントの左にあるチェックボックスを選択します。

   各ユーザーアカウントに割り当てられるキーは 1 つだけです。

6. **新しいキーの認証**をクリックします。
7. **公開キー**ボックスに公開キーを貼り付けます。
8. **公開キーのインポート**をクリックします。

   認証済み SSH キーテーブルがアップデートされ、ユーザーアカウントに関連付けられた SSH 公開キーのハッシュが表示されます。

CLI を使用した新しい SSH キーの認証

前提条件

ユーザーアカウント管理権限

手順

1. `ssh-keygen`、`puttygen.exe`、または別の SSH キーユーティリティを使用して、2,048-bit DSA または RSA SSH キーを生成します。

   iLO が CNSA セキュリティ状態を使用するように構成されている場合、NIST P-384 曲線を使用する ECDSA 384 ビットキーが必要です。
2. `key.pub` ファイルを生成します。
3. **アクセス設定**ページで**セキュアシェル（SSH）アクセス**が有効になっていることを確認します。
4. `putty.exe` を使用して、ポート 22 を使用した SSH セッションを開きます。
5. ★★`/Map1/Config1` ディレクトリに変更します。
6. 次のコマンドを入力します。

   ```
   load sshkey type "oemhpe_loadSSHkey -source <protocol://username:password@hostname:port/filename>"
   ```

   このコマンドを使用するときは次の点に留意してください。

   - `protocol` の値は必須で、HTTP または HTTPS を指定します。
   - `hostname` および `filename` の値は必須です。
   - `username:password` および `port` の値は省略可能です。

   CLI では、入力した値の構文は大まかにしか検証されません。よく見て、URL が正しいことを確認してください。次の例でコマンド構造を示します。

   ```
   oemhpe_loadSSHkey -source http://192.168.1.1/images/path/sshkey.pub
   ```

SSH キーの削除

SSH キーを 1 つ以上のユーザーアカウントから削除するには、以下の手順を使用します。

SSH キーを iLO から削除すると、SSH クライアントは、iLO に対して、対応するプライベートキーを使用して認証できなくなります。

前提条件

ユーザーアカウント管理権限

手順

1. ナビゲーションツリーで**セキュリティ**をクリックして、**セキュアシェルキー**タブをクリックします。
2. **認証済み SSH キー**リストで、1 つまたは複数のユーザーアカウントの左にあるチェックボックスを選択します。
3. **選択したキーの削除**をクリックします。

   iLO が要求を確認するように求めます。
4. **はい、削除します**をクリックします。

   選択した SSH キーが iLO から削除されます。

HPE SIM サーバーからの SSH キーを認証するための要件

`mxagentconfig` ユーティリティを使用すると、HPE SIM サーバーから SSH キーを認証できます。

- キーを認証するには、`mxagentconfig` を使用する前に、iLO で SSH が有効になっている必要があります。
- `mxagentconfig` に入力したユーザー名とパスワードは､iLO 設定の構成権限を持つユーザーアカウントに対応する必要がありますこのユーザーは、ディレクトリユーザーであってもローカルユーザーであってもかまいません。
- キーは、iLO で認証され、`mxagentconfig` コマンドで指定されるユーザー名に対応します。

`mxagentconfig` について詳しくは、iLO スクリプティング/CLI ガイドを参照してください。

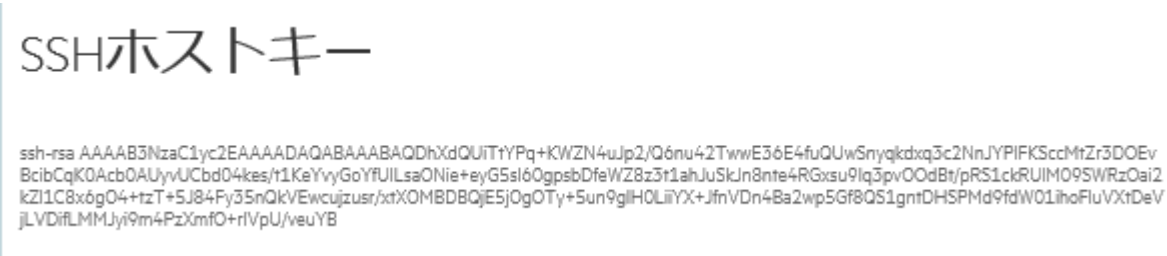
SSH ホストキーの表示

iLO によって報告される SSH ホストキーを表示するには、以下の手順に従ってください。

手順

1. ナビゲーションツリーで**セキュリティ**をクリックして、**セキュアシェルキー**タブをクリックします。

   SSH ホストキーが表示されます。

2. （オプション）ホスト名/IP アドレスと SSH ホストキーを SSH クライアント構成ファイルに追加します。

   以下に例を示します。

   - Linux の OpenSSH ユーザー：`.ssh/known_hosts` ファイルをアップデートします。
   - Windows の PuTTY ユーザー：Windows レジストリ（`HKEY_CURRENT_USER\SoftWare\SimonTatham\PuTTY\SshHostKeys`）をアップデートします。

3. （オプション）接続が安全であることを確認するには、**SSH ホストキー**の値を SSH クライアントから報告された値と比較します。

以下に例を示します。

```
Linux-client:~ # grep ilo.example.com .ssh/known_hosts
ilo.example.com,[redacted] ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC9E/XDH9xPU+NdMyTu5Oylw9AN6mJlH7woMqcf79lda6DeS1D+vX1I
Wg3GwDKFUobabQ+gZtkBrxWFzwAf51CPitsybQCK2hvLztsypb/W3p+MPZ9zU6/voCHzL2v0bAxeXuX8ack/8RA
w0l1agB5xY6B3pjP/qaeFJb29sGqPwoaXps6g5t/YFhxIQ8is8N+LnfuTzMtQDj74rfq6pcXGnXq+ErmbkcfHn
AdSMveT6rXPM1U+Je1B9VOVS23fUL7mfoshLnSHrJJtP7XkZ1rKf1QPKCChWLfpdmTprsaJrxDrwCNxX4+pPh
UXqHYLTlyPA8xsqaPxPZfHxZWTZrCp
```

4. キーが一致しない場合は、一致しない理由を確認してから続行してください。

   考えられる理由のいくつかを以下に示します。

   - 手順 **1** で表示した iLO システムが、SSH クライアントで接続したシステムと同じではない。
   - SSH 接続はリダイレクトされている。ネットワークが接続をリダイレクトするよう構成されているか管理者に尋ねてください。ネットワークが接続をリダイレクトするように構成されていない場合、ネットワークセキュリティが低下する可能性があります。
   - iLO が出荷時のデフォルト設定にリセットされたために、アクセスしようとしているシステムの iLO SSH ホストキーが変更された。あなたは自分の SSH クライアント構成を変更していません。

認証済み SSH キーの表示

手順

1. ナビゲーションツリーで**セキュリティ**をクリックして、**セキュアシェルキー**タブをクリックします。

   認証済み SSH キーテーブルには、各ユーザーアカウントに関連付けられた SSH 公開キーのハッシュが表示されます。

2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

SSH キー

SSH キーを iLO に追加すると、iLO ファームウェアによってキーがローカルユーザーアカウントに関連付けられます。

サポートされている SSH キーフォーマット

- RFC 4716
- OpenSSH キー形式
- レガシー iLO 形式

SSH キーの操作

- iLO Web インターフェイスおよび CLI では、サポートされている SSH キー形式がサポートされます。
- RIBCL スクリプトでは、レガシー iLO 形式のみがサポートされています。
- 対応するプライベートキーを使用して認証される SSH 接続は、キーの所有者として認証され、同じ権限を持ちます。
- iLO ファームウェアは、最大 1,366 バイトの長さの SSH キーをインポートすることができます。キーの長さが 1,366 バイトを超える場合、認証に失敗することがあります。認証に失敗する場合は、SSH クライアントソフトウェアを使用して、より短いキー生成してください。

- iLO の Web インターフェイスを使用してパブリックキーを入力する場合は、パブリックキーに関連付けられたユーザーを選択します。
- iLO RESTful API を使用してパブリックキーを入力する場合は、パブリックキーとともにユーザー名が POST 本文で提供されます。
- CLI を使用してパブリックキーを入力する場合は、パブリックキーが、iLO にログインするために入力したユーザーに結び付けられます。
- HPQLOCFG および RIBCL スクリプトを使用してパブリックキーを入力する場合は、パブリックキーデータに iLO ユーザー名を追加します。パブリックキーは、ユーザー名とともに格納されます。
- ユーザーに対して SSH キーが認証された後にそのユーザーが削除されると、SSH キーが削除されます。

サポートされている SSH キー形式の例

RFC 4716

```
---- BEGIN SSH2 PUBLIC KEY ---- CRLF
Comment: "Administrator"CRLF
AAAAB3NzaC1kc3MAAACAT27C04Dy2zr7fWhUL7TwHDKQdEdyuAlNLIivLFP3IoKZCRLF
ZtzF0VInP5x2VFVYmTvdVjSupD92CTlxxAtarOPON2qUqoOajKRtBWLmxcfqsLCTCRLF
3wI3ldxQvPYnhTYyhPQuoeJ/vYhoam+y0zi8D03pDv9KaeNA3H/zEL5mf9Ktgts8CRLF
/UAAAAVAJ4efo8ffq0hg4a/eTGEuHPCb3INAAAAgCbnhADYXu+Mv4xuXccXWP0PcCRLF
j477YiZgos3jt/Z0ezFX6/cN/RwwZwPC1HCsMuwsVBIqi7bvn1XczFPKOt06gVWcCRLF
jFteBY3/bKpQkn61SGPC8AhSu8ui0KjyUZrxL4LdBrtp/K2+lm1fqXHnzDIEJ0RHCRLF
g8ZJazhY920PpkD4hNbAAAAgDN3lba1qFV10UlRjj21MjXgr6em9TETSOO5b7SQ8CRLF
hX/Z/axobbrHCj/2s66VA/554chkVimJT2IDRRKVkcV8OVC3nb4ckpfFEZvKkAWYCRLF
aiFDLqRbHhh4qyRBIfBKQpvvhDj1aecdFbaO2UvZltMir4n8/E0hh19nfi3tjXAtCRLF
STV CRLF
---- END SSH2 PUBLIC KEY ---- CRLF
```

OpenSSH キー形式

```
ssh-dss
AAAAB3NzaC1kc3MAAACAYjEd8Rk8HLCLqDIlI+RkA1UXjVS28hNSk8YDljTaJpw1VOlBirrLGPdSt0avN
Sz0DNQuU7gTPfjj/8cXyHe3y95Oa3Rics1fARyLiNFGqFjr7w2ByQuoYUaXBzzghIYMQcmpc/W/kDMC0d
VOf2XnfcLpcVDIm3ahVPRkxFV9WKkAAAAVAI3J61F+oVKrbNovhoHh8pFfUa9LAAAAgA8pU5/M9F0s5Qx
qkEWPD6+FVz9cZ0GfwIbiuAI/9ARsizkbwRtpAlxAp6eDZKFvj3ZIyNjcQODeYYqOvVU45AkSkLBMGjpF
05cVtnWEGEvrW7mAvtG2zwMEDFSREw/V526/jR9TKzSNXTH/wqRtTc/oLotHeyV2jFZFGpxDOvNWAAAAg
Ff6pvWaco3CDELmH0jT3yUkRSaDztpqtoo4D7ev7VrNPPjnKKKmpzHPmAKRxz3g5S80SfWSnWM3n/pekB
a9QI91H1r3Lx4JoOVwTpkbwb0by4eZ2cqDw20KQ0A5J84iQE9TbPNecJ0HJtZH/K8YnFNwwYy2NSJyjLw
A0TSmQEOW Administrator CRLF
```

レガシー iLO 形式

iLO レガシー形式のキーは、RIBCL で必要な BEGIN および END ヘッダーで囲まれた OpenSSH キーです。

この形式は、BEGIN SSH KEY のテキストと END SSH KEY のテキストの間に 1 行で記す必要があります。

```
-----BEGIN SSH KEY----- CR LF
ssh-dss
AAAAB3NzaC1kc3MAAACBANA45qXo9cM1asav6ApuCREt1UvP7qcMbw+sTDrx91V22XvonwijdFiOM/0Vv
uzVhM9oKdGMC7sCGQrFV3zWDMJcIb5ZdYQSDt44X6bvlsQcAR0wNGBN9zHL6YsbXvNAsXN7uBM7jXwHwr
ApWVuGAI0QnwUYvN/dsE8fbEYtGZCRAAAAFQDofA47q8pIRdr6epnJXSNrwJRvaQAAAIBY7MKa2uH82I0
KKYTbNMi0o5mOqmqy+tg5s9GC+HvvYy/S7agpIdfJzqkpHF5EPhm0jKzzVxmsanO+pjju7lrE3xUxojev
lokTERSCMxLa+OVVbNcgTe0xpvc/cF6ZvsHs0UWz6gXIMCQ9Pk118VMOw/tyLp42YXOaLZzGfi5pKAAAA
IEAl7FsO7sDbPj02a5jO3qFXa7621Wvu5iPRZ9cEt5WJEYwMO/ICaJVDWVOpqF9spoNb53Wl1pUARJg1s
s8Ruy7YBv8Z1urWWAF3fYy7R/S1QqrsRYDPLM5eBkkLO28B8C6++HjLuc+hBvj90tsqeNVhpCfO9qrjYo
mYwnDC4m1IT4= ASmith CR LF
-----END SSH KEY-----CR LF
```


CAC Smartcard 認証

Common Access Card（CAC）とは、米国防総省（DoD）の多要素認証スマートカードです。Common Access Card は、現役軍人、予備員、軍属、DoD 外政府職員、州兵、指定業者社員の標準 ID として発行されます。ID カードとして使用されるだけでなく、共通アクセスカードは官庁施設やコンピューターネットワークへアクセスする際に必要です。

各 CAC に埋め込まれているスマートカード証明書は、iLO Web インターフェイスでローカルユーザーアカウントと関連付けられなければなりません。**証明書マップ**ページのコントロールを使用して、スマートカード証明書をアップロードし、アカウントと関連付けます。

LDAP ディレクトリサポートを備えた CAC 認証ではディレクトリサービスに対して認証するサービスアカウントを使用し、ユーザーアカウントは設定されたディレクトリサーバーと同じドメイン内に存在する必要があります。さらに、ユーザーアカウントは、設定されたグループまたは拡張スキーマロールの直接メンバーでなければなりません。クロスドメイン認証とネスト化グループはサポートされません。

ツーファクター認証

連邦政府認証を満たすために必要な要件の一部がツーファクター認証です。ツーファクター認証は、CAC の二重認証です。たとえば CAC では、実際にカードを所有していてそのカードに関連付けられた PIN 番号を知っていなければならないことで、ツーファクター認証が成立します。CAC 認証に対応するためには、スマートカードが PIN を必要とするように構成されていなければなりません。

CAC Smartcard 認証設定の構成

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- （オプション）LDAP サーバー CA 証明書がディレクトリ統合のためにインストールされている。
- （オプション）LDAP ディレクトリ統合がディレクトリデフォルトスキーマモードで構成されている。

手順

1. ナビゲーションツリーで**セキュリティ**をクリックし、**CAC Smartcard 認証**タブをクリックします。
2. **信頼済み CA 証明書のインポート**

   この証明書は、iLO に提示される証明書の検証に使用します。証明書は構成されている iLO セキュリティ状態に準拠していなければなりません。
3. 以下の**認証オプション**を設定します。

a. **CAC Smartcard 認証**を有効にします。

b.（オプション）**CAC 厳密モード**を有効にします。

4. （オプション）**CAC 厳密モード**の有効時にセキュリティを強化するために、Hewlett Packard Enterprise では、次を有効にすることをお勧めします。

   - **ホスト認証が必要** - この設定は**アクセス設定**ページで構成できます。
   - **FIPS** セキュリティ状態 - この設定は**暗号化**ページで構成できます。

5. （オプション）ディレクトリ統合を使用している場合は、**ディレクトリユーザー証明書名マッピング**セクションでオプションを選択します。

   この設定は、ユーザー証明書のどの部分がディレクトリユーザーアカウントの識別に使用されるかを特定します。

6. **認証オプション**および**ディレクトリユーザー証明書名マッピング**設定を保存するには、**適用**をクリックします。

   CAC 厳密モードを有効にした場合、iLO では、iLO のリセットを必要とする要求の確認が求められます。

   CAC 厳密モードを有効にしていない場合、iLO では、変更が保存されたことが通知されます。

7. 変更を確認してリセットを開始するように iLO から求められたら、**はい、適用およびリセット**をクリックします。

8. （オプション）**証明書失効リスト（CRL）をインポートします**

9. （オプション）オンライン証明書ステータスプロトコル（OCSP）を使用してユーザー証明書を確認するには、**OCSP 設定**セクションに HTTP または HTTPS URL を入力して、**適用**をクリックします。

10. **スマートカード証明書をアップロードして**ローカル iLO ユーザーアカウントにマップします（iLO をローカルユーザー認証で使用する場合のみ）。

詳しくは

CAC Smartcard 認証用の信頼済み証明書の管理
新しいローカルユーザー証明書の承認
スキーマフリーディレクトリ認証

CAC スマートカード認証設定

CAC スマートカード認証

共通アクセススマートカードを使用した認証を有効または無効にします。

CAC 厳密モード

iLO への接続ごとにクライアント証明書を要求する CAC 厳密モードを有効または無効にします。このモードが有効になっている場合、iLO はユーザー名やパスワードを受け付けず、キーベースの認証方法のみが許可されます。

注記: 信頼済みの証明書がない場合、iLO にアクセスできません。iLO Web インターフェイスにアクセスしようとすると、エラーが生成されます。

ディレクトリユーザー証明書名マッピング

ディレクトリユーザー名の場合を設定すると、ユーザー証明書の部分を選択して、ご自分のディレクトリのユーザー名として使用できます。

- **証明書 SAN UPN を使用** - サブジェクト代替名（SAN）の、userPrincipalName（UPN）タイプの最初のフィールドをユーザー名として使用します。これには、ユーザー名とドメイン名がメールアドレス形式で含まれています。たとえば、`upn:testuser@domain.com` の場合、`testuser@domain.com` となります。
- **証明書件名 CN を使用** - サブジェクトの CN または CommonName の部分だけをユーザー名として使用します。たとえば、`cn = test user, ou = users, dc = domain, dc = com` という DN では、共通名は `test user` です。
- **完全な証明書の Subject DN を使用** - ディレクトリサービスでユーザーを検索するとき、完全な識別名をユーザー名として使用します。たとえば、識別名は `cn = test user, ou = users, dc = domain, dc = com` と表されます。
- **証明書 SAN RFC822 名を使用** - SAN の、rfc822Name タイプの最初のフィールドをユーザー名として使用します。これにはメールアドレスが含まれています。たとえば、`rfc822Name:testuser@domain.com` の場合、ユーザー名は `testuser@domain.com` となります。

OCSP 設定

この機能を使用すると、オンライン証明書ステータスプロトコル（OCSP）を使用してユーザー証明書をチェックできます。

HTTP および HTTPS URL が受け付けられます。

応答が不明または失効状態の場合、認証は失敗します。

CAC Smartcard 認証用の信頼済み証明書の管理

信頼済み CA 証明書のインポート

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- 信頼済み CA 証明書を取得している。

  証明書は、PEM でエンコードされた Base64 フォーマットでなければなりません。

手順

1. ナビゲーションツリーで**セキュリティ**をクリックし、**CAC Smartcard 認証**タブをクリックします。
2. **ダイレクトインポート**セクションに信頼済み CA 証明書を貼り付けます。
3. **適用**をクリックします。

   操作が正常に実行されていないように思われる場合は、ページの上部にスクロールして、エラーメッセージが表示されていないかどうかを確認します。

信頼済み CA 証明書の削除

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**セキュリティ**をクリックし、**CAC Smartcard 認証**タブをクリックします。
2. **信頼できる CA 証明書を管理**セクションまでスクロールします。
3. 削除する証明書の横にあるチェックボックスを選択します。
4. **削除**をクリックします。

   iLO が要求を確認するように求めます。
5. **はい、削除します**をクリックします。

   証明書が削除されます。

   操作が正常に実行されていないように思われる場合は、ページの上部にエラーメッセージが表示されていないかどうかを確認します。

証明書失効リスト（CRL）を URL からインポート

取り消された発行済み証明書を無効にするには、CRL をインポートします。

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**セキュリティ**をクリックし、**CAC Smartcard 認証**タブをクリックします。
2. **失効リストのインポート**セクションに URL を入力するか貼り付けます。

   CRL のサイズ制限は 100 KB であり、CRL は DER フォーマットでなければなりません。
3. **適用**をクリックします。

   iLO によって要求の確認が求められ、CRL をインポートすると iLO がリセットされることが通知されます。
4. **はい、インポートします**をクリックします。

   CRL がインポートされ、iLO がリセットされます。

   証明書失効リスト（CRL）セクションに、CRL の説明とシリアル番号が表示されます。

証明書失効リストの削除

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**セキュリティ**をクリックし、**CAC Smartcard 認証**タブをクリックします。
2. **証明書失効リスト（CRL）**セクションまで下にスクロールします。
3. **削除**をクリックします。

   iLO が要求を確認するように求めます。
4. **はい、削除します**をクリックします。

証明書マッピング

証明書マッピングページには、システムのローカルユーザーと、それぞれに関連付けられた SHA-256 証明書指紋が表示されます。このページのコントロールを使用して、証明書を追加または削除します。

スマートカードまたは CAC 環境（**CAC/Smartcard** ページで構成）でスマートカードアクセスを許可するには、ローカルユーザーのスマートカード証明書が保存され、そのユーザーアカウントにマップされている必要があります。

新しいローカルユーザー証明書の承認

前提条件

- ユーザーアカウント管理権限
- 証明書が埋め込まれたスマートカードまたはその他の共通アクセスカード（CAC）を所持していること。

  証明書は設定されている iLO セキュリティ状態に準拠していなければならない。
- **CAC Smartcard 認証**が **CAC/Smartcard** タブで有効である。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで**セキュリティ**をクリックしてから、**証明書マッピング**タブをクリックします。

   iLO で、ローカルユーザーアカウントとそれぞれに関連付けられている SHA 256 証明書指紋のリストが表示されます。
2. **ログイン名**の横にあるチェックボックスをクリックして、ユーザーアカウントを選択します
3. **新しい証明書の承認**をクリックします。

   証明書インポートデータ貼り付けボックスが表示されます。

4. 選択したユーザーアカウントの証明書を PEM にエンコードされた Base64 形式でエクスポートします。
5. 証明書をテキストエディターで開きます。
6. 証明書をコピーして、**証明書**ボックスに貼り付けます。
7. **証明書のインポート**をクリックします。

ローカルユーザー証明書の削除

前提条件

- ユーザーアカウント管理権限
- 証明書が関連付けられた 1 つまたは複数のローカルユーザーアカウントがシステムに存在する。

手順

1. ナビゲーションツリーで**セキュリティ**をクリックしてから、**証明書マップ**タブをクリックします。

   iLO で、ローカルユーザーアカウントとそれぞれに関連付けられている SHA 256 証明書指紋のリストが表示されます。
2. 1 つまたは複数のローカルユーザーアカウントを、**ログイン名**の横にあるチェックボックスをクリックして選択します。
3. **選択された証明書の削除**をクリックします。

   証明書はすぐに削除されて、証明書が削除されました。のメッセージが表示されます。

認定された証明書の表示

手順

1. ナビゲーションツリーで**セキュリティ**をクリックしてから、**証明書マッピング**タブをクリックします。

   認定された証明書テーブルには、各ユーザーアカウントに関連付けられた証明書の拇印が表示されます。
2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

SSL 証明書の管理

SSL（Secure Sockets Layer）プロトコルは、データがネットワークを移動しているときに、他人がデータを見たり、変更したりできないようにデータを暗号化するための規格です。SSL 証明書は、暗号化キー（サーバーの公開キー）とサーバー名をデジタル的に結合した小さなコンピューターファイルです。対応するプライベートキーを所有するサーバーのみが、ユーザーとサーバー間で認証済みの双方向通信を実現できます。

証明書は署名がないと有効になりません。認証機関（CA）によって署名され、その CA が信頼される場合、CA によって署名されるすべての証明書も信頼されます。自己署名証明書は、証明書の所有者がそれ自身の CA として機能する証明書です。

iLO は、SSL 接続で使用するために自己署名の電子証明書をデフォルトで作成します。この電子証明書により、構成手順を追加することなく、iLO の動作を有効にすることができます。

重要: 自己署名証明書を使用するよりも、信頼済み証明書をインポートするほうが安全です。Hewlett Packard Enterprise では、信頼済み証明書をインポートして iLO ユーザーアカウント認証情報を保護することをお勧めします。

iLO のバックアップおよびリストア機能を使用する場合、証明書が含まれます。

SSL 証明書情報の表示

手順

ナビゲーションツリーで**セキュリティ**をクリックし、**SSL 証明書**タブをクリックします。

SSL 証明書の詳細

- **発行先** - 証明書の発行先の名前。

  iLO 自己署名証明書を表示する際、この値は、Hewlett Packard Enterprise ヒューストンオフィスに関する情報を表示します。
- **発行元** - 証明書を発行した CA。

  iLO 自己署名証明書を表示する際、この値は、Hewlett Packard Enterprise ヒューストンオフィスに関する情報を表示します。
- **有効開始日** - 証明書の有効期限の開始日。
- **有効期限** - 証明書の有効期限の終了日。
- **シリアル番号** - 証明書に割り当てられたシリアル番号。この値は、自己署名証明書の場合は iLO によって生成され、信頼済み証明書の場合は CA によって生成されます。

SSL 証明書の取得とインポート

iLO では、iLO にインポートする信頼済みの SSL 証明書を取得するために認証機関（CA）に送信できる証明書署名要求（CSR）を作成できます。

iLO は、3 KB まで（プライベートキーで使用される 1,187 バイトを含む）の 2,048 ビット SSL 証明書をサポートします。

SSL 証明書は、対応する CSR を使用して生成されたキーがないと動作しません。iLO が工場出荷時のデフォルト設定にリセットされる場合、または前の CSR に対応する証明書がインポートされる前に別の CSR が生成される場合、証明書は動作しません。その場合には、CA から新しい証明書を取得するために、新しい CSR を生成する必要があります。

前提条件

iLO の設定を構成する権限

手順

1. **CA から信頼済みの証明書を取得します。**
2. **信頼済みの証明書を iLO にインポートします**。

CA からの信頼済み証明書の取得

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**セキュリティ**をクリックし、**SSL 証明書**タブをクリックします。
2. **証明書のカスタマイズ**をクリックします。
3. 次の値を入力します。
   - **国（C）**
   - **州または県(ST)**
   - **都市または地域(L)**
   - **組織名(O)**
   - **組織ユニット(OU)**
   - **共通名(CN)**
4. （オプション）iLO IP アドレスを CSR に含めるには、**iLO の IP アドレスを含みます**チェックボックスを選択します。

   注記: 多くの認証機関（CA）では、この入力を受け入れることができません。使用中の CA でこの入力を受け入れることがわかっていない場合は、このオプションを選択しないでください。

   このオプションが有効な場合、iLO の IP アドレスが CSR サブジェクト代替名（SAN）の拡張子に含まれます。
5. **CSR の生成**をクリックします。

   CSR を生成中であり、その処理に最大で 10 分かかる可能性があることを伝えるメッセージが表示されます。
6. 数分（最大 10 分）後に、**CSR の生成**を再度クリックします。

   CSR が表示されます。
7. CSR テキストを選択してコピーします。
8. ブラウザーウィンドウを開き、第三者認証機関に移動します。
9. 画面の指示に従って、CSR を CA に送信します。
   - 証明書の目的を選択するように求められたら、必ずサーバー証明書のオプションを選択してください。
   - CSR を CA に送信するときに、ご使用の環境でサブジェクト代替名の指定が要求される可能性があります。必要に応じて、iLO DNS 名を入力します。

   CA は証明書を生成します。証明書署名ハッシュは、CA によって決定されます。
10. 証明書を取得したら、以下の事項を確認してください。
    - CN が iLO FQDN と一致している。この値は、**概要**ページに **iLO ホスト名**として表示されます。
    - 証明書が Base64 でエンコードされた X.509 証明書である。
    - 証明書に開始行と終了行が含まれている。

CSR 入力の詳細

CSR を作成するときは、次の詳細情報を入力します。

- **国（C）** - この iLO サブシステムを所有する会社または組織が存在する国を識別する 2 文字の国番号。2 文字の省略表記を大文字で入力します。
- **州または県（ST）** - この iLO サブシステムを所有する会社または組織が存在する州または県。
- **都市または地域（L）** - この iLO サブシステムを所有する会社または組織が存在する市町村。
- **組織名（O）** - この iLO サブシステムを所有する会社または組織の名前。
- **組織ユニット（OU）** - （省略可能）この iLO サブシステムを所有する会社または組織の中の単位。
- **共通名（CN）** - この iLO サブシステムの FQDN。

  FQDN は、**共通名（CN）**ボックスに自動的に入力されます。

  iLO が CSR に FQDN を入力できるように、**ネットワーク共通設定**ページで**ドメイン名**を設定します。
- **iLO の IP アドレスを含みます** - CSR に iLO IP アドレスを含めるには、このチェックボックスを選択します。

注記: 多くの CA では、この入力を受け入れられません。使用中の CA でこの入力を受け入れることがわかっていない場合は、このオプションを選択しないでください。

証明書署名要求

CSR には、クライアントブラウザーと iLO 間の通信を検証するパブリックキーとプライベートキーのペアが含まれています。iLO は、SHA-256 を使用して署名された 2048 ビット RSA キーまたは CNSA 準拠キーを生成します。生成された CSR は、新しい CSR が生成されるか、iLO が工場出荷時のデフォルト設定にリセットされるか、または証明書がインポートされるまで、メモリに保持されます。

信頼済みの証明書のインポート

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**セキュリティ**をクリックし、**SSL 証明書**タブをクリックします。
2. **証明書のカスタマイズ**をクリックします。
3. **証明書のインポート**をクリックします。
4. **証明書のインポート**ウィンドウで、テキストボックスに証明書を貼り付けて、**インポート**をクリックします。

   iLO が要求を確認して iLO をリセットするように求めます。
5. **はい、適用およびリセット**をクリックします。

   iLO は、証明書をインポートしてからリセットします。

SSL 証明書の削除

この機能を使用して、SSL 証明書を削除し、iLO 自己署名証明書を再生成します。

次の理由から、証明書を削除する場合があります。

- 証明書の有効期限が切れた。
- 証明書に無効な情報が含まれている。
- 証明書に関してセキュリティ上の問題がある。
- 実績のあるサポート組織から証明書を削除するよう勧められた。

前提条件

iLO 設定の構成権限

手順

1. ナビゲーションツリーで**セキュリティ**をクリックし、**SSL 証明書**タブをクリックします。
2. **削除**をクリックします。

   iLO が既存の証明書を削除し、iLO をリセットしてから、新しい自己署名証明書を生成することを確認するように求めます。
3. **はい、削除します**をクリックします。

   iLO がカスタム SSL 証明書を削除し、リセットしてから、新しい自己署名証明書を生成します。

   iLO で新しい証明書を生成するには数分かかる場合があります。
4. 推奨：信頼済みの証明書を取得してインポートします。

   Hewlett Packard Enterprise では、信頼済みの証明書をインポートすることをおすすめします。

詳しくは

SSL 証明書の取得とインポート

iLO のディレクトリの認証と認可設定

iLO ファームウェアは、Microsoft Active Directory による Kerberos 認証をサポートします。また、Active Directory や OpenLDAP ディレクトリサーバーとのディレクトリ統合もサポートします。

ディレクトリ統合を構成するときに、スキーマフリー構成と HPE 拡張スキーマ構成を選択できます。HPE 拡張スキーマは、Active Directory の場合のみサポートされます。iLO ファームウェアは、ディレクトリサービスに接続する場合に、SSL 接続を使用してディレクトリサーバーの LDAP ポートに接続します。

ディレクトリサーバー証明書検証機能は、CA 証明書をインポートすると有効にできます。この機能により、iLO が LDAP 認証時に正しいディレクトリサーバーに接続できます。

iLO の認証およびディレクトリサーバー設定の構成は、ディレクトリまたは Kerberos 認証を使用するための iLO 構成プロセスの手順の 1 つです。これらの機能を使用するように環境をセットアップするには、追加の手順が必要です。

認証およびディレクトリサーバー設定を構成するための前提条件

手順

1. ご使用の iLO ユーザーアカウントに iLO 設定の構成権限があることを確認します。
2. この機能をサポートするライセンスをインストールします。
3. Kerberos 認証またはディレクトリ統合をサポートするように環境を構成します。

詳しくは

Kerberos 認証の設定
ディレクトリ統合の設定（スキーマフリー構成）
ディレクトリ統合の設定（HPE 拡張スキーマ構成）

iLO で Kerberos 認証の設定を構成します

前提条件

- ご使用の環境がこの機能を使用するための前提条件を満たしていること。
- 環境のセットアップタスク中に作成した Kerberos キータブファイルを使用できること。

手順

1. ナビゲーションツリーで**セキュリティ**をクリックし、**ディレクトリ**タブをクリックします。
2. **Kerberos 認証**を有効にします。
3. Kerberos 認証と同時にローカルユーザーアカウントを使用する場合は、**ローカルユーザーアカウント**を有効に設定します。
4. **Kerberos レルム**の名前を入力します。
5. **Kerberos KDC サーバーアドレス**を入力します。
6. **Kerberos KDC サーバーポート**を入力します。
7. Kerberos キータブファイルを追加するには、**参照**または**ファイルを選択**（ブラウザーによって異なる）をクリックして、画面の指示に従います。
8. **設定の適用**をクリックします。
9. ディレクトリグループを構成するには、**ディレクトリグループ**リンクをクリックします。

詳しくは

認証およびディレクトリサーバー設定を構成するための前提条件
Kerberos 認証の設定
iLO ディレクトリグループ

Kerberos の設定

- **Kerberos 認証** - Kerberos ログインを有効または無効にします。Kerberos ログインが有効で、正しく構成されている場合、ログインページに**ゼロサインイン**ボタンが表示されます。
- **Kerberos レルム** ― iLO プロセッサーが動作している Kerberos レルムの名前。この値は最大 127 文字です。レルム名は、通常、大文字に変換された DNS 名です。レルム名は、大文字と小文字が区別されます。
- **Kerberos KDC サーバーアドレス** - Key Distribution Center（KDC）の IP アドレスまたは DNS 名。この値は最大 127 文字です。各レルムには、認証サーバーおよびチケット交付サーバーを含む 1 つ以上の Key Distribution Center（KDC）がある必要があります。これらのサーバーは、結合させることができます。

- **Kerberos KDC サーバーポート** - KDC がリスンしている TCP または UDP ポート番号。デフォルト値は 88 です。
- **Kerberos キータブ** - サービスプリンシパル名と暗号化されたパスワードのペアが含まれているバイナリファイル。Windows 環境下では、`ktpass` ユーティリティを使用してキータブファイルを生成します。

iLO におけるスキーマフリーディレクトリ設定の構成

前提条件

ご使用の環境がこの機能を使用するための前提条件を満たしていること。

手順

1. ナビゲーションツリーで**セキュリティ**をクリックし、**ディレクトリ**タブをクリックします。
2. **LDAP ディレクトリ認証**メニューで**ディレクトリデフォルトスキーマを使用**を選択します。
3. ディレクトリ統合と同時にローカルユーザーアカウントを使用する場合は、**ローカルユーザーアカウント**を有効に設定します。
4. OpenLDAP ユーザーのみ：**汎用 LDAP** を有効にします。

   この設定は、**ディレクトリデフォルトスキーマを使用**を選択している場合のみ使用可能です。
5. CAC/Smartcard 認証が有効な構成では、CAC LDAP サービスアカウントとパスワードを **iLO オブジェクト識別名 CAC LDAP サービスアカウント**および **iLO オブジェクトパスワード**ボックスに入力します。
6. **ディレクトリサーバーアドレス**ボックスに、ディレクトリサーバーの FQDN または IP アドレスを入力します。
7. **ディレクトリサーバー LDAP ポート**ボックスにディレクトリサーバーのポート番号を入力します。
8. （オプション）新しい CA 証明書をインポートします。

   a. **証明書ステータス**ボックスで**インポート**をクリックします。

   b. Base64 でエンコードされた X.509 証明書データを**証明書のインポート**ウィンドウに貼り付けて**インポート**をクリックします。
9. （オプション）既存の CA 証明書を置き換えます。

   a. **証明書ステータス**ボックスで**一覧**をクリックします。

   b. **証明書詳細**ウィンドウで**新規**をクリックします。

   c. Base64 でエンコードされた X.509 証明書データを**証明書のインポート**ウィンドウに貼り付けて**インポート**をクリックします。
10. 1 つまたは複数の**ディレクトリユーザーコンテキスト**ボックスに有効な検索コンテキストを入力します。
11. **設定の適用**をクリックします。
12. ディレクトリサーバーと iLO 間の<u>通信をテスト</u>するには、**設定のテスト**をクリックします。
13. <u>ディレクトリグループを構成</u>するには、**ディレクトリグループ**リンクをクリックします。

詳しくは

ディレクトリユーザーコンテキスト
ディレクトリサーバー CA 証明書
Kerberos 認証およびディレクトリ統合によるローカル ユーザー アカウント
認証およびディレクトリサーバー設定を構成するための前提条件
ディレクトリテストの実行
ディレクトリ統合の設定（スキーマフリー構成）
iLO ディレクトリグループ

スキーマフリーディレクトリの設定

- **ディレクトリデフォルトスキーマを使用** ― ディレクトリ内のユーザーアカウントを使用するディレクトリ認証および権限付与を選択します。ユーザーの認証と権限付与には、ユーザーアカウントとグループメンバーシップが使用されます。

  この構成では、Active Directory および OpenLDAP がサポートされます。

- **汎用 LDAP** - この構成では OpenLDAP でサポートされている BIND メソッドを使用することを指定します。

- **iLO オブジェクト識別名/CAC LDAP サービスアカウント** ― CAC/Smartcard 認証が構成され、スキーマフリーディレクトリオプションで使用される場合の、CAC LDAP サービスアカウントを指定します。

  iLO がディレクトリサーバーにアクセスするときに、ユーザー検索コンテキストは iLO オブジェクト DN に適用されません。

- **iLO オブジェクトパスワード** ― CAC/Smartcard 認証が構成され、スキーマフリーディレクトリオプションで使用される場合の、CAC LDAP サービスアカウントのパスワードを指定します。

- **ディレクトリサーバーアドレス** - ディレクトリサーバーのネットワーク DNS 名または IP アドレスを指定します。ディレクトリサーバーアドレスは最大 127 文字です。

  FQDN を入力する場合、iLO で DNS 設定が構成されていることを確認します。

  Hewlett Packard Enterprise は、ディレクトリサーバーを定義するときに DNS ラウンドロビンを使用することをおすすめします。

- **ディレクトリサーバー LDAP ポート** - サーバー上の安全な LDAP サービス用のポート番号を指定します。デフォルト値は 636 です。ディレクトリサービスが別のポートを使用するように構成されている場合は、別の値を指定できます。セキュリティ保護された安全な LDAP ポートを入力することを確認します。iLO セキュリティ保護されていない LDAP ポートには接続できません。

- **ディレクトリユーザーコンテキスト** - これらのボックスを使用して、ユーザーがログイン時に完全な DN を入力する必要がないように、共通のディレクトリサブコンテキストを指定できます。すべてのディレクトリユーザーコンテキストの合計で 1904 文字の制限があります。

- **証明書ステータス** - ディレクトリサーバーの CA 証明書がロードされているかどうかを示します。

  ステータスが**ロード済**の場合は、**一覧**をクリックすると CA 証明書の詳細が表示されます。CA 証明書がロードされていない場合、ステータスは**未ロード**と表示されます。iLO は、4 KB までのサイズの SSL 証明書をサポートしています。

iLO における HPE 拡張スキーマディレクトリ設定の構成

前提条件

ご使用の環境がこの機能を使用するための前提条件を満たしていること。

手順

1. ナビゲーションツリーで**セキュリティ**をクリックし、**ディレクトリ**タブをクリックします。
2. **LDAP ディレクトリ認証**メニューで **HPE 拡張スキーマを使用**を選択します。
3. ディレクトリ統合と同時にローカルユーザーアカウントを使用する場合は、**ローカルユーザーアカウント**を有効に設定します。
4. ディレクトリツリー内のこの iLO インスタンスの位置を **iLO オブジェクト識別名/CAC LDAP サービスアカウント**ボックスに入力します。
5. **ディレクトリサーバーアドレス**ボックスに、ディレクトリサーバーの FQDN または IP アドレスを入力します。
6. **ディレクトリサーバー LDAP ポート**ボックスにディレクトリサーバーのポート番号を入力します。
7. （オプション）新しい CA 証明書をインポートします。
   a. **証明書ステータス**テキストボックスで**インポート**をクリックします。
   b. Base64 でエンコードされた X.509 証明書データを**証明書のインポート**ウィンドウに貼り付けて**インポート**をクリックします。
8. （オプション）既存の CA 証明書を置き換えます。
   a. **証明書ステータス**テキストボックスで**一覧**をクリックします。
   b. **証明書詳細**ウィンドウで**新規**をクリックします。
   c. Base64 でエンコードされた X.509 証明書データを**証明書のインポート**ウィンドウに貼り付けて**インポート**をクリックします。
9. 1 つまたは複数の**ディレクトリユーザーコンテキスト**ボックスに有効な検索コンテキストを入力します。
10. **設定の適用**をクリックします。
11. ディレクトリサーバーと iLO 間の通信をテストするには、**設定のテスト**をクリックします。

詳しくは

ディレクトリユーザーコンテキスト
Kerberos 認証およびディレクトリ統合によるローカル ユーザー アカウント
認証およびディレクトリサーバー設定を構成するための前提条件
ディレクトリテストの実行
ディレクトリ統合の設定（HPE 拡張スキーマ構成）

HPE 拡張スキーマディレクトリの設定

- **HPE 拡張スキーマを使用** － HPE 拡張スキーマで作成されたディレクトリオブジェクトを使用するディレクトリ認証および権限付与を選択します。HPE 拡張スキーマを使用してディレクトリが拡張されている場合は、このオプションを選択します。HPE 拡張スキーマは、Microsoft Windows のみで動作します。この構成では、Active Directory をサポートしています。
- **iLO オブジェクト識別名/CAC LDAP サービスアカウント** - HPE 拡張スキーマ構成で、この設定はこの iLO インスタンスがディレクトリツリーのどこにリストされるかを指定します。以下に例を示します。

```
cn=Mail Server iLO,ou=Management Devices,o=ab
```

iLO がディレクトリサーバーにアクセスするときに、ユーザー検索コンテキストは iLO オブジェクト DN に適用されません。

- **ディレクトリサーバーアドレス** - ディレクトリサーバーのネットワーク DNS 名または IP アドレスを指定します。ディレクトリサーバーアドレスは最大 127 文字です。

  FQDN を入力する場合、iLO で DNS 設定が構成されていることを確認します。

  Hewlett Packard Enterprise は、ディレクトリサーバーを定義するときに DNS ラウンドロビンを使用することをおすすめします。

- **ディレクトリサーバー LDAP ポート** - サーバー上の安全な LDAP サービス用のポート番号を指定します。デフォルト値は 636 です。ディレクトリサービスが別のポートを使用するように構成されている場合は、別の値を指定できます。セキュリティ保護された安全な LDAP ポートを入力することを確認します。iLO セキュリティ保護されていない LDAP ポートには接続できません。

- **証明書ステータス** - ディレクトリサーバーの CA 証明書がロードされているかどうかを示します。

  ステータスが**ロード済**の場合は、**一覧**をクリックすると CA 証明書の詳細が表示されます。CA 証明書がロードされていない場合、ステータスは**未ロード**と表示されます。iLO は、4 KB までのサイズの SSL 証明書をサポートしています。

- **ディレクトリユーザーコンテキスト** - これらのボックスを使用して、ユーザーがログイン時に完全な DN を入力する必要がないように、共通のディレクトリサブコンテキストを指定できます。すべてのディレクトリユーザーコンテキストの合計で 1904 文字の制限があります。

ディレクトリユーザーコンテキスト

固有 DN を使用すると、ディレクトリに表示されるすべてのオブジェクトを識別できます。ただし、DN が長かったり、ユーザーが自分の DN を知らなかったり、ユーザーが異なるディレクトリコンテキストにアカウントを持っている場合があります。ユーザーコンテキストを使用した場合、iLO は DN でディレクトリサービスへの接続を試みたあと、ログインに成功するまで順番に検索コンテキストを適用します。

- **例 1** - 検索コンテキスト **`ou=engineering,o=ab`** を入力すると、`cn=user,ou=engineering,o=ab` の代わりにユーザーとしてログインできます。

- **例 2** - IM、サービス、およびトレーニング部門がシステムを管理している場合、次の検索コンテキストを使用することでこれらの部門のユーザーが彼らの共通名を使用してログインすることが可能となります。

  - ディレクトリユーザーコンテキスト 1:`ou=IM,o=ab`
  - ディレクトリユーザーコンテキスト 2:`ou=Services,o=ab`
  - ディレクトリユーザーコンテキスト 3:`ou=Training,o=ab`

  ユーザーが `IM` 部門とトレーニング部門の両方に所属する場合は、最初に `cn=user,ou=IM,o=ab` としてログインが試みられます。

- **例 3（Active Directory 専用）** - Microsoft Active Directory では、代替ユーザー認証情報フォーマットを使用できます。ユーザーは、`user@domain.example.com` としてログインすることができます。検索コンテキスト**`@domain.example.com`** を入力すると、ユーザーとしてログインできます。成功したログイン試行のみが、この形式の検索コンテキストをテストできます。

- **例 4（OpenLDAP ユーザー）** - ユーザーが DN `UID=user, ou=people, o=ab` を持っており、かつ検索コンテキストを **`ou=people, o=ab`** を入力した場合、ユーザーは DN を入力する代わりにユーザーとしてログインすることができます。

  この形式を使用するには、**セキュリティ - ディレクトリ**ページで**汎用 LDAP** を有効にする必要があります。

ディレクトリサーバー CA 証明書

LDAP 認証時に iLO がディレクトリサーバー証明書を、CA 証明書がすでにインポートされている場合に検証します。証明書が正しく検証されるように、必ず正しい CA 証明書をインポートしてください。証明書の検証が失敗すると、iLO ログインが拒否されてイベントが記録されます。CA 証明書がインポートされていない場合、ディレクトリサーバー証明書の検証手順はスキップされます。

ディレクトリサーバーと iLO 間の SSL 通信を検証するには、**設定のテスト**をクリックします。

Kerberos 認証およびディレクトリ統合によるローカル ユーザー アカウント

iLO がディレクトリまたは Kerberos 認証を使用するように設定した場合、ローカルユーザーアカウントをアクティブにすることができます。この構成では、ローカルおよびディレクトリベースのユーザーアクセスを使用できます。

以下事項に留意してください。

- ローカルユーザーアカウントが有効になっている場合、設定されているユーザーはローカルに保存されたユーザー認証情報を使用してログインできます。
- ローカルアカウントが無効になっている場合、ユーザーアクセスは有効なディレクトリ認証情報に制限されます。
- Kerberos またはディレクトリを介して有効なアクセスを確保するまでは、ローカルユーザーアクセスを無効にしないでください。
- Kerberos 認証またはディレクトリの統合を使用する場合、Hewlett Packard Enterprise は、ローカルユーザーアカウントを有効にして管理者権限を持つユーザーアカウントを構成することをおすすめします。iLO がディレクトリサーバーと通信できない場合、このアカウントを使用できます。
- ローカルユーザーアカウントを介したアクセスは、ディレクトリサポートが無効になっている場合、またはライセンスが取り消された場合に有効になります。

ディレクトリテストの実行

ディレクトリテストを使用すると、設定が済んだディレクトリの設定を検証できます。ディレクトリテストの結果は、ディレクトリ設定が保存されるとき、またはディレクトリテストが開始されるときにリセットされます。

手順

1. ナビゲーションツリーで**セキュリティ**をクリックし、**ディレクトリ**タブをクリックします。
2. **ディレクトリ**ページの下部にある**設定のテスト**をクリックします。

   iLO により、ディレクトリ設定の有効性を確認するために設計された一連の簡単なテストの結果が表示されます。ディレクトリ設定を正しく構成した後にこれらのテストを再実行する必要はありません。**ディレクトリテスト**ページでは、ディレクトリユーザーとしてログインする必要はありません。
3. **ディレクトリテスト制御**セクションで、**ディレクトリ管理者識別名**ボックスと**ディレクトリ管理者パスワード**ボックスに、ディレクトリ管理者の DN およびパスワードを入力します。

   Hewlett Packard Enterprise は、ディレクトリ内に iLO オブジェクトを作成する際に使用するものと同じ識別名とパスワードを使用することをおすすめします。これらの識別名とパスワードは、iLO によって保存されるものではなく、iLO オブジェクトとユーザー検索コンテキストを確認するために使用されます。
4. **ディレクトリテスト制御**セクションで、**テストユーザー名**ボックスと**テストユーザーパスワード**ボックスに、テストユーザーの名前およびパスワードを入力します。
5. **テストの開始**をクリックします。

複数のテストがバックグラウンドで開始し、最初にサーバーとの SSL 接続を確立し、ユーザー権限を評価して、ネットワーク経由でのディレクトリユーザーに対する Ping が実行されます。

テストの実行中、ページは定期的に更新されます。テストはいつでも停止でき、ページを手動で更新することもできます。

ディレクトリテストの入力値

ディレクトリテストを実行するときに次の値を入力します。

- **ディレクトリ管理者識別名** - iLO オブジェクト、ロール、および検索コンテキストについてディレクトリを検索します。このユーザーは、ディレクトリ読み取り権限を持っている必要があります。
- **ディレクトリ管理者パスワード** - ディレクトリ管理者を認証します。
- **テストユーザー名**および**テストユーザーパスワード** - iLO へのログインとアクセス権をテストします。ユーザー検索コンテキストを適用できるため、ユーザー名は完全修飾である必要はありません。このユーザーは、この iLO のロールに関連付けられている必要があります。

  通常、このアカウントは、iLO これはディレクトリ管理者アカウントでもかまいませんが、スーパーユーザーアカウントではテストでユーザー認証を検証できません。iLO には、これらの認証情報が保存されません。

ディレクトリテストのステータス値と制御

iLO に以下のディレクトリテストのステータス値が表示されます。

- **実行中** - ディレクトリテストが現在バックグラウンドで実行されていることを示します。

  現在のテストを取り消すには、**テストの中止** をクリックします。最新の結果でページの内容をアップデートするには、**更新** をクリックします。**テストの中止**ボタンを使用しても、テストがただちに終了されない場合があります。
- **未テスト** - ディレクトリテストは最新であり、新しいパラメーターを指定してテストを再度実行できることを示します。

  テストの開始ボタンを使用してテストを開始し、現在のテスト制御値を使用することができます。ディレクトリテストは、すでに実行中の場合には、開始できません。
- **停止中** - ディレクトリテストがまだ停止できる段階に達していないことを示します。ステータスが**未テスト**に変わるまでは、テストを再開できません。テストが完了したかどうかを確認するには、**更新**ボタンを使用してください。

ディレクトリテスト結果

ディレクトリテスト結果セクションには、ディレクトリテストのステータスが最後のアップデート日時とともに表示されます。

- **全体のステータス** - テストの結果の要約が示されます。
  - **未実行**- テストは実行されていません。
  - **不明** - 結果は報告されませんでした。
  - **パス** - エラーは報告されませんでした。
  - **問題が見つかりました** - 問題が報告されました。

- **失敗** - 特定のサブテストが失敗しました。問題を特定するには、画面上のログを調べます。
- **警告** - 1 つ以上のディレクトリテストが、**警告**ステータスを報告しました。

- **テスト** - 各テストの名前。
- **結果** - 特定のディレクトリ設定のステータス、または 1 つまたは複数のディレクトリ設定による動作のステータスが報告されます。これらの結果は、テストシーケンスを実行すると生成されます。結果は次の場合に停止します。
  - テストが完了するまで実行した。
  - テストの障害によって進行が妨げられた。
  - テストが停止した。

  テスト結果は次のようになります。
  - **パス** - テストは正常に実行されました。複数のディレクトリサーバーがテストされた場合は、テストを実行したすべてのサーバーで成功しています。
  - **未実行** - テストは実行されませんでした。
  - **失敗** - 1 つまたは複数のディレクトリサーバーについてテストが成功しませんでした。それらのサーバーでは、ディレクトリサポートを使用できない可能性があります。
  - **警告** - テストが実行され、証明書エラーなどの警告状態を報告しました。**注意**列で、警告状態を解消するために推奨される処置を確認してください。

- **注意** - ディレクトリテストのさまざまな段階の結果を示します。データは、エラーの詳細と、ディレクトリサーバー証明書のサブジェクトや、評価されたロールなどの情報によってアップデートされます。

iLO ディレクトリテスト

ディレクトリサーバー DNS 名

ディレクトリサーバーが FQDN フォーマット（directory.company.com）で定義されている場合、iLO は、名前を FQDN フォーマットから IP フォーマットに解決し、設定された DNS サーバーに問い合わせます。

iLO が、構成されたディレクトリサーバーの IP アドレスを取得した場合、テストは成功します。iLO がディレクトリサーバーの IP アドレスを取得できない場合、このテストと以後のテストすべてが失敗します。

ディレクトリサーバーが IP アドレスで構成されている場合、iLO はこのテストを省略します。

ディレクトリサーバーへの Ping

iLO は、設定されたディレクトリサーバーに対する ping を開始します。

iLO が ping 応答を受信する場合、テストは成功します。ディレクトリサーバーが iLO に応答しない場合、テストは失敗します。

テストが失敗した場合、iLO は以後のテストを続行します。

ディレクトリサーバーへの接続

iLO は、ディレクトリサーバーとの LDAP 接続交渉を試みます。

iLO が接続を開始できた場合、テストは成功します。

指定したディレクトリサーバーとの LDAP 接続を iLO が開始できなかった場合、テストは失敗します。以後のテストは、停止します。

SSL を使用しての接続

iLO は、ポート 636 経由で SSL ハンドシェーク、交渉、およびディレクトリサーバーとの LDAP 通信を開始します。

iLO とディレクトリサーバー間の SSL ハンドシェークと交渉が成功した場合、テストは成功します。

LDAP サーバー証明書の検証エラーはこのテストの結果に報告されます。

ディレクトリサーバーへのバインド

このテストでは、接続は、テストコントロールに指定したユーザー名とバインドされます。ユーザーを指定しない場合、 iLO は匿名バインドを実行します。

ディレクトリサーバーがバインドを受け付けると、テストは成功します。

ディレクトリ管理者のログイン

ディレクトリ管理者識別名と**ディレクトリ管理者パスワード**を指定した場合、iLO は、これらの値を使用して、管理者としてディレクトリサーバーにログインします。これらの値の指定は省略できます。

ユーザー認証

iLO は、指定したユーザー名とパスワードでディレクトリサーバーに認証されます。

提供したユーザー認証情報が正しい場合、テストは成功します。

ユーザー名および/またはパスワードが正しくない場合、テストは失敗します。

ユーザー承認

このテストは、指定したユーザー名が指定したディレクトリグループに属し、ディレクトリサービスの設定中に指定したディレクトリ検索コンテキストに含まれることを確認します。

ディレクトリユーザーコンテキスト

ディレクトリ管理者識別名を指定した場合、iLO は、指定したコンテキストを検索しようと試みます。

iLO が管理者認証情報を使用し、ディレクトリ内のコンテナーを検索してコンテキストを見つけると、テストは成功します。

@記号で始まるコンテキストをテストできる唯一の方法はユーザーログインです。

失敗は、コンテナーが見つからなかったことを示します。

LOM オブジェクトの存在

このテストは、**セキュリティ - ディレクトリ**ページで構成された **iLO オブジェクト識別名**を使用して、ディレクトリサーバー内の iLO オブジェクトを検索します。

iLO がそれ自体を表現するオブジェクトを見つけると、テストは成功します。

このテストは、**LDAP ディレクトリ認証**が無効になっていても実行されます。

iLO 暗号化設定

すべての Gen10 以降のサーバーに付属している HPE iLO Standard によって、お客様は次の 3 つのセキュリティ状態のいずれかでサーバーを構成することができます。iLO Advanced のライセンスでは、CNSA の最上位レベルの暗号化機能を必要とするお客様は 4 つ目のセキュリティ状態を利用できます。

セキュリティの段階が上がると、サーバーは、Web ページ、SSH、およびネットワーク通信に対してより強力な暗号化規則を適用します。各ネットワーク接続の両端が暗号化規則をサポートしている必要があることに注意してください。そうでないと通信はできず、インターフェイスによっては潜在的なセキュリティ上の脅威を制限するためにシャットダウンされます。

次のセキュリティ状態を利用できます。

- 本番環境
- 高セキュリティ
- FIPS
- CNSA

製品または「高セキュリティ」セキュリティ状態の有効化

前提条件

iLO の設定を構成する権限

手順

1. （オプション）必要に応じてファームウェアおよびソフトウェアのアップデートをインストールします。
2. ナビゲーションツリーで**セキュリティ**をクリックして、**暗号化**タブをクリックします。
3. **セキュリティ状態**メニューで**本番環境**または**高セキュリティ**を選択します。
4. **適用**をクリックします。

   iLO は、新しい設定を適用するために iLO の再起動を確認するよう要求します。
5. 使用中のブラウザー接続を終了し、iLO を再起動するには、**はい、適用してリセットします**をクリックします。

   接続が再確立されるまでに、数分かかることがあります。
6. 開いているブラウザー ウィンドウをすべて閉じます。

   ブラウザーセッションが開いたままになっていると、設定されたセキュリティ状態に誤った暗号が使用される場合があります。
7. （オプション）「高セキュリティ」セキュリティ状態を有効にした場合は、**アクセス設定**ページの**匿名データ**が無効になっていることを確認します。

詳しくは

iLO アクセス設定の構成
iLO セキュリティ状態

FIPS および CNSA セキュリティ状態を有効にする

この手順は、FIPS または CNSA のセキュリティ状態を構成するためのものです。iLO を FIPS 承認済み環境に構成するには、**iLO による FIPS 承認済み環境の構成**を参照してください。

前提条件

- iLO の設定を構成する権限
- オプションの CNSA セキュリティ状態を有効にする予定の場合は、この機能をサポートするライセンスがインストールされていること。
- デフォルトの iLO ユーザー認証情報があること。

手順

1. （オプション）現在の iLO 構成をバックアップします。

   以下を使用して、この手順を実行できます。

   - **iLO Web インターフェイス**
   - RESTful インターフェイスツール
   - iLO RESTful API
   - HPONCFG

2. （オプション）必要に応じてファームウェアおよびソフトウェアのアップデートをインストールします。
3. ナビゲーションツリーで**セキュリティ**をクリックして、**暗号化**タブをクリックします。
4. **セキュリティ状態**メニューで **FIPS** を選択して、**適用**をクリックします。

   iLO が要求を確認するように求めます。

   > **注意:** FIPS セキュリティ状態を有効にすると iLO が工場出荷時のデフォルト設定にリセットされます。ユーザーデータとほとんどの構成設定を含むすべての iLO 設定が消去されます。iLO イベントログ、IML、セキュリティログも消去されます。インストール済みのライセンスキーは保持されます。
   >
   > FIPS セキュリティ状態を無効にする唯一の方法は、iLO を工場出荷時のデフォルト設定にリセットすることです。

5. FIPS セキュリティ状態を有効にする要求を確認するためには、**はい、適用およびリセット**をクリックします。

   iLO が FIPS セキュリティ状態を有効にした状態で再起動します。接続の再確立が試みられるまでに 90 秒以上かかります。

6. （オプション）CNSA セキュリティ状態を有効にします。

   a. デフォルトのユーザー認証情報を使用して iLO にログインします。
   b. ナビゲーションツリーで**セキュリティ**をクリックして、**暗号化**タブをクリックします。
   c. **セキュリティ状態**メニューで **CNSA** を選択して、**適用**をクリックします。

      iLO が要求を確認するように求めます。

   d. CNSA セキュリティ状態を有効にする要求を確認するためには、**はい、適用およびリセット**をクリックします。

      iLO が CNSA セキュリティ状態を有効にした状態で再起動します。接続の再確立が試みられるまでに 90 秒以上かかります。

   e. デフォルトの iLO 認証情報を使用して iLO に再度ログインします。

   CNSA のセキュリティ状態を有効にした後、ライセンスが期限切れになるか、ライセンスをダウングレードした場合、iLO は構成されたセキュリティ状態で引き続き動作します。期限切れになったライセンス、またはダウングレードしたライセンスによってアクティブ化された他のすべての機能は使用できなくなります。

7. **信頼済みの証明書をインストールします**。

FIPS セキュリティ状態が有効な場合、デフォルトの自己署名 SSL 証明書は許可されません。それまでにインストールされていた信頼済みの証明書は、iLO が FIPS セキュリティ状態を使用するように設定されると、削除されます。

8. **アクセス設定**ページで **IPMI/DCMI over LAN アクセス**、**匿名データ**、および **SNMP アクセス**オプションを無効にします。

   重要: IPMI および SNMP の標準準拠実装など、一部の iLO インターフェイスは、FIPS に準拠しておらず、FIPS 準拠にすることはできません。

   構成が FIPS に準拠しているかどうかを確認するには、構成を iLO FIPS 妥当性確認プロセスの一部であったセキュリティポリシードキュメントと照合してください。

   検証済みバージョンの iLO のセキュリティポリシードキュメントは、**NIST の Web サイト**にあります。iLO 5 FIPS 情報にアクセスするには、検証済みモジュールの検索ページで証明書番号 3122 を入力します。

9. （オプション）iLO 構成をバックアップしている場合は、それをリストアします。

   以下を使用して、この手順を実行できます。

   - **iLO Web インターフェイス**
   - RESTful インターフェイスツール
   - iLO RESTful API
   - HPONCFG

10. （オプション）構成をリストアした場合は、ローカル iLO ユーザーアカウントに新しいパスワードを設定します。

11. （オプション）構成をリストアした場合は、**アクセス設定**ページで **IPMI/DCMI over LAN アクセス**、**匿名データ**、および **SNMP アクセス**が無効になっていることを確認します。

    これらの設定は、構成をリストアするとリセットされる可能性があります。

12. （オプション）**ログインセキュリティバナーを構成して** iLO ユーザーにシステムが FIPS セキュリティ状態を使用していることを知らせます。

詳しくは

iLO のバックアップとリストア
iLO アクセス設定の構成
SSL 証明書の取得とインポート
ログインセキュリティバナーの構成
iLO のデフォルトの DNS 名とユーザーアカウント

高いセキュリティ状態を使用する場合の iLO への接続

デフォルト値（本番環境）よりも高いセキュリティ状態を有効にすると、iLO は、AES 暗号を使用して安全なチャネルを通じて接続することを要求します。

iLO が CNSA セキュリティ状態を使用するように構成されている場合、AES 256 GCM 暗号が必要です。

Web ブラウザー

ブラウザーが TLS 1.2 および AES 暗号をサポートするよう設定します。ブラウザーが AES 暗号を使用していない場合、iLO に接続できません。

ブラウザーが異なると、交渉済み暗号を選択する方法も異なります。詳しくは、ブラウザーのドキュメントを参照してください。

ブラウザーの暗号設定を変更する前に、現在のブラウザーを通じて iLO からログアウトしてください。iLO にログインしている間に行った暗号設定の変更により、ブラウザーで AES 以外の暗号がそのまま使用できる場合があります。

SSH 接続

使用可能な暗号の設定については、SSH ユーティリティのドキュメントを参照してください。

RIBCL

- HPQLOCFG は、以下のような暗号詳細を出力表示します。

  ```
  Detecting iLO...
  Negotiated cipher: 256-bit Aes256 with 0-bit Sha384 and 384-bit 44550
  ```

- HPONCFG では、「高セキュリティ」、FIPS、または CNSA のセキュリティ状態が有効なときユーザー認証情報が必要になります。必要なユーザーの権限が割り当てられていない場合は、エラーメッセージが表示されます。

  ホスト認証が必要のアクセス設定は、ホストベースの構成ユーティリティに次の影響を与えます。

  - **有効** - すべての iLO セキュリティ状態のホストベースの構成ユーティリティを使用するには、有効な認証情報が必要です。
  - **無効** - iLO が製品または高セキュリティのセキュリティ状態を使用するように設定されている場合、有効な認証情報は必要ありません。

  ホスト認証が必要の設定は、FIPS または CNSA セキュリティ状態が使用されている場合は無効にすることはできません。

iLO RESTful API

TLS 1.2 と AES 暗号をサポートするユーティリティを使用します。

iLO による FIPS 承認済み環境の構成

以下の手順を使用して、iLO を FIPS 検証済み環境で操作します。FIPS セキュリティ状態を iLO で使用するには、**FIPS および CNSA セキュリティ状態を有効にする**を参照してください。

重要なのは、FIPS 検証済みバージョンの iLO がご使用の環境に必要かどうか、あるいは iLO を FIPS セキュリティ状態を有効にして実行することで十分かどうかを判断することです。検証プロセスに時間がかかるため、FIPS 検証済みバージョンの iLO が、新機能とセキュリティ強化が加わった非検証バージョンに置き換えられている場合があります。このような状況では、FIPS 検証済みバージョンの iLO が最新バージョンよりも安全性が低くなる場合があります。

手順

FIPS 検証済みバージョンの iLO による環境をセットアップするには、iLO FIPS 承認プロセスの一部であったセキュリティポリシードキュメントの手順に従ってください。

検証済みのセキュリティポリシードキュメントは、**NIST の Web サイト**にあります。iLO 5 FIPS 情報にアクセスするには、検証済みモジュールの検索ページで証明書番号 3122 を入力します。

FIPS セキュリティ状態の無効化

手順

1. FIPS セキュリティ状態を無効にするには（たとえばサーバーを運用停止する場合）、iLO を工場出荷時のデフォルト設定に設定します。

このタスクを実行するには、RIBCL スクリプト、iLO RESTful API、または iLO 5 構成ユーティリティを使用します。

> **注意:** iLO を工場出荷時のデフォルト設定にリセットすると、すべての iLO 設定が消去されます。消去される設定は、ユーザーデータ、ライセンスデータ、構成設定、ログなどです。サーバーに工場でインストールされたライセンスキーがある場合、このライセンスキーは保持されます。
>
> この手順により iLO ログ内のすべてのデータが消去されるため、リセットに関するイベントはログに記録されません。

2. サーバーのオペレーティングシステムを再起動します。

   工場出荷時のデフォルト設定へのリセット中に、SMBIOS レコードはクリアされます。メモリおよびネットワーク情報は、サーバー OS の再起動が完了するまで iLO Web インターフェイスに表示されません。

詳しくは

iLO の工場出荷時デフォルト設定へのリセット（iLO 5 構成ユーティリティ）

CNSA セキュリティ状態の無効化

手順

1. CNSA セキュリティ状態を無効にするには、次のいずれかを実行します。

   - CNSA セキュリティ状態を無効にして、FIPS セキュリティ状態を引き続き使用するには、セキュリティ状態を **CNSA** から **FIPS** に変更します。
   - CNSA および FIPS セキュリティ状態を無効にするには、iLO を工場出荷時のデフォルト設定に設定します。

     このタスクを実行するには、RIBCL スクリプト、iLO RESTful API、または iLO 5 構成ユーティリティを使用します。

     > **注意:** iLO を工場出荷時のデフォルト設定にリセットすると、すべての iLO 設定が消去されます。消去される設定は、ユーザーデータ、ライセンスデータ、構成設定、ログなどです。サーバーに工場でインストールされたライセンスキーがある場合、このライセンスキーは保持されます。
     >
     > この手順により iLO ログ内のすべてのデータが消去されるため、リセットに関するイベントはログに記録されません。

2. iLO を工場出荷時のデフォルト設定にリセットした場合、サーバーのオペレーティングシステムを再起動します。

   工場出荷時のデフォルト設定へのリセット中に、SMBIOS レコードはクリアされます。メモリおよびネットワーク情報は、サーバー OS の再起動が完了するまで iLO Web インターフェイスに表示されません。

詳しくは

iLO の工場出荷時デフォルト設定へのリセット（iLO 5 構成ユーティリティ）

iLO セキュリティ状態

本番環境（デフォルト）

iLO がこのセキュリティ状態に設定されている場合、次のようになります。

- iLO は工場出荷時のデフォルトの暗号化設定を使用します。
- iLO セキュリティをバイパスするためのシステムメンテナンススイッチ設定（iLO セキュリティオーバーライドスイッチと呼ばれる場合もある）は、iLO へのログインに関するパスワード要件を無効にします。

高セキュリティ

iLO がこのセキュリティ状態に設定されている場合、次のようになります。

- iLO は、以下を経由した安全な HTTP 伝送を含め、安全なチャネル経由の AES 暗号の使用を強制します。
  - ブラウザー
  - SSH ポート
  - iLO RESTful API
  - RIBCL

  サポートされている暗号を使用してこの安全なチャネル経由で iLO に接続します。このセキュリティ状態は、安全でないチャネル経由の通信と接続には影響しません。
- ホストシステムから実行される次のコマンドに対するユーザー名とパスワードの制限が適用されます。
  - iLO RESTful API
  - RIBCL
- リモートコンソールデータは、AES-128 双方向暗号化を使用します。
- HPQLOCFG ユーティリティは、iLO との SSL 接続をネゴシエーションした後、利用可能な最強の暗号を使用して RIBCL スクリプトをネットワーク経由で iLO に送信します。
- TLS 1.2 をサポートしていないネットワークベースのツールを使用してサーバーに接続することはできません。
- iLO セキュリティをバイパスするためのシステムメンテナンススイッチ設定（iLO セキュリティオーバーライドスイッチと呼ばれる場合もある）は、iLO へのログインに関するパスワード要件を無効にしません。

FIPS

Common Criteria コンプライアンス、Payment Card Industry コンプライアンス、またはその他の標準には FIPS セキュリティ状態が必要になる場合があります。

iLO がこのセキュリティ状態に設定されている場合、次のようになります。

- iLO は、FIPS 140-2 レベル 1 の要件への準拠を目的とするモードで動作します。

  FIPS は、米国政府機関および契約業者によって適用を義務付けられている一連のコンピューターセキュリティ規格です。

FIPS のセキュリティ状態は、FIPS 承認済みと同じではありません。FIPS 承認済みは、Cryptographic Module Validation Program を完了することにより承認を受けたソフトウェアを意味します。

- iLO は、以下を経由した安全な HTTP 伝送を含め、安全なチャネル経由の AES 暗号の使用を強制します。
  - ブラウザー
  - SSH ポート
  - iLO RESTful API
  - RIBCL

  サポートされている暗号を使用してこの安全なチャネル経由で iLO に接続します。このセキュリティ状態は、安全でないチャネル経由の通信と接続には影響しません。
- ホストシステムから実行される次のコマンドに対するユーザー名とパスワードの制限が適用されます。
  - iLO RESTful API
  - RIBCL
- リモートコンソールデータは、AES-128 双方向暗号化を使用します。
- HPQLOCFG ユーティリティは、iLO との SSL 接続をネゴシエーションした後、利用可能な最強の暗号を使用して RIBCL スクリプトをネットワーク経由で iLO に送信します。
- TLS 1.2 をサポートしていないネットワークベースのツールを使用してサーバーに接続することはできません。
- iLO セキュリティをバイパスするためのシステムメンテナンススイッチ設定（iLO セキュリティオーバーライドスイッチと呼ばれる場合もある）は、iLO へのログインに関するパスワード要件を無効にしません。

CNSA

CNSA セキュリティ状態（SuiteB モードとも呼ばれる）は、FIPS セキュリティ状態が有効になっている場合にのみ使用できます。

iLO がこのセキュリティ状態に設定されている場合、次のようになります。

- iLO は、NSA によって定義された CNSA 要件への準拠を目的とするモードで動作します。
- iLO は、米国政府機密として分類されたデータを保持するシステムの保護を目的とするモードで動作します。
- TLS 1.2 をサポートしていないネットワークベースのツールを使用してサーバーに接続することはできません。
- iLO セキュリティをバイパスするためのシステムメンテナンススイッチ設定（iLO セキュリティオーバーライドスイッチと呼ばれる場合もある）は、iLO へのログインに関するパスワード要件を無効にしません。
- iLO への接続に使用するソフトウェアまたはユーティリティはすべて、CNSA に準拠している必要があります。

  以下に例を示します。
  - ファームウェアアップデートユーティリティ
  - SSH クライアント

- HPE および他社製のスクリプティングツールとコマンドラインツール
- HPE および他社製の管理ツール
- アラートメール、syslog、LDAP、またはキーマネージャーサーバー
- Remote Support ソフトウェア

- HTML5 リモートコンソールを使用していることを確認してください。このコンソールでは、AES-256 ビット CNSA 準拠の暗号の使用が強制されます。.NET IRC と Java IRC は CNSA に準拠していません。

準拠を確認するには、ソフトウェアのベンダーに確認するか、Wireshark などのユーティリティを使用します。

Synergy セキュリティモード

サポートされるデバイスで使用される特別なセキュリティ状態。このモードを使用するデバイスのセキュリティ状態は変更できません。

SSH 暗号、キー交換、および MAC のサポート

iLO は、安全な CLP トランザクションのために、SSH ポート経由の強化された暗号化を提供します。

設定されているセキュリティ状態に基づいて、iLO は以下をサポートします。

本番稼働

- AES256-CBC、AES128-CBC、3DES-CBC、および AES256-CTR 暗号
- diffie-hellman-group14-sha1 および diffie-hellman-group1-sha1 キー交換
- hmac-sha1 または hmac-sha2-256 MAC

FIPS または高セキュリティ

- AES256-CTR、AEAD_AES_256_GCM、および AES256-GCM 暗号
- diffie-hellman-group14-sha1 キー交換
- hmac-sha2-256 または AEAD_AES_256_GCM MAC

CNSA

- AEAD_AES_256_GCM および AES256-GCM 暗号
- ecdh-sha2-nistp384 キー交換
- AEAD_AES_256_GCM MAC

Synergy セキュリティモード

- AEAD_AES_256_GCM および AES256-GCM 暗号
- ecdh-sha2-nistp384 キー交換
- AEAD_AES_256_GCM MAC

SSL 暗号および MAC のサポート

iLO は、分散型 IT 環境でのリモート管理用に強化されたセキュリティを提供します。SSL 暗号化により、Web ブラウザーのデータが保護されます。SSL で提供される HTTP データの暗号化により、データがネットワーク経由で転送されるときのデータの安全性が保証されます。

ブラウザーから iLO にログインすると、ブラウザーと iLO は、セッション中に使用する暗号設定をネゴシエートします。ネゴシエートされた暗号は**暗号化**ページに表示されます。

サポートされている暗号の次の一覧は、LDAP サーバー、キーマネージャーサーバー、SSO サーバー、Insight Remote Support サーバー、仮想メディアで使用される https:// URL、iLO RESTful API、CLI コマンド、iLO 連携グループのファームウェアアップデートへの接続など、すべての iLO SSL 接続に適用されます。

構成されているセキュリティ状態に基づいて、iLO は以下の暗号をサポートします。

本番稼働

- RSA、ECDH、および AEAD MAC（ECDHE-RSA-AES256-GCM-SHA384）による 256 ビット AES-GCM
- RSA、ECDH、および SHA384 MAC（ECDHE-RSA AES256-SHA384）による 256 ビット AES
- RSA、ECDH、および SHA1 MAC（ECDHE-RSA-AES256-SHA）による 256 ビット AES
- RSA、DH、および AEAD MAC（DHE-RSA-AES256-GCM-SHA384）による 256 ビット AES-GCM
- RSA、DH、および SHA256 MAC（DHE-RSA AES256-SHA256）による 256 ビット AES
- RSA、DH、および SHA1 MAC（DHE-RSA-AES256-SHA）による 256 ビット AES
- RSA および AEAD MAC（AES256-GCM-SHA384）による 256 ビット AES-GCM
- RSA および SHA256 MAC（AES256-SHA256）による 256 ビット AES
- RSA および SHA1 MAC（AES256-SHA）による 256 ビット AES
- RSA、ECDH、および AEAD MAC（ECDHE-RSA-AES128-GCM-SHA256）による 128 ビット AES-GCM
- RSA、ECDH、および SHA256 MAC（ECDHE-RSA-AES128-SHA256）による 128 ビット AES
- RSA、ECDH、および SHA1 MAC（ECDHE-RSA-AES128-SHA）による 128 ビット AES
- RSA、DH、および AEAD MAC（DHE-RSA-AES128-GCM-SHA256）による 128 ビット AES-GCM
- RSA、DH、および SHA256 MAC（DHE-RSA-AES128-SHA256）による 128 ビット AES
- RSA、DH、および SHA1 MAC（DHE-RSA-AES128-SHA）による 128 ビット AES
- RSA および AEAD MAC（AES128-GCM-SHA256）による 128 ビット AES-GCM
- RSA、および SHA256 MAC（AES128-SHA256）による 128 ビット AES
- RSA および SHA1 MAC（AES128-SHA）による 128 ビット AES
- RSA、ECDH、および SHA1 MAC（ECDHE-RSA-DES-CBC3-SHA）による 168 ビット 3DES
- RSA、DH、および SHA1 MAC（EDH-RSA-DES-CBC3-SHA）による 168 ビット 3DES
- RSA および SHA1 MAC（DES-CBC3-SHA）による 168 ビット 3DES

FIPS または高セキュリティ

これらのセキュリティ状態には TLS 1.2 が必要です。

- RSA、ECDH、および AEAD MAC（ECDHE-RSA-AES256-GCM-SHA384）による 256 ビット AES-GCM
- RSA、ECDH、および SHA384 MAC（ECDHE-RSA AES256-SHA384）による 256 ビット AES
- RSA、DH、および AEAD MAC（DHE-RSA-AES256-GCM-SHA384）による 256 ビット AES-GCM
- RSA、DH、および SHA256 MAC（DHE-RSA AES256-SHA256）による 256 ビット AES
- RSA および AEAD MAC（AES256-GCM-SHA384）による 256 ビット AES-GCM
- RSA および SHA256 MAC（AES256-SHA256）による 256 ビット AES
- RSA、ECDH、および AEAD MAC（ECDHE-RSA-AES128-GCM-SHA256）による 128 ビット AES-GCM
- RSA、ECDH、および SHA256 MAC（ECDHE-RSA-AES128-SHA256）による 128 ビット AES
- RSA、DH、および AEAD MAC（DHE-RSA-AES128-GCM-SHA256）による 128 ビット AES-GCM
- RSA、DH、および SHA256 MAC（DHE-RSA-AES128-SHA256）による 128 ビット AES
- RSA および AEAD MAC（AES128-GCM-SHA256）による 128 ビット AES-GCM
- RSA、および SHA256 MAC（AES128-SHA256）による 128 ビット AES

CNSA

このセキュリティ状態には TLS 1.2 が必要です。

- ECDSA、ECDH、および AEAD MAC（ECDHE-ECDSA-AES256-GCM-SHA384）による 256 ビット AES-GCM
- クライアントのみ：RSA、ECDH、および AEAD MAC（ECDHE_RSA_AES256_GCM_SHA384）による 256 ビット AES-GCM

Synergy セキュリティモード

- ECDSA、ECDH、および AEAD MAC（ECDHE-ECDSA-AES256-GCM-SHA384）による 256 ビット AES-GCM
- クライアントのみ：RSA、ECDH、および AEAD MAC（ECDHE_RSA_AES256_GCM_SHA384）による 256 ビット AES-GCM

HPE SSO

HPE SSO を使用すると、HPE SSO 準拠アプリケーションから、ログイン手順を間に挟むことなく iLO に直接接続できます。

この機能を使用するには、以下の手順に従ってください。

- サポートされるバージョンの、HPE SSO に準拠したアプリケーションが必要です。
- SSO 準拠アプリケーションを信頼するように iLO を構成します。
- CAC 厳密モードが有効な場合は、信頼済み証明書をインストールします。

iLO には、HPE SSO 証明書の最小要件を決定するために HPE SSO アプリケーションのサポートが含まれます。HPE SSO 準拠アプリケーションの中には、iLO に接続したときに自動的に信頼証明書をイン

ポートするものがあります。この機能を自動的に実行しないアプリケーションの場合は、HPE SSO ページを使用して SSO 設定を構成してください。

HPE SSO 用の iLO の設定

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**セキュリティ**をクリックし、**HPE SSO** タブをクリックします。
2. **SSO 信頼モード**設定を構成します。

   Hewlett Packard Enterprise では**証明書による信頼**モードを使用することをおすすめします。
3. 各役割の iLO 権限は、**シングルサインオン設定**セクションで設定します。
4. **適用**をクリックします。
5. **証明書による信頼**または**名前による信頼**を選択した場合は、信頼済みの証明書または DNS 名を iLO に追加します。

   手順については、**信頼済みの証明書の追加**または**直接 DNS 名のインポート**を参照してください。
6. （オプション）HPE SSO 準拠アプリケーションにログインし、iLO をブラウズして、SSO 接続をテストします。

   たとえば、HPE SIM にログインし、**システム**ページに移動して iLO プロセッサーを見つけて、**詳細情報**セクションの iLO リンクをクリックします。

   SSO 信頼モードが**信頼なし**に設定されている場合、信頼できるサーバーのリストは使用されません。iLO は SSO サーバー証明書失効を強制しません。

シングルサインオン信頼モードオプション

シングルサインオン信頼モードは、HPE SSO 要求に対する iLO の応答方法に影響します。

- **信頼なし（SSO 無効）**（デフォルト） - すべての SSO 接続要求を拒否します。
- **証明書による信頼**（最も安全） - iLO に事前にインポートされている証明書と一致させて、HPE SSO 対応アプリケーションから SSO 接続を有効にします。
- **名前による信頼** - 直接インポートされた IP アドレスまたは DNS 名を一致させて、HPE SSO 準拠アプリケーションから SSO 接続を有効にします。
- **すべて信頼**（最も安全性が低い） - どの HPE SSO 対応アプリケーションから開始された SSO 接続も、すべて受け入れます。

SSO ユーザー権限

HPE SSO 準拠アプリケーションにログインする場合、HPE SSO 準拠アプリケーションの役割割り当てに基づいて認可されます。割り当てられている役割は、SSO が試みられるときに、iLO に渡されます。

SSO は**シングルサインオン設定**セクションで割り当てられた権限のみを受け入れようとします。iLO ディレクトリ設定は適用されません。

デフォルトの権限設定は以下のとおりです。

- **ユーザー** — ログインのみ
- **オペレーター** - ログイン、リモートコンソール、仮想電源およびリセット、仮想メディア、およびホスト BIOS 構成
- **管理者** - ログイン、リモートコンソール、仮想電源およびリセット、仮想メディア、ホスト BIOS 構成、iLO の設定の構成、ユーザーアカウント管理、ホスト NIC 構成、およびホストストレージ構成

信頼済みの証明書の追加

証明書レポジトリは、標準的な証明書を 5 つ保持できます。標準的な証明書が発行されない場合、証明書のサイズは一定ではありません。割り当てられた保管領域がすべて使われると、それ以上のインポートは受け付けられません。

特定の HPE SSO 対応アプリケーションから証明書を抽出する方法については、HPE SSO 対応アプリケーションのドキュメントを参照してください。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**セキュリティ**をクリックし、**HPE SSO** タブをクリックします。
2. **インポート**をクリックします。
3. 次のいずれかの方法を使用して、信頼済み証明書を追加します。
   - **ダイレクトインポート** - Base64 でエンコードされた証明書の X.509 データをコピーし、**ダイレクトインポート**セクションのテキストボックスに貼り付けてから、**適用**をクリックします。
   - **インダイレクトインポート** - DNS 名、IP アドレス、または証明書 URL を **URL からのインポート**セクションのテキストボックスに入力してから、**適用**をクリックします。

     iLO はネットワーク経由で HPE SSO 対応アプリケーションに接続して、証明書を取得して保存します。

HPE SIM SSO 証明書の取得

次の方法で HPE SIM SSO 証明書を取得できます。詳しくは、HPE SIM のドキュメントを参照してください。

前提条件

HPE SIM 7.4 以降

手順

- Web ブラウザーで次のリンクの 1 つを入力します。
  - **http://<HPE SIM name or network address>:280/GetCertificate?certtype=sso**
  - **https://<HPE SIM name or network address>:50000/GetCertificate?certtype=sso**

すべての要求パラメーターは大文字と小文字が区別されます。小文字の `certtype` パラメーターを大文字にすると、このパラメーターは読み込まれず、HPE SIM は信頼済みの証明書ではなくデフォルトの HPE SIM サーバー証明書を返します。

- HPE SIM から証明書をエクスポートするには、以下の手順に従ってください。

  この手順を完了するには、**オプション** > **セキュリティ** > **証明書** > **HPE Systems Insight Manager シングルサインオンサーバー証明書**の順に選択して、**エクスポート**をクリックします。

直接 DNS 名のインポート

前提条件

iLO 設定の構成権限

手順

1. ナビゲーションツリーで**セキュリティ**をクリックし、**HPE SSO** タブをクリックします。
2. **インポート**をクリックします
3. **直接 DNS 名のインポート**セクションに DNS 名または IP アドレスを入力し（最大 64 文字）、**適用**をクリックします。

信頼済みの証明書とレコードの表示

信頼済み証明書および記録を管理テーブルに、現在の iLO 管理プロセッサーで SSO を使用するように構成されている信頼済みの証明書およびレコードのステータスが表示されます。

手順

ナビゲーションツリーで**セキュリティ**をクリックし、**HPE SSO** タブをクリックします。

信頼済みの証明書およびレコードの詳細

ステータス

証明書またはレコードのステータス。以下のステータス値が表示されます。

- ✅証明書またはレコードは有効です。
- ⚠証明書またはレコードに問題があります。考えられる原因は、以下のとおりです。
  - レコードに DNS 名が含まれており、信頼モードが**証明書による信頼**に設定されています（証明書のみが有効）。
  - 証明書が構成されており、信頼モードが**名前による信頼**に設定されています（直接インポートされた IP アドレスまたは DNS 名のみが有効）。
  - **信頼なし（SSO 無効）**が選択されています。
  - 証明書は構成されている iLO セキュリティ状態に準拠していません。
- ❖証明書またはレコードが無効です。考えられる原因は、以下のとおりです。

- 証明書の期限が切れています。証明書の詳細で詳細情報を確認してください。
- iLO のクロックが設定されていないか、正しく設定されていません。iLO のクロックは、証明書の**発効日**と**有効期限**で示される範囲内に含まれている必要があります。

証明書

レコードに証明書が保存されていることを示します。アイコンの上にマウスカーソルを移動すると、証明書の詳細情報（サブジェクト（被認証者）、発行元、日付など）が表示されます。

説明

サーバーの名前または証明書のサブジェクト（被認証者）。

信頼済みの証明書とレコードの削除

前提条件

iLO 設定の構成権限

手順

1. ナビゲーションツリーで**セキュリティ**をクリックし、**HPE SSO** タブをクリックします。
2. **信頼済みの証明書および記録を管理**テーブルから 1 つ以上の信頼済みの証明書またはレコードを選択します。
3. **削除**をクリックします。

   iLO に、選択した証明書またはレコードの削除を確認するプロンプトが表示されます。

   リモート管理システムの証明書を削除すると、iLO でリモート管理システムを使用する際に正常に機能しないことがあります。
4. **はい、削除します**をクリックします。

ログインセキュリティバナーの構成

ログインセキュリティバナー機能を使用すると、iLO ログインページに表示されるセキュリティバナーを設定できます。たとえば、メッセージとサーバー所有者の連絡先情報を入力できます。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**セキュリティ**をクリックして、**ログインセキュリティバナー**をクリックします。
2. **ログインセキュリティバナーを有効**設定を有効にします。

   iLO は、ログインセキュリティバナーに以下のデフォルトテキストを使用します。

   ```
   This is a private system. It is to be used solely by authorized users
   and may be monitored for all lawful purposes. By accessing this system,
   you are consenting to such monitoring.
   ```
3. （オプション）セキュリティメッセージをカスタマイズするには、**セキュリティメッセージ**テキストボックスにカスタムメッセージを入力します。

テキストボックスの上にあるバイトカウンターに、メッセージに使用できる残りのバイト数が表示されます。最大は 1,500 バイトです。

空白スペースまたは空白行をセキュリティメッセージに追加しないでください。空白スペースと空白行はバイト数にカウントされ、ログインページのセキュリティバナーには表示されません。

ヒント: デフォルトのテキストをリストアするには、**デフォルトのメッセージを使用**をクリックします。

4. **適用**をクリックします。

   次のログイン時にセキュリティメッセージが表示されます。

システムメンテナンススイッチ

Hewlett Packard Enterprise サーバーには、サーバーセキュリティのさまざまな側面を制御する、ハードウェアのシステムメンテナンススイッチがあります。

システムメンテナンススイッチは、サーバー内部にあるため、サーバーエンクロージャーを開かないとアクセスできません。システムメンテナンススイッチを操作するときは、サーバーの電源がオフであり、電源から切り離されていることを確認します。

システムメンテナンススイッチの使用について詳しくは、サーバーメンテナンスおよびサービスガイドを参照してください。

iLO セキュリティ（位置 1）

システムメンテナンススイッチの iLO セキュリティ設定により、管理者は、サーバーのシステムボードを物理的に制御して、緊急時にアクセスすることができます。

iLO セキュリティを制御するシステムメンテナンススイッチ位置は、iLO セキュリティオーバーライドスイッチと呼ばれることがあります。

iLO セキュリティを無効にすると、次の影響があります。

- iLO が本番環境セキュリティ状態を使用するように構成されている場合、すべてのセキュリティ認証確認が無効になります。
- iLO が、高セキュリティ、FIPS、または CNSA のセキュリティ状態を使用するように構成されている場合：
  - ホストシステムから実行される iLO RESTful API および RIBCL コマンドに対してユーザー名とパスワードの制限が適用されます。
  - iLO セキュリティをバイパスするためのシステムメンテナンススイッチ設定によって、iLO へのログインに関するパスワード要件は無効になりません。

  ホストサーバーがリセットされると、UEFI システムユーティリティソフトウェアが実行されます。
- iLO のネットワーク構成が工場出荷時のデフォルト設定にリセットされます。工場出荷時のデフォルトネットワークインターフェイスがネットワークに接続されている場合、iLO はネットワーク上で利用可能です。この変更は、iLO セキュリティが無効に設定され、iLO 機能が無効になった場合でも行われます。
- iLO Web インターフェイスページに、iLO セキュリティが無効であることを示す警告メッセージが表示される。

アラート

iLOセキュリティオーバーライドスイッチがセットされています。

- iLO のログに、iLO セキュリティの変更を記録するエントリーが追加される。
- SNMP アラートの送信先が構成されている場合、iLO が iLO セキュリティ構成の変更後に起動するとアラートが送信される。
- システムリカバリ権限が必要なアクションは実行できません。

  iLO にログインすると、既存のアカウントと一致するユーザー名とパスワードを入力した場合でも、匿名アカウントが使用される。

システムメンテナンススイッチの仕様について詳しくは、ご使用のサーバーのハードウェアガイドを参照してください。

iLO セキュリティを無効にする理由

次の状況で、システムメンテナンススイッチを使用して、iLO セキュリティを無効にすることができます。

- ユーザーアカウント管理権限を持つすべてのユーザーアカウントがロックアウトされた。
- 不適切な設定により、ネットワーク上に iLO が表示されず、ROM ベースの構成ユーティリティが無効になっている。
- iLO に、iLO の NIC がオフになっているか、iLO ネットワーク構成が正しくないため、ネットワーク経由で到達できない。UEFI システムユーティリティを使用して構成を修正することが不可能であるか、または不便である。

  iLO セキュリティを無効にすると、iLO のネットワーク構成が工場出荷時のデフォルト設定にリセットされます。

  - ほとんどのサーバーでは、このアクションによって DHCP および iLO 専用ネットワークポートが有効になります。
  - iLO 専用ネットワークポートがオプションのアドオンカードであるサーバーでは、このアクションによって DHCP および共有ネットワークポートが有効になります。
  - iLO ネットワーク有効化モジュールのあるサーバーでは、このアクションによって DHCP および iLO 専用ネットワークポートが有効になります。
- ユーザー名が 1 つだけ設定され、パスワードを忘れた。
- バッテリ駆動の SRAM メモリデバイスに保存されている構成情報を消去します。

  iLO を起動すると、バッテリ駆動の SRAM メモリデバイスに保存されている構成情報が不揮発性フラッシュメモリ（NAND）にバックアップされます。SRAM が削除されると、構成が自動的にリストアされます。iLO セキュリティを無効にすると、SRAM データが自動的にリストアされません。

iLO 管理設定の構成

Agentless Management と AMS

Agentless Management は、セキュリティと安定性を強化するためにアウトオブバンド通信を使用します。Agentless Management では、ヘルス監視とアラート通知機能がシステムに内蔵され、サーバーに電源コードを接続するとただちに動作を開始します。この機能は iLO ハードウェアで動作し、オペレーティングシステムやプロセッサーに依存しません。

iLO と直接通信できないデバイスおよびコンポーネントから情報を収集するには、**Agentless Management Service（AMS）**をインストールします。

AMS がある場合と AMS がない場合の Agentless Management により提供される情報

コンポーネント	Agentless Management（AMS がない場合）	AMS がインストールされている場合に提供される追加情報
サーバーヘルス	· ファン · 温度 · 電源装置 · メモリ · CPU · NVDIMM	該当なし
ストレージ	· Smart アレイ · SMART ドライブ監視（Smart アレイに接続） · Smart アレイに接続されている内蔵および外付けドライブ · Smart Storage Energy Pack 監視（サポート対象のサーバーのみ） · MCTP をサポートする NVMe ドライブ	· SMART ドライブ監視（Smart アレイ、Smart HBA、および AHCI に接続） · iSCSI（Windows） · NVMe ドライブ
ネットワーク	· NC-SI over MCTP をサポートしている内蔵 NIC の MAC アドレス · NC-SI over MCTP をサポートしている NIC の物理リンク接続性およびリンクアップ/リンクダウントラップ · Hewlett Packard Enterprise ベンダー定義の MCTP コマンドをサポートするファイバーチャネルアダプター	· 独立型および内蔵 NIC の MAC アドレスおよび IP アドレス · リンクアップ/リンクダウントラップ · NIC チーミングおよびブリッジング情報（Windows および Linux） · サポートされるファイバーチャネルアダプター · 仮想 LAN 情報（Windows および Linux）

表は続く

コンポーネント	Agentless Management（AMS がない場合）	AMS がインストールされている場合に提供される追加情報
その他	· iLO データ · ファームウェアインベントリ · デバイスインベントリ	· OS 情報（ホスト SNMP MIB） · ドライバー/サービスインベントリ · OS ログへのイベントの記録 [1、2]
事前障害警告アラート	· メモリ · ドライブ（物理および論理）	該当なし

[1] Linux の場合、AMS ベースの OS ログ記録（Red Hat Enterprise Linux および SUSE Linux Enterprise Server では/var/log/messages、VMware では/var/log/syslog。）
Windows の場合、Windows システムログ。

[2] Smart アレイのログ記録はサポートされていません。

Agentless Management Service

- AMS を Windows システムにインストールすると、Agentless Management Service のコントロールパネルがインストールされます。コントロールパネルを使用すると、SNMP の設定を行い、AMS を有効化/無効化を行い、AMS の削除を行うことができます。
- AMS は、オペレーティングシステムの構成情報およびクリティカルイベントを Active Health System ログに記録します。
- AMS をインストールする前に、iLO ドライバーをインストールします。
- iLO 5 では、AMS にオプションの **System Management Assistant** が含まれます。iLO Agentless Management と AMS によって提供される情報を処理するために OS ベースの SNMP サービスを使用する場合は、System Management Assistant を使用できます。
- AMS がインストールされていない場合：
  - iLO は、ナビゲーションツリーの**システム情報**および**ファームウェア & OS ソフトウェア**セクションに含まれるコンポーネント情報ページにすべてのデータを表示するとは限りません。
  - iLO は、OS 固有の情報にはアクセスできません。

詳しくは

System Management Assistant
iLO ドライバーのインストール

AMS のインストール

手順

1. 次のいずれかのソースから AMS を取得します。

- SPP（Windows、Red Hat Enterprise Linux、SUSE Linux Enterprise Server）を SPP ダウンロードページ **https://www.hpe.com/servers/spp/download** からダウンロードします。
- **https://www.hpe.com/support/hpesc** の Hewlett Packard Enterprise サポートセンター（Windows、Red Hat Enterprise Linux、SUSE Linux Enterprise Server、VMware）からソフトウェアをダウンロードします。
- Software Delivery Repository の Web サイト **https://www.hpe.com/support/SDR-Linux**（VMware）の **vibsdepot** セクションからソフトウェアをダウンロードします。

  AMS は、Hewlett Packard Enterprise 独自の VMware ISO イメージ（**https://www.hpe.com/support/SDR-Linux**）にも含まれています。

2. ソフトウェアをインストールします。

   SPP の使用方法については、**https://www.hpe.com/info/spp/documentation** にある SPP のドキュメントを参照してください。

   他のダウンロードタイプの場合、ソフトウェアに付属のインストール手順を実行します。

AMS のインストールの確認

AMS ステータスの確認：iLOWeb インターフェイス

手順

1. ナビゲーションツリーで**システム情報**をクリックします。

   AMS が**ヘルスサマリー**ページの**サブシステムとデバイス**テーブルにリストされています。値には、以下のものがあります。

   - **利用不可** - AMS が検出されなかった、サーバーが POST を実行している、またはサーバーの電源が入っていないため、AMS は使用できません。
   - **OK** - AMS がインストールされており、実行中です。

AMS ステータスの確認：Windows

手順

1. Windows のコントロールパネルを開きます。

   AMS コントロールパネルがあると、AMS はインストールされています。

2. AMS コントロールパネルを開きます。
3. **サービス**タブをクリックします。

   AMS が有効になっている場合は、次のメッセージが表示されます。

   `Agentless Management Service（AMS）は有効です。`

AMS ステータスの確認：SUSE Linux Enterprise Server および Red Hat Enterprise Linux

手順

1. AMS がインストールされていることを確認するには、コマンド **`rpm -qi amsd`** を入力します。
2. AMS が動作していることを確認するには、コマンド **`systemctl status smad; systemctl status amsd`** を入力します。

AMS ステータスの確認：VMware

手順

1. AMS がインストールされていることを確認します。
   a. VMware vSphere クライアントから VMware ホストにアクセスします。
   b. サーバーの**インベントリ** > **構成** > **健全性ステータス**タブに移動します。
   c. **ソフトウェアコンポーネント**の横にあるプラス記号（+）をクリックします。

      ホストにインストールされているソフトウェアのリストが表示されます。AMS コンポーネントには、`amsd` という文字列が含まれています。

      AMS コンポーネントのフルネームは、サポートされる ESX/ESXi バージョンごとに異なります。
2. AMS が動作していることを確認するには、コマンド**`/etc/init.d/ams.sh status`** を入力します。

AMS の再起動

手順

- **Windows** - Windows の**サービス**ページに移動して、AMS を再起動します。
- **SuSE Linux Enterprise Server および Red Hat Enterprise Linux** - コマンドとして `systemctl restart smad; systemctl restart amsd` を入力します。
- **VMware** - コマンドとして**`/etc/init.d/ams.sh restart`** を入力します。

System Management Assistant

iLO 5 では、OS ベースの SNMP エージェントはサポートされていません。System Management Assistant（SMA）は、OS から SNMP 情報を取得するアプリケーションを実行するユーザー向けの Agentless Management Service 機能です。

セキュリティ

SMA はセキュアな iLO チャネル経由で通信します。

AMS モード

- **AMS（フォワードモード）** - AMS の標準構成では、OS から iLO に情報が転送されます。
- **SMA（リバースモード）** - SMA が有効な場合は、iLO から OS に情報が転送されます。

インストール

SMA は AMS パッケージの一部としてインストールされ、デフォルトで無効になっています。

SMA の有効化

OS から iLO に情報を転送するには、デフォルトの AMS 構成を使用します。iLO から OS に情報を転送するには、SMA を有効にします。AMS の標準構成と SMA は、同時に有効にすることができます。

SMA 機能

SMA が有効になっている場合は、次のように処理されます。

- **Linux** - iLO とホストベースの SNMP マスター間で AgentX プロトコル要求がプロキシ転送されます。
- **Windows、Linux** - iLO とホストベースの SNMP サービス間で SNMP プロトコル要求がプロキシ転送されます。

  この方法は、ホストベースの SNMP サービスで AgentX サブエージェントがサポートされていない場合に使用されます。
- **VMware** - iLO および AMS からの SNMP トラップを、ESXi ホスト OS の SNMP サービスを通じて構成されているトラップの宛先に提供します。

SNMP マスター

デフォルトの AMS 構成では、AMS は SNMP マスターとして iLO を使用します。SMA では、SNMP マスターとして動作するホストベースのサービスが必要です。

SMA が有効になっている場合に提供される情報

- **Windows および Linux** - SMA は、**AMS がある場合と AMS がない場合の Agentless Management により提供される情報**テーブルの **Agentless Management（AMS がある場合）**列で一覧表示されている情報と同じものを提供します。
- **VMware** - SMA は SNMP トラップのみを提供します。

System Management Assistant の使用（Windows）

AMS の対話型インストール時に SMA を有効にするかどうかを選択できます。サイレントインストール時には、SMA が有効になりません。

SMA を使用するには、SMA サービスを起動し、Windows SNMP サービスがインストールされ、構成されていることを確認します。

前提条件

AMS がインストールされています。

手順

1. Windows SNMP サービスをインストールします。
   a. サーバーマネージャーを開きます。
   b. **役割と機能の追加**を選択します。
   c. **開始する前に**セクションで**次へ**をクリックします。
   d. **インストールの種類**セクションで**次へ**をクリックします。
   e. **サーバーの選択**セクションで**次へ**をクリックします。
   f. **サーバーの役割**セクションで**次へ**をクリックします。
   g. **リモートサーバー管理**セクションを展開します。

h. **機能管理ツール**を展開します。

i. **SNMP ツール**が選択されていることを確認します。

j. **SNMP サービス**オプションの左側にあるチェックボックスを選択します。

k. **次へ**をクリックします。

l. **インストール**をクリックし、インストールが完了するまで待機します。

2. Windows SNMP サービスを構成します。

a. Windows の**サービス**ウィンドウに移動します。

b. **SNMP** サービスを右クリックします。

c. **セキュリティ**タブをクリックします。

d. **受け付けるコミュニティ名**セクションで**追加**をクリックします。

e. **コミュニティの権利**セクションでアクセスタイプを選択します。

f. **コミュニティ名**セクションでコミュニティ名を入力します。

g. **追加**をクリックします。

h. **トラップ**タブをクリックします。

i. **コミュニティ名**セクションでコミュニティ名を入力し、**一覧に追加**をクリックします。

j. **トラップ先**セクションで、**追加**をクリックし、トラップ送信先の IP アドレスを入力します。

k. **OK** をクリックします。

3. SMA サービスを開始します。

a. Windows の**サービス**ウィンドウに移動します。

b. **System Management Assistant** を右クリックし、**プロパティ**を選択します。

c. **スタートアップの種類**メニューで**自動**を選択し、**OK** をクリックします。

d. **System Management Assistant** を右クリックし、**開始**を選択します。

注記: 次の方法でも、SMA サービスを開始できます。

- `<Program Files>\OEM\AMS\Service` に移動して、次のコマンドを実行します。
  `EnableSma.bat /f`
- コマンドプロンプトウィンドウでコマンド **`sc config sma start=auto`** および **`net start sma`** を入力します。

System Management Assistant の無効化（Windows）

手順

1. Windows の**サービス**ウィンドウに移動します。
2. **System Management Assistant** を右クリックし、**プロパティ**を選択します。

3. **スタートアップの種類**メニューで**無効**を選択し、**OK** をクリックします。
4. **System Management Assistant** を右クリックし、**停止**をクリックします。

注記: `<Program Files>\OEM\AMS\Service` に移動し、`DisableSma.bat /f` コマンドを実行して、SMA サービスを無効化することもできます。

VMware 用 System Management Assistant の使用

前提条件

AMS がインストールされています。

手順

1. ホスト上で SNMP を有効にし、トラップ先を指定します。

   例：

   ```
   esxcli system snmp set -e 1 -c public -t <trap dest IP address>@162/public
   ```

2. 次のコマンドを入力して、SNMP が有効になっていることを確認します。

   ```
   esxcli system snmp get
   ```

3. 次のコマンドを入力して、SMA を有効にして起動します。

   ```
   esxcli sma enable
   ```

4. 次のコマンドを入力して、SMA が動作していることを確認します。

   ```
   esxcli sma status
   ```

5. SMA プロセス（`smad_rev`）が動作していることを確認します。

System Management Assistant の無効化（VMware）

手順

次のコマンドを実行します。`esxcli sma disable`

Linux 用 System Management Assistant の使用

前提条件

- AMS がインストールされています。
- ホスト SNMP サービスが構成されています。
- ホストと SNMP クライアント間で SNMP パケットが転送されるようにネットワークが構成されています。

手順

1. `/etc/snmp/snmpd.conf` ファイルに最初の非コメント行として次の行を追加して、AgentX サブエージェントがサポートされるようにホストを構成します。

   ```
   master agentx
   ```

2. System Management Assistant を有効にします。

   SuSE Linux Enterprise Server および Red Hat Enterprise Linux - コマンドとして `systemctl enable smad_rev; systemctl start smad_rev` を入力します。

3. Agentless Management Service を有効にして、起動します。

   SuSE Linux Enterprise Server および Red Hat Enterprise Linux - コマンドとして **`systemctl enable amsd_rev; systemctl start amsd_rev`** を入力します。

SNMP 設定の構成

このページで構成する設定は、デフォルトの Agentless Management と AMS 構成用です。System Management Assistant と OS ベースの SNMP サービスを使用する場合は、ホストで同様の設定を構成しなければなりません。

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーの**管理**をクリックします。

   SNMP 設定ページが表示されます。

2. **SNMP 設定**セクションに次の値を入力します。

   - **システムの位置**
   - **システム連絡先**
   - **システムの役割**
   - **システムの役割詳細**
   - **読み込みコミュニティ 1**
   - **読み込みコミュニティ 2**
   - **読み込みコミュニティ 3**

   このページの **SNMP ポート**値および SNMP **ステータス**値は読み取り専用です。この値は、**アクセス設定**ページで変更できます。

3. 構成を保存するには、**適用**をクリックします。

詳しくは

System Management Assistant
iLO アクセス設定の構成

SNMP オプション

- **システムの位置** - サーバーの物理的位置を指定する最大 49 文字の文字列。
- **システムコンタクト** - システム管理者またはサーバーの所有者を指定する最大 49 文字の文字列。文字列には、名前、メールアドレス、または電話番号を含めることができます。
- **システムの役割** - サーバーの役割または機能を記述する最大 64 文字の文字列。
- **システムの役割詳細** - サーバーが実行する場合がある具体的なタスクを記述する最大 512 文字の文字列。
- **読み込みコミュニティ 1**、**読み込みコミュニティ 2**、および**読み込みコミュニティ 3** - 構成されている SNMP 読み取り専用コミュニティ文字列。

  次の形式がサポートされています。

  - コミュニティ文字列（たとえば、`public`）。
  - コミュニティ文字列とそれに続く IP アドレスまたは FQDN（たとえば、`public 192.168.0.1`）。

    指定した IP アドレスまたは FQDN からの SNMP アクセスが許可されることを指定するには、このオプションを使用します。

    IPv4 アドレス、IPv6 アドレス、または FQDN を入力できます。

  これらの値は、**SNMP アラート**セクションで **SNMPv1** が有効になっている場合にのみ編集できます。
- **ステータス** - SNMP アクセス設定のステータス（有効または無効）。この値は読み取り専用ですが、**アクセス設定**ページで変更できます。

  アクセス設定ページに移動するには、**ステータス**リンクをクリックします。
- **SNMP ポート** - SNMP 通信に使用されるポート。この値は読み取り専用ですが、**アクセス設定**ページで変更できます。

  アクセス設定ページに移動するには、**SNMP ポート**リンクをクリックします。

SNMPv3 認証

SNMPv3 の次のセキュリティ機能によって、iLO SNMP エージェントから安全にデータ収集できます。

- メッセージの整合性により、パケット送信中の改ざんを防ぎます。
- 暗号化により、パケットののぞき見を防ぎます。
- 認証により、パケットが有効なソースから送信されたものであることを確認します。

デフォルトでは、SNMPv3 はユーザーベースのセキュリティモデルをサポートします。このモデルでは、セキュリティパラメーターが SNMP エージェントレベル（iLO）と SNMP マネージャーレベル（クライアントシステム）の両方で構成されます。SNMP エージェントとマネージャーの間でやり取りされるメッセージは、データ整合性チェックおよびデータ発信元認証で管理されます。

iLO は、8 つのユーザープロファイルをサポートしており、ユーザーはこのプロファイル内で SNMPv3 USM パラメーターを設定できます。

SNMP アラートの送信先の追加

iLO では、最大 8 つの SNMP アラート送信先をサポートしています。

前提条件

- iLO の設定を構成する権限
- SNMPv1 アラートの送信先を構成する場合、SNMPv1 が有効であること。
- SNMPv3 アラートの送信先を構成する場合、少なくとも 1 人の SNMPv3 ユーザーが構成されていること。

手順

1. ナビゲーションツリーの**管理**をクリックします。

   SNMP 設定ページが表示されます。
2. **SNMP アラートの送信先**セクションで**新規**をクリックします。
3. 以下の値を入力します。
   - **SNMP アラートの送信先**
   - **トラップコミュニティ** （SNMPv1 アラートの送信先のみ）
   - **SNMP プロトコル**
   - **SNMPv3 ユーザー**
4. **追加**をクリックします。

SNMP アラートの送信先のオプション

- **SNMP アラートの送信先** - iLO から SNMP アラートを受信する管理システムの IP アドレスまたは FQDN。この値の最大長は 255 文字です。

  FQDN を使用して SNMP アラートの送信先を構成し、DNS が FQDN に対して IPv4 と IPv6 の両方のアドレスを提供する場合、iLO は、**IPv6** ページの **iLO クライアントアプリケーションは IPv6 を最初に使用**設定で指定されたアドレスにトラップを送信します。**iLO クライアントアプリケーションは IPv6 を最初に使用**を有効にすると、トラップは IPv6 アドレス（使用可能な場合）に送信されます。**iLO クライアントアプリケーションは IPv6 を最初に使用**を無効にすると、トラップは IPv4 アドレス（使用可能な場合）に送信されます。
- **トラップコミュニティ** - 構成されている SNMP トラップコミュニティ文字列。
- **SNMP プロトコル** - 構成されているアラート送信先で使用される SNMP プロトコル（**SNMPv1 トラップ**、**SNMPv3 トラップ**、または **SNMPv3 通知**）。

  SNMP アラートセクションで SNMPv1 が無効になっている場合、**SNMPv1 トラップ**オプションは利用できません。
- **SNMPv3 ユーザー** - 構成されているアラート送信先と関連付けられている SNMPv3 ユーザー。

  この値は **SNMP プロトコル**が SNMPv3 に設定されている場合にのみ使用できます。

SNMP アラート送信先の編集

iLO では、最大 8 つの SNMP アラート送信先をサポートしています。

前提条件

- iLO の設定を構成する権限
- **SNMPv1 トラップ**プロトコルオプションを使用するようにアラート送信先を変更する場合、SNMPv1 が有効になっていること。
- **SNMPv3 トラップ**プロトコルオプションまたは **SNMPv3 通知**プロトコルオプションを使用するようにアラート送信先を変更する場合、少なくとも 1 人の SNMPv3 ユーザーが構成されていること。

手順

1. ナビゲーションツリーの**管理**をクリックします。

   SNMP 設定ページが表示されます。
2. **SNMP アラートの送信先**セクションで、アラート送信先の横のチェックボックスを選択して、**編集**をクリックします。
3. 以下の値をアップデートします。
   - **SNMP アラートの送信先**
   - **トラップコミュニティ** （SNMPv1 アラートの送信先のみ）
   - **SNMP プロトコル**
   - **SNMPv3 ユーザー**
4. **アップデート** をクリックします。

SNMP アラート送信先の削除

前提条件

iLO 設定の構成権限

手順

1. ナビゲーションツリーの**管理**をクリックします。

   SNMP 設定ページが表示されます。
2. **SNMP アラート送信先**セクションで、削除する SNMP アラート送信先の横のチェックボックスを選択し、**削除**をクリックします。
3. 要求を確認するメッセージが表示されたら、**はい、削除します**をクリックします。

SNMPv3 ユーザーの構成

iLO では、最大 8 人の SNMPv3 ユーザーをサポートしています。

前提条件

iLO 設定の構成権限

手順

1. ナビゲーションツリーの**管理**をクリックします。

SNMP 設定ページが表示されます。

2. **SNMPv3 ユーザー**セクションで、次のいずれかの操作を実行します。
   - SNMPv3 ユーザーを追加するには、**新規**をクリックします。
   - 構成済みの SNMPv3 ユーザーを編集するには、ユーザーの横のチェックボックスを選択し、**編集**をクリックします。
3. 以下の値を入力します。
   - **セキュリティ名**
   - **認証プロトコル**
   - **認証パスフレーズ**
   - **プライバシプロトコル**
   - **プライバシーパスフレーズ**
   - **ユーザーエンジン ID**
4. ユーザープロファイルを保存するには、次のいずれかの操作を実行します。
   - 新規ユーザープロファイルを保存するには、**追加**をクリックします。
   - 編集したユーザープロファイルを保存するには、**アップデート**をクリックします。

SNMPv3 ユーザーオプション

- **セキュリティ名** - ユーザープロファイルの名前。1～32 文字の範囲で英数字の文字列を入力します。
- **認証プロトコル** - 認証パスフレーズのエンコーディングに使用するメッセージダイジェストアルゴリズムを設定します。メッセージダイジェストは SNMP メッセージの該当部分を対象に算出され、受信者に送信するメッセージの一部として、メッセージに含まれます。

  MD5、**SHA**、または **SHA256** を選択します。

  FIPS または CNSA セキュリティ状態を使用するよう iLO を構成すると、**MD5** がサポートされません。
- **認証パスフレーズ** - 署名操作に使用するパスフレーズを設定します。8～49 文字の範囲で値を入力します。
- **プライバシープロトコル** - プライバシーパスフレーズのエンコーディングに使用する暗号化アルゴリズムを設定します。SNMP メッセージの一部は、送信前に暗号化されます。**AES** または **DES** を選択します。

  FIPS または CNSA セキュリティ状態を使用するよう iLO を構成すると、**DES** がサポートされません。
- **プライバシーパスフレーズ** - 暗号化操作に使用するパスフレーズを設定します。8～49 文字の範囲で値を入力します。
- **ユーザーエンジン ID** - SNMPv3 通知パケット用のユーザーエンジン ID を設定します。この値は、「INFORM」メッセージで使用されるリモートアカウントの作成のみに使用されます。

  この値が設定されていない場合、「INFORM」メッセージはデフォルト値または構成された **SNMPv3 エンジン ID** で送信されます。

  この値は 10～64 文字で構成される 16 進数文字列で、文字数は先頭の 2 文字の 0x を除いて偶数でなければなりません。

例：**0x01020304abcdef**

SNMPv3 ユーザーの削除

前提条件

iLO 設定の構成権限

手順

1. ナビゲーションツリーの**管理**をクリックします。

   SNMP 設定ページが表示されます。

2. **SNMPv3 ユーザー**セクションで、削除するユーザープロファイルの横のチェックボックスを選択し、**削除**をクリックします。

   注意: 選択した SNMPv3 ユーザープロファイルが SNMP アラート送信先について構成されている場合、ユーザープロファイルを削除した後、そのアラートは送信されなくなります。

3. 要求を確認するメッセージが表示されたら、**はい、削除します**をクリックします。

SNMPv3 設定の構成

SNMPv3 エンジン ID および SNMPv3 通知設定を構成するには、**SNMPv3 設定**セクションを使用します。

iLO では、業界標準の SNMPv3 通知機能をサポートしています。SNMPv3 通知を送信する際、通知は保存され、受信者が肯定応答を iLO に送信するまで、または最大再試行回数に達するまで定期的に再送信されます。

前提条件

iLO 設定の構成権限

手順

1. ナビゲーションツリーの**管理**をクリックします。

   SNMP 設定ページが表示されます。

2. **SNMPv3 エンジン ID** ボックスに値を入力します。

   値を指定しない場合は、このボックスを空白にすることができます。

3. SNMPv3 通知設定を構成するには、以下の値を入力します。

   - **SNMPv3 通知リトライ**
   - **SNMPv3 通知時間間隔**

4. **適用**をクリックします。

SNMPv3 の設定オプション

SNMPv3 エンジン ID

SNMP エージェントエンティティに属する SNMP エンジンの一意の識別子。

この値は 6～48 文字で構成される 16 進数文字列で（先頭の 0x はカウントしない）、文字数は偶数でなければなりません（例：`0x01020304abcdef`）。この設定を構成しない場合、値はシステムで生成されます。

SNMPv3 通知リトライ

受信者が肯定応答を iLO に送信しない場合に iLO がアラートを再送する回数。

0～5 の値を入力します。デフォルト値は 2 です。

SNMP 通知時間間隔

SNMPv3 通知アラートの再送を試行する時間間隔の秒数。

5～120 秒の範囲で値を入力します。デフォルト値は 15 秒です。

SNMP アラートの構成

前提条件

iLO の設定を構成する権限

手順

1. ナビゲーションツリーの**管理**をクリックします。

   SNMP 設定ページが表示されます。

2. **SNMP アラート**セクションで、**iLO ホスト名**または **OS ホスト名**を選択して、**トラップソース識別子**を構成します。

3. 以下の値を構成します。

   - **iLO SNMP アラート**
   - **SNMPv1**
   - **コールドスタートトラップブロードキャスト**
   - **定期的な HSA トラップ構成**

4. （オプション）テストアラートを作成し、構成済みの SNMP アラート送信先にこれを送信するには、**テストアラートの送信**をクリックします。

   テストアラートは、構成済みの SNMP アラート送信先アドレスとの iLO のネットワーク接続を確認するために使用されます。アラートが生成されたら、アラート送信先でアラートの受信を確認します。

5. 構成を保存するには、**適用**をクリックします。

SNMP アラートの設定

トラップソース識別子

iLO が SNMP トラップを生成するときに SNMP で定義された **sysName** 変数に使用されるホスト名を決定します。デフォルト設定は、**iLO ホスト名**です。

ホスト名は OS の構成要素です。ハードドライブが新しいサーバープラットフォームに移動される場合など、サーバーに固定されているわけではありません。ただし、iLO の **sysName** は、システムボードに固定されています。

iLO SNMP アラート

ホストオペレーティングシステムとは関係なく iLO によって検出されたアラート状態は、指定された SNMP アラート送信先に送信できます。このオプションが無効になっている場合、トラップは構成された SNMP アラートの送信先に送信されません。

SNMPv1

iLO における、外部 SNMPv1 要求の受信と、**読み取りコミュニティ 1**、**読み取りコミュニティ 2**、**読み取りコミュニティ 3** の各ボックスで構成されたリモート管理システムへの SNMPv1 トラップの送信を有効にします。この設定は、デフォルトでは無効になっています。

コールドスタートトラップブロードキャスト

次の条件のいずれかを満たす場合、コールドスタートトラップは、サブネットブロードキャストアドレスにブロードキャストされます。

- **SNMP アラートの送信先**が構成されていない。
- **SNMP アラートの送信先**は構成されているが、SNMP プロトコルが無効である。
- iLO が一部の **SNMP アラートの送信先**を IP アドレスに解決できなかった。

IPv4 ホストのサブネットブロードキャストアドレスは、サブネットマスクとホスト IP アドレスのビット成分間のビット論理 `OR` 演算を実行することで取得されます。たとえば、サブネットマスクが `255.255.252.0` のホスト `192.168.1.1` のブロードキャストアドレスは、`192.168.1.1 | 0.0.3.255 = 192.168.3.255` になります。

定期的な HSA トラップ構成

デフォルト構成では、iLO はコンポーネントのステータスが変更された場合（たとえば、ファンステータスが障害に変更された場合）に限り、ヘルスステータスアレイ（HSA）トラップを送信します。

サポートされているコンポーネントが障害または機能低下状態のとき、HSA トラップを定期的に（日次、週次、月次）送信するよう iLO を構成できます。この設定は、デフォルトでは無効になっています。

AMS コントロールパネルを使用した SNMP および SNMP アラートの設定（Windows 専用）

手順

1. Agentless Management Service のコントロールパネルを開きます。
2. **SNMP** タブをクリックします。
3. SNMP 設定をアップデートします。
4. （オプション）テストアラートを作成し、構成済みの**トラップの宛先**にこれを送信するには、**テストトラップの送信**をクリックします。

   テストアラートは、iLO の**トラップ先**アドレスとのネットワーク接続を確認するために使用されます。アラートが生成されたら、アラート送信先でアラートの受信を確認します。
5. 構成を保存するには、**適用**をクリックします。

SNMP トラップ

次の表に、（対応するインテグレーテッドマネジメントログまたは iLO イベントログのクラスおよびコードとともに）iLO 5 およびサポートされる ProLiant サーバーおよび Synergy Compute Module によってサポートされている SNMP トラップを示します。

SNMP トラップと REST アラート情報を相互参照するには、**REST アラート**を参照してください。

イベントのトラブルシューティング情報を確認するには、イベントクラスおよびイベントコードの値を、Web サイト **https://www.hpe.com/support/ilo-docs** にある IML メッセージおよびトラブルシューティングガイドの値と照合してください。

トラップ ID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
0	該当なし	該当なし	`Cold Start Trap` SNMP が初期化され、システムで POST が完了した、または AMS が起動しました。	該当なし
4	該当なし	該当なし	`Authentication Failure Trap` SNMP が認証失敗を検出しました。	該当なし
1006	5h	3h	`cpqSeCpuStatusChange` 訂正不可能なマシンチェック例外がプロセッサーで検出されました。	メジャー
1010	28h	2h	`cpqSeUSBStorageDeviceReadErrorOccurred` 接続されている USB ストレージデバイスで読み取りエラーが発生しました。	OK
1011	28h	3h	`cpqSeUSBStorageDeviceWriteErrorOccurred` 接続されている USB ストレージデバイスで書き込みエラーが発生しました。	OK
1012	28h	4h	`cpqSeUSBStorageDeviceRedundancyLost` USB ストレージデバイスの冗長性が失われました。	警告
1013	28h	4h	`cpqSeUSBStorageDeviceRedundancyRestored` USB ストレージデバイスの冗長性が回復しました。	OK
1014	28h	5h	`cpqSeUSBStorageDeviceSyncFailed` USB ストレージデバイスの冗長性を回復するための同期操作に失敗しました。	警告

表は続く

トラップ ID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
1015	33h	5h	cpqSePCIeDiskTemperatureFailed PCIe ディスクの温度が上限クリティカルしきい値を超えました。	クリティカル
1016	33h	5h	cpqSePCIeDiskTemperatureOk PCIe ディスクの温度は正常です。	OK
1017	33h	2h	cpqSePCIeDiskConditionChange PCIe ディスクのステータスが変化しました。	クリティカル
1018	33h	3h	cpqSePCIeDiskWearStatusChange PCIe ディスク消耗ステータスが変化しました。	クリティカル
1019	33h	4h	cpqSePciDeviceAddedOrPoweredOn PCI デバイスが追加されたか、電源がオンになりました。	OK
1020	33h	5h	cpqSePciDeviceRemovedOrPoweredOff PCI デバイスが削除されたか、電源がオフになりました。	OK
1021	Ah	3152h	cpqSeNVMeSecureEraseFailed NVMe ドライブのセキュア消去に失敗しました。	クリティカル
1022	32h	3020h 3021h	cpqSePcieTrainingFailed PCI Express スロットは、連結に失敗しました。	クリティカル
1023	Ah	3158h	cpqSePciResetFail システムはスロットの PCI コントローラーでリセットを実行できません。	クリティカル
2014	2h	2Dh	cpqSiIntrusionInstalled システム侵入ハードウェアが取り付けられました。	OK
2015	2h	2Eh	cpqSiIntrusionRemoved システム侵入ハードウェアが取り外されました。	OK

表は続く

トラップ ID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
2016	2h	30h	`cpqSiHoodReplaced` システムフードが交換されました。	OK
2017	Ah	401h	`cpqSiHoodRemovedOnPowerOff` サーバーの電源オフ時にシステムフードが取り外されました。	メジャー
2018	35h	1h	`cpqSiSysTelemetryThresholdAlert` システムテレメトリのメトリック値が上限しきい値を超過したか、または下限しきい値より低くなっています。	情報
3033	13h	12h	`cpqDa6CntlrStatusChange` Smart アレイコントローラーのステータスの変化が検出されました。	クリティカル
3034	13h	21h	`cpqDa6LogDrvStatusChange` Smart アレイ論理ドライブのステータスの変化が検出されました。	クリティカル
3038	13h	17h	`cpqDa6AccelStatusChange` Smart アレイキャッシュモジュールのステータスの変化が検出されました。	クリティカル
3039	13h	23h	`cpqDa6AccelBadDataTrap` Smart アレイキャッシュモジュールのバックアップ電源が失われました。	クリティカル
3040	13h	24h	`cpqDa6AccelBatteryFailed` Smart アレイキャッシュモジュールのバックアップ電源が故障しました。	クリティカル
3046	13h	14h	`cpqDa7PhyDrvStatusChange` Smart アレイ物理ドライブのステータスの変化が検出されました。	クリティカル
3047	13h	2Ch	`cpqDa7SpareStatusChange` Smart アレイスペアドライブのステータスの変化が検出されました。	クリティカル

表は続く

トラップ ID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
3049	13h	15h	`cpqDaPhyDrvSSDWearStatusChange` Smart アレイ物理ドライブの SSD Wear ステータスの変化が検出されました。	クリティカル
3903	Ah	3151h	`cpqDaSmartArraySecureEraseFailed` Smart アレイのセキュア消去に失敗しました。	クリティカル
5022	13h	1Eh	`cpqSasPhyDrvStatusChange` AMS が、SAS または SATA 物理ドライブのステータスが変化したことを検出しました。	クリティカル
5026	13h	1Fh	`cpqSasPhyDrvSSDWearStatusChange` AMS が、SAS または SATA 物理ドライブの SSD Wear ステータスが変化したことを検出しました。	クリティカル
6026	2h	38h	`cpqHe3ThermalConfirmation` 温度上昇のためにサーバーがシャットダウンされましたが、現在は稼働しています。	OK
6027	Ah	101h	`cpqHe3PostError` 1 つまたは複数の POST エラーが発生しました。	警告
6032	Bh	36h	`cpqHe3FltTolPowerRedundancyLost` 指定されたシャーシのフォールトトレラント電源装置の冗長性が失われました。	メジャー
6033	Bh	31h	`cpqHe3FltTolPowerSupplyInserted` フォールトトレラント電源装置が取り付けられました。	OK
6034	Bh	2Ch	`cpqHe3FltTolPowerSupplyRemoved` フォールトトレラント電源装置が取り外されました。	メジャー
6035	2h	1Ah	`cpqHe3FltTolFanDegraded` フォールトトレラントファン状態が、劣化に設定されました。	クリティカル

表は続く

トラップ ID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
6036	2h	17h	cpqHe3FltTolFanFailed フォールトトレラントファン状態が、障害に設定されました。	クリティカル
6037	2h	23h	cpqHe3FltTolFanRedundancyLost フォールトトレラントファンの冗長性が失われました。	メジャー
6038	2h	1Fh	cpqHe3FltTolFanInserted フォールトトレラントファンが取り付けられました。	OK
6039	2h	1Bh	cpqHe3FltTolFanRemoved フォールトトレラントファンが取り外されました。	メジャー
6040	2h	27h	cpqHe3TemperatureFailed サーバーの温度を超えました。	クリティカル
6041	2h	14h	cpqHe3TemperatureDegraded 温度ステータスが劣化に設定され、温度が正常な動作範囲にありません。システム構成によっては、このシステムがシャットダウンされる可能性があります。	クリティカル
6042	2h	13h	cpqHe3TemperatureOk 温度ステータスが、OK に設定されました。	OK
6048	Bh	28h	cpqHe4FltTolPowerSupplyOk フォールトトレラント電源装置の状態が OK に設定されました。	OK
6049	Bh	15h	cpqHe4FltTolPowerSupplyDegraded フォールトトレラント電源装置の状態が、劣化に設定されました。	クリティカル
6050	Bh	28h	cpqHe4FltTolPowerSupplyFailed フォールトトレラント電源装置の状態が、障害に設定されました。	クリティカル

表は続く

トラップ ID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
6051	該当なし	該当なし	cpqHeResilientMemMirroredMemoryEngaged アドバンストメモリプロテクションサブシステムが、メモリ障害を検出しました。ミラーメモリがアクティブになりました。	メジャー
6054	Bh	36h	cpqHe3FltTolPowerRedundancyRestore フォールトトレラント電源装置が冗長化の状態に回復しました。	OK
6055	2h	23h	cpqHe3FltTolFanRedundancyRestored フォールトトレラントファンが冗長化の状態に回復しました。	OK
6061	該当なし	該当なし	cpqHeManagementProcInReset 管理プロセッサーはリセット中です。	マイナー
6062	該当なし	該当なし	cpqHeManagementProcReady 管理プロセッサーは使用可能です。	情報
6064	該当なし	該当なし	cpqHe5CorrMemReplaceMemModule メモリエラーが訂正されました。メモリモジュールを取り付けます。	メジャー
6069	Bh	52h	cpqHe4FltTolPowerSupplyACpowerloss 指定されたシャーシおよびベイのフォールトトレラント電源装置が AC 電源の消失を報告しました。	クリティカル
6070	Bh	3Eh	cpqHeSysBatteryFailed HPE Smart ストレージバッテリが故障しました。	警告
6071	Bh	1Eh	cpqHeSysBatteryRemoved HPE Smart ストレージバッテリが取り外されました。	警告
6072	27h	4h	cpqHeSysPwrAllocationNotOptimized iLO は所要電力を特定できませんでした。サーバーの電力割り当てが最適化されていません。	警告

表は続く

トラップ ID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
6073	Bh	24h	cpqHeSysPwrOnDenied ハードウェアを識別できないために、サーバーの電源をオンにできませんでした。	クリティカル
6074	14h	7h	cpqHePowerFailureError デバイスの電源障害が検出されました。	クリティカル
6075	29h	1h	cpqHeInterlockFailureError デバイスがシステムボードにない、または適切に取り付けられていません。	クリティカル
6076	Ah	340h	cpqHeNvdimmBackupError NVDIMM バックアップエラーが検出されました。	クリティカル
6077	Ah	341h	cpqHeNvdimmRestoreError NVDIMM の復元エラーが検出されました。	クリティカル
6078	Ah	342h	cpqHeNvdimmUncorrectableMemoryError 訂正不能なメモリエラーが検出されました。	クリティカル
6079	Ah	343h	cpqHeNvdimmBackupPowerError NVDIMM のバックアップ電源エラーが発生しました。バックアップ電源を使用できません。これ以上のバックアップは不可能です。	クリティカル
6080	Ah	344h	cpqHeNvdimmNVDIMMControllerError NVDIMM コントローラーのエラーが発生しました。OS では NVDIMM は使用されません。	クリティカル
6081	Ah	345h	cpqHeNvdimmEraseError NVDIMM を消去できませんでした。これ以上のバックアップは不可能です。	クリティカル
6082	Ah	346h	cpqHeNvdimmArmingError NVDIMM を取り付けることができませんでした。これ以上のバックアップは不可能です。	クリティカル

表は続く

トラップ ID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
6083	Ah	355h	`cpqHeNvdimmSanitizationOk` この NVDIMM-N がサニタイズ/消去の対象として選択されました。NVDIMM に保存されているデータはすべて消去されました。	OK
6084	Ah	356h	`cpqHeNvdimmSanitizationError` この NVDIMM-N はサニタイズ/消去の対象として選択されましたが、このプロセスが正常に終了しませんでした。	クリティカル
6085	Ah	364h	`cpqHeNvdimmControllerFirmwareError` NVDIMM コントローラーファームウェアのエラーが発生しました。コントローラーファームウェアが壊れているため、OS で NVDIMM は使用されません。	クリティカル
6086	Ah	374h	`cpqHeNvdimmErrorInterleaveOn` メモリの初期化エラーまたは訂正不能エラーが発生しました。プロセッサーの NVDIMM はすべて無効です。	クリティカル
6087	Ah	375h	`cpqHeNvdimmInterleaveOff` メモリの初期化エラーまたは訂正不能エラーが発生しました。NVDIMM は無効になっています。	クリティカル
6088	Ah	394h	`cpqHeNvdimmEventNotifyError` この NVDIMM のイベント通知を設定できません。	クリティカル
6089	Ah	395h	`cpqHeNvdimmPersistencyLost` NVDIMM の持続性が失われました。これ以上のデータバックアップは不可能です。	クリティカル
6090	Ah	396h	`cpqHeNvdimmPersistencyRestored` NVDIMM の持続性が復元されました。これ以上のデータバックアップが可能です。	情報
6091	Ah	397h	`cpqHeNvdimmLifecycleWarning` NVDIMM ライフサイクルの警告。NVDIMM の寿命に達しました。	メジャー

表は続く

トラップ ID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
6092	Ah	430h	cpqHeNvdimmLogicalNvdimmError 論理 NVDIMM のエラーが発生しました。	メジャー
6093	Ah	354h	cpqHeNvdimmConfigurationError NVDIMM 構成エラーが発生しました。	クリティカル
6094	Ah	351h	cpqHeNvdimmBatteryNotChargedwithWait スマートバッテリは、取り付けられた NVDIMM をサポートするほど十分に充電されていません。	OK
6095	Ah	352h	cpqHeNvdimmBatteryNotChargedwithNoWait スマートバッテリは、取り付けられた NVDIMM をサポートするほど十分に充電されていません。	OK
6096	Ah	388h	cpqHeDimmMemoryMapChanged 訂正不能なメモリエラー - 障害が発生しているメモリモジュールを判別できませんでした。	警告
6097	Ah	440h	cpqHeNvdimmPersistantMemoryAddressError Persistent Memory アドレス範囲スクラブでエラーが検出されました。	クリティカル
6098	Ah	483h	cpqHeNvdimmInitializationError 内部エラーのため、1 つまたは複数の NVDIMM を初期化できません。	警告
6099	Bh	54h	cpqHePwrSupplyError システム電源装置のエラーが発生しました。	警告
6100	Bh	54h	cpqHePwrSupplyErrorRepaired システム電源装置のエラーが修復されました。	OK
6101	Bh	55h	cpqHeBbuError バッテリバックアップユニットのエラーが発生しました。	警告
6102	Bh	55h	cpqHeBbuErrorRepaired バッテリバックアップユニットのエラーが修復されました。	OK

表は続く

トラップ ID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
6103	Bh	1Ch	cpqHeNoPowerSupplyDetected 電源装置または電源バックプレーンは検出されませんでした。	メジャー
6104	Bh	1Bh	cpqHePowerProtectionFault システムボードの電源保護障害が発生しました。	クリティカル
6105	14h	9h	cpqHePowerFuseDegraded 電源の劣化が検出され、サーバーシステムボードを交換する必要があります。	クリティカル
6106	Ah	3134h	cpqHeTPMSecureEraseFailed Trusted Platform Module のセキュア消去に失敗しました。	クリティカル
6107	Ah	3140h	cpqHeSPISecureEraseFailed システムファームウェア構成のセキュア消去に失敗しました。	クリティカル
6108	Ah	3137h	cpqHeNvdimmSecureEraseFailed HPE Persistent Memory のセキュア消去に失敗しました。	クリティカル
6109	28h	6h	cpqHeNANDSecureEraseFailed 管理プロセッサーの内蔵メディアデバイスのセキュア消去に失敗しました。	クリティカル
6110	Ah	3143h 3145h 3146h	cpqHeSedPassphrasefail デバイスの暗号化エラー。暗号化の有効化または無効化あるいはパスフレーズの変更に失敗しました。	クリティカル
6111	Ah	3148h	cpqHeSedUnlockfail 自己暗号化デバイスのロックを解除する不正な試行が 3 回実行されました。デバイスは次回のリブートまでロックされます。	メジャー
6118	2h	39h	cpqHeInletAmbientPreCautionThresAlert インレット周囲センサーの読み取り値がユーザー定義の値以上です。	マイナー

表は続く

トラップ ID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
8029	13h	28h	cpqSs6FanStatusChange ストレージエンクロージャーのファンステータスが変化しました。	クリティカル
8030	13h	29h	cpqSs6TempStatusChange ストレージエンクロージャーの温度ステータスが変化しました。	クリティカル
8031	13h	2Ah	cpqSs6PwrSupplyStatusChange ストレージエンクロージャーの電源ステータスが変化しました。	クリティカル
8032	13h	2Bh	cpqSsConnectionStatusChange ストレージエンクロージャーのステータスが変化しました。	クリティカル
9001	23h	5h	cpqSm2ServerReset サーバー電源がリセットされました。	クリティカル
9003	23h	1100h	cpqSm2UnauthorizedLoginAttempts 認証されないログイン試行回数の最大値を超えました。	情報
9005	23h	1101h	cpqSm2SelfTestError iLO がセルフテストエラーを検出しました。	クリティカル
9012	23h	104h	cpqSm2SecurityOverrideEngaged iLO が、セキュリティオーバーライドジャンパーが接続位置に切り替えられていることを検出しました。	情報
9013	23h	105h	cpqSm2SecurityOverrideDisengaged iLO が、セキュリティオーバーライドジャンパーが切断位置に切り替えられていることを検出しました。	情報
9017	23h	3h	cpqSm2ServerPowerOn サーバーの電源が入れられました。	OK
9018	23h	1h	cpqSm2ServerPowerOff サーバーの電源が切られました。	OK

表は続く

トラップ ID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
9019	23h	1102h	`cpqSm2ServerPowerOnFailure` 電源オン要求がありましたが、サーバーが障害状態にあったために電源を入れることができませんでした。	クリティカル
9020	23h	1138h	`cpqSm2IrsCommFailure` Insight Remote Support または Insight Online との通信に失敗しました。	警告
9021	32h	3h	`cpqSm2FirmwareValidationScanFailed` ファームウェア検証エラーが発生しました（iLO、IE、または SPS ファームウェア）。	クリティカル
9022	32h	3h	`cpqSm2FirmwareValidationScanErrorRepaired` 報告されたファームウェア整合性スキャンの問題は修復されました。	OK
9023	32h	4h	`cpqSm2FirmwareValidationAutoRepairFailed` ファームウェアのリカバリ時にエラーが発生しました。	警告
9024	14h	2h	`cpqSm2AutoShutdownInitiated` iLO がオペレーティングシステムの自動シャットダウンを開始しました。	メジャー
9025	14h	2h	`cpqSm2AutoShutdownCancelled` オペレーティングシステムの自動シャットダウンがキャンセルされました。	OK
9026	23h	448h	`cpqSm2FwUpdateUploadFailed` ファームウェアアップデートまたはアップロードに失敗しました。	警告
9027	23h	464h	`cpqSm2SecurityStateChange` iLO セキュリティの状態が変化しました。	OK

表は続く

トラップ ID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
9028	23h	B3h	cpqSm2WDTimerReset iLO がウォッチドッグ タイマーのタイムアウトを検出しました。オペレーティングシステムに装備された後は、フェイルセーフタイマーは定期的に扱われません。	メジャー
9029	23h	491h	cpqSm2OverallSecStateAtRisk システムセキュリティ状態にリスクがあります。	メジャー
9030	23h	490h	cpqSm2OverallSecStatusChange 全体セキュリティステータスが変更されました。	メジャー
11003	1h	1h	cpqHo2GenericTrap 汎用トラップ。SNMP 設定、クライアント SNMP コンソール、およびネットワークが正しく動作していることを確認します。iLO の Web インターフェイスを使用すると、このアラートを生成して、SNMP コンソールでアラートが受信されることを確認できます。	情報
11018	23h	CEh	cpqHo2PowerThresholdTrap 電力しきい値を超えました。	メジャー
11020	該当なし	該当なし	cpqHoMibHealthStatusArrayChangeTrap サーバーのヘルスステータスが変化しました。	該当なし
14004	13h	20h	cpqIdeAtaDiskStatusChange AMS が、ATA ディスクドライブのステータスが変化したことを検出しました。	クリティカル
14007	Ah	3150h	cpqIdeAtaSecureEraseFailed SATA ドライブのセキュア消去に失敗しました。	クリティカル
16028	11h	Bh	cpqFca3HostCntlrStatusChange AMS が、ファイバーチャネルホストコントローラーのステータスが変化したことを検出しました。	クリティカル
18011	11h	Ah	cpqNic3ConnectivityRestored 論理ネットワークアダプターとの接続が回復しました。	OK

表は続く

トラップ ID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
18012	11h	Ah	cpqNic3ConnectivityLost 論理ネットワークアダプターのステータスが障害に変化しました。	警告
18013	11h	Ch	cpqNic3RedundancyIncreased AMS が、接続されている論理アダプターグループ内の障害が発生していた物理アダプターが良好ステータスに復帰したことを検出しました。	OK
18014	11h	Ch	cpqNic3RedundancyReduced AMS が、論理アダプターグループ内の物理アダプターが障害ステータスに変化したが、少なくとも 1 台の物理アダプターが OK ステータスで残っていることを検出しました。	警告
18015	11h	Dh	cpqNicAllLinksDown ネットワークアダプターのすべてのリンクがダウンしています。	メジャー
18016	Bh	Eh	cpqNicAllLinksDownRepaired ネットワークアダプターの 1 つまたは複数のリンクが修復されました。	OK
18017	32h	3023h	cpqNicFlexLomTrainingFailed Flexlom スロットは、連結に失敗しました。	クリティカル
169001	12h	1h	cpqiScsiLinkUp iSCSI リンクがアップしています。	OK
169002	12h	2h	cpqiScsiLinkDown iSCSI リンクがダウンしています。	メジャー

これらの SNMP トラップについて詳しくは、HPE SIM 用の Insight Management MIB アップデートキットに含まれている以下の MIB ファイルを参照してください。

cpqida.mib	ドライブアレイ
cpqhost.mib	サーバーホストシステムの詳細
cpqhlth.mib	サーバーヘルスシステム

表は続く

cpqsm2.mib	Remote Insight/Integrated Lights-Out
cpqide.mib	IDE サブシステム
cpqscsi.mib	SCSI システム
cpqiscsi.mib	iSCSI システム
cpqnic.mib	システム NIC
cpqstsys.mib	ストレージシステム
cpqstdeq.mib	サーバー標準装置
cpqfca.mib	ファイバーチャネルアレイ
cpqsinfo.mib	システム情報
cpqstsys.mib	Smart Array ストレージ

REST アラート

次の表に、iLO 5 およびサポートされる ProLiant サーバーおよび Synergy コンピュートモジュールによってサポートされている REST アラートを示します。REST アラートと SNMP トラップ情報を相互参照するには、**SNMP トラップ**を参照してください。

トラップ ID	REST アラート ID	REST の重大度
0	該当なし	該当なし
4	SNMPAuthenticationFailure	OK
1006	ProcessorStatusUnknown	警告
	ProcessorStatusOK	OK
	ProcessorStatusDegraded	警告
	ProcessorStatusDisabled	警告
	ProcessorStatusFailed	クリティカル
1010	USBStorageDeviceReadError	OK
1011	USBStorageDeviceWriteError	OK
1012	USBStorageDeviceRedundancyLost	警告

表は続く

トラップ ID	REST アラート ID	REST の重大度
1013	USBStorageDeviceRedundancyRestored	OK
1014	USBStorageDeviceSyncFailed	警告
1015	PCIeDiskTemperatureFailed	クリティカル
1016	PCIeDiskTemperatureOk	OK
1017	PCIeDriveConditionOk	OK
	PCIeDriveConditionDegraded	警告
	PCIeDriveConditionFailed	クリティカル
1018	PCIeDriveWearStatusOk	OK
	PCIeDriveWearStatusFiftySixDayThreshold	警告
	PCIeDriveWearStatusFivePercentThreshold	警告
	PCIeDriveWearStatusTwoPercentThreshold	警告
	PCIeDriveWearStatusWearOut	クリティカル
1019	PCIeDriveAddedOrPowerOn	OK
1020	PCIeDriveRemovedOrPowerOff	OK
1021	NVMeSecureEraseFailed	クリティカル
1022	該当なし	該当なし
1023	PciResetFail	クリティカル
2014	IntrusionHWInstalled	OK
2015	IntrusionHWRemoved	OK
2016	HoodReplaced	OK
2017	HoodRemovedOnPowerOff	警告
2018	MetricValueExceededUpperThreshold	警告
	MetricValueBelowLowerThreshold	警告

表は続く

トラップ ID	REST アラート ID	REST の重大度
3033	DrvArrControllerFailed	クリティカル
	DrvArrControllerOK	OK
3034	DrvArrLogDrvFailed	クリティカル
	DrvArrLogDrvUnconfigured	クリティカル
	DrvArrLogDrvRecovering	警告
	DrvArrLogDrvReadyRebuild	警告
	DrvArrLogDrvRebuilding	警告
	DrvArrLogDrvWrongDrive	クリティカル
	DrvArrLogDrvBadConnect	クリティカル
	DrvArrLogDrvOverheating	警告
	DrvArrLogDrvShutdown	クリティカル
	DrvArrLogDrvExpanding	OK
	DrvArrLogDrvNotAvailable	警告
	DrvArrLogDrvQueuedForExpansion	警告
	DrvArrLogDrvMultiPathAccessDegraded	警告
	DrvArrLogDrvErasing	警告
	DrvArrLogDrvPredictiveSpareRebuildReady	OK
	DrvArrLogDrvRapidParityInitializationInProgress	警告
	DrvArrLogDrvRapidParityInitializationPending	警告
	DrvArrLogDrvNoAccessEncryptedMissingKey	クリティカル
	DrvArrLogDrvUnencryptedToEncryptedTransformationInProgress	警告
	DrvArrLogDrvRekeyInProgress	警告
	DrvArrLogDrvNoAccessEncryptedWithControllerEncryptionNotEnabled	クリティカル
	DrvArrLogDrvUnencryptedToEncryptedTransformationNotStarted	OK
	DrvArrLogDrvNewLogDrvKeyRekeyRequestReceived	OK
	DrvArrLogDrvOK	OK

表は続く

トラップ ID	REST アラート ID	REST の重大度
3038	DrvArrayAccBoardInvalid	警告
	DrvArrayAccBoardEnabled	OK
	DrvArrayAccBoardTempDisabled_BadConfiguration	クリティカル
	DrvArrayAccBoardTempDisabled_LowBatteryPower	クリティカル
	DrvArrayAccBoardTempDisabled_DisableCommandIssued	警告
	DrvArrayAccBoardTempDisabled_NoResourcesAvailable	警告
	DrvArrayAccBoardTempDisabled_BoardNotConnected	クリティカル
	DrvArrayAccBoardPermDisabled_BadMirrorData	警告
	DrvArrayAccBoardPermDisabled_ReadFailure	警告
	DrvArrayAccBoardPermDisabled_WriteFailure	警告
	DrvArrayAccBoardPermDisabled_ConfigCommand	警告
	DrvArrayAccBoardTempDisabled_ExpandInProgress	OK
	DrvArrayAccBoardTempDisabled_SnapshotInProgress	OK
	DrvArrayAccBoardTempDisabled_RedundantLowBattery	OK
	DrvArrayAccBoardTempDisabled_RedundantSizeMismatch	OK
	DrvArrayAccBoardTempDisabled_RedundantCacheFailure	警告
	DrvArrayAccBoardPermDisabled_ExcessiveECCErrors	クリティカル
	DrvArrayAccBoardTempDisabled_RAID_ADG_EnablerModuleMissing	クリティカル
	DrvArrayAccBoardPermDisabled_PostECCErrors	OK
	DrvArrayAccBoardPermDisabled_BackupPowerSourceHotRemoved	クリティカル
	DrvArrayAccBoardPermDisabled_CapacitorChargeLow	クリティカル
	DrvArrayAccBoardPermDisabled_NotEnoughBatteries	警告
	DrvArrayAccBoardPermDisabled_NotSupportedByFirmware	警告
	DrvArrayAccBoardPermDisabled_BatteryNotSupported	クリティカル
	DrvArrayAccBoardPermDisabled_NoCapacitorAttached	クリティカル
	DrvArrayAccBoardPermDisabled_FlashBackedBackupFailed	警告
	DrvArrayAccBoardPermDisabled_FlashBackedRestoreFailed	クリティカル
	DrvArrayAccBoardPermDisabled_FlashBackedHardwareFailure	クリティカル
		クリティカル

表は続く

トラップ ID	REST アラート ID	REST の重大度
	DrvArrayAccBoardPermDisabled_CapacitorFailedToCharge	クリティカル
	DrvArrayAccBoardPermDisabled_IncompatibleCacheModule	クリティカル
	DrvArrayAccBoardPermDisabled_ChargerCircuitFailure	警告
	DrvArrayAccBoardTempDisabled_MegaCellNotCabled	
	DrvArrAcceleratorFlashMemoryNotAttached	
3039	DrvArrayAccBoardBadData	クリティカル
3040	DrvArrayAccBoardBatteryFailed	クリティカル
3046	DrvArrPhysDrvFailed	クリティカル
	DrvArrPhysDrvPredictiveFailure	警告
	DrvArrPhysDrvWearOut	警告
	DrvArrPhysDrvErasing	警告
	DrvArrPhysDrvNotAuthenticated	警告
	DrvArrPhysDrvEraseDone	警告
	DrvArrPhysDrvEraseQueued	警告
	DrvArrPhysDrvOK	OK
3047	DrvArrSpareDriveFailed	クリティカル
	DrvArrSpareDriveInactive	OK
	DrvArrSpareDriveBuilding	クリティカル
	DrvArrSpareDriveActive	OK
3049	DrvArrSolidStateDiskFiftySixDayThresholdPassed	警告
	DrvArrSolidStateDiskFivePercentThresholdPassed	警告
	DrvArrSolidStateDiskTwoPercentThresholdPassed	警告
	DrvArrSolidStateDiskWearOut	クリティカル
	DrvArrSolidStateDiskWearOK	OK
3903	SmartArraySecureEraseFailed	クリティカル
5022	該当なし	該当なし
5026	該当なし	該当なし

表は続く

トラップ ID	REST アラート ID	REST の重大度
6026	ServerOperational	警告
6027	POSTErrorsOccurred	警告
6032	PowerRedundancyLost	警告
6033	PowerSupplyInserted	OK
6034	PowerSupplyRemoved	警告
6035	FanDegraded	クリティカル
6036	FanFailed	クリティカル
6037	FanRedundancyLost	警告
6038	FanInserted	OK
6039	FanRemoved	警告
6040	ThermalStatusFailure	クリティカル
6041	ThermalStatusDegradedSysShutdown ThermalStatusDegradedSysContinue	クリティカル クリティカル
6042	ThermalStatusOK	OK
6048	PowerSupplyOK	OK
6049	PowerSupplyDegraded	クリティカル
6050	PowerSupplyFailed	クリティカル
6051	MirroredMemoryEngaged	警告
6054	PowerRedundancyRestored	OK
6055	FanRedundancyRestored	OK
6061	該当なし	該当なし
6062	該当なし	該当なし

表は続く

トラップ ID	REST アラート ID	REST の重大度
6064	CorrectableOrUncorrectableMemoryErrors	警告
6069	PowerSupplyACPowerLoss	クリティカル
6070	SystemBatteryFailed	警告
6071	SystemBatteryRemoved	警告
6072	SystemPowerAllocationNotOptimized	クリティカル
6073	SystemPowerOnDenied	クリティカル
6074	PowerFailureErrorTempAboveCritical	クリティカル
	PowerFailureErrorInputPowerLoss	クリティカル
	PowerFailureErrorBadFuse	クリティカル
	PowerFailureStandby	クリティカル
	PowerFailureRuntime	クリティカル
	PowerFailurePowerOn	クリティカル
	PowerFailureUnknown	クリティカル
	PowerFailureCpuThermalTrip	クリティカル
6075	InterlockFailureErrorStandby	クリティカル
	InterlockFailureErrorRuntime	クリティカル
	InterlockFailureErrorPowerOn	クリティカル
	InterlockFailureErrorUnknown	クリティカル
6076	NvdimmBackupError	クリティカル
6077	NvdimmRestoreError	クリティカル
6078	NvdimmUncorrectableMemoryError	クリティカル
6079	NvdimmBackupPowerError	クリティカル
6080	NvdimmControllerError	クリティカル
6081	NvdimmEraseError	クリティカル
6082	NvdimmArmingError	クリティカル

表は続く

トラップ ID	REST アラート ID	REST の重大度
6083	HeNvdimmSanitizationOk	警告
6084	NvdimmSanitizationError	クリティカル
6085	HeNvdimmControllerFirmwareError	クリティカル
6086	NvdimmInterleaveOn	クリティカル
6087	NvdimmInterleaveOff	クリティカル
6088	NvdimmEventNotifyError	クリティカル
6089	NvdimmPersistencyLost	クリティカル
6090	NvdimmPersistencyRestored	OK
6091	HeNvdimmLifecycleWarning	警告
6092	NvdimmLogicalNvdimmError	警告
6093	NvdimmConfigurationError	クリティカル
6094	NvdimmBatteryNotChargedwithWait	警告
6095	NvdimmBatteryNotChargedwithNoWait	警告
6096	NvdimmMemoryMapChanged	警告
6097	NvdimmPersistantMemoryAddressError	クリティカル
6098	NvdimmInitializationError	警告
6099	PwrSupplyError	警告
6100	PwrSupplyErrorRepaired	OK
6101	BatteryBackupUnitError	クリティカル
6102	BatteryBackupUnitErrorRepaired	OK
6103	NoPowerSupplyDetected	クリティカル
6104	PowerProtectionFault	クリティカル

表は続く

トラップ ID	REST アラート ID	REST の重大度
6105	PowerDegradedEventDetected	クリティカル
6106	TPMSecureEraseFailed	クリティカル
6107	SPISecureEraseFailed	クリティカル
6108	AEPSecureEraseFailed	クリティカル
6109	EmbeddedMediaSecureEraseFailed	クリティカル
6110	SEDPassPhraseFailed	クリティカル
6111	SEDUnlockFailed	警告
8029	StorageSystemFanFailed	クリティカル
	StorageSystemNoFan	警告
	StorageSystemFanDegraded	クリティカル
	StorageSystemFanOK	OK
8030	StorageSystemTemperatureFailed	クリティカル
	StorageSystemTemperatureDegraded	クリティカル
	StorageSystemNoTemperature	警告
	StorageSystemTemperatureOK	OK
8031	StorageSystemPwrSupplyDegraded	クリティカル
	StorageSystemNoPwrSupply	警告
	StorageSystemPwrSupplyOK	OK
8032	該当なし	該当なし
9001	ServerResetDetected	警告
9003	UnauthorizedLoginAttempts	OK
9005	該当なし	該当なし
9012	SecurityOverrideEngaged	OK
9013	SecurityOverrideDisengaged	OK

表は続く

トラップ ID	REST アラート ID	REST の重大度
9017	ServerPoweredOn	OK
9018	ServerPoweredOff	OK
9019	ServerPowerOnFailure	クリティカル
9020	ILOToInsightRemoteSupportCommunicationFailure	警告
9021	FirmwareValidationScanFailed	クリティカル
9022	FirmwareValidationScanErrorRepaired	OK
9023	FirmwareValidationAutoRepairFailed	警告
9024	AutoShutdownInitiated	クリティカル
9025	AutoShutdownCancelled	OK
9026	該当なし	該当なし
9027	該当なし	該当なし
9028	IPMIWatchdogTimerReset	警告
9029	OverallSecStateAtRisk	警告
9030	OverallSecStatusChange	警告
11003	TestAlert	OK
11018	PowerThresholdBreach	警告
11020	該当なし	該当なし
14004	該当なし	該当なし
14007	IdeAtaSecureEraseFailed	クリティカル
16028	該当なし	該当なし
18011	NicConnectivityRestored	OK
18012	NicConnectivityLost	警告

表は続く

トラップ ID	REST アラート ID	REST の重大度
18013	該当なし	該当なし
18014	該当なし	該当なし
18015	NicAllLinksDown	クリティカル
18016	NicAllLinksDownRepaired	OK
18017	該当なし	該当なし
169001	該当なし	該当なし
169002	該当なし	該当なし

IPMI アラート

#	名前	IPMI SEL イベント（Y/N）	IPMI SEL イベントの詳細	SNMP のサポート (Y/N)	OID
1	CPU 障害	Y	IERR | 訂正不能なマシンチェックの例外がアサートされた | 構成エラーがアサートされた | アサート済み	Y	cpqSeCpuUncorrectableError cpqSeCpuStatusChange
3	メモリ ECC エラー	Y	訂正不能な ECC | アサート済み	Y	cpqHe5CorrMemReplaceMemModule
4	訂正可能なメモリエラー	Y	訂正可能な ECC | アサート済み	N	該当なし
5	メモリ障害	Y	メモリデバイスが無効になっている | 構成エラーがアサートされた | アサート済み	Y	cpqHe5CorrMemReplaceMemModule
9	電源装置で障害が発生している	Y	障害が検出された | 電源 AC の損失がアサートされた | アサート済み	Y	cpqHe4FltTolPowerSupplyFailed cpqHePwrSupplyError cpqHe4FltTolPowerSupplyACpowerloss cpqHeNoPowerSupplyDetected

表は続く

#	名前	IPMI SEL イベント（Y/N）	IPMI SEL イベントの詳細	SNMP のサポート (Y/N)	OID
10	電源装置が取り外された	Y	存在が検出された | ディアサート済み	Y	cpqHe3FltTolPowerSupplyRemoved
14	ハードディスクの障害	Y	ドライブの障害 | 事前障害がアサートされた | In Failed Array がアサートされた | アサート済み	Y	cpqDa7PhyDrvStatusChange
16	ファン障害	Y	OK に移行 | OK から重大でないへの移行がアサートされた | 軽度から回復不能への移行がアサートされた | より深刻から重大でないへの移行がアサートされた | アサート済み	Y	cpqHe3FltTolFanDegraded cpqHe3FltTolFanFailed cpqHe3FltTolFanRedundancyLost cpqHe3FltTolFanInserted
17	ファンの取り外し	N	-	Y	cpqHe3FltTolFanRemoved

iLO アラートメール

iLO アラートメールを使用すると、ホストオペレーティングシステムとは関係なく検出されたアラート条件を、1 つ以上のメールアドレスに送信するように iLO を構成することができます。iLO アラートメールのメッセージには、ML に表示される主要なホストシステムイベントが含まれます。たとえば、ファン障害が発生すると、イベントが IML に記録され、メールメッセージが詳細とともに構成されたメールアドレスに送信されます。

一部のメールサービスプロバイダーでは、スパム、商用コンテンツ、不要な容量など、問題のあるメールをブロックするためのフィルターやルールが確立されています。これらのツールによって、iLO で生成されたメッセージを受け取れない場合があります。この問題を回避するには、Hewlett Packard Enterprise ではセキュアな SMTP 接続（SSL/TLS）を有効にし、構成された SMTP サーバーによって認識された送信者のメールアドレスを構成することをお勧めします。

アラートメールを有効にする

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **SMTP 認証を有効**が有効になっている構成の場合は、メールアカウントのユーザー名とパスワードが **SMTP サーバー**に表示されます。

- **SMTP セキュア接続（SSL/TLS）を有効**が有効になっている構成の場合は、SSL/TLS がサーバーで有効になっています。
- パブリックまたは ISP の SMTP サーバーを使用する場合、受信者アドレスに使用するメールアドレスが、安全性が低いアプリケーションを許可するように構成されていることを確認します。

手順

1. ナビゲーションツリーで**管理**をクリックしてから、**アラートメール**タブをクリックします。
2. **iLO アラートメールを有効**オプションを有効に設定します。
3. 次の情報を入力します。
   - **受信者のメールアドレス**
   - **送信ドメインまたはメールアドレス**
   - **SMTP ポート**

     SMTP セキュア接続（SSL/TLS）を有効オプションを使用する場合、Hewlett Packard Enterprise ではこの値を 587 に設定することをお勧めします。
   - **SMTP サーバー**
4. セキュアな接続を介してアラートメールメッセージを送信するには、**SMTP セキュア接続（SSL/TLS）を有効**オプションを有効にします。
5. メールアカウントのユーザー名とパスワードで SMTP 接続を認証するには、**SMTP 認証を有効**オプションを有効にします。
6. **SMTP セキュア接続（SSL/TLS）を有効**および **SMTP 認証を有効**が有効になっている場合：
   a. **SMTP ユーザー名**ボックスに、構成されている SMTP サーバー上のメールアカウントのユーザー名を入力します。
   b. **SMTP パスワードの変更**チェックボックスを選択します。
   c. **新しい SMTP パスワード**ボックスと **SMTP パスワードの確認**ボックスにメールアカウントのユーザー名のパスワードを入力します。
7. 変更を保存するには、**適用**をクリックします。
8. （オプション）構成したメールアドレスにテストメッセージを送信するには、**テストアラートメールを送信**をクリックします。

   このボタンは、アラートメールが有効な場合にのみ使用できます。

   テストアラートメールが送信されます。
9. （オプション）テストメッセージを送信した場合は、iLO イベントログで正常に送信されたかどうかを確認します。

アラートメールのオプション

受信者のメールアドレス

iLO メールアラートを受信する 1 つ以上の宛先メールアドレス。複数の電子メールアドレスをセミコロンで区切って入力できます。標準メールアドレス形式でアドレスを入力します。**受信者のメールアドレス**ボックスには最大 260 文字まで入力できます。

パブリックまたは ISP の SMTP サーバーを使用する場合、入力するメールアドレスが、安全性が低いアプリケーションを許可するように構成されていることを確認します。

送信ドメインまたはメールアドレス

送信者（送信元）のメールアドレス（最大 63 文字）。この値は、以下の方法を使用して構成できます。

- iLO ホスト名に統合する送信ドメインを入力します。この方法を使用すると、送信者のメールアドレスは<iLO Hostname>@<Sender Domain>になります。
- 内部ネットワークドメインを含むカスタムのメールアドレスを入力します。たとえば、<name>@<internal domain>.com のように入力します。
- パブリックメールサーバーを使用するカスタムメールアドレスを入力します。たとえば、<name>@<email provider>.com のように入力します。

  このアドレスは、構成済みの SMTP サーバーで認識される有効なメールアドレスである必要があります。

SMTP ポート

SMTP サーバーが認証済みまたは未認証の SMTP 接続に使用するポート。デフォルト値は 25 です。セキュアな接続のために、Hewlett Packard Enterprise ではポート 587 を使用することをお勧めします。

SMTP サーバー

SMTP サーバーまたはメール送信エージェントの IP アドレスまたは DNS 名。このサーバーは、メール転送エージェントと連携して電子メールを配信します。IPv4 アドレス、IPv6 アドレス、または FQDN を入力できます。この文字列は最大 63 文字です。

SMTP セキュア接続（SSL/TLS）を有効

このオプションを有効にして、セキュアな接続を介してアラートメールメッセージを送信します。メッセージが送信されると、iLO および構成済みの **SMTP サーバー**が共通の SSL/TLS 接続を選択するようにネゴシエートします。

iLO は明示的/便宜的 TLS SMTP サーバー（STARTTLS SMTP サーバー）のみをサポートします。

この値はデフォルトで有効になっています。

SMTP 認証を有効

このオプションを有効にして、セキュアな接続経由で接続した後に構成済みの **SMTP サーバー**に対して認証します。このオプションを使用するには、**SMTP セキュア接続（SSL/TLS）を有効**が有効になっているほか、SMTP サーバー上のメールアカウントのユーザー名とパスワードを指定する必要があります。

SMTP ユーザー名

構成済みの **SMTP サーバー**上のアカウントのユーザー名（最大 63 文字）。**SMTP 認証を有効**が有効になっている場合はこの値が必要です。

この値をクリアするには、**SMTP 認証を有効**オプションを無効にし、このボックス内のテキストを削除してから、**適用**をクリックします。

SMTP パスワードの変更

このチェックボックスをクリックし、**SMTP ユーザー名**のアカウントのパスワードを入力またはアップデートして確認します。**SMTP 認証を有効**が有効になっている場合はこの値が必要です。入力できる値は 63 文字までです。

iLO Web インターフェイスからパスワードの値を表示またはコピーすることはできません。

パスワードをクリアするには、**SMTP 認証を有効**オプションを無効にし、パスワードおよびパスワード再入力の値を入力せずに**適用**をクリックします。

アラートメールを無効にする

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**管理**をクリックしてから、**アラートメール**タブをクリックします。
2. **iLO アラートメールを有効**オプションを無効に設定します。
3. 変更を保存するには、**適用**をクリックします。

リモート syslog

リモート syslog 機能を使用すると、iLO はイベント通知メッセージを syslog サーバーに送信できます。iLO ファームウェアのリモート syslog には、IML および iLO イベントログが含まれます。

iLO リモート syslog の有効化

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- リモート syslog サーバーは、UDP を使用するように構成されます。

手順

1. ナビゲーションツリーで**マネジメント**をクリックしてから、**リモート Syslog** タブをクリックします。
2. **iLO リモート Syslog を有効**オプションを有効に設定します。
3. 次の情報を入力します。
   - **リモート Syslog ポート**
   - **リモート Syslog サーバー**
4. 変更を保存するには、**適用**をクリックします。
5. （オプション）構成した Syslog サーバーにテストメッセージを送信するには、**テスト Syslog を送信**をクリックします。

   このボタンは、iLO リモート syslog が有効な場合のみ使用できます。

リモート syslog オプション

- **リモート Syslog ポート** - syslog サーバーがリスンしているポート番号。このボックスに入力できるポート番号は 1 つだけです。複数のリモート syslog サーバーを入力する場合、それらは同じポートを使用する必要があります。デフォルト値は、514 です。
- **リモート Syslog サーバー** - syslog サービスを実行しているサーバーの IP アドレス、FQDN、IPv6 名、または省略名。複数のサーバーを入力するには、サーバーの IP アドレス、FQDN、IPv6 名、または短い名前をセミコロンで区切ります。**リモート Syslog サーバー**ボックスには最大 511 文字まで入力できます。

  Linux システムでは、システムイベントは「syslog」というツールによって記録されます。iLOiLO システムの中央ログシステムとして機能するリモートシステムに Syslog サーバーを設定することができます。iLO リモート syslog 機能を有効にした場合、そのログを syslog サーバーに送信できます。

iLO リモート syslog の無効化

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- iLO の設定を構成する権限

手順

1. ナビゲーションツリーで**マネジメント**をクリックしてから、**リモート Syslog** タブをクリックします。
2. **iLO リモート Syslog を有効**オプションを無効に設定します。
3. 変更を保存するには、**適用**をクリックします。

リモート Syslog アラートレベル（Linux）

iLO の一部のステータス値は、標準の Linux rsyslog ステータス値とは異なります。次の表に、同等の値を示します。

iLO ステータス	Linux rsyslog ステータス
クリティカル	クリティカル
注意	警告
修正済み	通知
情報	情報

ライフサイクル管理機能の使用

Always On Intelligent Provisioning

Always On Intelligent Provisioning は、OS の展開の実行やハードウェア構成の詳細の確認に使用できる Web インターフェイスです。

iLO からの Intelligent Provisioning の起動

前提条件

- リモートコンソール権限
- ホスト BIOS 構成権限
- Intelligent Provisioning がサーバーにインストールされている。

手順

1. ナビゲーションツリーの**ライフサイクル管理**をクリックします。

   Intelligent Provisioning ページが表示されます。

   インストールされている **Intelligent Provisioning** のバージョンが **Intelligent Provisioning** ページに表示されます。

2. **Always On** をクリックして、Intelligent Provisioning を起動します。

   Intelligent Provisioning Web インターフェイスが新しいブラウザーウィンドウで起動します。

   Intelligent Provisioning の使用方法については、Web サイトにある Intelligent Provisioning のドキュメントを参照してください（**https://www.hpe.com/info/intelligentprovisioning/docs**）。

One-button セキュア消去

サーバーを運用廃止するか、または別の用途で準備する場合、One-button セキュア消去機能を使用できます。

One-button セキュア消去は、NIST Special Publication 800-88 Revision 1 のメディアサニタイズのガイドラインに準拠しています。

仕様について詳しくは、**https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf** を参照してください。仕様のセクション 2.5 では、サニタイズのレベルについて説明しています。付録では、メディアの最小サニタイズレベルを提示しています。

One-button セキュア消去は、ユーザーデータの**パージ**に対する NIST SP 800-88 Revision 1 のサニタイズに関する勧告を実装しており、サーバーおよびサポートされたコンポーネントをデフォルトの状態に戻します。この機能は、サーバーの揮発性に関する報告のドキュメントでユーザーが行う多くのタスクを自動化します。

One-button セキュア消去アクセス方式

次の製品から One-button セキュア消去プロセスを開始できます。

- iLO 5 2.30 以降
- Intelligent Provisioning 3.30 以降
- iLO RESTful API

iLO から One-button セキュア消去プロセスを開始するための前提条件

手順

1. 自分の iLO ユーザーアカウントにすべての iLO ユーザーアカウント権限が割り当てられていることを確認します。
2. この機能をサポートする iLO ライセンスをインストールします。

   使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
3. 消去するサーバーが SPP バージョン 2019.03.0 以降でアップデートされています。
4. 次の機能が有効になっている場合は、無効にします。
   - サーバー構成ロック

     手順については、HPE ProLiant Gen10 サーバーおよび HPE Synergy 用 UEFI システムユーティリティユーザーガイドを参照してください。
   - Smart アレイ暗号化

     手順については、HPE Smart アレイ SR Secure Encryption インストール/ユーザーガイドの「暗号化構成のクリア」セクションを参照してください。
5. c-Class および HPE Synergy システムでは、HPE OneView またはシステムに割り当てられている Virtual Connect プロファイルを削除します。
6. システムメンテナンススイッチの iLO セキュリティ設定の位置が OFF であることを確認します。
7. 消去するストレージドライブで、ネイティブのサニタイズ方式をサポートしています。

   たとえば、SATA および SAS ドライブには `SANITIZE` コマンド、NVM Express ドライブには `FORMAT` などです。NIST 文書では、上記のデバイスタイプでデータをパージするには上記のコマンドを勧めています。これらのコマンドを使用するほうが、ソフトウェアを使用してストレージドライブ上のデータを上書きするよりも安全です。
8. HPE 拡張スキーマで LDAP ディレクトリ認証を使用している場合、One-button セキュア消去プロセスを開始するために、iLO にログインする別の方法があります。

   サポートされている方法には、ローカルアカウント、Kerberos 認証、CAC スマートカード、およびスキーマフリーディレクトリアカウントが含まれます。

   HPE 拡張スキーマでは、One-button セキュア消去プロセスを開始するために必要なユーザー権限をサポートしていません。

iLO からの One-button セキュア消去プロセスの開始

前提条件

ご使用の環境が **iLO から One-button セキュア消去プロセスを開始するための前提条件**を満たしている。

手順

1. 消去しないストレージデバイスを切断またはデタッチします。

   Hewlett Packard Enterprise では、データ損失の可能性を低減するため、消去しないドライブを切断またはデタッチすることをお勧めします。この手順には、リムーバブルドライブ、外部ストレージ、共有ストレージ、およびネイティブのサニタイズ方式をサポートしていないデバイスが含まれます。

   接続されたストレージデバイスがネイティブのサニタイズ方式をサポートしていない場合、そのストレージデバイスは One-button セキュア消去プロセス中に消去されません。インテグレーテッドマネジメントログ（IML）エントリーにより、デバイスの消去の障害が報告されます。

2. （オプション）SNMP、アラートメール、または iLO RESTful API アラートを構成します。

   Hewlett Packard Enterprise では、この手順を完了することをお勧めします。

   各コンポーネントが消去されるときにエラーが発生した場合は、各エラーについて、IML エントリーが記録されます。アラートを構成している場合、通知を受け取ります。IML は、One-button セキュア消去プロセス中に消去されます。IML が消去されると、**セキュア消去レポート**テーブルに高レベルのステータス情報が表示されます。

   iLO 5 2.30 以降がインストールされている Gen10 サーバーの場合、セキュア消去レポートには、**内蔵 NAND フラッシュ**と **NVRAM** のステータスのみが含まれます。Gen10 Plus サーバーでは、レポートに、サポートされているすべてのデバイスが含まれます。

3. ナビゲーションツリーで**ライフサイクル管理**をクリックし、**廃棄**タブをクリックします。

4. **システムを消去**をクリックします。

   iLO が要求を確認するように求めます。

   △ **注意:** この機能は、システムを廃棄する場合、または別の目的で使用する場合にのみ使用してください。このプロセスは、サーバーおよびサポートされるコンポーネントを工場出荷時の状態にリセットします。ストレージ容量によっては、サーバーとコンポーネントのセキュア消去が完了するまでに 1 日以上かかる場合があります。このプロセスはいったん開始すると、元に戻すことはできません。プロセスが完了するまで、構成の変更やシステムの電源オフに関係する iLO またはシステムとの対話は避けてください。

5. セキュア消去の確認**チェックボックスをオンにして、**はい、システムを永久に消去します**をクリックします。**

   サーバーが再起動し、One-button セキュア消去プロセスが開始します。

   One-button セキュア消去の進捗は、すべての iLO Web インターフェイスページのバナー領域に表示されます。表示される情報には、完了率と推定の残り時間が含まれます。個々のハードウェアまたはソフトウェアコンポーネントの詳細は、**セキュア消去ステータス**テーブルに表示されます。

   One-button セキュア消去プロセス中に、構成を変更しないでください。このプロセス中は、iLO によってファームウェアアップデートが妨げられ、iLO がリセットされます。

   One-button セキュア消去が完了すると iLO がリセットされ、ネットワーク上で使用できなくなります。

   c-Class サーバーおよび HPE Synergy コンピュートモジュールでは、プロセスの完了後に iLO のネットワーク設定が再割り当てされることがあり、システムの電源がオンになる場合があります。

6. （オプション）システムを稼働状態に戻します。

7. （オプション）One-button セキュア消去レポートを表示、保存、または削除します。

   Hewlett Packard Enterprise では、この手順を完了することをお勧めします。

8. （オプション）デバイスが消去プロセスに失敗した場合、またはデバイスがネイティブのサニタイズ方式をサポートしていない場合は、次のいずれかを実行します。

- これらのデバイスを分離し、他の方式を使用してデータを削除します。
- 組織のセキュリティポリシーに従ってデバイスを安全に廃棄します。

Hewlett Packard Enterprise では、この手順を完了することをお勧めします。

One-button セキュア消去ステータス値

One-button セキュア消去プロセスを開始すると、全体の進捗が iLO バナーに表示されます。個々のコンポーネントのステータスは、 **セキュア消去ステータス**テーブルに表示されます。

- **アイドル** - プロセスは開始されていません。
- **開始** - プロセスは開始されました。
- **進行中** - 消去が進行中です。
- **成功** - プロセスは正常に完了しました。
- **エラー** – プロセスが完了しましたが、エラーが発生しています。
- **障害** - プロセスは失敗しました。

注記: セキュア消去ステータステーブル内の **iLO 設定**には、内蔵 NAND フラッシュと NVRAM の結果が含まれています。これらのコンポーネントのいずれかで消去の障害が発生すると、**iLO 設定**の全体的な障害になります。

セキュア消去ステータステーブル内の **BIOS 設定**には、UEFI 構成ストアと RTC（システム日付時刻）の結果が含まれます。これらのコンポーネントのいずれかで消去の障害が発生すると、**BIOS 設定**の全体的な障害になります。

One-button セキュア消去後にシステムを動作状態に戻す

One-button セキュア消去プロセスでシステムが消去された後に、次の手順を使用して操作状態に戻します。

手順

1. iLO ネットワーク設定を構成します。
2. Intelligent Provisioning リカバリイメージを使用して Intelligent Provisioning をインストールします。

   詳しくは、Intelligent Provisioning のユーザーガイドを参照してください。
3. オペレーティングシステムをインストールします。
4. オプション：iLO ライセンスをインストールします。
5. BIOS 設定および環境に適用される iLO 設定を構成します。
6. （オプション）システムリカバリセットを作成します。

One-button セキュア消去レポートの表示

前提条件

- サーバーで One-button セキュア消去プロセスが完了している。
- One-button セキュア消去プロセスの完了後、iLO が IP アドレスで構成されている。

手順

1. ナビゲーションツリーで**ライフサイクル管理**をクリックし、**廃棄**タブをクリックします。

   サーバーで One-button セキュア消去プロセスが完了したら、**最新の消去レポートの参照**ボタンが使用できます。

2. **最新の消去レポートの参照**をクリックします。

   セキュア消去レポートが表示されます。

3. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

4. （オプション） **One-button セキュア消去レポートを保存します**。

   Hewlett Packard Enterprise では、今後の参照用に消去レポートのコピーを保存することをお勧めします。

5. （オプション） **One-button セキュア消去レポートを削除します**。

   Hewlett Packard Enterprise では、サーバーを廃棄するか、または別の目的で使用する前に、消去レポートを削除することをお勧めします。

One-button セキュア消去レポートの詳細

- **サーバーシリアル番号** - サーバーのシリアル番号。
- **次によって開始** - One-button セキュア消去プロセスを開始したユーザー。

次の情報がデバイスごとにリストされます。

- **デバイスタイプ** - 消去されたデバイスタイプ。

  影響を受けるデバイスタイプについては、**One-button セキュア消去の完了後のシステムへの影響**を参照してください。

  iLO 5 2.30 以降がインストールされている Gen10 サーバーの場合、セキュア消去レポートには、**内蔵 NAND フラッシュ**と **NVRAM** のステータスのみが含まれます。Gen10 Plus サーバーでは、レポートに、サポートされているすべてのデバイスが含まれます。

- **位置** - サーバー内のデバイスの位置。
- **シリアル番号** - デバイスのシリアル番号。
- **ステータス** - デバイスの One-button セキュア消去ステータス。
- **消去タイプ** - 消去操作のタイプ。実行された操作について詳しくは、**One-button セキュア消去の FAQ** を参照してください。

- **開始時刻** - 特定のデバイスの One-button セキュア消去の開始時刻。
- **終了時間** - 特定のデバイスの One-button セキュア消去の終了時間。

CSV ファイルへの One-button セキュア消去レポートの保存

One-button セキュア消去機能を使用する場合、Hewlett Packard Enterprise では、今後の参照用に消去レポートのコピーを保存することをお勧めします。

前提条件

- サーバーで One-button セキュア消去プロセスが完了している。
- One-button セキュア消去プロセスの完了後、iLO が IP アドレスで構成されている。

手順

1. ナビゲーションツリーで**ライフサイクル管理**をクリックし、**廃棄**タブをクリックします。
2. 終了ボックスにある CSV をクリックします。

   CSV アウトプットウィンドウが表示されます。
3. **保存**をクリックし、ブラウザーのプロンプトに従ってファイルを保存するか、ファイルを開きます。

One-button セキュア消去レポートの削除

サーバーを廃棄または再利用する場合、iLO Web インターフェイスで One-button セキュア消去レポートを使用可能なままにしたくない場合があります。

Hewlett Packard Enterprise では、サーバーを廃棄するか、または別の目的で使用する前に、消去レポートを削除することをお勧めします。

前提条件

- iLO の設定を構成する権限
- サーバーで One-button セキュア消去プロセスが完了している。
- One-button セキュア消去プロセスの完了後、iLO が IP アドレスで構成されている。
- 後で参照するために One-button セキュア消去レポートのコピーが必要な場合に、レポートを保存している。

手順

1. ナビゲーションツリーで**ライフサイクル管理**をクリックし、**廃棄**タブをクリックします。

   サーバーで One-button セキュア消去プロセスが完了したら、**最新の消去レポートの参照**ボタンが使用できます。
2. **最新の消去レポートの参照**をクリックします。

   セキュア消去レポートが表示されます。
3. 🗑をクリックします。

   iLO によって、レポートファイルがセキュア消去され、すぐにリセットされます。

この時点までに作成されたイベントログ、IML、セキュリティログ、および構成設定が、工場出荷時のデフォルト設定にリセットされます。iLO は、起動時に自動リストア操作を試みる場合があります。詳しくは、**iLO のバックアップとリストア**を参照してください。

One-button セキュア消去の完了後のシステムへの影響

One-button セキュア消去機能は、システムおよびサポートされたコンポーネントを工場出荷時の状態に戻します。システムを使用するには、再度サーバーをプロビジョニングします。

- 影響を受けたストレージドライブおよび不揮発性メモリ上にあるすべてのデータは消去され、回復可能ではありません。

  すべての RAID 設定、ディスクパーティション、および OS インストールは削除されます。
- BIOS および iLO 5 設定は工場出荷時デフォルト設定にリセットされます。
  - iLO ネットワークやその他の設定は消去され、再構成が必要となります。
  - インストールされた iLO ライセンスは削除され、ライセンスのステータスは iLO Standard に戻ります。

    工場で iLO Advanced ライセンスが#0D1 オプションでプリインストールされている場合、One-button セキュア消去プロセスが終了するとライセンスは再インストールされます。このライセンスオプションについて詳しくは、HPE iLO ライセンスガイドを参照してください。
  - システムリカバリセットは削除され、再作成が必要となります。
  - iLO のユーザーアカウントが削除されます。プロセスが完了したら、デフォルトの工場出荷時の管理者アカウントとパスワードを使用してログインします。
  - Active Health System、インテグレーテッドマネジメントログ、セキュリティログ、および iLO イベントログは消去されます。
  - BIOS および SmartStorage Redfish API データの削除され、次回のブート時に再作成されます。
  - セキュアブートは無効になり、工場出荷時にインストールされている証明書を除き、登録された証明書は削除されます。
  - ブートオプションとユーザーが定義した BIOS のデフォルトは削除されます。
  - TPM または BIOS に格納されたパスワード、パスフレーズ、および暗号化キーは削除されます。
  - 日付、時刻、DST、およびタイムゾーンはリセットされます。
  - システムは、BIOS の最新リビジョンがフラッシュされた状態で起動されます。
- Intelligent Provisioning は起動せず、再インストールする必要があります。

工場出荷時の状態に戻されるハードウェアコンポーネント

次のコンポーネントは、One-button セキュア消去プロセス中に、工場出荷時の状態に戻されます。

- UEFI 構成ストア
- RTC（システムの日付と時刻）
- Trusted Platform Module。トラステッドプラットフォームモジュール
- NVRAM
  - BIOS 設定
  - iLO 構成設定

- iLO イベントログ
- インテグレーテッドマネジメントログ
- セキュリティログ

- 内部ポートに接続された HPE Smart アレイ SR コントローラーおよびドライブ。たとえば、3I:1:1 です。
- HPE Smart アレイ S100i ソフトウェア RAID
- ドライブデータ（ネイティブのサニタイズ方式をサポートするドライブの場合）
  - SATA、SAS ドライブ（SSD および HDD）
  - NVM Express
- 不揮発性メモリ
  - NVDIMM-N
  - インテル Optane DC 不揮発性メモリ
- 内蔵フラッシュ
  - iLO RESTful API データ
  - Active Health System
  - ファームウェアレポジトリ

工場出荷時の状態に戻されないハードウェアコンポーネント

次のコンポーネントは One-button セキュア消去プロセスの影響を受けません。

- USB ドライバー
- SD カード
- iLO 仮想メディア
- PCI コントローラー上の構成
- HPE Smart アレイ MR コントローラーおよび接続されたストレージ
- HPE Smart アレイ SR コントローラー上の外部ポートに接続されたドライブ、たとえば 1E:1:1 です。
- SAS HBA および接続されたドライブ
- ネイティブのサニタイズ方式をサポートしていない SATA、SAS、および NVM Express ドライブ。たとえば、Gen9 以前のサーバーで使用されるほとんどのドライブです。
- FCoE、iSCSI ストレージ
- GPGPU
- その他の FPGA、アクセラレータ、キーまたはストレージを持つオフロードエンジン

One-button セキュア消去の FAQ

One-button セキュア消去は USB デバイスおよび内部 SD カードをパージしますか。

いいえ。One-button セキュア消去は USB デバイスおよび内部 SD カードをパージしません。

HDD がパージ機能をサポートしていない場合、One-button セキュア消去はパージを試みますか。

いいえ。One-button セキュア消去はパージ機能をサポートしていないドライブをスキップします。

One-button セキュア消去は Smart アレイコントローラーをサポートしていますか。

One-button セキュア消去をサポートするのは、HPE Smart アレイ「SR」コントローラーのみです。

Smart アレイはパージをサポートしていないドライブを消去しますか。

Smart アレイは、パージ操作をサポートしていないドライブをワイプ（あるパターンで上書きする）できます。One-button セキュア消去では、Smart アレイでこのセキュリティ保護されていないワイプを実行する必要はありません。Intelligent Provisioning の「システムの消去およびリセット」機能を使用して、このようなドライブのデータをワイプします。

One-button セキュア消去はバッテリバックアップ式キャッシュを消去しますか。

詳しくは、次の表を参照してください。

One-button セキュア消去は消去コマンドをどのように処理しますか。

One-button セキュア消去がデータをパージまたは上書きする方法に関する情報については、次の表を参照してください。

One-button セキュア消去を起動するために必要な権限は何ですか。

One-button セキュア消去を起動するには、すべての iLO 権限が必要です。

One-button セキュア消去はシリアル番号とプロダクト ID を削除しますか。

いいえ、これらの項目は One-button セキュア消去によって消去されません。

この処理はどの程度かかりますか。

ハードウェアによって異なります。HDD のサニタイズは SSD よりも時間がかかります。

One-button セキュア消去はサポートされたドライブにどのように作用しますか。

デバイス	必要な操作	結果
NVRAM	3 パス書き込み : 0x5a、0xa5、0xff	すべてのバッテリバックアップ式 iLO SRAM メモリが上書きされます。
内蔵フラッシュ（NAND）	拡張 CSD レジスタの SECURE_REMOVAL_TYPE が物理メモリ消去に設定されている eMMC 5.1（JEDEC 84-B51）セキュア消去コマンド（デバイスでサポートされている場合）。	物理メモリ内のデータが消去されます。

表は続く

デバイス	必要な操作	結果
インテル Optane DC PMM	完全消去 + DIMM を上書き	暗号化キーが削除され、すべての物理メモリブロック内のデータ（ユーザーがアクセス可能なデータとスペアブロック内の両方のデータ）がゼロで上書きされます。すべての構成とメタデータを含む PCD 領域も上書きされます。
NVDIMM-N	JEDEC JESD245B 工場出荷時設定	保証情報を除く、すべての物理メモリブロック内のデータが消去されます。読み取り可能なすべてレジスターはデフォルト設定にリセットされます。
UEFI 構成ストア	3 パス：チップ消去（0xff）、0x00、チップ消去（0xff）	すべての物理セクターが上書きされます。
RTC	時刻を 01-01-2001 00:00:00 にリセット	日付、時刻、タイムゾーン、および DST がデフォルト設定にリセットされます。
TPM	TPM クリア + NV インデックスをクリア + プラットフォーム対象キーを削除 + PPS を変更 + EPS を変更	すべての不揮発性情報を含む、TPM のすべてのデータがクリアされます。

表は続く

デバイス	必要な操作	結果
HPE Smart アレイ SR コントローラー	論理ドライブを削除 + 構成のメタデータをクリア + 工場出荷時設定へのリセット + 物理ドライブのサニタイズ **注意** : One-button セキュア消去を開始する前に、HPE Smart Storage Administrator を介して、セキュリティリセット機能を手動で実行する必要があります（Smart アレイ Secure Encryption が有効化されていた場合）。	· セキュリティリセット機能は、リモートキー管理のためにキーマネージャーに保存されているドライブキーを削除します。コントローラーおよびドライブのすべてのシークレット、キー、およびパスワードがクリアされます。この操作は、キーマネージャー上のコントローラーキーを削除しません。 · すべてのアレイ構成、論理ドライブ、およびメタデータが削除されます。すべてのコントローラー設定は工場出荷時の設定にリセットされます。 · フラッシュバックアップはクリアされ、DRAM のライトバックキャッシュ内のデータは電源が取り外されたときに失われます。 接続されたすべてのドライブをサニタイズする必要があります。ドライブ上で必要な操作については、以下を参照してください。
HPE Smart アレイ S100i ソフトウェア RAID	SATA AHCI モードにリセット + 物理ドライブのサニタイズ	コントローラーは、デフォルトの SATA AHCI モードにリセットされます。すべてのアレイ構成、論理ドライブ、およびメタデータが削除されます。接続されたすべての SATA ドライブを以下のようにサニタイズする必要があります。
SATA HDD[1]	ATA SANITIZE with CRYPTO SCRAMBLE EXT（サポートされている場合）	CRYPTO SCRAMBLE EXT コマンドは、ユーザーデータに使用される内部暗号化キーを変更するため、ユーザーデータを元に戻すことはできません。
	シングルパスの ATA SANITIZE with OVERWRITE EXT オプション	ユーザーがアクセスできない物理セクターを含む、すべての物理セクターがゼロで上書きされます。キャッシュ内のすべての旧データもアクセスできなくなります。

表は続く

デバイス	必要な操作	結果
SATA SSD[1]	ATA SANITIZE with CRYPTO SCRAMBLE EXT（サポートされている場合）	CRYPTO SCRAMBLE EXT コマンドは、ユーザーデータに使用される内部暗号化キーを変更するため、ユーザーデータを元に戻すことはできません。
	シングルパスの ATA SANITIZE with BLOCK ERASE オプション	ユーザーがアクセスできない物理メモリブロックを含む、すべての物理メモリブロック内の旧データは元に戻すことができなくなります。キャッシュ内のすべての旧データもアクセスできなくなります。
SAS HDD[2]	シングルパスの SCSI SANITIZE with OVERWRITE EXT オプション	ユーザーがアクセスできない物理セクターを含む、すべての物理セクターが上書きされます。キャッシュ内のすべてのデータもサニタイズされます。
SAS SSD[2]	シングルパスの SCSI SANITIZE with BLOCK ERASE オプション	ユーザーがアクセスできない物理メモリブロックを含む、すべての物理メモリブロックがベンダー固有値に設定されます。キャッシュ内のすべてのデータもサニタイズされます。
NVM Express	NVM Express FORMAT with Secure Erase Setting（SES）= 2（サポートされている場合）	これは、暗号化キーを削除することで行われる暗号による消去です。
	シングルパスの NVM Express FORMAT with SES = 1	すべてのネームスペースに関連付けられているすべてのデータとメタデータは破棄されます。NVM サブシステムに存在するユーザーのすべての内容は消去されます。

[1] これらのドライブは、HPE Smart アレイ「SR」コントローラーまたはチップセット SATA コントローラーに接続される場合があります。

[2] HPE Smart アレイ「SR」コントローラーにのみに接続された SAS ドライブがサポートされます。

消去プロセスが失敗するサポート済みデバイス、およびサポートされていないデバイスの消去は安全ではありません。これらのデバイスに機密データが含まれている可能性があります。消去されないデバイスを分離し、他の方法を使用してデータを削除するか、所属する組織のセキュリティポリシーに従ってデバイスを安全に破棄します。

iLO のバックアップとリストア

自動でのバックアップとリストア

iLO の初期化プロセスが終了すると、バッテリ駆動の SRAM メモリデバイスに保存されている構成情報が不揮発性フラッシュメモリ（NAND）にバックアップされます。

SRAM が消去された、またはデータ破壊が検出された場合、iLO はバックアップファイルから構成情報をリストアしようとします。自動リストア操作は IML に記録されます。

システムメンテナンススイッチを使用して iLO セキュリティを無効にすると、SRAM データは自動的にリストアされません。

自動でのバックアップとリストアのプロセスによって作成されたバックアップファイルには、ユーザーはアクセスできません。手動リストア操作を実行するために使用することはできません。

手動でのバックアップとリストア

iLO では、バッテリ駆動の SRAM メモリデバイスに保存された構成情報の手動リストアがサポートされています。この機能は、バックアップされたシステムと同じハードウェア構成を持つシステムで使用するためのものです。構成を複製して別の iLO システムに適用するものではありません。

Hewlett Packard Enterprise では、リストア操作を実行する理由が生じることは想定されていません。ただし、構成のバックアップを取っておくことで、通常の動作環境にすばやく戻ることができる場合があります。

あらゆるコンピューターシステムと同様に、データをバックアップして障害の影響を最小限に抑えることをお勧めします。Hewlett Packard Enterprise は、iLO ファームウェアをアップデートするたびにバックアップを実行することをお勧めします。

詳しくは、**iLO Management Backup and Restore** のビデオをご覧ください。

バックアップとリストアのための iLO ファームウェア要件

- iLO 5 ファームウェアバージョン 2.10 以降では、iLO ファームウェアのバージョンが同じシステムや異なるシステムでバックアップおよびリストアのタスクが実行される、バックアップおよびリストア操作がサポートされています。
- 2.10 より前の iLO 5 ファームウェアバージョンでは、iLO ファームウェアのバージョンが同じシステムでバックアップおよびリストアのタスクが実行される、バックアップおよびリストア操作がサポートされています。

バックアップとリストアの操作中にリストアされる情報

iLO 構成には、電源、ネットワーク、セキュリティ、ライセンスキー、ユーザーデータベースなど、多くのカテゴリが含まれます。ほとんどの構成情報は、バッテリ駆動の SRAM メモリデバイスに保存されており、バックアップとリストアが可能です。

注記: 環境変数をリストアしたときは、リストアした設定を有効にするためにサーバーのリセットが必要です。

たとえば、**パフォーマンス**設定はリストアされてもサーバーリセットが完了するまで有効になりません。

バックアップとリストアの操作中にリストアされない情報

一部の情報は、バックアップとリストアの操作中にリストアするのに適していません。リストアできない情報は iLO 構成には含まれません。その情報は iLO またはサーバーのシステム状態に関連します。

以下の情報は、バックアップまたはリストアされません。

セキュリティ状態

リストア操作によって iLO のセキュリティ状態を変更することを許可すると、セキュリティの原則が破られ、セキュリティの適用が無効になります。

インテグレーテッドマネジメントログ

バックアップから、リストアが必要になったイベントまでに発生したイベントの情報を保持するため、この情報はリストアされません。

iLO イベントログ

バックアップから、リストアが必要になったイベントまでに発生したイベントの情報を保持するため、この情報はリストアされません。

セキュリティログ

バックアップから、リストアが必要になったイベントまでに発生したセキュリティイベントの情報を保持するため、この情報はリストアされません。

Active Health System データ

バックアップおよびリストアプロセス中に記録された情報を保持するため、この情報はリストアされません。

サーバーの状態情報

- サーバーの電源状態（オン/オフ）
- サーバーの UID LED の状態
- iLO およびサーバーのクロック設定

iLO 構成を手動でリストアする理由

次のような状況では iLO 構成のリストアが必要になる場合があります。

バッテリの障害または取り外し

さまざまな構成パラメーターがバッテリ駆動の SRAM に保存されています。まれですが、バッテリ障害が発生する場合があります。状況によっては、バッテリの取り外しと交換が必要になる場合があります。構成情報の消失を避けるために、バッテリの交換後にバックアップファイルから iLO 構成をリストアします。

デフォルト設定へのリセット

場合によっては、iLO を工場出荷時のデフォルト設定にリセットし、iLO 以外の設定を消去することが必要になることがあります。iLO を工場出荷時の設定にリセットすると、iLO の構成は消去されます。iLO 構成をすばやく復旧するには、工場出荷時設定へのリセットが完了した後、バックアップファイルから構成をリストアします。

構成の偶発的または不適切な変更

場合によって、iLO 構成が不適切に変更され、重要な設定が消失することがあります。iLO を工場出荷時のデフォルト設定に設定したり、ユーザーアカウントを削除したりした場合にこのような状況が発生することがあります。元の構成を回復するには、バックアップファイルから構成をリストアします。

システムボードの交換

ハードウェアの問題に対処するためにシステムボードの交換が必要な場合、この機能を使用して iLO 構成を元のシステムボードから新しいシステムボードに転送できます。

ライセンスキーの喪失

ライセンスキーが誤って置き換えられた、または iLO を工場出荷時のデフォルトの設定にリセットした場合に、インストールするキーがわからないときは、ライセンスキーと他の構成設定をバックアップファイルからリストアできます。

iLO 構成のバックアップ

前提条件

- iLO の設定を構成する権限
- iLO は、本番環境または高度なセキュリティのセキュリティ状態を使用するように構成されています。iLO が高いセキュリティ状態を使用するように構成されている場合、構成のバックアップとリストアはサポートされていません。

手順

1. ナビゲーションツリーで**ライフサイクル管理**をクリックし、**バックアップとリストア**をクリックします。
2. **バックアップ**をクリックします。
3. （オプション）バックアップファイルをパスワード保護するには、**バックアップファイルパスワード**ボックスにパスワードを入力します。

   パスワードは最大 32 文字です。
4. **ダウンロード**をクリックします。

   ファイルがダウンロードされ、この動作がイベントログに記録されます。

   ファイル名は、次の形式を使用します。`<サーバーシリアル番号>_<YYYYMMDD>_<HHMM>.bak`.

iLO 構成のリストア

前提条件

- iLO の設定を構成する権限
- ユーザーアカウント管理権限
- バックアップファイルが存在する。
- 以前に iLO を工場出荷時のデフォルト設定にリセットした場合は、デフォルトの iLO アカウント認証情報を使用できる。
- 使用する iLO セキュリティ状態が構成されている。

  本番環境または高セキュリティよりも高いセキュリティ状態を構成すると、iLO は工場出荷時のデフォルト設定にリセットされます。これらのセキュリティ状態を構成せずにリストアを実行した場合、リストアされた情報はセキュリティ状態のアップデート時に削除されます。

手順

1. ナビゲーションツリーで**ライフサイクル管理**をクリックし、**バックアップとリストア**をクリックします。
2. **リストア**をクリックします。

3. 使用しているブラウザーに応じて**参照**または**ファイルを選択**をクリックし、バックアップファイルに移動します。
4. バックアップファイルがパスワードで保護されている場合、パスワードを入力します。
5. **アップロードおよびリストア**をクリックします。

   iLO が要求を確認するように求めます。
6. **リストア**をクリックします。
   iLO が再起動され、ブラウザー接続が閉じます。接続が再確立されるまでに、数分かかることがあります。

詳しくは

iLO のバックアップとリストア
iLO 暗号化設定
iLO のデフォルトの DNS 名とユーザーアカウント

システムボード交換後の iLO 構成のリストア

システムボードを交換する場合、交換前のシステムボードから構成をリストアできます。

前提条件

- iLO の設定を構成する権限
- ユーザーアカウント管理権限
- バックアップファイルが存在する。
- 以前に iLO を工場出荷時のデフォルト設定にリセットした場合は、デフォルトの iLO アカウント認証情報を使用できる。
- 使用する iLO セキュリティ状態が構成されている。

  本番環境または高セキュリティよりも高いセキュリティ状態を構成すると、iLO は工場出荷時のデフォルト設定にリセットされます。これらのセキュリティ状態を構成せずにリストアを実行した場合、リストアされた情報はセキュリティ状態のアップデート時に削除されます。

手順

1. システムボードを交換し、ハードウェアコンポーネントを古いシステムボードから新しいシステムボードに転送します。
2. システムの電源を入れ、すべてのコンポーネントが正常に動作していることを確認します。
3. 新しいシステムボードのデフォルトのユーザー認証情報を使用して iLO にログインします。
4. **バックアップファイルから構成をリストアします。**

詳しくは

iLO のバックアップとリストア
iLO 暗号化設定
iLO のデフォルトの DNS 名とユーザーアカウント

エンクロージャー、フレーム、およびシャーシの操作

Onboard Administrator

OA は、エンクロージャー管理プロセッサー、サブシステム、ファームウェアベースです。
HPE BladeSystem と、エンクロージャー内部のすべての管理対象デバイスをサポートします。

アクティブ Onboard Administrator ページでは、iLO プロセッサーがあるエンクロージャーのプライマリ OA に関する全般的な情報が提供されます。エンクロージャー情報の表示、OA Web インターフェイスの起動、サーバーまたはエンクロージャー UID LED の切り替えができます。このページは、エンクロージャーが存在する場合のみ表示されます。

OA 情報の表示

手順

1. ナビゲーションツリーで **BL c-Class** をクリックします。
2. （オプション）サーバーの詳細を表示するには、エンクロージャー図のサーバーの上でカーソルを動かします。

   表示される詳細は、ヘルスステータス、ホスト名、モデル、および UID ステータスです。
3. （オプション）エンクロージャーのヘルスステータスまたは UID LED ステータスを表示するには、エンクロージャー図のエンクロージャーアイコン上でカーソルを動かします。

エンクロージャーおよびサーバーの詳細

- **エンクロージャーヘルス** - OA から報告されるアクティブな OA のヘルス。

  不明という値は、OA のヘルス情報が iLO に報告されていないことを示します。

  このステータスはエンクロージャー図にも表示されます。
- **エンクロージャー UID ライト** - エンクロージャーの UID LED の状態。UID LED を使用すると、エンクロージャーを特定して確認できます。

  このステータスはエンクロージャー図にも表示されます。
- **サーバー位置** - 現在の iLO セッションをホスティングしているブレードの位置（エンクロージャーベイ）。
- **割り当てられた電力** - サーバーの電源が入っているときのサーバーの最大割り当て電力。
- **エンクロージャーシリアル番号** - エンクロージャーのシリアル番号。
- **エンクロージャーユニーク ID（UUID）** - エンクロージャーの UUID。
- **エンクロージャー名** - アクティブな OA が管理しているエンクロージャー。この値は、OA を通じて変更できます。

OA アドレス

- **MAC アドレス** - アクティブな OA の MAC アドレス。
- **IPv4**、**IPv6 SLAAC**、**静的 IPv6**、および **IPv6 DHCP** - OA の Web インターフェイスへのアクセスに使用できるアドレス。使用できるアドレスの種類は、OA の構成によって異なります。

OA Web インターフェイスの起動

手順

1. ナビゲーションツリーで **BL c-Class** をクリックします。
2. **Onboard Administrator アドレス**セクションのリンクをクリックします。

   構成に応じて、以下のオプションを利用できる可能性があります。

   - **IPv4**
   - **IPv6 SLAAC**
   - **IPv6（静的）**
   - **IPv6（DHCP）**

   OA Web インターフェイスが新しいブラウザーウィンドウで起動します。

サーバーまたはエンクロージャー UID LED の切り替え

手順

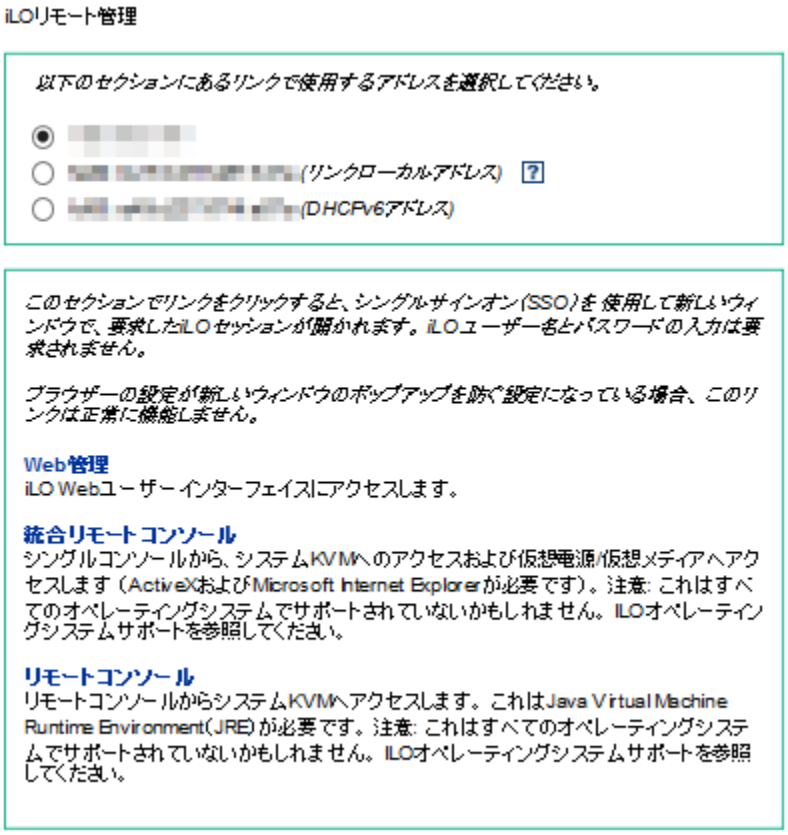
1. ナビゲーションツリーで **BL c-Class** をクリックします。
2. エンクロージャーまたはサーバー UID LED の状態を変更するには、エンクロージャー図にある⊙をクリックします。

   iLO がステータス変更を検知すると、**アクティブ Onboard Administrator** ページの UID LED ステータス値は自動的にアップデートされます。ステータスをすぐにアップデートするには、ページを更新します。

iLO オプション

OA の **iLO - デバイスベイ <XX>**ページには、以下のリンクがあります。

- **Web 管理** - iLO の Web インターフェイスを起動します。
- **統合リモートコンソール** - .NET IRC を起動します。
- **リモートコンソール** - Java IRC を起動します。



このページのリンクをクリックすると、SSO を使用して新しいウィンドウに要求した iLO セッションが開きます。この場合、iLO ユーザー名やパスワードは不要です。ブラウザーの設定によって新しいウィンドウを表示できない場合は、これらのリンクは正常に動作しません。

フレーム情報の表示

フレーム情報ページには、iLO プロセッサーを搭載した Synergy コンピュートモジュールを格納するフレームに関する情報が表示されます。

手順

1. ナビゲーションツリーで **Synergy フレーム**をクリックします。
2. （オプション）コンピュートモジュール詳細を表示するには、フレーム図のコンピュートモジュール上でカーソルを動かします。

   コンピュートモジュールについての以下の詳細を表示できます：ヘルスステータス、ホスト名、モデル、および UID ステータス。
3. （オプション）フレームのヘルスステータスまたは UID LED ステータスを表示するには、フレーム図のフレームアイコン上でカーソルを動かします。

フレームの詳細

- **フレームヘルス** - フレームのヘルスステータス。

このステータスはフレーム図にも表示されます。

- **フレーム UID ライト** - フレームの UID LED の状態。UID LED を使用すると、フレームを特定して確認できます。

  このステータスはフレーム図にも表示されます。

- **サーバー位置** - フレーム内のコンピュートモジュールのベイ番号。
- **割り当てられた電力** - コンピュートモジュールの電源が入っているときのコンピュートモジュールの最大割り当て電力。
- **フレームシリアル番号** - フレームのシリアル番号。
- **フレームユニーク ID（UUID）** - フレームの UUID。

フレームまたはコンピュートモジュール UID の切り替え

手順

1. ナビゲーションツリーで **Synergy フレーム**をクリックします。
2. フレームまたはコンピュートモジュール UID LED の状態を変更するには、フレーム図にある⊙をクリックします。

   iLO がステータス変更を検知すると、**フレーム情報**ページの UID LED ステータス値は自動的にアップデートされます。ステータスをすぐにアップデートするには、ページを更新します。

シャーシ情報の表示

手順

1. ナビゲーションツリーで**シャーシ情報**をクリックします。
2. （オプション）詳細をさらに表示するには、電源装置または Smart Storage Energy Pack のリストをクリックします。

シャーシ情報

- **ノード番号** - サーバーノード番号。
- **シャーシ名** - サーバーノードを内蔵するシャーシの名前。
- **シャーシシリアル番号** - サーバーノードを内蔵するシャーシのシリアル番号。
- **シャーシ部品番号** - サーバーノードを内蔵するシャーシの部品番号。
- **シャーシの電源（ワット）** - シャーシによって使用される電力。

  この値は 10 秒ごとにアップデートされます。最新の値を表示するには、ブラウザーウィンドウを更新します。

- **ノード電源（ワット）** - シャーシ内の現在のノードによって使用される電力。

  この値には、シャーシ内の他のノードやデバイスは含まれません。
  この値は 15 秒ごとにアップデートされます。最新の値を表示するには、ブラウザーウィンドウを更新します。

電源装置のリスト

シャーシ情報ページには、シャーシ内の電源装置に関する以下の詳細が表示されます。

このページの一部の値について情報を提供しない電源装置もあります。ある値について電源装置からの情報がない場合は、**N/A** が表示されます。

ベイ

シャーシの電源装置のベイ番号。

設置

電源装置が搭載されているかどうかを示します。表示される値は、**OK** および**なし**です。

ステータス

電源装置のステータス。表示される値は、ステータスアイコン（**OK**、**劣化**、**障害**、または**その他**）、および詳細情報を提供するテキストを示します。値には、以下のものがあります。

- **不明**
- **良好、使用中**
- **良好、スタンバイ**
- **一般障害**
- **過電圧障害**
- **過電流障害**
- **過熱障害**
- **入力電圧消失**
- **ファン障害**
- **高入力 A/C 警告**
- **低入力 A/C 警告**
- **高出力警告**
- **低出力警告**
- **入口温度警告**
- **内部温度警告**
- **高電圧補助電源警告**
- **低電圧補助電源警告**
- **電源装置の不一致**

容量

電源装置の容量（W）。

ファームウェア

電源装置のファームウェアバージョン。

各電源装置の詳細

電源装置セクションでリストをクリックすると、次の情報が表示されます。

設置

電源装置が搭載されているかどうかを示します。表示される値は、**OK** および**なし**です。

ステータス

電源装置のステータス。表示される値は、ステータスアイコン（**OK**、**劣化**、**障害**、または**その他**）、および詳細情報を提供するテキストを示します。値には、以下のものがあります。

- **不明**
- **良好、使用中**
- **良好、スタンバイ**
- **一般障害**
- **過電圧障害**
- **過電流障害**
- **過熱障害**
- **入力電圧消失**
- **ファン障害**
- **高入力 A/C 警告**
- **低入力 A/C 警告**
- **高出力警告**
- **低出力警告**
- **入口温度警告**
- **内部温度警告**
- **高電圧補助電源警告**
- **低電圧補助電源警告**
- **電源装置の不一致**

容量

電源装置の容量（W）。

ファームウェア

電源装置のファームウェアバージョン。

PDS

搭載された電源装置が Power Discovery Service（電力情報検出機能）用に有効になっているかどうか。

Power Discovery Service は、iPDU テクノロジーの拡張機能です。シャーシの電源装置が iPDU に接続されている場合、**インテリジェントパワーディストリビューションユニット**セクションに追加情報が表示されます。

ホットプラグ

電源装置ベイがシャーシの電源が入った状態での電源装置の交換をサポートするかどうか。値が**はい**で、電源装置が冗長化されている場合は、シャーシの電源がオンのときに電源装置を取り外したり、交換したりすることができます。

モデル

電源装置のモデル番号。

スペア

スペア電源装置の部品番号。

シリアル番号

電源装置のシリアル番号。

インテリジェント PDU の詳細

Intelligent Power Distribution ユニットセクションは、シャーシの電源装置が iPDU に接続されている場合にのみ表示されます。

iLO をリセットしてから、または iPDU を接続してから、iLO Web インターフェイスに **Intelligent Power Distribution ユニット**テーブルが表示されるまで約 2 分かかります。この遅延は、iPDU 検出プロセスによるものです。

テーブルには以下の情報が表示されます。

- **ID** - 電源装置のベイ番号。
- **製品番号** - iPDU の製品番号。
- **シリアル番号** - iPDU のシリアル番号。
- **IP アドレス** - iPDU の IP アドレス。
- **SSL ポート** - iPDU の SSL ポート。
- **MAC アドレス** - iPDU ネットワークポートの MAC アドレス。各 iPDU が固有の MAC アドレスを持っているため、この値を参照すると接続されている各 iPDU を特定できます。

Smart Storage Energy Pack のリスト

シャーシ情報ページには、Smart Storage Energy Pack をサポートするサーバーに関する以下の情報が表示されます。

索引

Energy Pack 索引番号です。

装着

Energy Pack の装着状態。表示される値は、**OK** および**未装着**です。

ステータス

Energy Pack のステータス。表示される値は、**OK**、**劣化**、**障害**、または**その他**です。

タイプ

Energy Pack のタイプ。

ファームウェア

インストールされている Energy Pack ファームウェアのバージョン。

個々の Energy Pack の詳細

Smart Storage Energy Pack セクションでリストをクリックすると、次の情報が表示されます。

設置

Energy Pack の装着状態。指定できる値は、**OK** および**未インストール**です。

ステータス

Energy Pack のステータス。指定できる値は、**OK**、**劣化**、**障害**、または**その他**です。

タイプ

Energy Pack のタイプ。

ファームウェア

インストールされている Energy Pack ファームウェアのバージョン。

モデル

モデル番号。

スペア

スペア Energy Pack の部品番号。

シリアル番号

Energy Pack のシリアル番号。

パワーレギュレーション

パワーレギュレーションページでは、Apollo シャーシとこれに含まれるサーバーのパワーレギュレーション設定を構成できます。

電力レギュレーターモード設定の構成

前提条件

- iLO の設定を構成する権限
- **ユーザー構成可能モード**オプションを有効にするユーザーの場合のみ：このモードをサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- シャーシが、APM 消費電力上限モードを使用するように構成されていないこと。シャーシがこのモードに設定されている場合は、この手順を実行する前に APM を別のモードに変更してください。

手順

1. ナビゲーションツリーで**シャーシ情報**をクリックし、**パワーレギュレーション**タブをクリックします。
2. 以下のパワーレギュレーターモードからいずれかを選択します。
   - **スロットル付き AC 冗長化モード**
   - **ユーザー構成可能モード**
   - **電源フィード保護モード**

   APM 消費電力上限モードを構成するには、APM ソフトウェアを使用します。
3. **適用**をクリックします。

   iLO が、電力レギュレーターモード設定が変更されたことを通知します。

次のイベントが iLO イベントログに追加されます。

`Chassis power zone configuration updated by user name.`（シャーシの電力ゾーン構成がユーザー名でアップデートされました。）

電力レギュレーターモードオプション

- **スロットル調整付き AC 冗長化モード** - このモードは、シャーシから取り出した電力がアクティブな電源装置によってサポートされた負荷を超えようとした場合、消費電力上限機能により最大数のノードを実行できます。このモードでは、1 つまたは複数の電源装置で予期しない電力損失が起こっても、（パフォーマンスの低下なしで）システムの存続が見込まれます。
- **ユーザー構成可能モード** - ユーザーは、事前定義された範囲から有効な消費電力上限値を指定できます。上限を最小値より小さくしたり、最大値より大きくしたりすることはできません。上限には、すべてのサーバーのノード、ファン、およびドライブが含まれます。

  このオプションにはライセンスが必要です。このオプションをサポートするライセンスがインストールされていない場合、このオプションは表示されません。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。
- **APM 消費電力上限モード** - ユーザーは APM と組み合わせることで、ラック全体の最大電力容量を指定できます。APM では、使用可能な電力が指定された場合にパフォーマンスが最大になるように、ラック内の適用可能なシャーシに電力が動的に割り当てられます。

  このモードを構成できるのは、APM を使用した場合のみです。iLO でこのモードを構成することはできません。
- **電力フィード保護モード** - このモードを A+B 電力供給構成とともに使用すると、システムが完全に調整されます。この動作により、電力供給の損失が発生した場合に、ノードが完全な停止状態になります。完全な調整は、電力供給がオンラインに戻るまで継続します。このモードでは、半数の電源装置への電力供給全体で予期しない損失が起こっても、システムの存続が見込まれます。

グローバルパワーレギュレーション設定の構成

前提条件

- iLO の設定を構成する権限
- 電力較正アクションが進行中でないこと。
- シャーシが、APM 消費電力上限モードを使用するように構成されていないこと。シャーシがこのモードに設定されている場合は、この手順を実行する前に APM を別のモードに変更してください。

手順

1. ナビゲーションツリーで**シャーシ情報**をクリックし、**パワーレギュレーション**タブをクリックします。
2. 以下のオプションを有効または無効にします。
   - **パワーレギュレーションを有効化**
   - **EEPROM 保存/リストアを有効化**
3. **適用**をクリックします。

   グローバル設定が変更されたことが iLO によって通知されます。

次のイベントが iLO イベントログに追加されます。

`Chassis Power Regulation setting changed by user name.`（シャーシのパワーレギュレーション設定がユーザー名によって変更されました。）

グローバル設定オプション

- **パワーレギュレーション有効** - パワーレギュレーション機能が有効です。
- **EEPROM 保存/リストア有効** - 電源情報は EEPROM に保存され、リストアすることができます。

ゾーンマッピングの構成

ゾーンマッピングセクションで、シャーシ全体でグループ化されるか、既存のユーザー定義ゾーンでグループ化されるように各ノードを設定します。

iLO の Web インターフェイスを使用してゾーンを作成することはできません。

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

  この機能をサポートするライセンスがインストールされていない場合、この機能は iLO Web インターフェイスに表示されません。
- **パワーレギュレーションを有効にする**オプションが無効になっていること。
- 電力較正アクションが進行中でないこと。
- シャーシが、APM 消費電力上限モードを使用するように構成されていないこと。シャーシがこのモードに設定されている場合は、この手順を実行する前に APM を別のモードに変更してください。

手順

1. ナビゲーションツリーで**シャーシ情報**をクリックし、**パワーレギュレーション**タブをクリックします。
2. ノードごとに、**シャーシ**または***ゾーンの数値をゾーン***メニューで選択します。
3. **適用**をクリックします。

   次のイベントが iLO イベントログに追加されます。

   `Chassis power zone configuration updated by user name.`（シャーシの電力ゾーン構成がユーザー名でアップデートされました。）
4. （オプション）**ゾーンマッピング**セクションでデータの更新方法を選択します。
   - **スロットル**および**警告ステータス**を即座に更新するには、↻をクリックします。
   - **スロットル**および**警告ステータス**の値の更新を自動的に開始するには、更新アイコンの横にある▷をクリックします。**スロットル**および**警告ステータス**の値は、停止アイコン□をクリックするか、別のページに移動するまで、ページは自動的に更新されます。

詳しくは

グローバルパワーレギュレーション設定の構成

ゾーンマッピングの詳細

シャーシ内の各ノードに対して、以下の詳細が表示されます。

- **ノード** - ノード番号。
- **スロットル** - CPU 周波数上の電力管理設定の影響。

  以下に例を示します。

  - 0%は、CPU のスロットル調整が実行されていないこと、また最大周波数で稼働していることを意味します。
  - 50%は、CPU のスロットル調整が実行されていること、また最大周波数の 50%で稼働していることを意味します。
  - 100%は、CPU のスロットル調整が実行されていること、またサポートされる最小周波数で稼働していることを意味します。

- **警告ステータス** - ノードの警告ステータス。CPU のスロットル調整が 50%以上で 5 分間実行されている場合に、警告の状態が発生します。
- **ゾーン** - ゾーンの割当（シャーシ、またはユーザー定義のゾーン）。

ゾーンの優先度設定の構成

ゾーンを構成すると、各ゾーンのパワーレギュレーションの優先順位を設定できます。消費電力上限が設定されている場合、優先順位が高いゾーンには、優先順位が低い設定があるゾーンよりも多くの電力が割り当てられます。

設定可能な優先順位の値は 1～5 です。最も優先順位の高いものは 1、最も優先順位の低いものは 5 です。デフォルトでは、各ゾーンは、優先順位 5 に設定されます。同じ優先順位を複数のゾーンに設定できます。

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

  この機能をサポートするライセンスがインストールされていない場合、この機能は iLO Web インターフェイスに表示されません。
- ゾーンが構成されていること。
- **パワーレギュレーションを有効にする**オプションが無効になっていること。
- 電力較正アクションが進行中でないこと。
- シャーシが、APM 消費電力上限モードを使用するように構成されていないこと。シャーシがこのモードに設定されている場合は、この手順を実行する前に APM を別のモードに変更してください。

手順

1. ナビゲーションツリーで**シャーシ情報**をクリックし、**パワーレギュレーション**タブをクリックします。
2. **ゾーンマッピング**セクションで、**優先度設定**をクリックします。

3. 各ゾーンまたは個々のノードの優先度の値（1～5）を入力します。
4. **適用**をクリックします。

   次のイベントが iLO イベントログに追加されます。

   `Chassis power zone configuration updated by` *`user name`*.（シャーシの電力ゾーン構成がユーザー名でアップデートされました。）

詳しくは

グローバルパワーレギュレーション設定の構成

消費電力上限値設定の構成

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

  この機能をサポートするライセンスがインストールされていない場合、この機能は iLO Web インターフェイスに表示されません。
- パワーレギュレーションが有効で、iLO が、パワーレギュレーターの**ユーザー構成可能モード**を使用するように構成されていること。

手順

1. ナビゲーションツリーで**シャーシ情報**をクリックし、**パワーレギュレーション**タブをクリックします。
2. **消費電力上限値設定**をクリックします。

   このオプションは、新しいゾーンを構成するまでは利用できません。
3. 以下のいずれかを実行します。
   - シャーシまたはゾーンの消費電力上限を追加または変更するには、**上限**値をワット単位で入力します。

     ゾーンの消費電力上限の合計は、構成済みのシャーシの消費電力上限を超えることはできません。消費電力上限値は、シャーシやゾーンの最小上限値および最大上限値との間で設定する必要があります。

     最小上限列および**最大上限**列に**不明**と表示された場合は、電力較正が構成されていないことを意味します。電力使用量の要件がわかっている場合は、電力較正を構成することなく消費電力上限を設定できます。
   - シャーシまたはゾーンの消費電力上限を解除するには、既存の値を削除します。
4. **適用**をクリックします。

   構成済みの消費電力上限が変更されたことが iLO によって通知されます。

   最小消費電力上限値および最大消費電力上限値が不明の場合は、消費電力上限が有効にならない可能性があることが iLO によって通知されます。

   パワーレギュレーションが有効ではなく、**ユーザー構成可能なモード**に設定されている場合は、iLO によって、構成がアップデートされるまで消費電力上限値設定がアップデートされないことが通知されます。

消費電力上限を追加したか削除したかに関係なく、iLO イベントログには次のイベントのいずれかが記録されます。

`Power Cap for scope set to value (watts) by user name.`（範囲の消費電力上限のワット単位の値がユーザー名で設定されました。）

`Power Cap for scope disabled by user name.`（範囲の消費電力上限がユーザー名で無効にされました。）

詳しくは

電力レギュレーターモード設定の構成

消費電力上限の詳細

- **スコープ** - スコープ（シャーシまたはユーザー定義のゾーン）。
- **最小上限** - 構成可能な最小電力量（ワット）。**不明**という値は、電力較正が構成されていないことを意味します。
- **最大上限** - 電源定格（ワット）。**不明**という値は、電力較正が構成されていないことを意味します。
- **上限** - 構成されている消費電力上限（ワット）。
- **実際の上限** - 実際の消費電力上限。この値は、構成されている消費電力上限未満の場合があります。

電力較正の構成

前提条件

- iLO の設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Web サイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

  この機能をサポートするライセンスがインストールされていない場合、この機能は iLO Web インターフェイスに表示されません。
- パワーレギュレーションが有効になっていないこと。
- シャーシが、APM 消費電力上限モードを使用するように構成されていないこと。シャーシがこのモードに設定されている場合は、この手順を実行する前に APM を別のモードに変更してください。

手順

1. ナビゲーションツリーで**シャーシ情報**をクリックし、**パワーレギュレーション**タブをクリックします。
2. **電力較正**をクリックします。
3. **較正の構成**オプションを設定します。
   - **スコープ**
   - **アクション**
   - **秒**
   - **保存**
4. **実行**をクリックします。

次のイベントが iLO イベントログに追加されます。

`Chassis power zone configuration updated by user name.`（シャーシの電力ゾーン構成がユーザー名でアップデートされました。）

詳しくは

グローバルパワーレギュレーション設定の構成

電力較正の構成オプション

- **スコープ**—較正設定が適用される範囲。
  - **AllZone**—Chassis Manager は、すべてのゾーンの較正を行います。消費電力上限値の最小値と最大値が計算され、**消費電力上限値設定**テーブルに表示されます。
  - **シャーシ**—Chassis Manager は、シャーシ全体の較正を行います。スロットルピーク電力データ（0～100%）が計算され、**較正データ**グラフに表示されます。
  - ***ゾーン番号***—Chassis Manager は、選択されたゾーンの較正を行います。スロットルピーク電力データ（0～100%）が計算され、**較正データ**グラフに表示されます。
- **操作**—シャーシまたは指定されたゾーンの較正の起動または停止を選択します。

  進行中の場合は、較正を停止できます。
- **秒**—較正データに含める秒数。60～3600 秒の範囲で値を入力します。

  デフォルト値は 60 です。
- **保存**—この設定を有効または無効にして、構成設定を保存するかどうを制御します。

較正データの表示

手順

1. ナビゲーションツリーで**シャーシ情報**をクリックし、**パワーレギュレーション**タブをクリックします。
2. 較正を設定します。
3. **ロード**をクリックします。

較正の詳細

較正グラフは、選択した期間における電力使用量（ワット）と選択した較正スコープに使用された利用可能な電力の割合を示します。

- **スコープ** - 較正設定を構成したときに選択されたスコープ。
- **ステータス** - iLO が有効な電力データを受信したかどうか。表示される値は、**OK** および**無効**です。
- **開始時間** - データサンプルの開始時刻。
- **終了時間** - データサンプルの終了時刻。

ドライブベイのマッピング

HPE Apollo r2800 Gen10 シャーシを備えた HPE Apollo 2000 Gen10 システム（SAS エキスパンダーバックプレーンおよび SAS エキスパンダードーターボードを含む）は、24 台のスモールフォームファクタ

（2.5 型）ドライブをサポートしています。2.5 型ドライブベイは特定のサーバーノードに割り当てることができます。

デフォルト構成では、24 台の 2.5 型ドライブベイをシャーシ内のサーバーホストポートの数で割っています。4 台の 1U サーバーで構成されている場合は、6 台のドライブベイが 4 つのサーバースロットにそれぞれ割り当てられている形がデフォルトドライブベイ構成になります。2 台の 2U サーバーで構成されている場合は、12 台のドライブベイが 2 つのサーバースロットにそれぞれ割り当てられている形がデフォルトドライブベイ構成になります。

ドライブベイのマッピング情報の表示

前提条件

- iLO ファームウェア 1.20 以降
- ストレージエンクロージャーのプロセッサーファームウェア 1.00 以降
- シャーシファームウェア 1.2.10 以降

手順

ナビゲーションツリーで**シャーシ情報**をクリックし、**ドライブベイのマッピング**タブをクリックします。

バックプレーンの詳細

SEP ファームウェアバージョン

ストレージエンクロージャー プロセッサーバックプレーンのファームウェアバージョン。

SEP WWID

ストレージエンクロージャー プロセッサーの World Wide 識別子。

システム構成タイプ

構成タイプ 現時点で、iLO ではタイプ 1 （1 つのストレージエンクロージャー プロセッサー（複数のベイを搭載）を複数のノードで共有）をサポートしています。

トータルベイ

ストレージエンクロージャー プロセッサーに取り付けられているストレージベイの合計数。

開始ベイ番号

ストレージベイ範囲の開始番号。

終了ベイ番号

ストレージベイ範囲の終了番号。

ホストポートトポロジの詳細

ホストポートトポロジセクションには、ノード番号と各サーバーホストポートに関連付けられている SAS Controller が表示されます。

ドライブベイのマッピングの詳細

ドライブベイのマッピングセクションには、ホストポートに割り当てられていない場合でも、マッピングされている場合でも、すべてのドライブベイが表示されます。

- 緑色のアイコンは、ドライブベイがホストポートにマップされていることを示します。
- 赤色のアイコンは、ドライブベイの割り当てが保留中のステータスであることを示します。

シャーシがリセットされるか、すべてのシャーシノードの電源が少なくとも 5 秒間オフになると、変更が有効になります。

たとえば、**ドライブベイ 1** で、ポート 1 に緑色のアイコン、ポート 2 に赤色のアイコンが表示される場合があります。これらのアイコンは、シャーシがリセットされるか、シャーシノードの電源が少なくとも 5 秒間オフになると、**ドライブベイ 1** がポート 2 に割り当てられることを示します。

ドライブベイのマッピングの構成

前提条件

- iLO の設定を構成する権限
- iLO ファームウェア 1.20 以降
- ストレージエンクロージャーのプロセッサーファームウェア 1.00 以降
- シャーシファームウェア 1.2.10 以降

手順

1. ナビゲーションツリーで**シャーシ情報**をクリックし、**ドライブベイのマッピング**タブをクリックします。

   各ドライブベイは、選択できるホストポート番号とともにテーブルに表示されます。

2. ホストポートにドライブベイを割り当てるには、○（**ホストポート番号**列内）をクリックします。

   複数の割り当てをアップデートするには、**Shift** キーを押したまま、アップデートする各割り当ての選択アイコンをクリックします。

3. （オプション）選択した値をクリアするには、○（**未割当て**列内）をクリックします。
4. （オプション）すべての値の割り当てを解除するには、**すべてを未割当**をクリックします。
5. **適用**をクリックします。

   iLO は、ドライブベイのマッピング構成を変更すると、データ損失またはデータ破壊が発生する可能性があることを通知します。

   △ **注意:** ドライブベイのマッピング構成を変更すると、データ損失やデータ破壊の原因となることがあります。たとえば、ドライブベイ 1～6 からノード 1 に割り当てられ、ドライブが RAID0 ボリュームとして設定されているような構成を検討してください。ドライブベイのマッピングを変更して構成済みのドライブが利用できなくなると、データ破壊が発生する可能性があります。

6. **はい、ドライブベイマッピングを適用します**をクリックします。

   保留中の変更は、**ドライブベイのマッピング**テーブル内で赤く表示されます。

7. シャーシ内のすべてのサーバーノードをシャットダウンします。
8. シャーシファームウェアによってストレージエキスパンダーバックプレーンがリセットされるまで、少なくとも 5 秒間お待ちください。
9. サーバーノードを再起動します。

ドライブベイのマッピング構成をデフォルト構成に設定

前提条件

- iLO の設定を構成する権限
- iLO ファームウェア 1.20 以降
- ストレージエンクロージャーのプロセッサーファームウェア 1.00 以降
- シャーシファームウェア 1.2.10 以降

手順

1. ナビゲーションツリーで**シャーシ情報**をクリックし、**ドライブベイのマッピング**タブをクリックします。

   各ドライブベイは、選択できるホストポート番号とともにテーブルに表示されます。

2. **デフォルトにリセット**をクリックします。

   iLO は、ドライブベイのマッピング構成を変更すると、データ損失またはデータ破壊が発生する可能性があることを通知します。

   > **注意:** ドライブベイのマッピング構成を変更すると、データ損失やデータ破壊の原因となることがあります。たとえば、ドライブベイ 1～6 からノード 1 に割り当てられ、ドライブが RAID0 ボリュームとして設定されているような構成を検討してください。ドライブベイのマッピングを変更して構成済みのドライブが利用できなくなると、データ破壊が発生する可能性があります。

3. **はい、ドライブベイマッピングを適用します**をクリックします。

   保留中の変更は、**ドライブベイのマッピング**テーブル内で赤く表示されます。

4. シャーシ内のすべてのサーバーノードをシャットダウンします。
5. シャーシファームウェアによってストレージエキスパンダーバックプレーンがリセットされるまで、少なくとも 5 秒間お待ちください。
6. サーバーノードを再起動します。

ドライブベイのマッピング構成のエクスポートとインポート

iLO では、ローカルファイルまたは iLO 不揮発性メモリを使用した、ドライブベイのマッピング構成のエクスポートとインポートがサポートされています。

ドライブベイのマッピング構成をエクスポートするとき、データには現在の構成が含まれますが、保留中の変更は含まれません。

ドライブベイのマッピング構成をローカルファイルにエクスポートする

前提条件

- iLO の設定を構成する権限
- iLO ファームウェア 1.20 以降
- ストレージエンクロージャーのプロセッサーファームウェア 1.00 以降
- シャーシファームウェア 1.2.10 以降

手順

1. ナビゲーションツリーで**シャーシ情報**をクリックし、**ドライブベイのマッピング**タブをクリックします。
2. **ローカルファイルへエクスポート**をクリックします。

   JSON 出力ウィンドウが表示されます。
3. **保存**をクリックし、ブラウザーのプロンプトに従ってファイルを保存するか、ファイルを開きます。

ドライブベイのマッピング構成を iLO 不揮発性メモリにエクスポートする

前提条件

- iLO の設定を構成する権限
- iLO ファームウェア 1.20 以降
- ストレージエンクロージャーのプロセッサーファームウェア 1.00 以降
- シャーシファームウェア 1.2.10 以降

手順

1. ナビゲーションツリーで**シャーシ情報**をクリックし、**ドライブベイのマッピング**タブをクリックします。
2. **iLO ベイにエクスポート**をクリックします。

   バックアップが成功したことが iLO から通知されます。

ローカルファイルからドライブベイのマッピング構成をインポートする

前提条件

- iLO の設定を構成する権限
- iLO ファームウェア 1.20 以降
- ストレージエンクロージャーのプロセッサーファームウェア 1.00 以降
- シャーシファームウェア 1.2.10 以降
- ドライブベイのマッピング構成がローカルファイルにエクスポート済みであること。

手順

1. ナビゲーションツリーで**シャーシ情報**をクリックし、**ドライブベイのマッピング**タブをクリックします。
2. **データからインポート**をクリックします。

   データからインポートインターフェイスが開きます。
3. エクスポートされたドライブベイマッピングファイルの内容をクリップボードにコピーします。
4. 内容を**データからインポート**テキストボックスに貼り付けて、**インポート**をクリックします。

   ドライブベイのマッピングテーブルは、ローカルファイルにバックアップされたドライブベイのマッピング構成でアップデートされます。

5. **適用**をクリックします。

   iLO は、ドライブベイのマッピング構成を変更すると、データ損失またはデータ破壊が発生する可能性があることを通知します。

   > **注意:** ドライブベイのマッピング構成を変更すると、データ損失やデータ破壊の原因となることがあります。たとえば、ドライブベイ 1～6 からノード 1 に割り当てられ、ドライブが RAID0 ボリュームとして設定されているような構成を検討してください。ドライブベイのマッピングを変更して構成済みのドライブが利用できなくなると、データ破壊が発生する可能性があります。

6. **はい、ドライブベイマッピングを適用します**をクリックして、変更を確認します。

   保留中の変更は、**ドライブベイのマッピング**テーブル内で赤く表示されます。

7. シャーシ内のすべてのサーバーノードをシャットダウンします。

8. シャーシファームウェアによってストレージエキスパンダーバックプレーンがリセットされるまで、少なくとも 5 秒間お待ちください。

9. サーバーノードを再起動します。

iLO 不揮発性メモリからドライブベイのマッピング構成をインポートする

前提条件

- iLO の設定を構成する権限
- iLO ファームウェア 1.20 以降
- ストレージエンクロージャーのプロセッサーファームウェア 1.00 以降
- シャーシファームウェア 1.2.10 以降
- ドライブベイのマッピング構成が iLO 不揮発性メモリにバックアップ済みであること。

手順

1. ナビゲーションツリーで**シャーシ情報**をクリックし、**ドライブベイのマッピング**タブをクリックします。

2. **iLO からインポート**をクリックします。

   ドライブベイのマッピングテーブルは、iLO 不揮発性メモリにバックアップされたドライブベイのマッピング構成でアップデートされます。

3. **適用**をクリックします。

   iLO は、ドライブベイのマッピング構成を変更すると、データ損失またはデータ破壊が発生する可能性があることを通知します。

   > **注意:** ドライブベイのマッピング構成を変更すると、データ損失やデータ破壊の原因となることがあります。たとえば、ドライブベイ 1～6 からノード 1 に割り当てられ、ドライブが RAID0 ボリュームとして設定されているような構成を検討してください。ドライブベイのマッピングを変更して構成済みのドライブが利用できなくなると、データ破壊が発生する可能性があります。

4. **はい、ドライブベイマッピングを適用します**をクリックします。

   保留中の変更は、**ドライブベイのマッピング**テーブル内で赤く表示されます。

5. シャーシ内のすべてのサーバーノードをシャットダウンします。

6. シャーシファームウェアによってストレージエキスパンダーバックプレーンがリセットされるまで、少なくとも 5 秒間お待ちください。
7. サーバーノードを再起動します。

iLO と他のソフトウェア製品およびツールとの使用

iLO およびリモート管理ツール

iLO 5 では、HPE OneView などのサポート対象ツールによるリモート管理がサポートされます。

iLO とリモート管理ツールの関連付けは、リモート管理ツールを使用して構成します。手順については、リモート管理ツールのドキュメントを参照してください。

iLO がリモート管理ツールで制御されているとき、iLO の Web インターフェイスには次の拡張機能が含まれます。

- iLO ログインページに、以下のようなメッセージが表示されます。

  このシステムは以下によって管理されています：<リモート管理ツール名>。
  iLO 内でローカルで変更すると、その変更は、集中管理された設定と同期が取れなくなります。

- **<リモート管理ツール名>**というページが、iLO ナビゲーションツリーに追加されます。

リモート管理ツールの iLO からの起動

iLO がリモート管理ツールで制御されているときは、以下の手順に従って iLO からリモートマネージャーのユーザーインターフェイスを開きます。

手順

1. ナビゲーションツリーで**<リモート管理ツールの名前>**をクリックします。
2. **起動**をクリックします。

   リモート管理ツールが、独立したブラウザーウィンドウで起動します。

詳しくは

ログインページからのリモート管理ツールの起動

リモートマネージャー構成の削除

ネットワークでリモート管理ツールの使用を停止する場合は、ツールと iLO 間の関連付けを削除できます。

この機能は、Synergy コンピュートモジュールではサポートされません。

重要: Hewlett Packard Enterprise では、iLO でリモートマネージャーの構成を削除する前に、リモート管理ツールからサーバーを削除することをお勧めします。ネットワーク上で使用中のツールのうち、現在の iLO システムを含んでいるサーバーを管理しているツールのリモートマネージャー構成を削除しないでください。

手順

1. ナビゲーションツリーで**<リモート管理ツール名>**をクリックします。
2. **この iLO からリモートマネージャー構成を削除します**セクションで、**削除**ボタンをクリックします。

管理対象サーバーをリモート管理ツールで管理しなくなった場合のみ先へ進むよう iLO が警告します。

3. **OK** をクリックします。

   <リモート管理ツール名>ページが、iLO のナビゲーションツリーから削除されます。

iLO を HPE OneView と一緒に使用する

HPE OneView は、iLO 管理プロセッサーとやり取りして、サポート対象のサーバーの構成、監視、および管理を行います。また、iLO のリモートコンソールへのシームレスなアクセスを設定します。これにより、HPE OneView ユーザーインターフェイスから iLO リモートコンソールを 1 回のクリックで起動できるようになります。iLO 権限は、アプライアンスアカウントに割り当てられた役割によって決まります。

HPE OneView は、以下の iLO 設定を管理します。

- リモート管理ツール
- SNMP v1 トラップ宛先
- SNMP v1 読み取りコミュニティ
- SSO 証明書 - 信頼された証明書が **HPE SSO** ページに追加されます。
- NTP（タイムサーバー）構成
- ユーザーアカウント - 管理者ユーザーアカウントが iLO に追加されます。
- ファームウェアバージョン - サーバーを HPE OneView に追加するときに、サポートされているバージョンの iLO ファームウェアがまだインストールされていない場合、iLO ファームウェアが自動的にアップデートされます。詳しくは、HPE OneView のサポートマトリックスを参照してください。
- iLO RESTful API イベントの宛先としてアプライアンスが追加されます。
- リモートサポートの登録

重要: HPE OneView を iLO 5 と使用するときに最高のパフォーマンスを得るために、Hewlett Packard Enterprise は、iLO Web インターフェイスを使用してこれらの設定を削除したり変更しないことをおすすめします。iLO ファームウェアからデバイス構成を変更すると、デバイス構成が HPE OneView と同期しなくなる可能性があります。

サーバー署名（Synergy コンピュートモジュール）

HPE OneView が Synergy コンピュートモジュールを管理する場合、iLO では、HPE OneView が固有のネットワーク設定、仮想識別子、およびアダプター設定を管理できるサーバーの署名を生成します。

iLO が起動するたびに、サーバーの署名が更新され、適合について検証されます。これには、フレームベイと UUID、HPE OneView ドメインの IP アドレス、サーバーのデバイスの署名などの情報が含まれます。

サーバーが別のフレームまたはベイに移動したり、サーバーをベイに挿入したときにそのハードウェア構成が変わったりした場合は、サーバーの署名が変わります。この変更が発生した場合、HPE OneView によって構成された設定は消去され、iLO イベントログにイベントのログが記録され、iLO RESTful API イベントが生成されます。このプロセスによって、アドレスの重複が回避され、HPE OneView はサーバーが固有のプロファイルを確実に持つことができます。

ほとんどの場合、HPE OneView は自動的にサーバーを再検出して、構成します。この検出と構成が実行されなかった場合は、HPE OneView ソフトウェアを使用してサーバーを含むフレームを更新します。

サーバーの署名データは iLO Web インターフェイスで表示または編集できませんが、REST クライアントを使用した読み取りができます。詳しくは、**https://www.hpe.com/support/restfulinterface/docs** を参照してください。

IPMI サーバー管理

IPMI によるサーバー管理は、サーバーを制御し、監視するための標準的な方法です。iLO ファームウェアは、以下を定義する IPMI バージョン 2.0 仕様に基づくサーバー管理を提供します。

- ファン、温度、パワーサプライなどのシステム情報の監視
- システムのリセットおよび電源オン/オフ操作などのリカバリ機能
- 温度上昇読み取りやファン障害などの異常なイベントのロギング機能
- 障害のあるハードウェアコンポーネントの特定などのインベントリ機能

IPMI 通信は、BMC と SMS に依存します。BMC は、SMS とプラットフォーム管理ハードウェアの間のインターフェイスを管理します。iLO ファームウェアは BMC 機能をエミュレートし、各種業界標準ツールで SMS 機能が提供されます。詳しくは、Intel の Web サイト **http://www.intel.com** の IPMI 仕様を参照してください。

iLO ファームウェアは、SMS 通信に KCS インターフェイスまたはオープンインターフェイスを提供します。KCS インターフェイスは、1 組の I/O マップ通信レジスタを提供します。I/O マップ SMS インターフェイスのデフォルトシステムベースアドレスは、`0xCA2` で、このシステムアドレスでバイトアラインされています。

KCS インターフェイスは、ローカルシステムで動作する SMS ソフトウェアにアクセス可能です。互換性のある SMS ソフトウェアアプリケーションの例は、次のとおりです。

- **IPMI バージョン 2.0 Command Test Tool** - ローレベル MS-DOS コマンドラインツールです。KCS インターフェイスを実装した IPMI BMC に、16 進数形式の IPMI コマンドを送信できるようにします。このツールは Intel の Web サイト **http://www.intel.com** からダウンロードできます。
- **IPMItool** - IPMI バージョン 1.5 およびバージョン 2.0 仕様をサポートするデバイスを管理したり設定するためのユーティリティです。IPMItool は、Linux 環境で使用できます。このツールは IPMItool の Web サイト **http://ipmitool.sourceforge.net/index.html** からダウンロードできます。
- **FreeIPMI** - IPMI バージョン 1.5 およびバージョン 2.0 仕様をサポートするデバイスを管理したり設定するためのユーティリティです。FreeIPMI は Web サイト **http://www.gnu.org/software/freeipmi/**からダウンロードできます。
- **IPMIUTIL** - IPMI バージョン 1.0、1.5 およびバージョン 2.0 仕様をサポートするデバイスを管理したり設定するためのユーティリティです。IPMIUTIL は、次のサイトからダウンロードできます。**http://ipmiutil.sourceforge.net/**

IPMI インターフェイスに対する BMC をエミュレートする場合に、iLO は、IPMI バージョン 2.0 仕様にリストされている必須コマンドをすべてサポートします。SMS は、その仕様に記述された方法を使用して BMC 内で有効または無効にする IPMI 機能を決定する必要があります（たとえば、`Get Device ID` コマンドを使用）。

サーバーの OS が動作中で iLO ドライバーが有効な場合は、KCS インターフェイスを介した IPMI のデータ通信量が iLO のパフォーマンスとシステムヘルスに影響を与える可能性があります。KCS インターフェイスを介して IPMI コマンドを実行しないでください。これは IPMI サービスに悪影響を与えることがあります。この制限には、IPMI パラメーター（たとえば、`Set Watchdog Timer` および `Set BMC Global Enabled`）を設定または変更するあらゆるコマンドが含まれています。単にデータを返す IPMI コマンド（たとえば、`Get Device ID` および `Get Sensor Reading`）は、どれでも安全です。

Linux 環境での IPMI ツールの高度な使用方法

Linux の IPMI ツールは、IPMI 2.0 RMCP+プロトコルを使用して iLO ファームウェアと安全に通信できます。この機能は、`ipmitool lanplus` プロトコル機能です。

次に例を示します。iLO のイベントログを取得するには、次のコマンドを入力します。

```
ipmitool -I lanplus -H <iLO IP アドレス> -U <ユーザー名> -P <パスワード> sel list
```

出力例：

```
1 | 03/18/2000 | 00:25:37 | Power Supply #0x03 | Presence detected | Deasserted
2 | 03/18/2000 | 02:58:55 | Power Supply #0x03 | Presence detected | Deasserted
3 | 03/18/2000 | 03:03:37 | Power Supply #0x04 | Failure detected | Asserted
4 | 03/18/2000 | 03:07:35 | Power Supply #0x04 | Failure detected | Asserted
```

HPE SIM での iLO の使用

iLO ファームウェアは主なオペレーティング環境で HPE SIM と統合され、標準の Web ブラウザーから単一の管理コンソールを提供します。オペレーティングシステムの動作中、HPE SIM を使用することで iLO への接続を確立することができます。

HPE SIM と統合すると、以下を実現できます。

HPE SIM コンソールへの SNMP トラップの配信サポート

HPE SIM コンソールを構成して、SNMP トラップをポケットベルや電子メールアドレスに転送することができます。

管理プロセッサーのサポート

ネットワーク上のサーバーにインストールされたすべての iLO デバイスは、HPE SIM では管理プロセッサーとして検出されます。

iLO 管理プロセッサーのグループ化

すべての iLO デバイスを、論理的なグループとしてまとめて 1 つのページに表示することができます。

Agentless Management

iLO を Agentless Management と組み合わせると、iLO の Web インターフェイス経由でシステム管理情報にリモートアクセスできます。

SNMP 管理のサポート

HPE SIM は、iLO 経由で SNMP 情報にアクセスできます。

HPE SIM の機能

HPE SIM では以下を実行できます。

- iLO プロセッサーの識別
- iLO プロセッサーとそのサーバーの関連付け
- iLO プロセッサーとそのサーバー間のリンクの作成
- iLO とサーバーの情報およびステータスの表示
- iLO について表示する情報の量の制御

以下の項で、これらの機能について説明します。詳しくは、HPE SIM ユーザーガイドを参照してください。

HPE SIM での SSO の確立

手順

1. HPE SIM SSO 用に iLO を設定し、HPE SIM 信頼済みサーバーを追加します。
2. 前の手順で指定した HPE SIM サーバーにログインし、iLO プロセッサーを検出します。

   検出プロセスが完了したら、iLO に対して SSO が有効になります。

   HPE SIM 検出タスクについて詳しくは、HPE SIM ユーザーガイドを参照してください。

iLO の識別および関連付け

HPE SIM は、iLO プロセッサーを識別し、iLO とサーバーを関連付けます。iLO が HPE SIM の識別要求に応答するように設定するには、**アクセス設定**ページで**匿名データ**設定を有効にします。

詳しくは

iLO アクセス設定の構成

HPE SIM での iLO ステータスの表示

HPE SIM は、iLO デバイスを管理プロセッサーとして識別します。HPE SIM は、**すべてのシステム**ページに管理プロセッサーのステータスを表示します。

iLO 管理プロセッサーは、そのホストサーバーと同じ行にアイコンとして表示されます。管理プロセッサーのステータスは、アイコンの色で示されます。

デバイスステータスのリストについては、HPE SIM ユーザーガイドを参照してください。

HPE SIM での iLO リンク

HPE SIM は、管理を簡単にするために、次の位置へのリンクを作成します。

- 任意の**システム**リストから iLO およびホストサーバーへ
- iLO の**システム**ページからサーバーへ
- サーバーの**システム**ページから iLO へ

システムリストページには、iLO、サーバー、およびその関係が表示されます。

- iLO の Web インターフェイスを表示するには、ステータスアイコンをクリックします。
- デバイスの**システム**ページを表示するには、iLO またはサーバー名をクリックします。

HPE SIM のシステムリストでの iLO の表示

iLO 管理プロセッサーを HPE SIM に表示できます。完全な設定権限を持つユーザーは、管理プロセッサーをグループにまとめて、カスタマイズされたシステムの集合を作成し、使用することができます。詳しくは、HPE SIM ユーザーガイドを参照してください。

HPE SIM での SNMP アラートの受信

HPE SIM では、SNMP を完全に管理できます。iLO は、HPE SIM への SNMP トラップ送信をサポートします。ユーザーは、イベントログを表示し、イベントを選択し、アラートについての詳細情報を表示できます。

手順

1. SNMP トラップを送信するように iLO を有効にするには、以下のようにします。

   a. ナビゲーションツリーの**管理**をクリックします。

   b. **SNMP 設定**および **SNMP アラート**を構成します。

      SNMP アラートの送信先ボックスに、HPE SIM コンピューターの IP アドレスを入力します。

2. HPE SIM で iLO を検出するには、HPE SIM の管理対象デバイスとして iLO を設定します。

   この構成により、iLO 上の NIC インターフェイスが専用の管理ポートとして機能するようになり、管理トラフィックはリモートのホストサーバーの NIC インターフェイスから分離されます。手順については、HPE SIM ユーザーガイドを参照してください。

   主要な、クリアされていないイベントについて、iLO トラップが**すべてのイベント**に表示されます。イベントについて詳しくは、**イベントタイプ**をクリックしてください。

詳しくは

SNMP アラートの送信先の追加

iLO と HPE SIM の HTTP ポート一致要件

HPE SIM は、デフォルトの **Web サーバー非 SSL ポート**（ポート 80）で、HTTP セッションを開始して iLO を確認するように設定されています。ポート番号を変更する場合は、iLO と HPE SIM の両方で変更する必要があります。

- iLO でポートを変更するには、**アクセス設定**ページで **Web サーバー非 SSL ポート**値をアップデートします。
- HPE SIM でポート番号を変更するには、ポートを、HPE SIM のインストールディレクトリの `config\identification\additionalWsDisc.props` ファイルに追加します。

  ポートエントリーは 1 行でなければならず、最初にポート番号を指定し、以後の他のすべての項目は（大文字を含めて）次の例と同じです。次の例は、ポート 55000 で iLO を検出するための正しいエントリーを示しています。

  55000=iLO 5, ,true,false,com.hp.mx.core.tools.identification.mgmtproc.MgmtProcessorParser

詳しくは

iLO アクセス設定の構成

HPE SIM での iLO ライセンス情報の確認

HPE SIM は、iLO 管理プロセッサーのライセンスステータスを表示します。この情報を使用すると、どの iLO デバイスに、また何台の iLO デバイスにライセンスがインストールされているかを確認できます。

ライセンス情報を表示するには、**展開** > **ライセンスマネージャー**を選択します。

データが最新であることを確認するには、管理プロセッサーに対して**システム識別**タスクを実行します。詳しくは、HPE SIM ユーザーガイドを参照してください。

Kerberos 認証とディレクトリサービスの設定

iLO での Kerberos 認証

Kerberos のサポートにより、ユーザーはユーザー名とパスワードを入力する代わりに、ログインページの **Zero サインイン**ボタンをクリックして、iLO にログインすることができます。正常にログインするには、クライアントワークステーションがドメインにログインし、ユーザーが、iLO が設定されているディレクトリグループのメンバーでなければなりません。ワークステーションがドメインにログインしていない場合でも、ユーザーは、Kerberos UPN とドメインパスワードを使用して iLO にログインできます。

システム管理者はユーザーサインオンの前に iLO とドメイン間の信頼関係を確立するため、(Two-Factor 認証を含む)任意の形式の認証がサポートされます。Two-Factor 認証をサポートするようにユーザーアカウントを設定する方法については、サーバー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。

Kerberos 認証の設定

手順

1. **iLO ホスト名およびドメイン名を設定します**。
2. **iLO ライセンスをインストールして Kerberos 認証を有効にします**。
3. **ドメインコントローラーで Kerberos サポートを準備します**。
4. **Kerberos キータブファイルを生成します**。
5. **ご使用の環境が Kerberos 認証の時刻要件を満たしていることを確認します**。
6. **iLO で Kerberos パラメーターを設定します**。
7. **iLO ディレクトリグループを設定します**。
8. **サポートされるブラウザーでシングルサインオンを設定します**

Kerberos 認証用の iLO ホスト名とドメイン名の構成

使用したいドメイン名または DNS サーバーが DHCP サーバーによって提供されない場合は、次の手順を使用します。

手順

1. ナビゲーションツリーで **iLO 専用ネットワークポート**をクリックします。
2. **IPv4** タブをクリックします。
3. 次のチェックボックスの選択を解除して、**送信**をクリックします。
   - **DHCPv4 のドメイン名の使用**
   - **DHCPv4 の DNS サーバーの使用**
4. **IPv6** タブをクリックします。
5. 次のチェックボックスの選択を解除して、**送信**をクリックします。

- **DHCPv6 のドメイン名の使用**
- **DHCPv6 の DNS サーバーの使用**

6. **全般**タブをクリックします。
7. （オプション）**iLO サブシステム名（ホスト名）をアップデートします。**
8. **ドメイン名**をアップデートします。
9. **送信**をクリックします。
10. iLO を再起動するには、**リセット**をクリックします。

詳しくは

iLO ホスト名の設定
iLO ホスト名とドメイン名の制限
Kerberos 認証の iLO ホスト名とドメイン名の要件

Kerberos 認証の iLO ホスト名とドメイン名の要件

- **ドメイン名** - iLO ドメイン名の値は、通常大文字に変換されたドメイン名である Kerberos レルム名と一致している必要があります。たとえば、親ドメイン名が `somedomain.net` である場合、Kerberos レルム名は、`SOMEDOMAIN.NET` になります。
- **iLO サブシステム名（ホスト名）** - 設定された iLO ホスト名は、キータブファイルを生成するときに使用する iLO ホスト名と同じでなければなりません。iLO ホスト名は大文字小文字が区別されます。

ドメインコントローラーでの Kerberos サポートの準備

Windows Server 環境で、Kerberos サポートはドメインコントローラーに含まれ、Kerberos レルム名は通常、大文字に変換されたドメイン名になります。

手順

1. iLO システムごとにドメインディレクトリにコンピューターアカウントを作成して有効にします。

   Active Directory ユーザーとコンピュータースナップインでユーザーアカウントを作成します。例：

   - iLO ホスト名：`myilo`
   - 親ドメイン名：`somedomain.net`
   - iLO ドメイン名（完全修飾）：`myilo.somedomain.net`

2. iLO へのログインが許可されている各ユーザーについて、ドメインディレクトリにユーザーアカウントが存在していることを確認します。
3. ドメインディレクトリにユニバーサルおよびグローバルユーザーグループを作成します。

   iLO で権限を設定するには、ドメインディレクトリにセキュリティグループを作成する必要があります。iLO にログインするユーザーには、そのユーザーがメンバーとなっているすべてのグループの一切の権限が付与されます。権限の設定には、グローバルユーザーグループおよびユニバーサルユーザーグループのみを使用できます。ドメインローカルグループは、サポートされていません。

Windows 環境での iLO 用キータブファイルの生成

手順

1. `Ktpass.exe` ツールを使用して、キータブファイルを生成し、共有秘密を設定します。
2. （オプション）`Setspn` コマンドを使用して、Kerberos SPN を iLO システム用 SPN を表示します。
3. （オプション）`Setspn -L <iLO name>`コマンドを使用して、iLO システム用 SPN を表示します。

   `HTTP/myilo.somedomain.net` サービスが表示されることを確認します。

詳しくは

Ktpass
Setspn

Ktpass

構文

```
Ktpass [options]
```

説明

`Ktpass` は、Kerberos 認証用のサービスプリンシパル名と暗号化されたパスワードのペアが含まれているキータブファイルと呼ばれるバイナリファイルを生成します。

パラメーター

+rndPass

ランダムパスワードを指定します。

-ptype KRB5_NT_SRV_HST

プリンシパルタイプ。ホストサービスインスタンス（KRB5_NT_SRV_HST）タイプを使用します。

-princ <principal name>

大文字と小文字が区別されるプリンシパル名を指定します。たとえば、`HTTP/myilo.somedomain.net@SOMEDOMAIN.net` などです。

- サービスタイプは大文字を使用する必要があります（`HTTP`）。
- iLO ホスト名は小文字を使用する必要があります（`myilo.somedomain.net`）。
- レルム名は大文字を使用する必要があります（`@SOMEDOMAIN.NET`）。

-mapuser <user account>

プリンシパル名を iLO システムドメインアカウントにマップします。

-out <file name>

`.keytab` ファイルのファイル名を指定します。

-crypto <encryption>

`.keytab` ファイルに生成されるキーの暗号化を指定します。

iLO で、高度なセキュリティ、FIPS、または CNSA セキュリティ状態を使用するように構成されている場合、AES Kerberos キータイプを使用する必要があります。

kvno

キーバージョン番号を上書きします。

> **重要:** このパラメーターは使用しないでください。このオプションを使用すると、キータブファイルの `kvno` と Active Directory の `kvno` が同期しなくなります。

コマンド例

```
Ktpass +rndPass -ptype KRB5_NT_SRV_HST -princ
HTTP/myilo.somedomain.net@SOMEDOMAIN.NET -mapuser myilo$@somedomain.net
-out myilo.keytab
```

出力例

```
Targeting domain controller: domaincontroller.example.net
Using legacy password setting method
Successfully mapped HTTP/iloname.example.net to iloname.
WARNING: pType and account type do not match. This might cause problems.
Key created.
Output keytab to myilo.keytab:
Keytab version: 0x502
keysize 69 HTTP/iloname.example.net@EXAMPLE.NET ptype 3
(KRB5 _NT_SRV_HST) vno 3 etype 0x17 (RC4-HMAC) keylength 16
(0x5a5c7c18ae23559acc2 9d95e0524bf23)
```

`Ktpass` コマンドでは、UPN を設定できないことに関するメッセージが表示される場合があります。この結果は、iLO がユーザーではなくサービスであるため、問題ありません。コンピューターオブジェクトで、パスワード変更を確認するように求められる場合があります。ウィンドウを閉じ、キータブファイルの作成を続行するには、**OK** をクリックします。

Setspn

構文

```
Setspn [options]
```

説明

`Setspn` コマンドは、SPN を表示、修正、および削除します。

パラメーター

-A <SPN>

追加する SPN を指定します。

-L

システムの現在の SPN を一覧表示します。

コマンド例

```
SetSPN -A HTTP/myilo.somedomain.net myilo
```

SPN コンポーネントでは大文字と小文字が区別されます。プライマリ（サービスタイプ）は、たとえば `HTTP` のように大文字でなければなりません。インスタンス（iLO ホスト名）は、たとえば `myilo.somedomain.net` のように小文字でなければなりません。

`SetSPN` コマンドでは、UPN を設定できないことに関するメッセージが表示される場合があります。この結果は、iLO がユーザーではなくサービスであるため、問題ありません。コンピューターオブジェクト

で、パスワード変更を確認するように求められる場合があります。**OK** をクリックしてウィンドウを閉じ、キータブファイルの作成を続行します。

ご使用の環境が Kerberos 認証の時刻要件を満たしていることの確認

Kerberos 認証が正常に機能するには、iLO プロセッサー、KDC、およびクライアントワークステーションの間で日付と時刻が同期している必要があります。サーバーで iLO の日付および時刻を設定するか、iLO 内で SNTP 機能を有効にしてネットワークから日付および時刻を取得してください。

手順

1. 以下の日付と時間が互いに 5 分以内で設定されていることを確認します。
   - iLO の日付と時刻の設定
   - Web ブラウザーを実行するクライアント
   - 認証を実行するサーバー

サポートされるブラウザーでのシングルサインオンの設定

ユーザーが iLO にログインするには、権限が割り当てられたグループのメンバーになっている必要があります。Windows クライアントの場合、ワークステーションのロックまたはロック解除によって、iLO へのログインに使用される認証情報が更新されます。Home バージョンの Windows オペレーティングシステムは、Kerberos ログインをサポートしていません。

iLO に関して Active Directory が適切に設定されており、Kerberos ログインに関して iLO が適切に設定されている場合には、このセクションの手順によって、ログインが有効になります。

詳しくは

サポートされているブラウザー

Microsoft Internet Explorer でのシングルサインオンの有効化

手順

1. Internet Explorer で認証を有効にします。
   a. **ツール** > **インターネットオプション**の順に選択します。
   b. **詳細構成**タブをクリックします。
   c. **セキュリティ**セクションで、**統合 Windows 認証を使用する**オプションが選択されていることを確認します。
   d. **OK** をクリックします。
2. iLO ドメインをイントラネットゾーンに追加します。
   a. **ツール** > **インターネットオプション**の順に選択します。
   b. **セキュリティ**タブをクリックします。
   c. **ローカルイントラネット**アイコンをクリックします。
   d. **サイト**ボタンをクリックします。
   e. **詳細設定**ボタンをクリックします。
   f. **この Web サイトをゾーンに追加する**ボックスに、追加するサイトを入力します。

企業ネットワークでは、`*.example.net` で十分です。

g. **追加**をクリックします。

h. **閉じる**をクリックします。

i. **ローカルイントラネット**ダイアログボックスを閉じるには、**OK** をクリックします。

j. **インターネットオプション**ダイアログボックスを閉じるには、**OK** をクリックします。

3. **イントラネットゾーンでのみ自動的にログオンする**設定を有効にします。

   a. **ツール** > **インターネットオプション**の順に選択します。

   b. **セキュリティ**タブをクリックします。

   c. **ローカルイントラネット**アイコンをクリックします。

   d. **レベルのカスタマイズ**をクリックします。

   e. **ユーザー認証**セクションで、**イントラネットゾーンでのみ自動的にログオンする**オプションが選択されていることを確認します。

   f. **セキュリティ設定 - ローカルイントラネットゾーン**ウィンドウを閉じるには、**OK** をクリックします。

   g. **インターネットオプション**ダイアログボックスを閉じるには、**OK** をクリックします。

4. 手順 **1**～**3** でオプションを変更した場合は、Internet Explorer を閉じて再起動します。

5. **シングルサインオンの設定を確認します。**

Mozilla Firefox でのシングルサインオンの有効化

手順

1. ブラウザーの場所ツールバーに **`about:config`** と入力して、ドメインの設定ページを開きます。

   Firefox には次のメッセージが表示されます。

   動作保証対象外になります!

2. **危険性を承知の上で使用する**ボタンをクリックします。

3. **検索**ボックスに **`network.negotiate`** と入力します。

4. `network.negotiate-auth.trusted-uris` をダブルクリックします。

5. iLO の DNS ドメイン名を入力し（たとえば、`example.net`）、**OK** をクリックします。

6. **シングルサインオンの設定を確認します。**

Google Chrome でのシングルサインオン

Google Chrome では設定は必要ありません。

Microsoft Edge でのシングルサインオンの有効化

Microsoft Edge では設定は必要ありません。

シングルサインオン（Zero サインイン）設定の確認

手順

1. iLO ログインページ（例：`http://iloname.example.net`）に移動します。
2. **Zero サインイン**ボタンをクリックします。

名前によるログインが動作していることの確認

手順

1. iLO ログインページに移動します。
2. Kerberos UPN 形式のユーザー名（例：**`user@EXAMPLE.NET`**）を入力します。
3. 関連付けられているドメインパスワードを入力します。
4. **ログイン** をクリックします。

ディレクトリ統合の利点

- **スケーラビリティ** - ディレクトリサービスを利用して、数千台の iLO プロセッサー上で数千のユーザーをサポートできます。
- **セキュリティ** - ディレクトリサービスから強力なユーザーパスワードポリシーが継承されます。ポリシーには、ユーザーパスワードの複雑度、ローテーション頻度、有効期限などがあります。
- **ユーザーの責任** - 環境によっては、ユーザーが iLO アカウントを共有することがあり、その場合、操作を実行したユーザーの特定が困難になります。
- **ロールベースの管理**（HPE 拡張スキーマ） - ロール（たとえば、事務処理、ホストのリモート制御、完全な制御）を作成して、ユーザーやユーザーグループに関連付けることができます。1 つのロールで変更が行われると、その変更は、そのロールに関連付けられたすべてのユーザーおよび iLO デバイスに適用されます。
- **集中管理**（HPE 拡張スキーマ） - MMC などオペレーティングシステム固有の管理ツールを使用して、iLO ユーザーを管理できます。
- **緊急性** - ディレクトリでの 1 つの変更が、関連付けられた iLO プロセッサーにただちに公開されます。この機能により、このプロセスをスクリプト化する必要がなくなります。
- **認証情報の簡素化** - ディレクトリでは、iLO 用の新しい認証情報を記録せずに、既存のユーザーアカウントとパスワードを使用できます。
- **柔軟性**（HPE 拡張スキーマ） - 企業の環境に合わせて、1 台の iLO プロセッサーについて 1 ユーザーを対象に 1 つのロールを作成することも、複数の iLO プロセッサーについて複数のユーザーを対象に 1 つのロールを作成することも、ロールを組み合わせて使用することもできます。HPE 拡張スキーマ構成では、アクセスを特定の時間だけに制限したり、特定の IP アドレス範囲に制限したりすることができます。
- **互換性** - iLO ディレクトリ統合は、Active Directory および OpenLDAP をサポートします。
- **規格** - iLO ディレクトリサポートは、安全なディレクトリアクセスに関する LDAP 2.0 規格に基づいています。iLO の Kerberos サポートは LDAP v3 に基づいています。

iLO で使用するディレクトリ構成の選択

ディレクトリに対して iLO を構成する前に、スキーマフリー構成オプションか HPE 拡張スキーマ構成オプションかを選択します。

以下の質問について検討します。

1. **使用するディレクトリにスキーマ拡張を適用できますか。**

   - **「はい」の場合** - 質問 2 に進みます。
   - **「いいえ」の場合** - Active Directory を使用しており、お客様の会社のポリシーにより拡張を適用できません。

     「いいえ」の場合 - OpenLDAP を使用しています。HPE 拡張スキーマは、現時点では OpenLDAP でサポートされていません。

     「いいえ」の場合 - お使いの環境には、HPE 拡張スキーマとのディレクトリ統合は適しません。

     グループベースのスキーマフリーディレクトリ統合を使用します。試用版のサーバーをインストールして、HPE 拡張スキーマ構成とのディレクトリ統合の利点を検討してみるとよいでしょう。

2. **スケーラブルな設定を使用していますか。**

   次の質問に回答すると、設定がスケーラブルかどうかがわかります。

   - ディレクトリユーザーのグループの権限を変更する可能性がありますか。
   - iLO の変更を定期的にスクリプト化するつもりですか。
   - iLO 権限の制御に 6 つ以上のグループを使用しますか。

   これらの質問に対する答えに応じて、次のオプションから選択します。

   - **「いいえ」の場合** - スキーマフリーディレクトリ統合のインスタンスをインストールして、この方式がお使いのポリシーおよび手順の要件に合っているかどうかを検討してみましょう。必要に応じて、後で、HPE 拡張スキーマ構成を展開できます。
   - **「はい」の場合** - HPE 拡張スキーマ構成を使用します。

詳しくは

スキーマフリーディレクトリ認証
HPE 拡張スキーマディレクトリ認証

スキーマフリーディレクトリ認証

スキーマフリーディレクトリ認証を使用すると、ユーザーおよびグループがディレクトリに存在し、グループ権限が iLO の設定に存在します。iLO はディレクトリログイン証明書を使用してディレクトリ内のユーザーオブジェクトを読み取り、ユーザーグループのメンバーシップを取得します。これらのグループは、iLO のグループ構成と比較されます。ディレクトリユーザーアカウントが、構成されている iLO ディレクトリグループのメンバーとして確認されると、iLO のログインに成功します。

スキーマフリーディレクトリ統合の利点

- ディレクトリスキーマを拡張する必要がありません。
- ディレクトリ内のユーザーについては、設定はほとんど必要ありません。設定が存在しない場合、ディレクトリは既存のユーザーおよびグループメンバーシップを使用して iLO にアクセスします。たとえば、User1 というドメイン管理者がいるとすると、このドメイン管理者のセキュリティグループの DN を iLO にコピーして、フル権限を与えます。すると、User1 は iLO にアクセスできるようになります。

スキーマフリーディレクトリ統合の欠点

グループ権限は、各 iLO システムで管理されます。この欠点は、グループ権限がほとんど変更されないため最小限に抑えられ、グループのメンバーシップを変更するタスクは、各 iLO システムでなく、ディレクトリで管理されます。Hewlett Packard Enterprise は、同時に複数の iLO システムを構成できるツールを提供しています。

構成オプション

スキーマフリーのセットアップオプションは、ディレクトリ用の設定にどの方法を用いても同じです。最も柔軟でないログイン、より柔軟なログイン、または非常に柔軟なログインのディレクトリ設定を構成できます。

- **最も柔軟でないログイン** - この構成を使用すると、完全 DN とパスワードを入力して iLO にログインできます。iLO が認識するグループのメンバーでなければなりません。

  この構成を使用するには、次の設定を入力します。

  - ディレクトリサーバーの DNS 名または IP アドレスと LDAP ポート。通常、SSL 接続用の LDAP ポートは、636 です。
  - 少なくとも 1 つのグループの DN。このグループは、セキュリティグループ（例：Active Directory の場合は `CN=Administrators,CN=Builtin,DC=EXAMPLE,DC=COM`、OpenLDAP の場合は `UID=username,ou=People,dc=hpe,dc=com`）、または目的の iLO ユーザーがグループメンバーであれば、別のどのグループでもかまいません。

- **より柔軟なログイン** - この構成を使用すると、ログイン名とパスワードを入力して iLO にログインできます。iLO が認識するグループのメンバーでなければなりません。ログイン時に、ログイン名とユーザーコンテキストが結合されて、ユーザー DN になります。

  この構成を使用するには、最も柔軟でないログインの設定と少なくとも 1 つのディレクトリユーザーコンテキストを入力します。

  たとえば、ユーザーが `JOHN.SMITH` としてログインし、ユーザーコンテキスト `CN=USERS,DC=EXAMPLE,DC=COM` が構成されている場合は、iLO で `CN=JOHN.SMITH,CN=USERS,DC=EXAMPLE,DC=COM` という DN が使用されます。

- **非常に柔軟なログイン** - この構成を使用すると、完全な DN とパスワード、ディレクトリに表示される名前、NetBIOS 形式（domain/login_name）、または電子メール形式（login_name@domain）を使用して iLO にログインできます。

  この構成を使用するには、IP アドレスの代わりにディレクトリの DNS 名を入力して、iLO にディレクトリサーバーアドレスを構成します。DNS 名は、iLO およびクライアントシステムの両方から、IP アドレスに解決できなければなりません。

ディレクトリ統合の設定（スキーマフリー構成）

手順

1. ご使用の環境がスキーマフリーのディレクトリ統合を使用するための前提条件を満たしていることを確認します。
2. iLO スキーマフリーディレクトリのパラメーターを設定します。
3. ディレクトリグループを設定します。

スキーマフリーディレクトリ統合を使用するための前提条件

手順

1. Active Directory および DNS をインストールします。
2. ルート CA をインストールして、SSL を有効にします。

   iLO は、安全な SSL 接続でのみ、ディレクトリと通信します。

   Active Directory での証明書サービスの使用について詳しくは、Microsoft のドキュメントを参照してください。
3. 少なくとも 1 人のユーザーのディレクトリ DN とそのユーザーが含まれているセキュリティグループの DN が、使用可能であることを確認します。この情報は、ディレクトリのセットアップを検証するために使用されます。
4. ディレクトリサービス認証を有効にする iLO ライセンスをインストールします。
5. iLO ネットワーク設定の IPv4 または IPv6 のページで、正しい DNS サーバーが指定されていることを確認します。

HPE 拡張スキーマディレクトリ認証

HPE 拡張スキーマディレクトリ認証オプションを使用すると、以下のことを行うことができます。

- 統合されたスケーラブルな共有ユーザーデータベースからユーザーを認証します。
- ディレクトリサービスを使用して、ユーザーの権限を制御（権限付与）します。
- ディレクトリサービスでは､iLO 管理プロセッサーおよび iLO ユーザーのグループレベルの管理にロールを使用します。

HPE 拡張スキーマディレクトリ統合の利点

- グループが各 iLO 上ではなく、ディレクトリ内で維持管理されます。
- 柔軟なアクセス制御 - アクセスを特定の時間だけに制限したり、特定の IP アドレス範囲に制限したりすることができます。

ディレクトリサービスのサポート

iLO ソフトウェアは、Microsoft Active Directory ユーザーとコンピュータースナップイン内で動作するように設計されており、ユーザーは、ディレクトリ経由でユーザーアカウントを管理できます。

iLO は、HPE 拡張スキーマ構成で Microsoft Active Directory をサポートします。

ディレクトリ統合の設定（HPE 拡張スキーマ構成）

手順

計画

1. 以下の内容を確認してください。
   - ディレクトリ対応リモート管理（HPE 拡張スキーマ構成）
   - ディレクトリサービススキーマ

インストール

2. 次のように操作します。
   a. ご使用の環境が Active Directory と HPE 拡張スキーマを構成するための前提条件を満たしていることを確認します。
   b. ディレクトリサービス認証を有効にする iLO ライセンスをインストールします。
   c. ProLiant マネジメントプロセッサー用のディレクトリサポートパッケージをダウンロードし、ご使用の環境に必要なユーティリティをインストールします。

      Schema Extender、スナップイン、および ProLiant マネジメントプロセッサー用のディレクトリサポートユーティリティをインストールすることができます。
   d. スキーマエクステンダーを使用してスキーマを拡張します。

アップデート

3. iLO の Web インターフェイスで、管理プロセッサーオブジェクトのディレクトリサーバー設定と DN を設定します。

   このステップは、ProLiant 管理プロセッサーのディレクトリサポートソフトウェアを使用して実行することもできます。

ロールとオブジェクトの管理

4. HPE Active Directory スナップインを使用して、デバイスオブジェクトとロールオブジェクトを設定します。
   a. マネジメントデバイスオブジェクトとロールオブジェクトを作成します。
   b. 必要に応じて、ロールオブジェクトに権限を割り当て、役割を管理デバイスオブジェクトと関連付けます。
   c. ユーザーをロールオブジェクトに追加します。

例外の取り扱い

5. 複雑なロール関連付けについては、ディレクトリスクリプティングユーティリティの使用を検討してください。

   iLO ユーティリティは、単一のロールで簡単に使用できます。ディレクトリに複数の役割を作成することを計画している場合は、`LDIFDE` または VBScript ユーティリティのようなディレクトリスクリプティングユーティリティを使用することができます。これらのユーティリティは複雑なロールの関係を作成します。

詳しくは

Active Directory と HPE 拡張スキーマの構成（構成例）

HPE 拡張スキーマ構成で Active Directory を設定するための前提条件

手順

1. Active Directory および DNS をインストールします。
2. ルート CA をインストールして、SSL を有効にします。

   iLO は、安全な SSL 接続でのみ、ディレクトリと通信します。

   Active Directory での証明書サービスの使用について詳しくは、Microsoft のドキュメントを参照してください。

   iLO には、ディレクトリサービスと通信するためにセキュリティ保護された接続が必要です。この接続には、Microsoft CA をインストールする必要があります。詳しくは、Microsoft Knowledge Base の Article ID 番号 321051 を参照してください。サードパーティの証明機関が SSL 経由で LDAP を有効にする方法
3. .NET Framework のバージョン 3.5 以降がインストールされていることを確認します。

   iLO LDAP コンポーネントはこのソフトウェアを必要とします。

   Windows Server Core 環境では LDAP コンポーネントを使用できません。
4. 次の Microsoft Knowledge Base の記事を参照してください。299687 MS01-036: LDAP over SSL の機能によりパスワードの変更が可能になる

iLO ディレクトリサポートソフトウェアのインストール

手順

1. ProLiant マネジメントプロセッサー用のディレクトリサポートパッケージを Web サイト **https://www.hpe.com/support/ilo5** からダウンロードします。
2. .NET Framework 3.5 以降をターゲットサーバーにインストールします。

   .NET Framework 3.5 以降は、ProLiant マネジメントプロセッサーソフトウェア用のディレクトリサポートをインストールするために使用します。
3. ダウンロードした EXE ファイルをダブルクリックします。
4. **次へ**をクリックします。
5. **I accept the terms of the license agreement** をクリックし、**次へ** をクリックします。
6. **ディレクトリサポート**ウィンドウで、**スキーマエクステンダー**をクリックし、スキーマエクステンダーソフトウェアをインストールします。

   a. スキーマエクステンダーセットアップウィザードウィンドウで、**次へ**をクリックします。

   b. **ライセンス契約**ウィンドウで、**同意する**を選択し、**次へ**をクリックします。

   c. **インストール先フォルダの選択**ウィンドウで、インストールディレクトリとユーザー設定を選択し、**次へ**をクリックします。

   d. インストール要求を確認するメッセージが表示されたら、**次へ**をクリックします。

      インストールの完了ウィンドウが開きます。

   e. **閉じる**をクリックします。
7. コンソールのスナップインをインストールするには、MMC コンソールが閉じられていることを確認してから、**Snap-ins (x86)**または **Snap-ins (x64)**をクリックします。

a. スナップインセットアップウィザードウィンドウで、**次へ**をクリックします。

b. **ライセンス契約**ウィンドウで、**同意する**を選択し、**次へ**をクリックします。

c. **情報**ウィンドウで詳細を読んで、**次へ**をクリックします。

d. インストール要求を確認するメッセージが表示されたら、**次へ**をクリックします。

   インストールの完了ウィンドウが開きます。

e. **閉じる**をクリックします。

スナップインのインストール後、iLO オブジェクトと iLO ロールをディレクトリ内で作成できます。ディレクトリオブジェクトの管理に使用される各コンピューターにスナップインをインストールします。詳しくは、**ディレクトリサービスオブジェクト**を参照してください。

8. ProLiant 管理プロセッサー用のディレクトリサポートソフトウェアをインストールするには、**ProLiant マネジメントプロセッサー用のディレクトリサポート**をクリックします。

   a. **ようこそ**ウィンドウで、**次へ**をクリックします。

   b. **ライセンス契約**ウィンドウで、**同意する**を選択し、**次へ**をクリックします。

   c. **インストール先フォルダの選択**ウィンドウで、インストールディレクトリとユーザー設定を選択し、**次へ**をクリックします。

   d. インストール要求を確認するメッセージが表示されたら、**次へ**をクリックします。

      インストールの完了ウィンドウが開きます。

   e. **閉じる**をクリックします。

詳しくは

Schema Extender の実行
ProLiant 管理プロセッサー用のディレクトリサポート（HPLOMIG）
HPE Active Directory スナップインによって追加される管理オプション

ProLiant 管理プロセッサー用のディレクトリサポートのインストールオプション

- **Schema Extender** - Schema Extender とバンドルされている `.xml` ファイルには、ディレクトリに追加されるスキーマが格納されます。通常、これらのファイルのうち 1 つに、サポートされているすべてのディレクトリサービスに共通のコアスキーマが格納されます。他のファイルには、製品固有のスキーマが格納されます。スキーマインストーラーには、.NET Framework が必要です。

  Windows Server Core をホストするドメインコントローラー上でスキーマインストーラーを実行することはできません。セキュリティおよびパフォーマンス上の理由から、Windows Server Core は、GUI を使用しません。スキーマインストーラーを使用するには、ドメインコントローラーに GUI をインストールするか、より古いバージョンの Windows をホストするドメインコントローラーを使用する必要があります。

- **Snap-ins (x86)**または **Snap-ins (x64)** - マネジメントスナップインインストーラーは、Microsoft Active Directory Users and Computers ディレクトリまたは Novell ConsoleOne ディレクトリで、iLO オブジェクトを管理するためのスナップインをインストールします。

  iLO スナップインは、iLO ディレクトリを作成する際に次のタスクを実行するために使用されます。

- iLO オブジェクトとロールオブジェクトを作成して管理する
- iLO オブジェクトとロールオブジェクトとの関連を作成する

- **ProLiant 管理プロセッサー用のディレクトリサポート** - このユーティリティでは、iLO での Kerberos 認証およびディレクトリサービスを設定できます。

  `HPLOMIG.exe` ファイル、必要な DLL、ライセンス契約、およびその他のファイルが、`C:\Program Files (x86)\Hewlett Packard Enterprise\Directories Support for ProLiant Management Processors` ディレクトリにインストールされます。別のディレクトリを選択することもできます。インストーラーが、**スタート**メニューに ProLiant 管理プロセッサー用のディレクトリサポートへのショートカットを作成します。

  インストールユーティリティは、.NET Framework がインストールされていないことを検出すると、エラーメッセージを表示して終了します。

Schema Extender の実行

手順

1. Windows の**スタート**メニューから Management Devices Schema Extender を起動します。
2. **Lights Out Management** が選択されていることを確認してから、**次へ**を選択します。
3. **Preparation** ウィンドウの情報を読んでから、**次へ**を選択します。
4. **Schema Preview** ウィンドウで**次へ**をクリックします。
5. **Setup** ウィンドウで、
   - ディレクトリサーバーの種類、名前、およびポートを入力します。
   - ディレクトリログイン情報と SSL の設定

   Results ウィンドウには、スキーマを拡張できたかどうかや変更された属性など、インストールの結果が表示されます。

Schema Extender で必要な情報

ディレクトリサーバー

- **タイプ** - ディレクトリサーバーのタイプ。
- **名前** - ディレクトリサーバーの名前。
- **ポート** - LDAP 通信に使用するポート。

ディレクトリログイン

- **ログイン名** - ディレクトリにログインするユーザーの名前。

  スキーマの拡張を完了するためにディレクトリユーザーの名前とパスワードが必要である場合があります。

  認証情報を入力するときに、`Administrator` ログインをドメイン名とともに使用する必要があります（例：`Administrator@domain.com` または `domain\Administrator`）。

  Active Directory でスキーマを拡張するには、ユーザーが認証されているスキーマ管理者でなければなりません。また、スキーマが書き込み禁止であってはなりません。さらに、そのディレクトリ

がツリー内で FSMO ロールオーナでなければなりません。インストーラーは、ターゲットディレクトリサーバーをフォレストの FSMO スキーママスターにしようとします。

- **パスワード** - ディレクトリにログインするためのパスワード。
- **Use SSL for this Session** - 使用する安全な認証の形式を設定します。このオプションを選択すると、SSL 経由でのディレクトリ認証が使用されます。このオプションを選択せず、Active Directory を選択すると、Windows 認証が使用されます。

ディレクトリサービスオブジェクト

ディレクトリベースの管理で大切なことの 1 つは、ディレクトリサービス内の管理対象デバイスを正しく仮想化することです。この仮想化によって、管理者は、ディレクトリサービス内の管理対象デバイスとユーザーまたはグループとを関連付けることができます。iLO のユーザー管理では、ディレクトリサービス内に以下の基本オブジェクトが必要です。

- Lights-Out Management オブジェクト
- Role オブジェクト
- User オブジェクト

各オブジェクトは、ディレクトリベースの管理に必要なデバイス、ユーザー、関連を意味します。

スナップインのインストール後、iLO オブジェクトと iLO ロールを、ディレクトリ内で作成できます。次のタスクは、Active Directory Users and Computers ツールを使用して行います。

- iLO オブジェクトとロールオブジェクトの作成
- ロールオブジェクトへのユーザーの追加
- ロールオブジェクトの権限と制限の設定

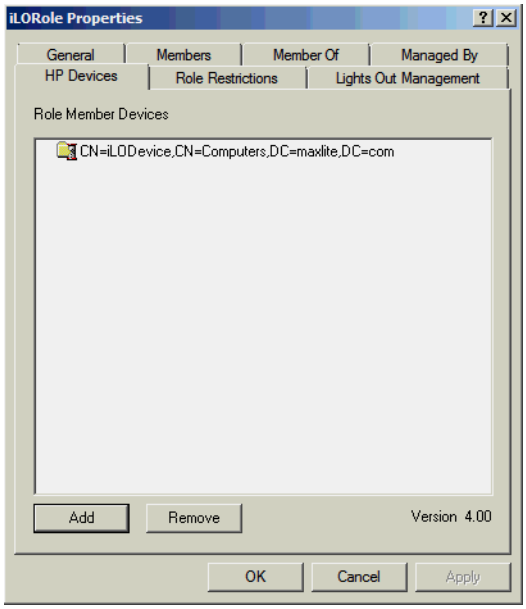
詳しくは

ディレクトリ対応リモート管理（HPE 拡張スキーマ構成）
組織構造に基づいたロール
ロールアクセス制限の適用方法
ユーザーアクセス制限
ロールアクセス制限
Active Directory と HPE 拡張スキーマの構成（構成例）
HPE Active Directory スナップインによって追加される管理オプション

HPE Active Directory スナップインによって追加される管理オプション

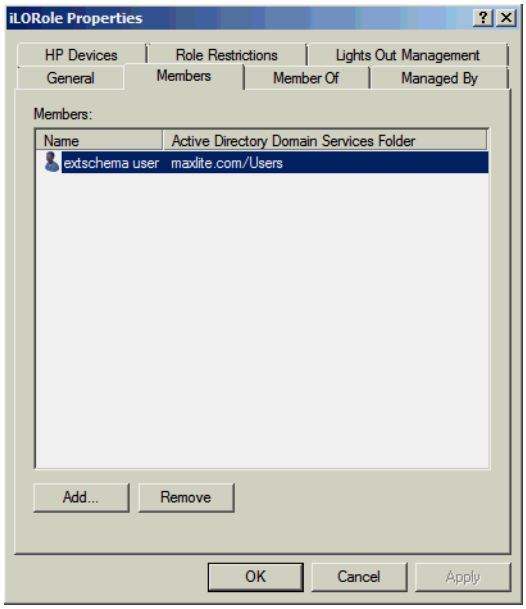
Hewlett Packard Enterprise スナップインをインストールした後、Active Directory ユーザーとコンピューターで次の管理オプションが使用できるようになります。

デバイスタブ



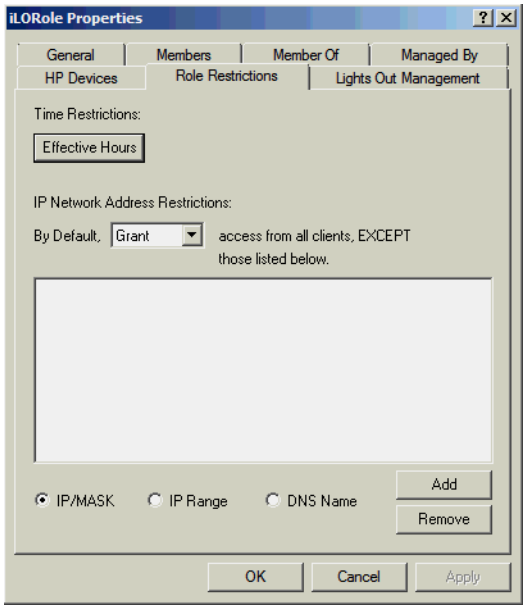
このタブでは、ロール内で管理する Hewlett Packard Enterprise デバイスを追加できます。**Add** をクリックすると、デバイスにアクセスして、そのデバイスをメンバーデバイスのリストに追加することができます。既存のデバイスを選択して、**Remove** をクリックすると、そのデバイスは有効なメンバーのデバイスリストから削除されます。

Members タブ



ユーザーオブジェクトが作成された後、このタブを使用してロール内でユーザーを管理できます。**Add** をクリックすると、追加するユーザーにアクセスできます。既存ユーザーを強調表示して、**Remove** をクリックすると、そのユーザーは有効なメンバーのリストから削除されます。

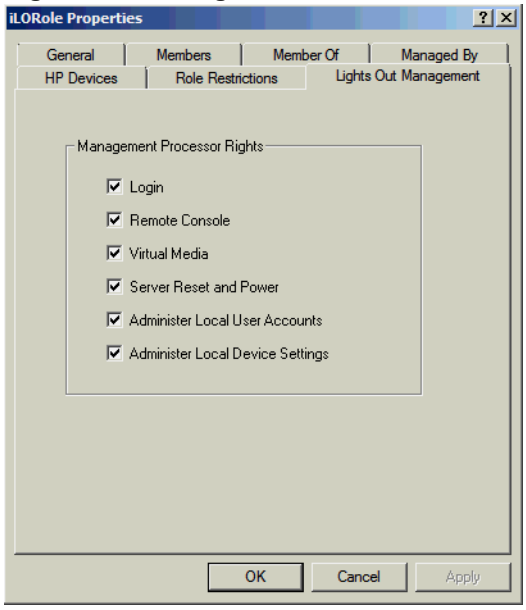
Role Restrictions タブ



このタブでは、以下のタイプのロールの制限を設定できます。

- Time restrictions - **Effective Hours** をクリックして、曜日ごとにログオンできる時間を 30 分単位で選択します。1 つの四角形を変更するには、クリックして変更できます。複数の四角形のボックスをまとめて変更するには、マウスボタンを押したまま、ボックス上でカーソルをドラッグして、マウスボタンを離してください。デフォルトでは、常時アクセスできるように設定されています。
- IP/マスク、IP 範囲、および DNS 名を含む IP ネットワークアドレス制限。

Lights Out Management タブ



ロールを作成した後で、このタブを使用してロールの権限を選択できます。ユーザーオブジェクトおよびグループオブジェクトをロールのメンバーにすることにより、ユーザーまたはユーザーグループにロールが付与する権限を与えることができます。

iLO に対するユーザー権限は、そのユーザーがメンバーとして所属し、その iLO が管理対象デバイスとなっているすべてのロールによって割り当てられたすべての権限の和とみなされます。**Active Directory 内で、iLO で使用するために、ディレクトリオブジェクトを作成して設定する**の例では、あるユーザーが

`remoteAdmins` ロールと `remoteMonitors` ロールの両方に所属する場合、`remoteAdmins` ロールがすべての権限を持っているため、そのユーザーは使用できるすべての権限を持つことになります。

使用できる権限は、次のとおりです。

- **Login** - 関連付けられたデバイスにユーザーがログインできるかどうかを制御します。
- **Remote Console** - ユーザーが iLO リモートコンソールにアクセスできるようにします。
- **Virtual Media** - ユーザーが iLO 仮想メディア機能にアクセスできるようにします。
- **Server Reset and Power** - ユーザーが iLO 仮想電源ボタンを使用できるようにします。
- **Administer Local User Accounts** - ユーザーがユーザーアカウントを管理できるようにします。ユーザーは、自身および他のユーザーのアカウント設定の変更、ユーザーの追加と削除を行うことができます。
- **Administer Local Device Settings** - ユーザーが iLO 管理プロセッサーを設定できるようにします。

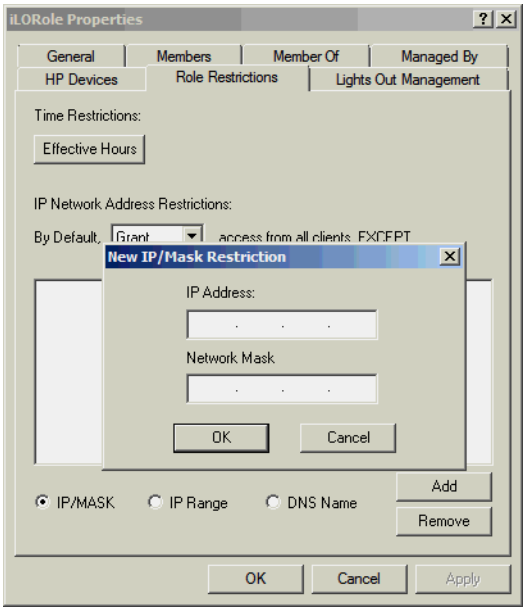
注記: システムリカバリ、ホスト NIC、ホストストレージ、およびホスト BIOS 権限は、Schema Extender で使用できません。

クライアント IP アドレスまたは DNS 名の制限の設定

手順

1. **Role Restrictions** タブ上の **By Default** リストで、指定した IP アドレスを除くすべてのアドレス、IP アドレス範囲、および DNS 名からのアクセスを、**許可する**か**取り消す**かを選択します。
2. 次の制限タイプのいずれかを選択し、**追加**をクリックします。
   - **DNS Name** - 単一の DNS 名またはサブドメインベースでアクセスを制限できます。入力は、`host.company.com` または`*.domain.company.com` という形式で行います。
   - **IP/MASK** - IP アドレスまたはネットワークマスクを入力できます。
   - **IP Range** - IP アドレス範囲 を入力できます。
3. 制限の設定ウィンドウで必要な情報を入力して、**OK** をクリックします。

   次の例では、**New IP/Mask Restriction** ウィンドウを示します。



4. **OK** をクリックします。

   変更が保存されると、**iLORole Properties** ダイアログボックスが閉じます。

ディレクトリ対応リモート管理（HPE 拡張スキーマ構成）

ディレクトリ対応リモート管理により、以下の作業を実行できます。

Lights-Out Management オブジェクトの作成

ディレクトリサービスを使用してユーザーの認証や権限付与を行うデバイスごとに、そのデバイスを表す LOM デバイスオブジェクトを 1 つ作成する必要があります。Hewlett Packard Enterprise スナップインを使用して LOM オブジェクトを作成することができます。

Hewlett Packard Enterprise は、LOM デバイスオブジェクトに意味のある名前を付けることをおすすめします。たとえば、デバイスのネットワークアドレス、DNS 名、ホストサーバー名、シリアル番号などを使用できます。

Lights-Out マネジメントデバイスの設定

ユーザーの認証や権限付与にディレクトリサービスを使用するすべての LOM デバイスは、適切なディレクトリ設定を使用して設定する必要があります。一般に、各デバイスを、適切なディレクトリサーバーアドレス、LOM オブジェクト DN、およびユーザーコンテキストを使用して設定します。サーバーアドレスは、ローカルディレクトリサーバーの IP アドレスまたは DNS 名です。冗長性を高くするために、マルチホスト DNS 名を使用できます。

組織構造に基づいたロール

組織内の管理者は、下級管理者が上級管理者から独立して権限を割り当てなければならない階層体制に属している場合があります。このような場合、上級管理者によって割り当てられる権限を表すロールを 1 つ作成するとともに、下級管理者が独自のロールを作成して管理することを許可すると便利です。

既存のグループの使用

多くの組織では、ユーザーや管理者をグループ分けしています。多くの場合、既存のグループを使用し、そのグループを 1 つまたは複数の LOM ロールオブジェクトに関連付けると便利です。デバイスがロールオブジェクトに関連付けられている場合、管理者は、グループのメンバーを追加または削除することによって、そのロールに関連付けられた Lights-Out デバイスへのアクセスを制御します。

Microsoft Active Directory を使用する場合は、あるグループを別のグループ内に配置できます（つまり、入れ子型のグループを使用できます）。ロールオブジェクトはグループとみなされ、他のグループを直接

含むことができます。既存の入れ子型グループを直接ロールに追加し、適切な権限と制限を割り当ててください。新しいユーザーを、既存のグループまたはロールのいずれかに追加できます。

トラスティまたはディレクトリ権限割り当てを使用してロールのメンバーシップを拡張する場合、ユーザーは、LOM デバイスを表す LOM オブジェクトを読み出すことができる必要があります。一部の環境では、正常なユーザー認証を行うために、ロールのトラスティが、オブジェクトの読み出すトラスティでもある必要があります。

複数のロールの使用

ほとんどのデプロイメントでは、同じユーザーが、同じデバイスを管理する複数のロールに入っている必要はありません。ただし、これらの構成は、複雑な権限関係を構築する際には便利です。ユーザーが複数のロールの関係を構築すると、そのユーザーには、該当する各ロールによって割り当てられるすべての権限が付与されます。ロールは、権限を付与することしかできず、権限を取り消すことはできません。あるロールがユーザーに権限を付与する場合、そのユーザーは、その権限を付与しない別のロールに入っていても、その権限を持ちます。

一般に、ディレクトリ管理者は、最小の数の権限が割り当てられたベースロールを作成し、追加のロールを作成して権限を追加します。これらの追加権限は、特定の状況で、またはベースロールユーザーの特定のサブセットに追加されます。

たとえば、組織は、LOM デバイスまたはホストサーバーの管理者と LOM デバイスのユーザーという 2 つのタイプのユーザーを持つことがあります。この状況では、管理者のロールとユーザーのロールという 2 つのロールを作成することが有効です。両方のロールにはいくつかの同じデバイスが含まれますが、これらのロールは異なる権限を付与します。より小さなロールに包括的な権限を割り当てて、LOM 管理者をそのロールと管理者ロールに入れると便利な場合があります。

<u>図 6: 複数の（重複する）ロール</u>には、管理者ユーザーがユーザーロールからログイン権限を取得し、管理者ロールから高度な権限が割り当てられる例を示します。

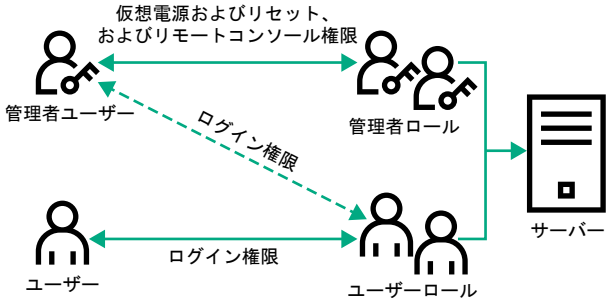


図 6: 複数の（重複する）ロール

重複するロールを使用しない場合は、<u>図 7: 複数の（独立した）ロール</u>に示すように、ログイン、仮想電源およびリセット、およびリモートコンソール権限を管理者ロールに割り当て、ログイン権限をユーザーロールに割り当てることがあります。

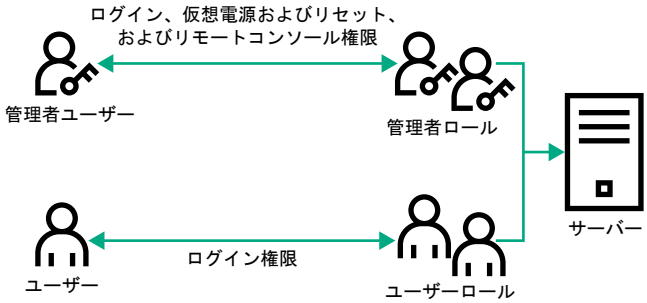


図 7: 複数の（独立した）ロール

ロールアクセス制限の適用方法

ディレクトリユーザーによる LOM デバイスへのアクセスは、2 段階の制限によって限定することができます。

- **ユーザーアクセス制限**は、ディレクトリへの認証を受けるためのユーザーアクセスを限定します。
- **ロールアクセス制限**は、1 つまたは複数のロールでの指定に基づいて LOM 権限を受けることができる認証済みユーザーの機能を限定します。

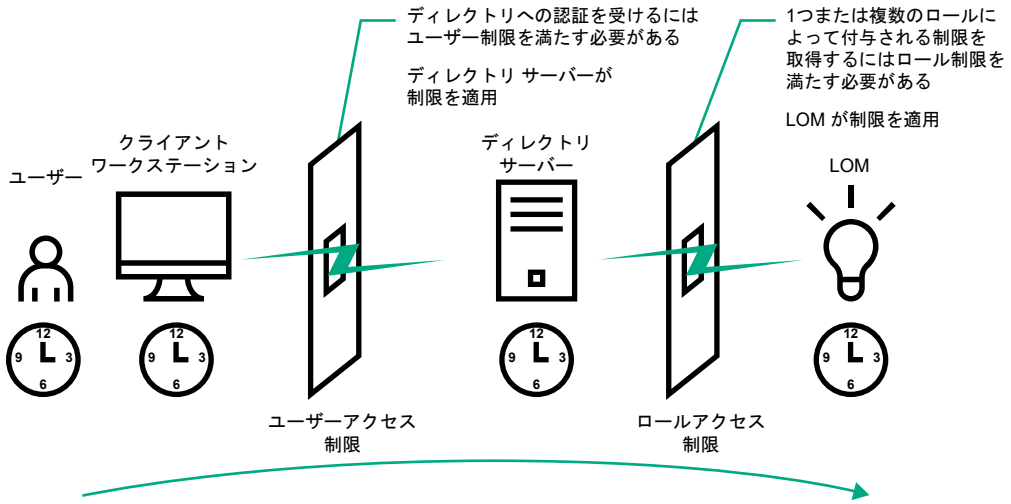


図 8: ディレクトリのログイン制限

ユーザーアクセス制限

アドレス制限

管理者は、ディレクトリユーザーアカウントにネットワークアドレス制限を設定できます。ディレクトリサーバーには、これらの制限が適用されます。

LDAP クライアント（LOM デバイスへのユーザーのログインなど）へのアドレス制限の適用について詳しくは、ディレクトリサービスのドキュメントを参照してください。

ディレクトリのユーザーに設定したネットワークアドレス制限は、ディレクトリユーザーがプロキシサーバー経由でログインする場合は、予期したとおりに適用されない場合があります。ユーザーがディレクトリユーザーとして LOM デバイスにログインする場合は、LOM デバイスが、そのユーザーとしてのディレクトリへの認証を試みます。つまり、ユーザーアカウントに設定されたアドレス制限が、LOM デバイスへのアクセス時に適用されます。プロキシサーバーが使用される場合は、認証が試みられるネットワークアドレスがクライアントワークステーションのものではなく、LOM デバイスのものになります。

IPv4 アドレス範囲制限

IP アドレス範囲制限によって、管理者は、アクセスを許可または拒否するネットワークアドレスを指定することができます。

アドレス範囲は、一般に、「最小-最大」範囲フォーマットで指定します。アドレス範囲を指定して、単一のアドレスのアクセスを許可または拒否することもできます。「最小-最大」IP アドレス範囲内のアドレスには、IP アドレス制限が適用されます。

IPv4 アドレスおよびサブネットマスク制限

IP アドレスおよびサブネットマスク制限によって、管理者は、アクセスを許可または拒否するアドレスの範囲を指定することができます。

このフォーマットは、IP アドレス範囲制限に似ていますが、ご使用のネットワーク環境によっては特有のものになる場合があります。IP アドレスおよびサブネットマスク範囲は、一般に、同じ論理ネットワーク上のアドレスを特定するサブネットアドレスおよびアドレスビットマスクによって指定します。

2 進数演算で、クライアントマシンのアドレスのビットにサブネットマスクのビットを加えたものが制限にあるサブネットアドレスと一致する場合、クライアントは制限を満たします。

DNS ベース制限

DNS ベース制限では、ネットワークネームサービスを使用して、クライアント IP アドレスに割り当てられたマシン名を検出することによって、クライアントマシンの論理名を調べます。DNS 制限には、正常に動作しているネームサーバーが必要です。ネームサービスがダウンしていたり、利用できなかったりすると、DNS 制限が満たされず、クライアントマシンは制限を満たすことができなくなります。

DNS ベース制限を使用すると、特定マシン名や、共通のドメインサフィックスを共有するマシンへのアクセスを制限できます。たとえば、**www.example.com** という DNS 制限は、**www.example.com** というドメイン名が割り当てられているホストによって満たされ、***.example.com** という DNS 制限は、**example** 社が提供元になっているすべてのマシンによって満たされます。

マルチホームホストを使用している場合があるので、DNS 制限では、あいまいさが発生する可能性があります。DNS 制限は、必ずしも単一のシステムに一対一で適用されるわけではありません。

DNS ベース制限を使用すると、セキュリティが複雑になる場合があります。ネームサービスプロトコルは、安全ではありません。ネットワークにアクセスできる悪意を持ったユーザーは、誰でも、不正な DNS サーバーをネットワークに配置して偽のアドレス制限基準を作成することができます。DNS ベースのアドレス制限を実装している場合は、組織的なセキュリティポリシーを考慮に入れてください。

ユーザーの時間制限

時間制限によって、ディレクトリへのユーザーのログイン（認証）が限定されます。通常、時間制限は、ディレクトリサーバーの時間を使用して適用されます。ディレクトリサーバーが異なるタイムゾーンにある場合または異なるタイムゾーンにあるレプリカサーバーにアクセスしている場合は、管理対象オブジェクトからのタイムゾーン情報を使用して相対的な時間を調整することができます。

ディレクトリサーバーは、ユーザーの時間制限を確認しますが、判定方法は、タイムゾーンの変化や認証メカニズムによって複雑になる場合があります。

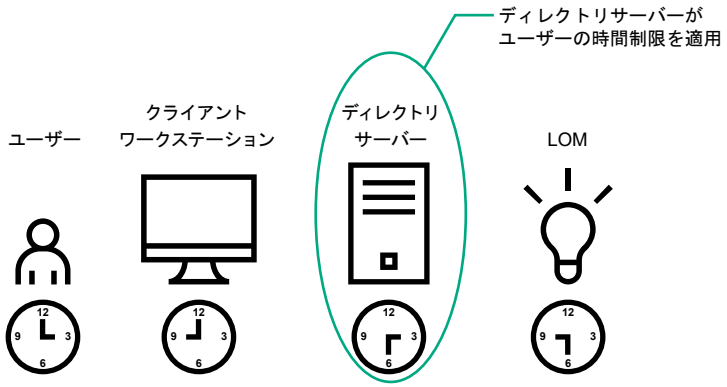


図 9: ユーザーの時間制限

ロールアクセス制限

制限によって、管理者は、ロールの範囲を限定することができます。ロールは、ロールの制限を満たすユーザーだけに権限を付与します。制限付きロールを使用することによって、ユーザーに、時間帯やクライアントのネットワークアドレスによって変化する動的権限を付与することができます。

ディレクトリが有効な場合、iLO システムへアクセス可能かどうかは、該当する iLO オブジェクトを含むロールオブジェクトへの読み取りアクセス権が、ユーザーにあるかどうかによって決まります。このユーザーには、ロールオブジェクトで許可されているメンバーも含まれますが、そのメンバーに限定されませ

ん。継承可能な権限を親から伝達できるようにロールを設定すると、読み出し権限を持つ親のメンバーも iLO にアクセスできます。

アクセス制御リストを表示するには、**Active Directory Users and Computers** に移動し、ロールオブジェクトの**プロパティ**ページを開き、**セキュリティ**タブをクリックします。**セキュリティ**タブを表示するには、MMC で Advanced View を有効にする必要があります。

ロールベースの時間制限

管理者は、LOM ロールに時間制限を設定することができます。ユーザーには、そのユーザーがロールのメンバーであり、そのロールの時間制限を満たしている場合にのみ、そのロールに示されている LOM デバイスについて、指定された権限が付与されます。

ロールベースの時間制限は、LOM デバイスで時間が設定されている場合にのみ、機能します。LOM デバイスは、ローカルホストの時間に従って、時間制限を適用します。LOM デバイスの時計が設定されていない場合、ロールに対して時間制限が指定されていない限り、ロールベースの時間制限は適用されません。時間は、通常、ホストの起動時に設定されます。

時間設定は、SNTP を設定することで維持できます。SNTP によって、LOM デバイスでうるう年を補正することや、ホストとの時間のずれを最小限に抑えることができます。予定外の停電や LOM ファームウェアのフラッシュなどのイベントによって、LOM デバイスの時計が設定されないことがあります。また、LOM デバイスがファームウェアをフラッシュする時間の設定を保持するために、ホストの時間は正確でなければなりません。

ロールベースのアドレス制限

LOM ファームウェアでは、クライアントの IP ネットワークアドレスに基づいてロールベースのアドレス制限が適用されます。ロールのアドレス制限が満たされる場合、そのロールによって付与される権利が適用されます。

ファイアウォールの外からのアクセスやネットワークプロキシ経由のアクセスが試みられる場合、アドレス制限は、管理が困難になる場合があります。これらの方式のアクセスが可能な場合、クライアントの見かけ上のネットワークアドレスが変更されることがあるので、アドレス制限の予期しない適用が発生する場合があります。

複数の制限およびロール

権限の適用される状況が限定されるように 1 つまたは複数のロールを制限したい場合には、多数のロールを作成すると非常に便利です。他のロールが、異なる権限を異なる制限で付与します。複数の制限とロールを使用すると、管理者は、任意の複雑な権限関係を最小限のロールで作成できます。

たとえば、組織が、LOM 管理者について、「企業ネットワーク内から LOM デバイスを使用できるが通常の業務時間外にはサーバーのリセットしかできない」というセキュリティポリシーを設定しているとします。

ディレクトリ管理者は、2 つのロールを作成してこの状況に対応しようと考えるかもしれませんが、この場合には特別の注意が必要です。必要なサーバーリセット権限を付与するロールを作成し、このロールを業務時間外に制限すると、管理者が企業ネットワークの外からサーバーをリセットできるようになる場合があり、多くの場合セキュリティポリシーに反します。

図 10: 制限およびロールの作成では、セキュリティポリシーで、一般的な使用を企業サブネット内のクライアントに制限しており、サーバーリセット操作を業務時間外に制限していることを示しています。

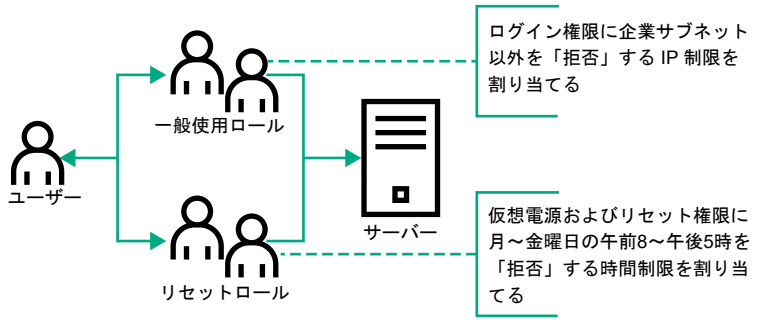


図 10: 制限およびロールの作成

また、ディレクトリ管理者は、ログイン権限を付与するロールを作成し、このロールを企業ネットワークに制限した後、サーバーリセット権限だけを付与する別のロールを作成し、これを業務時間外に制限しようと考えるかもしれません。この設定では管理が簡単になりますが、継続的な管理によって企業ネットワーク外部のアドレスからのユーザーにログイン権限を付与する別のロールが作成される場合があるため、危険性が増します。サーバーリセットロールに属する LOM 管理者がロールの時間制限を満たす場合、このロールは意図せずに、この LOM 管理者にどこからでもサーバーをリセットできる権限を付与する可能性があります。

図 10: 制限およびロールの作成に示されている設定は、企業のセキュリティ要件を満たしています。ただし、ログイン権限を付与する別のロールを追加することによって、間違って、業務時間外に企業サブネットの外からサーバーをリセットする権限を付与する可能性があります。**図 11: リセットロールと一般使用ロールの制限**で示すように、リセットロールと一般使用ロールを制限することによって、より管理しやすいソリューションを実現できます。

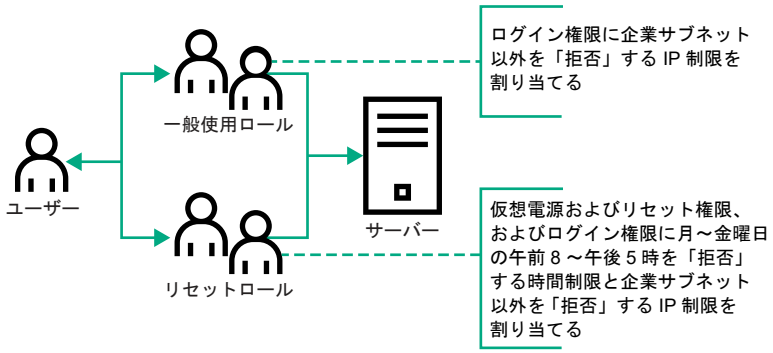


図 11: リセットロールと一般使用ロールの制限

Active Directory と HPE 拡張スキーマの構成（構成例）

この手順では、HPE 拡張スキーマを使用して Active Directory を構成する方法の例を示します。

手順

1. **ご使用の環境が HPE Active Directory と拡張スキーマを構成するための前提条件を満たしていることを確認します**。
2. **ディレクトリサービス認証を有効にする iLO ライセンスをインストールします**。
3. **iLO ディレクトリサポートソフトウェアをインストールします。**
4. **Schema Extender を使用してスキーマを拡張します。**
5. **デバイスオブジェクトとロールオブジェクトを設定します**。

6. iLO にログインし、ディレクトリページで、ディレクトリ設定を入力します。
7. iLO ネットワーク設定の IPv4 または IPv6 のページで、正しい DNS サーバーが指定されていることを確認します。

Active Directory 内で、iLO で使用するために、ディレクトリオブジェクトを作成して設定する

次の例は、ドメイン **testdomain.local** があるエンタープライズディレクトリでロールと Hewlett Packard Enterprise デバイスをセットアップする方法を示します。このドメインは、2 つの組織単位（**Roles** および **iLOs**）で構成されます。このセクションの手順は、Hewlett Packard Enterprise Active Directory Users and Computers スナップインを使用して完了します。

手順

1. iLOs 組織単位を作成し、LOM オブジェクトを追加します。
2. Roles 組織単位を作成し、ロールオブジェクトを追加します。
3. ロールに権限を割り当て、ロールをユーザーおよびデバイスと関連付けます。

詳しくは

HPE Active Directory スナップインによって追加される管理オプション
ディレクトリサービスオブジェクト

iLOs 組織ユニットの作成および LOM オブジェクトの追加

手順

1. ドメインによって管理される iLO デバイスを含む、**iLOs** という組織単位を作成します。
2. **testdomain.local** ドメイン内にある組織単位 **iLOs** を右クリックして、**New HP Object** を選択します。
3. **新しいオブジェクトの作成**ダイアログボックスで、**デバイス**を選択します。
4. **Name** ボックスに該当する名前を入力します。

   この例では、iLO デバイスの DNS ホスト名 **rib-email-server** が Lights-Out Management オブジェクト名として使用されます。
5. **OK** をクリックします。

Roles 組織ユニットの作成およびロールオブジェクトの追加

手順

1. **Roles** という組織単位を作成します。
2. **Roles** 組織単位を右クリックし、**New HP Object** を選択します。
3. **新しい管理オブジェクトの作成**ダイアログボックスで、**役割**を選択します。
4. **Name** ボックスに該当する名前を入力します。

   この例では、ロールには、リモートサーバーの管理を行うことのできる信頼されるユーザーを所属させるので、**remoteAdmins** と名付けます。

5. **OK** をクリックします。
6. 手順を繰り返して、リモートサーバーの監視を行う **remoteMonitors** という名前のロールを作成します。

ロールへの権限の割り当てとロールのユーザーおよびデバイスへの関連付け

手順

1. **testdomain.local** ドメインの **Roles** 組織単位の **remoteAdmins** ロールを右クリックして、**Properties** を選択します。
2. **remoteAdmins Properties** ダイアログボックスで、**HP Devices** タブをクリックし、**Add** をクリックします。
3. **Select Users** ダイアログボックスで、**testdomain.local/iLOs** フォルダーに作成した Lights-Out Management オブジェクト **rib-email-server** を入力します。
4. **OK** をクリックして、**Apply** をクリックします。
5. **Members** タブをクリックし、**Add** ボタンを使用してユーザーを追加します。
6. **OK** をクリックして、**Apply** をクリックします。

   これで、デバイスとユーザーが関連付けられます。
7. **Lights Out Management** タブをクリックします。

   ロールに所属するすべてのユーザーとグループが、ロールによって管理されるすべての iLO デバイス上でロールに割り当てられた権限を所有します。
8. 各権限の横のチェックボックスを選択して、**適用**をクリックします。

   この例では、**remoteAdmins** ロール内のユーザーに iLO の機能へのフルアクセス権限が付与されます。
9. **OK** をクリックします。
10. **remoteMonitors** ロールを編集するには、手順を繰り返します。

    a. **HP Devices** タブのリストに、**rib-email-server** デバイスを追加します。

    b. **Members** タブの **remoteMonitors** ロールにユーザーを追加します。

    c. **Lights Out Management** タブで、**Login** 権限を選択します。

       この権限を設定すると、**remoteMonitors** ロールのメンバーは、サーバーステータスへのアクセスの認証を受けることができ、サーバーステータスを表示できます。

iLO の構成および Lights-Out Management オブジェクトとの関連付け

手順

ディレクトリページで、次のような設定を入力します。

```
LOM Object Distinguished Name = cn=rib-email-
server,ou=ILOs,dc=testdomain,dc=local Directory User Context 1 =
cn=Users,dc=testdomain,dc=local
```

詳しくは

iLO における HPE 拡張スキーマディレクトリ設定の構成

ディレクトリサービスによるユーザーログイン

iLO のログインページの **Login Name** ボックスでは、ディレクトリユーザーとローカルユーザーを受け入れます。

ログイン名の最大長は、ローカルユーザーの場合が 39 文字、ディレクトリユーザーの場合が 127 文字です。

（ブレードサーバー上の）診断ポート経由で接続すると、Zero サインインおよびディレクトリユーザーログインがサポートされず、ローカルアカウントを使用する必要があります。

ディレクトリユーザー

次の形式がサポートされています。

- LDAP 完全識別名（Active Directory と OpenLDAP）

  例：`CN=John Smith,CN=Users,DC=HPE,DC=COM`、または`@HPE.com`

  ログイン名の短い形式は、アクセスしようとしているドメインをディレクトリに通知しません。ドメイン名を入力するか、またはアカウントの LDAP DN を使用します。

- ドメイン\ユーザー名**形式**（Active Directory）

  例：`HPE\jsmith`

- ユーザー名@ドメイン**形式**（Active Directory）

  例：`jsmith@hpe.com`

  @検索可能形式を使用して指定されるディレクトリユーザーは、3 つの検索可能コンテキストのいずれかに配置できます。このコンテキストは、**ディレクトリ**ページで構成します。

- **ユーザー名形式**（Active Directory）

  例：John Smith

  ユーザー名形式を使用して指定されるディレクトリユーザーは、3 つの検索可能コンテキストのいずれかに配置できます。このコンテキストは、**ディレクトリ**ページで構成します。

ローカルユーザー

iLO ローカルユーザーアカウントのログイン名を入力します。

一度に複数の iLO システムを構成するためのツール

Kerberos 認証およびディレクトリサービスに多数の LOM オブジェクトを構成すると時間がかかります。次のユーティリティを使用すると、一度に複数の LOM オブジェクトを構成できます。

ProLiant 管理プロセッサー用のディレクトリサポート

このソフトウェアには、多数の管理プロセッサーを使用した Kerberos 認証およびディレクトリサービスを構成する段階的なアプローチを提供する GUI が含まれています。Hewlett Packard Enterprise は、複数の管理プロセッサーを構成するときに、このツールを使用することをおすすめします。

従来のインポートユーティリティ

LDIFDE や NDS Import/Export Wizard などのツールを熟知している管理者は、これらのユーティリティを使用して、LOM デバイスディレクトリオブジェクトをインポートまたは作成できます。管理者はデバイスを手動で構成する必要がありますが、いつでもこの構成を行うことができます。プログラマチックインターフェイスまたはスクリプティングインターフェイスを使用して、LOM デバイスオブジェクトをユーザーオブジェクトや他のオブジェクトと同じように作成できます。LOM オブジェクトを作成する際の属性や属性データフォーマットについては、ディレクトリサービススキーマを参照してください。

詳しくは

ディレクトリサービススキーマ
HPLOMIG によるディレクトリ認証の設定
ProLiant 管理プロセッサー用のディレクトリサポート（HPLOMIG）

ProLiant 管理プロセッサー用のディレクトリサポート（HPLOMIG）

HPLOMIG は、iLO プロセッサーをディレクトリによる管理に簡単に移行したいお客様向けです。このソフトウェアは、管理プロセッサーがディレクトリサービスをサポートするために必要な手順の一部を自動化します。

HPLOMIG は、次の Web サイトで入手できます。**https://www.hpe.com/support/ilo5**

オペレーティングシステムのサポート

HPLOMIG は、Microsoft Windows で動作し、Microsoft .NET Framework バージョン 3.5 以降を必要とします。次のオペレーティングシステムがサポートされています。

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

要件

拡張セキュリティ機能（FIPS、CNSA、または高セキュリティセキュリティ状態など）を HPLOMIG を使用して iLO システムで構成できるようになっている場合、HPLOMIG クライアントは以下の要件を満たす必要があります。

- Windows .NET Framework v4.5 がインストールされている。
- オペレーティングシステムで TLS v1.1 または v1.2 がサポートされている。

HPLOMIG を使用する場合の OS および Windows .NET Framework の要件を次の表に示します。

オペレーティングシステム	Windows .NET Framework	iLO で製品セキュリティ状態が有効になっている HPLOMIG。	iLO で高セキュリティ、FIPS、または CNSA セキュリティ状態が有効になっている HPLOMIG。
Windows Server 2008[1]	4.0 またはそれ以前	サポート	未サポート
	4.5	サポート	未サポート
Windows 7 Windows Server 2008 R2	4.0 またはそれ以前	サポート	未サポート
	4.5	サポート	サポート
Windows 8 Windows 8.1 Windows 10 Windows Server 2012 Windows Server 2012 R2 Microsoft Windows Server 2016 Microsoft Windows Server 2019	4.0 またはそれ以前	サポート	未サポート
	4.5	サポート	サポート

[1] NET Framework バージョン 4.5 がインストールされている場合でも、Windows Server 2008 では、TLS v1.1 または v1.2 はサポートされません。

HPLOMIG によるディレクトリ認証の設定

手順

1. **ネットワーク内の iLO マネジメントプロセッサーを検出します。**
2. **（オプション）マネジメントプロセッサーで iLO ファームウェアをアップデートします。**
3. **ディレクトリ構成設定を指定します。**
4. ご使用の構成に固有の手順を完了します。
   a. **マネジメントプロセッサーに名前を付けます（HPE 拡張スキーマのみ）**
   b. **ディレクトリを構成します（HPE 拡張スキーマのみ）**
   c. **デフォルトスキーマを使用するようにマネジメントプロセッサーを設定します（スキーマフリーのみ）**
5. **iLO とディレクトリの間の通信を設定します。**

6. LDAP CA 証明書をインポートします。
7. （オプション）iLO ディレクトリテストを実行します。

管理プロセッサーの検出

手順

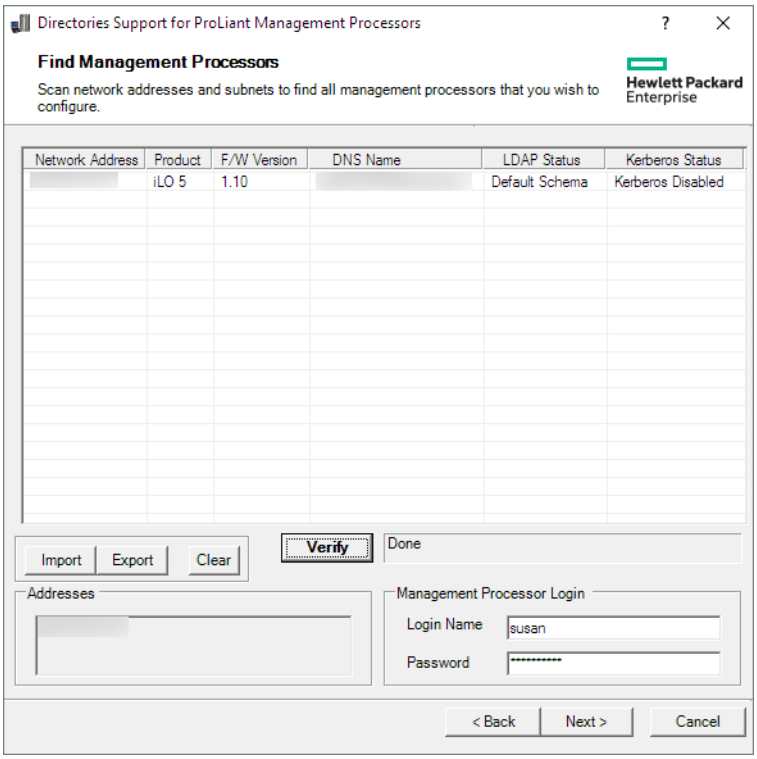
1. **スタート** > **すべてのプログラム** > **Hewlett-Packard Enterprise** > **ProLiant マネジメントプロセッサー用のディレクトリサポート**の順に選択します。
2. **ようこそ**ページで、**Next** をクリックします。
3. **Find Management Processors** ウィンドウで、**Addresses** ボックスに、管理プロセッサーの検索条件を入力します。

   ヒント: また、**Import** をクリックしてからファイルを選択して、ファイルから管理プロセッサーのリストを入力することもできます。

4. iLO の Login Name と Password を入力して、**Find** をクリックします。

   検出時に**次へ**や **Back** をクリックするかユーティリティを終了すると、現在のネットワークアドレスでの作業は完了しますが、次のネットワークアドレスでの作業はキャンセルされます。

   検索が完了すると、管理プロセッサーが表示され、**Find** ボタンが **Verify** に変化します。



HPLOMIG 管理プロセッサーの検索条件

DNS 名、IP アドレス、または IP アドレスワイルドカードを使用して管理プロセッサーを検索することができます。

Addresses ボックスに値を入力する場合、以下のルールが適用されます。

- DNS 名、IP アドレス、および IP アドレスワイルドカードは、セミコロンまたはカンマのいずれかで区切る必要があり、区切り文字として両方を使用することはできません。
- IP アドレスワイルドカードでは、3 番目と 4 番目のオクテットフィールドでアスタリスク（*）文字を使用します。たとえば、`16.100.*.*`という IP アドレスは有効ですが、`16.*.*.*`という IP アドレスは無効です。
- ハイフンを使用して範囲を指定することができます。たとえば、`192.168.0.2-10` は有効な範囲です。ハイフンは、一番右のオクテットフィールドでのみ使用できます。
- **Find** をクリックすると、HPLOMIG は、ping とポート 443（デフォルト SSL ポート）への接続を開始します。この動作の目的は、ターゲットネットワークアドレスが管理プロセッサーであるかどうかを判定することです。ping に対するデバイスからの応答がなく、ポート 443 に適切に接続できなかった場合、ユーティリティは、ターゲットが管理プロセッサーではないと判定します。

HPLOMIG マネジメントプロセッサーのインポートリストの要件

各行に 1 つのマネジメントプロセッサーを記載した単純なテキストファイルをインポートできます。

セミコロンで区切られた、サポートされる各列は次のとおりです。

- Network Address
- Product
- F/W Version
- DNS Name
- TPM Status
- User Name
- Password
- LDAP Status
- Kerberos Status
- License Type
- FIPS Status

たとえば、テキストファイルのある行に次の情報が含まれる場合があります。

```
16.100.225.20;iLO;1.10;ILOTPILOT2210;Not Present;user;password;Default
Schema;Kerberos Disabled;iLO Advanced;Enabled
```

ユーザー名とパスワードを（セキュリティ上の理由で）ファイル内に含めることができない場合は、それらの列を空白にして、セミコロンだけを入れてください。

（オプション）管理プロセッサーのファームウェアのアップグレード（HPLOMIG）

Find Management Processors ウィンドウの**次へ**をクリックしたら、次のタスクは、必要に応じて iLO ファームウェアをアップデートすることです。選択した管理プロセッサーの数によっては、アップグレードプロセスに長い時間がかかる場合があります。単一の管理プロセッサーのファームウェアアップグレードは、約 5 分で完了します。

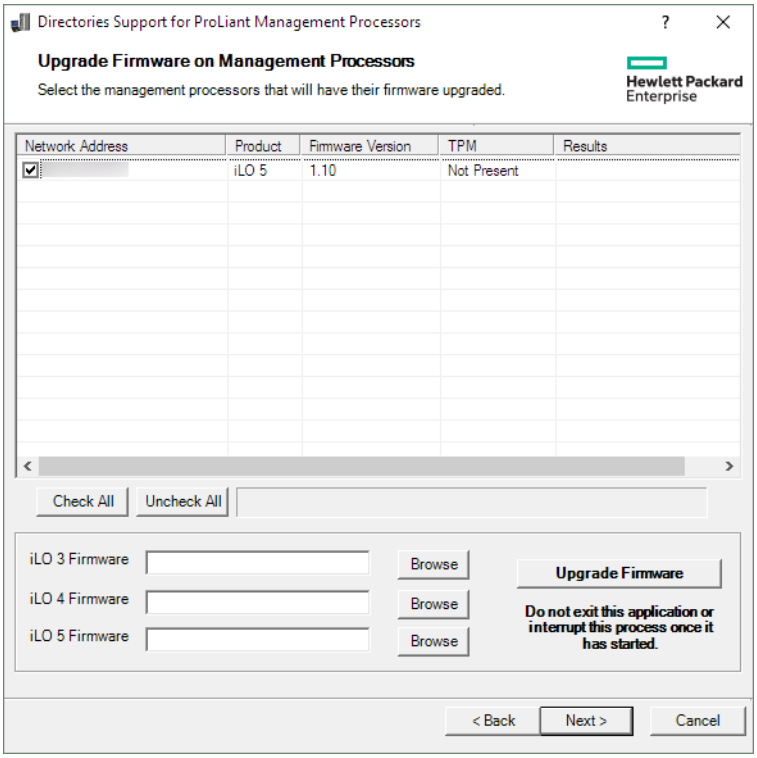
重要: Hewlett Packard Enterprise は、本番環境ネットワークで HPLOMIG を実行する前に、テスト環境でアップグレードプロセスをテストし、結果を確認することをおすすめします。管理プロセッサーへのファームウェアイメージの不完全な転送によって、管理プロセッサーをローカルで再プログラミングしなければならなくなる場合があります。

前提条件

管理プロセッサーのファームウェアのバイナリイメージは、HPLOMIG を実行しているシステムからアクセスできる必要があります。これらのバイナリイメージは **https://www.hpe.com/support/ilo5** からダウンロードできます。

手順

1. **Upgrade Firmware on Management Processors** ウィンドウがまだ開いていない場合は移動します。



2. アップグレードするマネジメントプロセッサーを選択します。
3. 選択した管理プロセッサーごとに、**参照**をクリックし、ファームウェアイメージファイルを選択します。また、手動でファームウェアイメージのパスを入力することもできます。
4. **ファームウェアのアップグレード**をクリックします。

   ファームウェアアップグレードプロセス時は、すべてのボタンが非アクティブになり、操作できません。

   選択したマネジメントプロセッサーがアップグレードされます。HPLOMIG を使用すると、数百の管理プロセッサーをアップグレードできますが、同時にアップグレードできるのは最大 25 の管理プロセッサーです。このプロセス時には、大量のネットワーク動作が発生します。

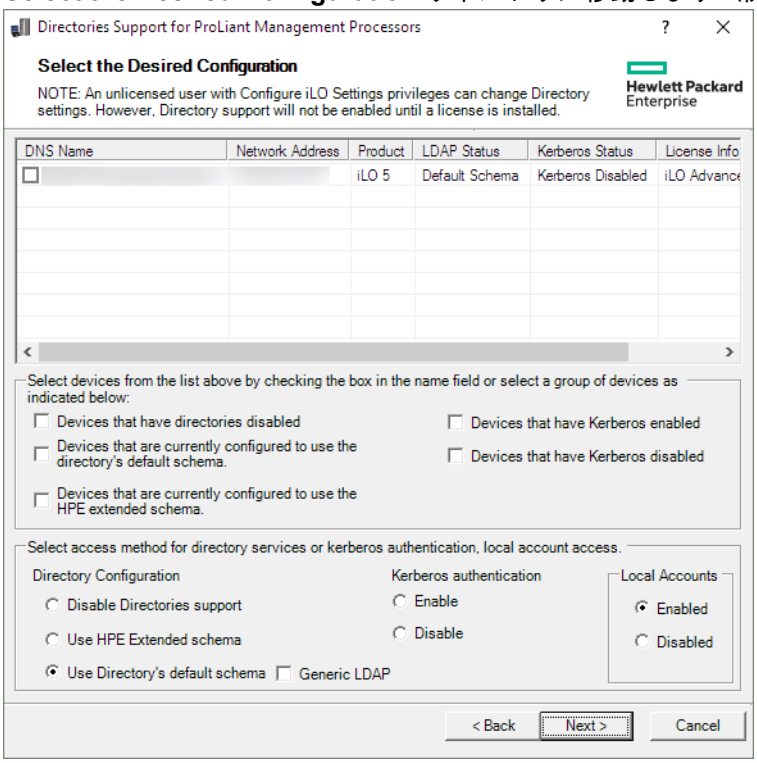
   アップグレードに失敗すると、**Results** 欄にメッセージが表示され、ユーティリティは、選択された他の管理プロセッサーのアップグレードを継続します。
5. アップグレードが完了したら、**Next** をクリックします。

ディレクトリ構成オプションの選択

Upgrade Firmware on Management Processors ウィンドウで**次へ**をクリックした後の次のタスクは、構成する管理プロセッサーの選択と有効にするディレクトリオプションの指定です。

手順

1. **Select the Desired Configuration** ウィンドウに移動します（開いていない場合）。



2. 構成する iLO 管理プロセッサーを選択します。
3. （オプション）選択フィルターを使用して、Kerberos 認証またはディレクトリサービス用にすでに構成されている iLO 管理プロセッサーを除外します。Kerberos 認証とディレクトリサービスが無効になっている管理プロセッサーを除外することもできます。
4. **Directory Configuration**、**Kerberos authentication**、および **Local accounts** セクションで、ディレクトリ、Kerberos、およびローカルアカウントの設定を選択します。
5. **次へ**をクリックします。

   このページでの選択によって、**次へ**をクリックしたときに表示されるウィンドウが決まります。
6. スキーマフリー構成を選択した場合は、**管理プロセッサーの設定（スキーマフリー構成のみ）**に進みます。HPE 拡張スキーマ構成を選択した場合は、**マネジメントプロセッサーの命名（HPE 拡張スキーマのみ）**を続行します。

管理プロセッサーの選択方法

次の方法で構成する iLO 管理プロセッサーを選択します。

- 構成するリスト内の各管理プロセッサーの横のチェックボックスをクリックします。
- 特定のステータスに一致する iLO 管理プロセッサーを選択するには、次のいずれかのフィルターの横にあるチェックボックスをクリックします。

- **Devices that have directories disabled**
- **Devices that are currently configured to use the directory’s default schema**
- **Devices that are currently configured to use the HPE Extended Schema**
- **Devices that have Kerberos enabled**
- **Devices that have Kerberos disabled**

ディレクトリアクセス方法および設定

- **Disable Directories support** - 選択したシステムでディレクトリサポートを無効にします。
- **Use HPE Extended Schema** - 選択したシステムのディレクトリで HPE 拡張スキーマを使用します。
- **Use Directory’s default schema** - 選択したシステムでスキーマフリーディレクトリを使用します。
- **Generic LDAP** - 選択したシステムで OpenLDAP がサポートする BIND 方式を使用します。
- **Kerberos authentication** - 選択したシステムで Kerberos 認証を有効または無効にします。
- **Local Accounts** - 選択したシステムでローカルユーザーアカウントを有効または無効にします。

マネジメントプロセッサーの命名（HPE 拡張スキーマのみ）

Select the Desired Configuration ウィンドウの**次へ**をクリックしたら、次のタスクはディレクトリ内の iLO 管理デバイスオブジェクトに名前を付けることです。

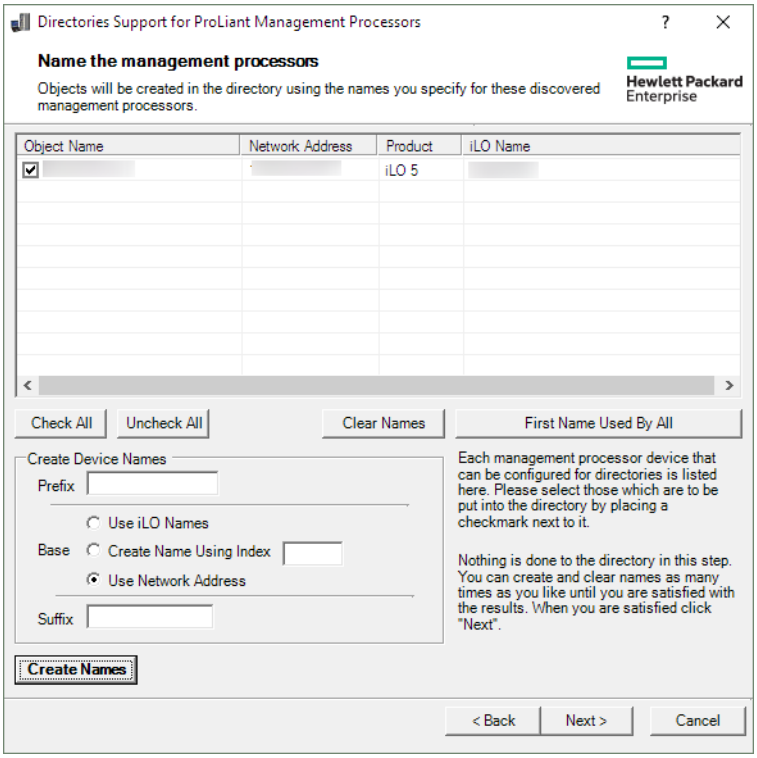
以下の 1 つまたは複数のコンポーネントを使用して名前を作成できます。

- ネットワークアドレス
- DNS 名
- インデックス
- 名前の手動作成
- すべてにプレフィクスを追加
- すべてにサフィックスを追加

マネジメントプロセッサーに名前を付けるには、**Object Name** 列をクリックして名前を入力するか、以下の手順に従ってください。

手順

1. **Use iLO Names**、**Create Name Using Index**、または **Use Network Address** を選択します。
2. （オプション）すべての名前の先頭または末尾に追加するテキストを入力します。
3. **Create Names** をクリックします。



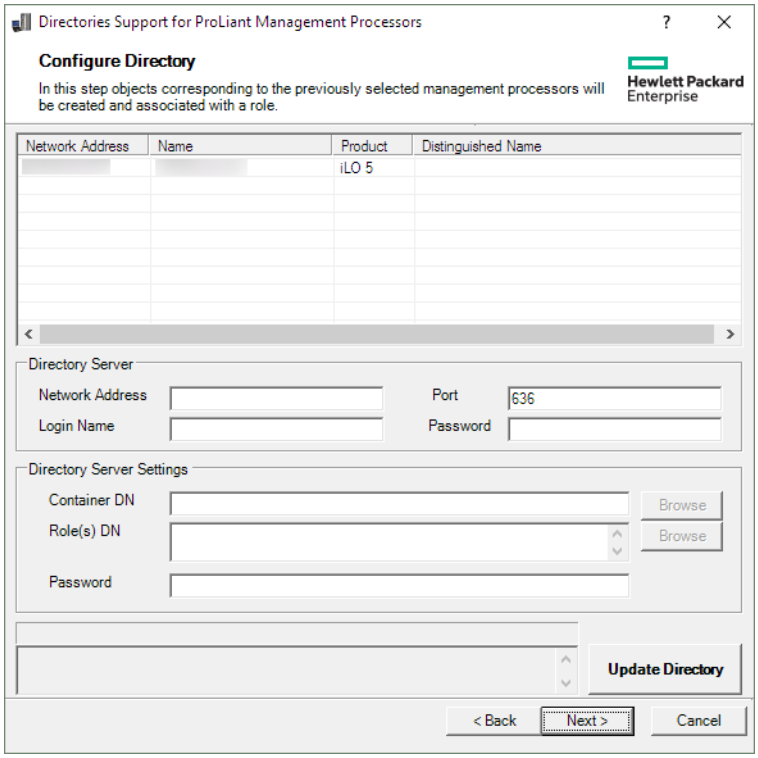
生成された名前が **Object Name** 欄に表示されます。この時点では、名前は、ディレクトリやマネジメントプロセッサーに書き込まれていません。名前は、次の ProLiant マネジメントプロセッサー用のディレクトリサポートウィンドウが表示されるまで保存されます。

4. （オプション）名前を変更するには、**Clear Names** をクリックしてマネジメントプロセッサーの名前を修正します。
5. 名前が正しい場合は、 **Next** をクリックします。

   Configure Directory ウィンドウが開きます。 **HPE 拡張スキーマを選択したときのディレクトリの設定**に進みます。

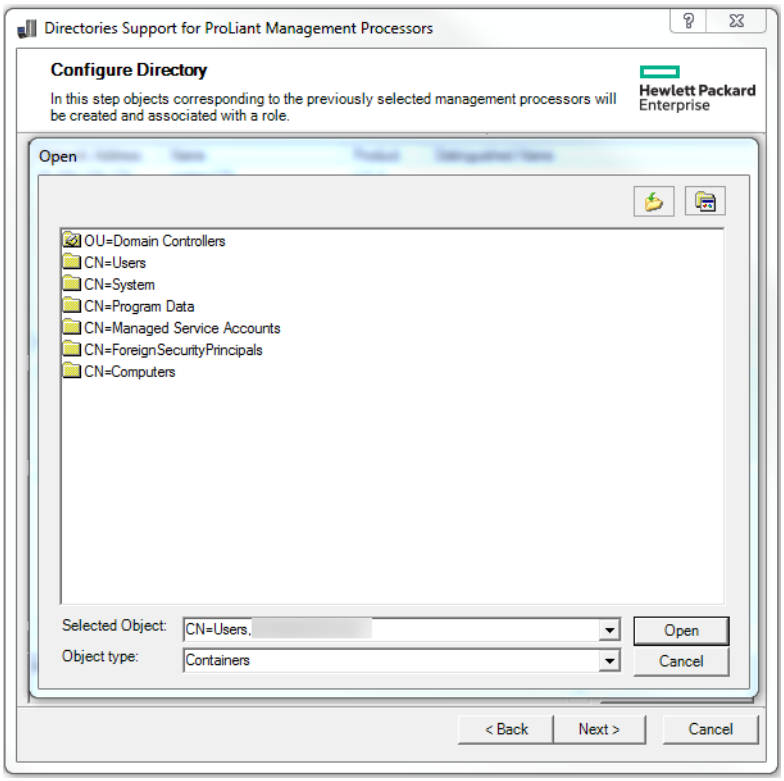
HPE 拡張スキーマを選択したときのディレクトリの設定

Name the management processors ウィンドウで **Next** をクリックした後、**Configure Directory** ウィンドウでは、検出された各管理プロセッサー用のデバイスオブジェクトを作成し、新しいデバイスオブジェクトを定義済みのロールに関連付けることができます。たとえば、ディレクトリは、ユーザーを、特定のデバイスオブジェクトに対するいくつかの権限を持つロール（管理者など）のメンバーとして定義します。

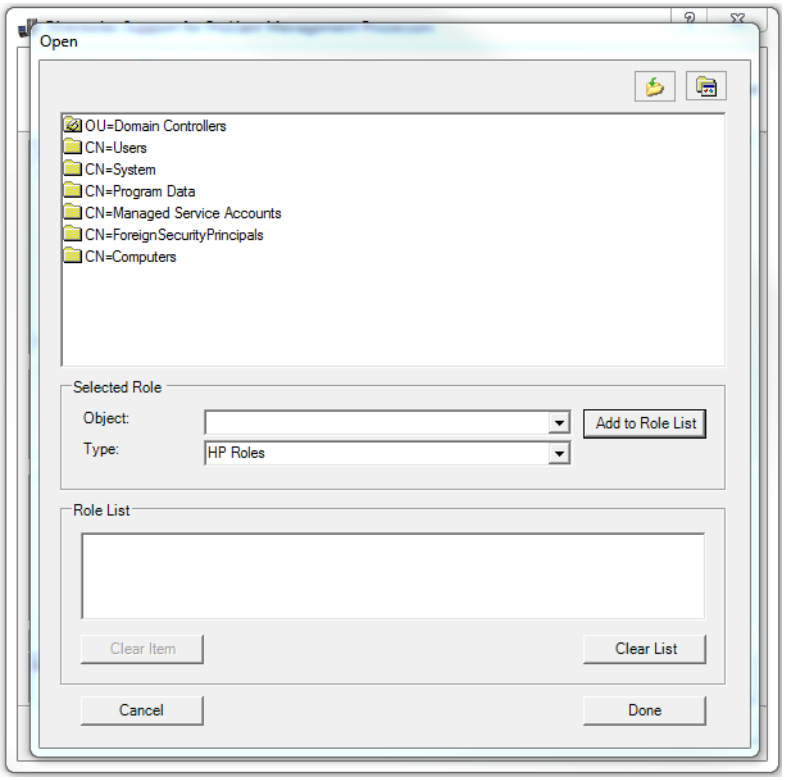


手順

1. **Directory Server** セクションで、指定されたディレクトリサーバーの **Network Address**、**Login Name**、および **Password** を入力します。
2. **Container DN** の値を入力するか、**Browse** をクリックしてコンテナー DN を選択します。



3. **Role(s) DN** の値を入力するか、**Browse** をクリックしてロール DN を選択します。

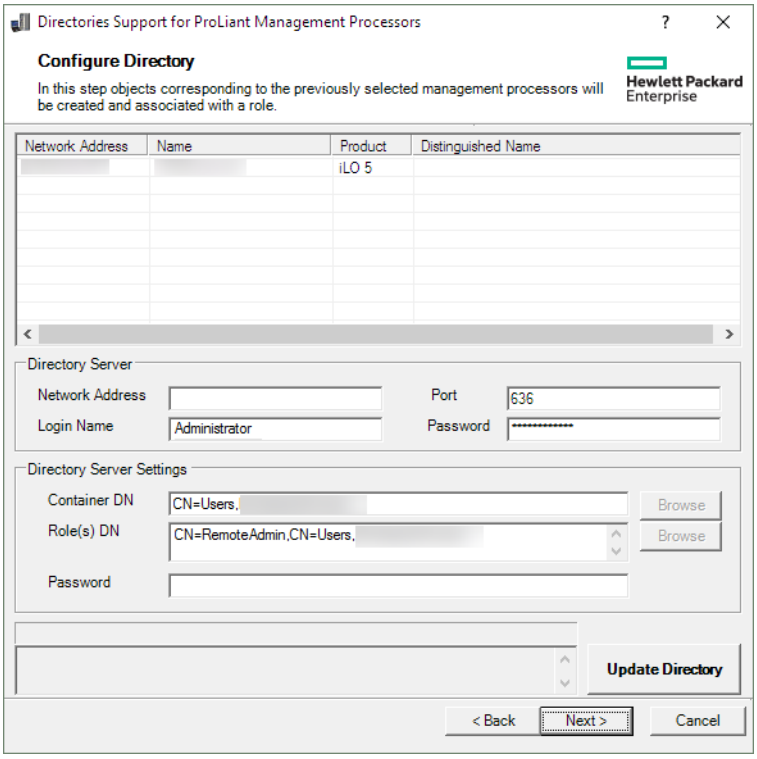


4. **Update Directory** をクリックします。

   HPLOMIG は、ディレクトリに接続し、管理プロセッサーオブジェクトを作成して、それらを選択されたロールに追加します。

5. デバイスオブジェクトがロールに関連付けられたら、**Next** をクリックします。

   入力した値は、**Configure Directory** ウィンドウに表示されます。



6. **次へ**をクリックします。

   Set up Management Processors for Directories ウィンドウが開きます。

7. ディレクトリ用の管理プロセッサーのセットアップに進みます。

Configure Directory ウィンドウのオプション

Configure Directory ウィンドウには以下のボックスがあります。

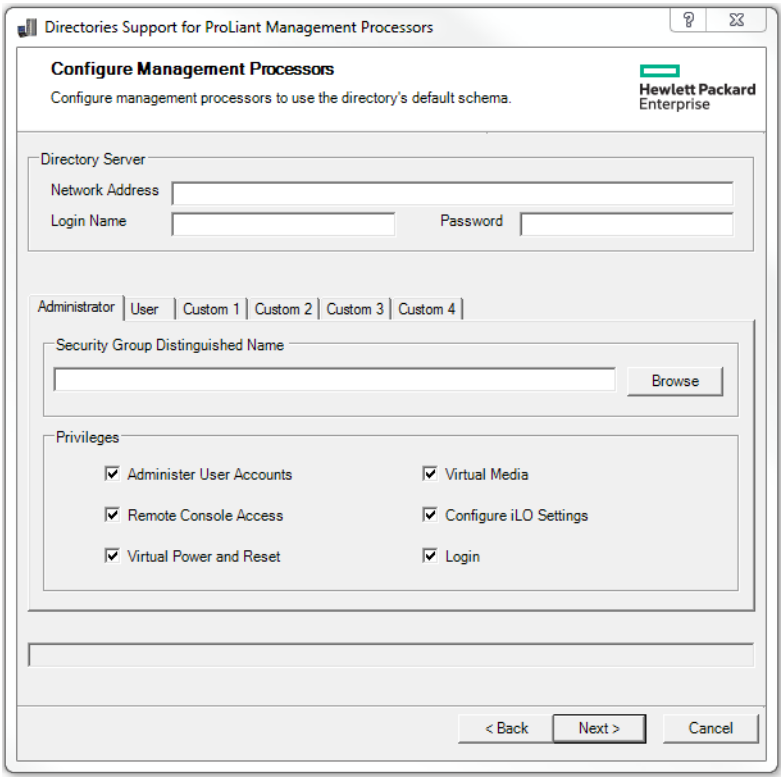
- **Network Address** - ディレクトリサーバーのネットワークアドレス（有効な DNS 名または IP アドレス）です。
- **Port** - ディレクトリへの SSL ポートです。デフォルトポートは 636 です。マネジメントプロセッサーは、SSL を使用してのみディレクトリと通信できます。
- **Login Name** および **Password** - ディレクトリへのドメイン管理者アクセスを持つアカウントのログイン名とパスワードを入力します。
- **Container DN** - ネットワークアドレス、ポート、およびログイン情報を入力したら、**Browse** をクリックして、コンテナー DN を検索できます。コンテナーとは、マイグレーションユーティリティがディレクトリ内のマネジメントプロセッサーオブジェクトを作成する場所です。
- **Role(s) DN** - ネットワークアドレス、ポート、およびログイン情報を入力したら、**Browse** をクリックして、ロール DN を検索できます。ロールとは、デバイスオブジェクトに関連付けられるロールが存在する場所です。ロールは、このユーティリティの実行前に作成する必要があります。
- **Password** － CAC/Smartcard 認証がスキーマフリーディレクトリオプションで使用される場合の、CAC LDAP サービスアカウントのパスワードを指定します。

管理プロセッサーの設定（スキーマフリー構成のみ）

Select the Desired Configuration ウィンドウで **Next** をクリックした後、次のタスクは、選択したマネジメントプロセッサーをデフォルトのディレクトリスキーマを使用するように設定することです。

手順

1. **Configure Management Processors** ウィンドウがまだ開いていない場合は、そのウィンドウに移動します。



2. ディレクトリサーバー設定を入力します。
3. セキュリティグループ DN を入力します。
4. セキュリティグループと関連付ける iLO 権限を選択します。
5. **次へ**をクリックします。

   Set up Management Processors for Directories ウィンドウが開きます。
6. ディレクトリ用の管理プロセッサーのセットアップに進みます。

管理プロセッサー設定

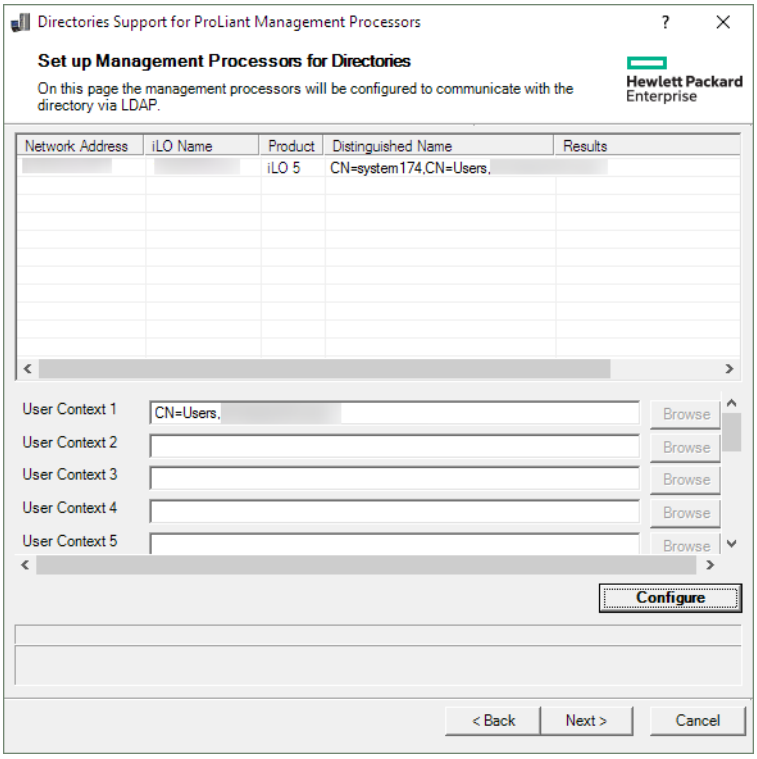
- **Network Address** - ディレクトリサーバーのネットワークアドレス（有効な DNS 名または IP アドレス）です。
- **Login Name** および **Password** - ディレクトリへのドメイン管理者アクセスを持つアカウントのログイン名（DN）とパスワードを入力します。
- **Security Group Distinguished Name** - 共通の権限を持つ一連の iLO ユーザーを含むディレクトリ内のグループの DN です。ディレクトリ名、ログイン名、およびパスワードが正しい場合は、**Browse** をクリックしてグループにアクセスし、選択することができます。
- **Privileges** - 選択されたグループに関連付けられた iLO 権限です。ユーザーがグループのメンバーである場合は、ログイン権限が暗黙に設定されています。

ディレクトリ用の管理プロセッサーのセットアップ

Configure Directory または **Configure Management Processors** ウィンドウで **Next** をクリックした後の次の手順は、ディレクトリと通信するマネジメントプロセッサーのセットアップです。

手順

1. **Set up Management Processors for Directories** ウィンドウがまだ開いていない場合は、そのウィンドウに移動します。
2. ユーザーコンテキストを定義します。



ユーザーコンテキストは、iLO にログインするユーザーの LDAP 構造内の位置を定義します。**User Context** ボックス組織単位の DN を入力するか、**Browse** をクリックしてユーザーコンテキストを選択することができます。

最大 15 個のユーザーコンテキストがサポートされています。

3. **構成**をクリックします。
4. プロセスが完了したら、**Next** をクリックします。

   LDAP CA Certificate Import ウィンドウが開きます。
5. **LDAP CA 証明書のインポート**に進みます。

詳しくは

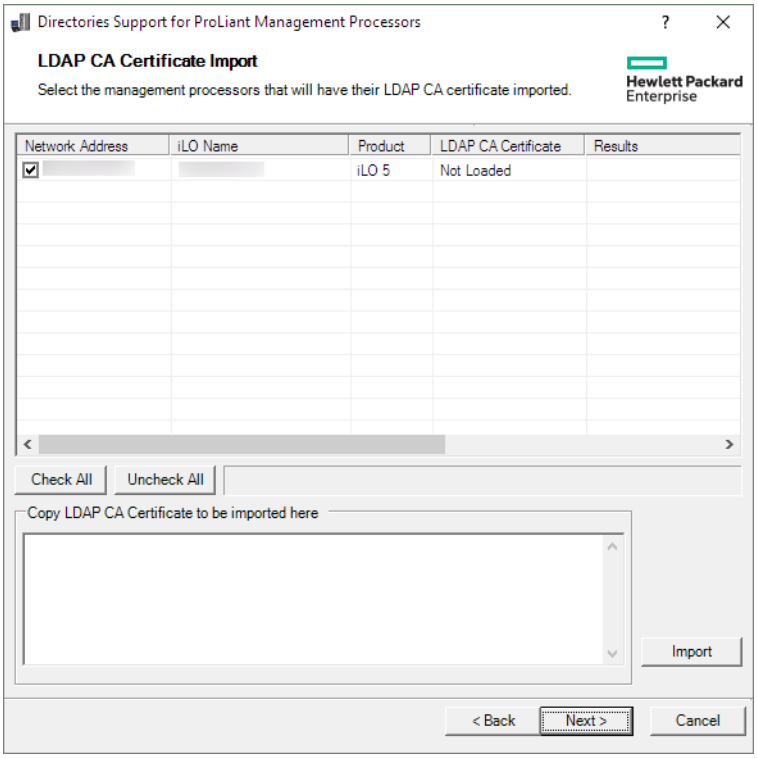
ディレクトリユーザーコンテキスト

LDAP CA 証明書のインポート

Set up Management Processors for Directories で**次へ**をクリックしたら、次の手順は LDAP CA 証明書をインポートすることです。

手順

1. **LDAP CA Certificate Import** ウィンドウがまだ開いていなければ、移動します。



2. 証明書をインポートする対象の iLO システムを選択します。
3. テキストボックスに証明書を貼り付け、**インポート**をクリックします。
4. 証明書のインポートが完了したら、**次へ**をクリックします。

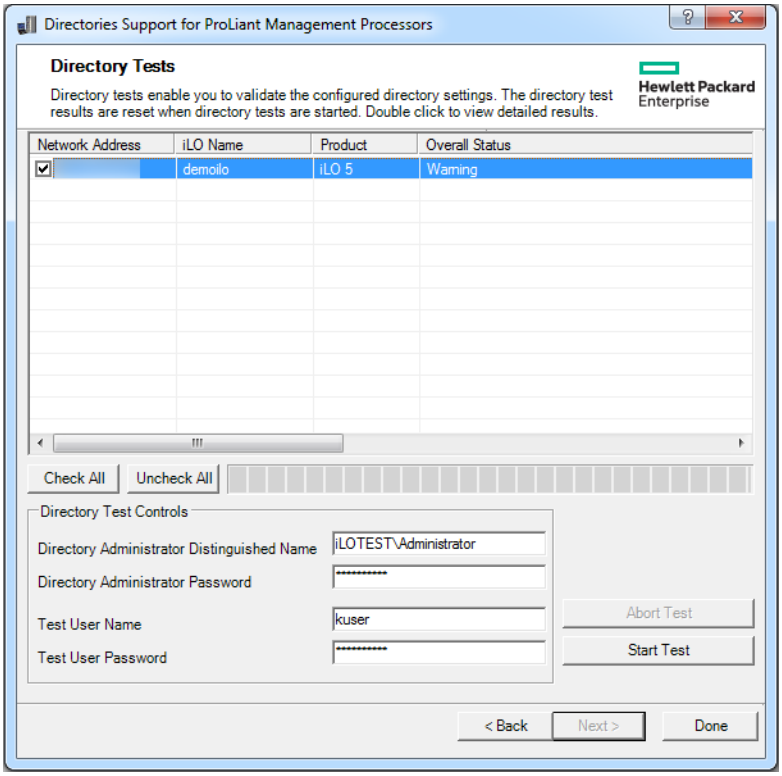
   ディレクトリテストウィンドウが開きます。
5. **（オプション）HPLOMIG を使用したディレクトリテストの実行**に進みます。

（オプション）HPLOMIG を使用したディレクトリテストの実行

LDAP CA Certificate Import で**次へ**をクリックした後の次の手順は、ディレクトリ構成のテストです。

手順

1. **ディレクトリテスト**ウィンドウに移動します（開いていない場合）。



2. ディレクトリ設定をテストします。

   a. 1 つまたは複数の iLO システムを選択します。

   b. **ディレクトリテスト制御**セクションで、以下を入力します。

      - **ディレクトリ管理者識別名**および**ディレクトリ管理者パスワード** - iLO オブジェクト、ロール、および検索コンテキストについてディレクトリを検索します。このユーザーは、ディレクトリ読み取り権限を持っている必要があります。

        Hewlett Packard Enterprise では、ディレクトリ内に iLO オブジェクトを作成する際に使用するものと同じ識別名とパスワードを使用することをおすすめします。これらの識別情報は、iLO に保存されるものではなく、iLO オブジェクトとユーザー検索コンテキストを確認するために使用されます。

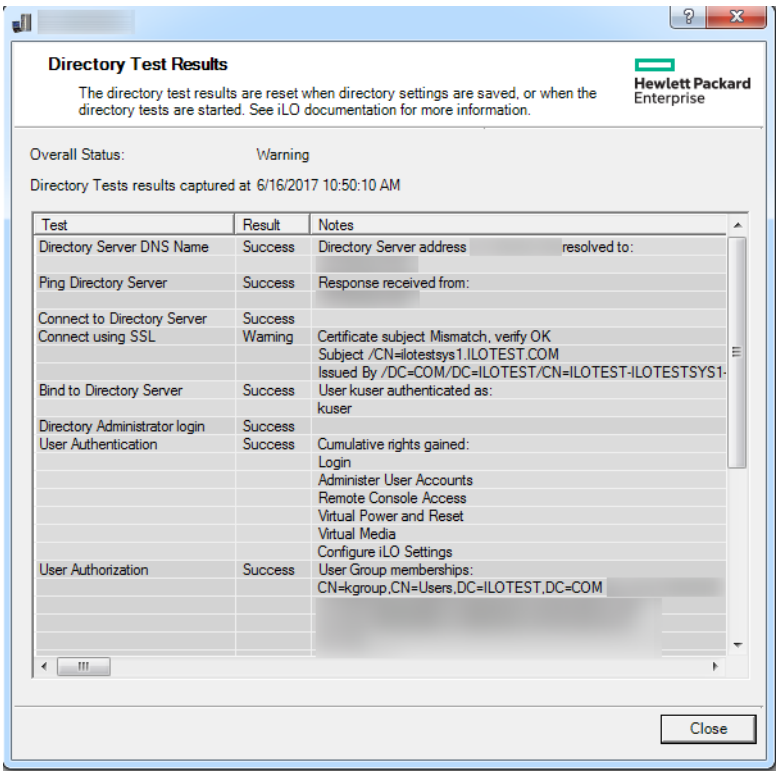
      - **テストユーザー名**および**テストユーザーパスワード** - iLO へのログインとアクセス権をテストします。ユーザー検索コンテキストを適用できるため、ユーザー名は完全修飾である必要はありません。このユーザーは、この iLO のロールに関連付けられている必要があります。

        通常、このアカウントは、テスト対象の iLO プロセッサーへのアクセスに利用します。これはディレクトリ管理者アカウントでも構いませんが、スーパーユーザーアカウントではテストでユーザー認証を検証できません。iLO には、これらの認証情報が保存されません。

   c. **テストの開始**をクリックします。

      複数のテストがバックグラウンドで開始します。最初のテストでは、サーバーとの SSL 接続を確立し、ユーザー権限を評価して、ネットワーク経由でのディレクトリユーザーに対するネットワーク Ping が実行されます。

3. 個々のテスト結果を表示するには、iLO システムをダブルクリックします。



詳しくは、**ディレクトリテストの実行**を参照してください。

4. **完了**をクリックします。

ディレクトリサービススキーマ

ディレクトリサービススキーマでは、Hewlett Packard Enterprise Lights-Out マネジメント権限付与データをディレクトリサービスに保存するために使用されるクラスおよび属性について説明します。

HPE Management コア LDAP OID クラスおよび属性

スキーマのセットアッププロセスでスキーマに加える変更には、次の変更が含まれます。

- コアクラス
- コア属性

コアクラス

クラス名	割り当てられる OID
hpqTarget	1.3.6.1.4.1.232.1001.1.1.1.1
hpqRole	1.3.6.1.4.1.232.1001.1.1.1.2
hpqPolicy	1.3.6.1.4.1.232.1001.1.1.1.3

コア属性

属性名	割り当てられる OID
hpqPolicyDN	1.3.6.1.4.1.232.1001.1.1.2.1
hpqRoleMembership	1.3.6.1.4.1.232.1001.1.1.2.2
hpqTargetMembership	1.3.6.1.4.1.232.1001.1.1.2.3
hpqRoleIPRestrictionDefault	1.3.6.1.4.1.232.1001.1.1.2.4
hpqRoleIPRestrictions	1.3.6.1.4.1.232.1001.1.1.2.5
hpqRoleTimeRestriction	1.3.6.1.4.1.232.1001.1.1.2.6

コアクラスの定義

以下の表に、Hewlett Packard Enterprise Management コアクラスの定義を示します。

hpqTarget

OID	1.3.6.1.4.1.232.1001.1.1.1.1
説明	このクラスは、ターゲットオブジェクトを定義し、ディレクトリ対応管理を使用する Hewlett Packard Enterprise 製品の基礎を提供します。
クラスのタイプ	Structural
スーパークラス	user
属性	hpqPolicyDN - 1.3.6.1.4.1.232.1001.1.1.2.1 hpqRoleMembership - 1.3.6.1.4.1.232.1001.1.1.2.2
注意事項	なし

hpqRole

OID	1.3.6.1.4.1.232.1001.1.1.1.2
説明	このクラスは、ロールオブジェクトを定義し、ディレクトリ対応管理を使用する Hewlett Packard Enterprise 製品の基礎を提供します。
クラスのタイプ	Structural

表は続く

スーパークラス	group
属性	hpqRoleIPRestrictions - 1.3.6.1.4.1.232.1001.1.1.2.5 hpqRoleIPRestrictionDefault - 1.3.6.1.4.1.232.1001.1.1.2.4 hpqRoleTimeRestriction - 1.3.6.1.4.1.232.1001.1.1.2.6 hpqTargetMembership - 1.3.6.1.4.1.232.1001.1.1.2.3
注意事項	なし

hpqPolicy

OID	1.3.6.1.4.1.232.1001.1.1.1.3
説明	このクラスは、ポリシーオブジェクトを定義し、ディレクトリ対応管理を使用する Hewlett Packard Enterprise 製品の基礎を提供します。
クラスのタイプ	Structural
スーパークラス	top
属性	hpqPolicyDN - 1.3.6.1.4.1.232.1001.1.1.2.1
注意事項	なし

コア属性の定義

以下の表に、HPE Management コアクラス属性の定義を示します。

hpqPolicyDN

OID	1.3.6.1.4.1.232.1001.1.1.2.1
説明	このターゲットの一般設定を制御するポリシーの識別名です。
構文	識別名 - 1.3.6.1.4.1.1466.115.121.1.12
オプション	単一値
注意事項	なし

hpqRoleMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.2
説明	このオブジェクトに所属する hpqRole オブジェクトのリストを提供します。
構文	識別名 - 1.3.6.1.4.1.1466.115.121.1.12
オプション	複数値
注意事項	なし

hpqTargetMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.3
説明	このオブジェクトに所属する hpqTarget オブジェクトのリストを提供します。
構文	識別名 - 1.3.6.1.4.1.1466.115.121.1.12
オプション	複数値
注意事項	なし

hpqRoleIPRestrictionDefault

OID	1.3.6.1.4.1.232.1001.1.1.2.4
説明	IP ネットワークアドレス制限のもとでの権限の制限を部分的に指定する未指定クライアントによるアクセスを表す Boolean 値。
構文	Boolean 値 - 1.3.6.1.4.1.1466.115.121.1.7
オプション	単一値
注意事項	この属性が `TRUE` の場合、IP 制限が通常のネットワーククライアントに適用されます。この属性が `FALSE` の場合、IP 制限が通常のネットワーククライアントに適用されません。

hpqRoleIPRestrictions

OID	1.3.6.1.4.1.232.1001.1.1.2.5
説明	IP ネットワークアドレス制限のもとでの権限の制限を部分的に指定する IP アドレス、DNS 名、ドメイン、アドレス範囲、およびサブネットのリストを提供します。

表は続く

構文	オクテット文字列 - 1.3.6.1.4.1.1466.115.121.1.40
オプション	複数値
注意事項	この属性は、ロールオブジェクトについてのみ使用されます。 アドレスが一致し、一般アクセスが拒否される場合、IP 制限は適用されます。アドレスが一致し、一般アクセスが許可される場合、IP 制限が適用されません。 値には、ID バイトの後にネットワークアドレスを指定する（タイプ別の数の）バイトを続けたものを使用します。 ・ IP サブネットの場合、ID バイトは<0x01>で、その後にネットワーク順の IP ネットワークアドレスとネットワーク順の IP ネットワークサブネットマスクを続けます。たとえば、127.0.0.1/255.0.0.0 という IP サブネットの場合は、<0x01 0x7F 0x00 0x00 0x01 0xFF 0x00 0x00 0x00>となります。IP 範囲の場合、ID バイトは<0x02>で、その後に下限の IP アドレスと上限の IP アドレスを続けます。両方とも範囲に含まれ、ネットワーク順に指定します。たとえば、10.0.0.1～10.0.10.255 という IP 範囲の場合は、<0x02 0x0A 0x00 0x00 0x01 0x0A 0x00 0x0A 0xFF>となります。 ・ DNS 名またはドメインの場合、ID バイトは<0x03>で、その後に ASCII エンコードの DNS 名を続けます。DNS 名には、指定された文字列で終了するすべての名前と一致させるために、先頭に*（ASCII コードでは 0x2A）を付けることができます。たとえば、DNS ドメイン*.acme.com は、<0x03 0x2A 0x2E 0x61 0x63 0x6D 0x65 0x2E 0x63 0x6F 0x6D>となります。一般アクセスが許可されます。

hpqRoleTimeRestriction

OID	1.3.6.1.4.1.232.1001.1.1.2.6
説明	時間制限のもとでの権限の制限を指定する 1 週間の時間枠（30 分単位）です。
構文	オクテット文字列 {42}-1.3.6.1.4.1.1466.115.121.1.40

表は続く

オプション	単一値
注意事項	この属性は、ロールオブジェクトについてのみ使用されます。 デバイスがある場所の現在の現地時間に対応するビットが 1 の場合には、時間制限が適用され、ビットが 0 の場合には、時間制限が適用されません。 · 最初のバイトの最下位ビットは、日曜日の午前 0 時から午前 0 時 30 分に対応します。 · 最下位ビットよりも上位のビットおよび後続のバイトは、日曜日の午前 0 時 30 分以降の、1 週間を 30 分ごとに区切った時間枠に、順番に対応します。 · 42 番目のバイトの最上位ビット（8 番目）は、土曜日の午後 11 時 30 分から日曜日の午前 0 時に対応します。

Lights-Out Management 固有の LDAP OID クラスおよび属性

以下のスキーマ属性およびクラスは、Hewlett Packard Enterprise Management コアクラスおよび属性で定義される属性およびクラスに依存する場合があります。

表 5: Lights-Out Management クラス

クラス名	割り当てられる OID
hpqLOMv100	1.3.6.1.4.1.232.1001.1.8.1.1

Lights-Out Management 属性

クラス名	割り当てられる OID
hpqLOMRightLogin	1.3.6.1.4.1.232.1001.1.8.2.3
hpqLOMRightRemoteConsole	1.3.6.1.4.1.232.1001.1.8.2.4
hpqLOMRightVirtualMedia	1.3.6.1.4.1.232.1001.1.8.2.6
hpqLOMRightServerReset	1.3.6.1.4.1.232.1001.1.8.2.5
hpqLOMRightLocalUserAdmin	1.3.6.1.4.1.232.1001.1.8.2.2
hpqLOMRightConfigureSettings	1.3.6.1.4.1.232.1001.1.8.2.1

Lights-Out Management クラスの定義

以下の表に、Lights-Out Management コアクラスの定義を示します。

表 6: hpqLOMv100

OID	1.3.6.1.4.1.232.1001.1.8.1.1
説明	このクラスは、HPE Lights-Out Management 製品で使用される権限と設定を定義します。
クラスのタイプ	Auxiliary
スーパークラス	なし
属性	hpqLOMRightConfigureSettings - 1.3.6.1.4.1.232.1001.1.8.2.1 hpqLOMRightLocalUserAdmin - 1.3.6.1.4.1.232.1001.1.8.2.2 hpqLOMRightLogin - 1.3.6.1.4.1.232.1001.1.8.2.3 hpqLOMRightRemoteConsole - 1.3.6.1.4.1.232.1001.1.8.2.4 hpqLOMRightServerReset - 1.3.6.1.4.1.232.1001.1.8.2.5 hpqLOMRightVirtualMedia - 1.3.6.1.4.1.232.1001.1.8.2.6
注意事項	なし

Lights-Out Management 属性の定義

以下の表に、Lights-Out Management コアクラス属性の定義を示します。

hpqLOMRightLogin

OID	1.3.6.1.4.1.232.1001.1.8.2.3
説明	Lights-Out Management 製品のログイン権限です。
構文	Boolean 値 - 1.3.6.1.4.1.1466.115.121.1.7
オプション	単一値
注意事項	この属性は、ロールオブジェクトについてのみ有効です。`TRUE` の場合は、ロールのメンバーに権限が付与されます。

hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.4
説明	Lights-Out Management 製品のリモートコンソール権限です。この属性は、ロールオブジェクトについてのみ有効です。

表は続く

構文	Boolean 値 - 1.3.6.1.4.1.1466.115.121.1.7
オプション	単一値
注意事項	この属性は、ロールオブジェクトについてのみ使用されます。値が TRUE の場合は、ロールのメンバーに権限が付与されます。

hpqLOMRightVirtualMedia

OID	1.3.6.1.4.1.232.1001.1.8.2.6
説明	Lights-Out Management 製品の仮想メディア権限です。
構文	Boolean 値 - 1.3.6.1.4.1.1466.115.121.1.7
オプション	単一値
注意事項	この属性は、ロールオブジェクトについてのみ使用されます。値が TRUE の場合は、ロールのメンバーに権限が付与されます。

hpqLOMRightServerReset

OID	1.3.6.1.4.1.232.1001.1.8.2.5
説明	Lights-Out Management 製品のリモートサーバーリセットおよび電源ボタン権限です。
構文	Boolean 値 - 1.3.6.1.4.1.1466.115.121.1.7
オプション	単一値
注意事項	この属性は、ロールオブジェクトについてのみ使用されます。値が TRUE の場合は、ロールのメンバーに権限が付与されます。

hpqLOMRightLocalUserAdmin

OID	1.3.6.1.4.1.232.1001.1.8.2.2
説明	Lights-Out Management 製品のローカルユーザーデータベース管理権限です。
構文	Boolean 値 - 1.3.6.1.4.1.1466.115.121.1.7
オプション	単一値
注意事項	この属性は、ロールオブジェクトについてのみ使用されます。値が TRUE の場合は、ロールのメンバーに権限が付与されます。

hpqLOMRightConfigureSettings

OID	1.3.6.1.4.1.232.1001.1.8.2.1
説明	Lights-Out Management 製品のデバイス設定権限です。
構文	Boolean 値 - 1.3.6.1.4.1.1466.115.121.1.7
オプション	単一値
注意事項	この属性は、ロールオブジェクトについてのみ使用されます。値が `TRUE` の場合は、ロールのメンバーに権限が付与されます。

iLO の工場出荷時設定へのリセット

場合によっては、iLO を工場出荷時のデフォルト設定にリセットする必要があることがあります。たとえば、FIPS のセキュリティ状態を無効にすると、iLO を工場出荷時設定にリセットする必要があります。

工場出荷時設定へのリセット方法

- iLO 5 構成ユーティリティ - この機能には UEFI システムユーティリティからアクセスします。
- iLO RESTful API - 詳しくは、次の Web サイトを参照してください。**https://www.hpe.com/support/restfulinterface/docs**
- コマンドラインとスクリプティングツール - 手順については、HPE iLO 5 スクリプティング/コマンドラインガイドを参照してください。

詳しくは

iLO の工場出荷時デフォルト設定へのリセット（iLO 5 構成ユーティリティ）

iLO の工場出荷時デフォルト設定へのリセット（iLO 5 構成ユーティリティ）

注意: iLO を工場出荷時のデフォルト設定にリセットすると、iLO のユーザーおよびライセンスデータ、構成設定、およびログを含むすべての設定が消去されます。サーバーに工場でインストールされたライセンスキーがある場合、このライセンスキーは保持されます。

この手順によりログ内のすべてのデータが消去されるため、リセットに関するイベントは iLO イベントログおよびインテグレーテッドマネジメントログに記録されません。

手順

1. （オプション）サーバーにリモートアクセスする場合、iLO リモートコンソールセッションを開始します。
2. サーバーを再起動するかまたは電源を入れます。
3. サーバーの POST 画面で **F9** キーを押します。

   UEFI システムユーティリティが起動します。
4. **システムユーティリティ**画面で、**システム構成**、**iLO 5 構成ユーティリティ**の順にクリックします。
5. **工場出荷時のデフォルトにセット**メニューで**はい**を選択します。

   iLO 5 構成ユーティリティに、要求の確認を求めるメッセージが表示されます。
6. **OK** をクリックします。
7. iLO が工場出荷時のデフォルト設定にリセットされます。iLO をリモートで管理している場合は、リモートコンソールセッションが自動的に終了します。次にシステムを再起動するまで iLO 5 構成ユーティリティに再びアクセスすることはできません。
8. ブートプロセスを再開します。

   a. （オプション）iLO をリモート管理している場合は、iLO のリセットが完了するのを待ってから、iLO リモートコンソールを起動します。

以前のセッションの iLO 5 構成ユーティリティ画面がまだ開いています。

b. メインメニューが表示されるまで **Esc** キーを押します。

c. **システムを終了して再起動**をクリックします。

d. 要求の確認を求めるメッセージが表示されたら、**OK** をクリックして画面を終了し、ブートプロセスを再開します。

9. （オプション）リセット後にデフォルトの iLO アカウント情報を使用して、iLO にログインします。

10. サーバーのオペレーティングシステムを再起動します。

工場出荷時のデフォルト設定へのリセット中に、SMBIOS レコードはクリアされます。メモリおよびネットワーク情報は、サーバー OS の再起動が完了するまで iLO Web インターフェイスに表示されません。

パフォーマンス管理の**プロセッサージッターコントロール最適化**機能は、サーバー OS の再起動が完了するまで使用できません。

iLO モバイルアプリの使用

iLO モバイルアプリケーションの機能

- サーバーの電源スイッチの操作
- BIOS や ROM の構成変更など、リモートコンソールを使用した OS の操作
- Web サーバーに保存されたイメージファイルからの ISO CD/DVD イメージのマウント（http または https）。サーバーでは、ディスクイメージは USB CD/DVD ドライブとして使用できます。CD/DVD イメージから起動し、OS を展開できます。
- iLO スクリプトの起動およびスクリプトの進行状況の監視
- iLO の Web インターフェイスへのアクセス
- 管理したいサーバーのリストの保存

iLO モバイルアプリの制限事項

- iLO 3 以降を搭載した ProLiant サーバーがサポートされます。Lights-Out 100i を搭載した ProLiant G7 100 シリーズサーバーを除き、すべての ProLiant G7 以降のサーバーがサポートされます。
- 管理する iLO システムにネットワークアクセスできる必要があります。セルラーネットワークから接続する場合は、ファイアウォールの再構成または VPN の構成が必要になる場合があります。

  VPN を使用してファイアウォール経由で接続するか、以下のポートを開くか転送することができます。

  - **HTTP**：ポート 80
  - **HTTPS**：ポート 443
  - **リモートコンソール**：ポート 17990

  これらのポートは、デフォルト値です。これらのポート設定は、iLO の Web インターフェイスの**アクセス設定**ページで表示または変更できます。

  モバイルデバイスで VPN 機能を使用する方法については、デバイスのユーザーガイドを参照してください。
- 以下の機能を使用するには、サーバー上に iLO ライセンスが必要です。
  - iLO 仮想メディア
  - リモートコンソール - この機能はブレードサーバーに含まれています。他のすべてのサーバーではライセンスが必要です。
  - スクリプティング - この機能は、すべてのサーバーで使用できます。iLO 仮想メディアのような特定の機能のスクリプティングにはライセンスが必要です。

  iLO のライセンスについて詳しくは、Web サイト **https://www.hpe.com/support/ilo-docs** にある iLO ライセンスガイドを参照してください。

- iLO モバイルアプリは、かなりのネットワーク帯域幅を消費することがあります。携帯電話ネットワークを使用するときは、無制限データプランに加入していない場合、データ使用量を監視してください。可能な場合は、Wi-Fi を使用するようにしてください。
- リモートコンソールと共有リモートコンソールの取得は、モバイルアプリではサポートされていません。

Android デバイスでの iLO モバイルアプリの使用

モバイルアプリへの iLO システムの追加

手順

1. **iLO を選択**ページで **iLO の構成**をタップします。
2. **iLO ネットワークアドレス**を入力します。

   iLO の DNS 名または IP アドレスを使用できます。
3. iLO ユーザーアカウントの**ログイン名**と**パスワード**を入力します。
4. （オプション）ログイン認証情報を保存するには、**ログイン情報を保存**オプションを**はい**に設定します。

   デフォルト値は**はい**です。

   ログイン認証情報は、iLO との接続が成功する場合のみ保存されます。
5. （オプション）この iLO をお気に入りリストに追加するには、**お気に入り**オプションを**はい**に設定します。

   デフォルト値は**はい**です。
6. **完了**をタップしてこの iLO を保存し、リストページに戻ります。

   リストに iLO システムが表示されます。接続が成功すると、ネットワークアドレスの下にシステムの説明が表示されます。

QR コードのスキャンによるモバイルアプリへの iLO システムの追加

手順

1. QR コードジェネレーターをダウンロードしてインストールします。
2. コードタイプが**テキスト**に設定された QR コードを作成します。
3. **address;login_name;password** のフォーマットで iLO のネットワークアドレス、ログイン名、およびパスワードを入力します。
4. QR コードイメージを保存します。
5. iLO モバイルアプリを起動します。
6. **iLO を選択**ページで **iLO の構成**をタップします。
7. **スキャン**をタップします。
8. デバイスのカメラを使用して QR コードをスキャンします。

QR コードのネットワークアドレス、ログイン名、パスワードがモバイルアプリに表示されます。

9. **完了**をタップして、iLO システムの詳細を保存します。

   リストに iLO システムが表示されます。接続が成功すると、表示名またはネットワークアドレスの下にシステムの説明が表示されます。

iLO システムのリストの編集

手順

1. **iLO を選択**ページでリスト内の iLO システムをタップしたままにします。

   選択した iLO システムを編集するか、削除するかを求められます。

2. **編集**をタップします。
3. iLO 情報を編集し、**完了**をタップします。

   アプリに、変更の確認を求めるメッセージが表示されます。

4. **上書き**をタップします。

リストからの iLO システムの削除

手順

1. **iLO を選択**ページでリスト内の iLO システムをタップしたままにします。

   選択した iLO システムを編集するか、削除するかを求められます。

2. **削除**をタップします。

   iLO システムがリストから削除されます。

iLO システムのリストの表示

手順

1. iLO モバイルアプリを開きます。

   表示されているすべての iLO システムのリスト。

2. （オプション）**お気に入り**リストの iLO システムのみを表示するには、**お気に入り**をタップします。
3. （オプション）アクセスしたことのある iLO システムを表示するには、**履歴**をタップします
4. （オプション）リストの順序を変更するには、水平バーアイコンをドラッグします。

リモートコンソールの起動

前提条件

リモートコンソールが使用中ではありません。

手順

1. **iLO を選択**ページで iLO システムをタップします。
2. **リモートコンソール**をタップします。
3. プロンプトが表示されたら、iLO のログイン認証情報を入力します。

リモートコンソールの使用方法

iLO モバイルアプリは、全画面モードで仮想マウスとキーボードのあるサーバーコンソールを表示します。

リモートコンソール機能は、ステータスバーアイコンから使用できます。デバイスでサポートされている場合は、2 本の指で一度タップすると、ステータスバーの表示/非表示を切り替えることができます。

- キーボードにアクセスするには、キーボードアイコンをタップします。
- iLO Web インターフェイスにアクセスするには、サーバーヘルスアイコンをタップします。このアイコンは、灰色、緑色、黄色、または赤色でサーバーヘルスを表します。

  Web インターフェイスを開始するとき、追加のログインは不要です。

  リモートコンソールに戻るには、**X** をタップするか、**戻る**ボタンをタップします。
- 仮想電源スイッチにアクセスするには、電源アイコンをタップします。
- 仮想メディア機能に使用するには、CD/DVD-ROM アイコンをタップします。
- iLO から切断するには、**X** をタップするか、**戻る**ボタンをタップします。

  一定時間にわたって何も実行しないと、iLO はセッションを切断します。この時間は、iLO Web インターフェイスで設定できます。

詳しくは

iLO アクセス設定の構成
サブシステムおよびデバイスステータスの値

モバイルアプリのキーボードの使用方法

- 以下のキーをタップすると、キーを押し続けるのと同じ効果があります。**Ctrl**、**Alt**、**Shift**。

  これらのキーのいずれかがアクティブ化されると、緑色で表示されます。
- Windows システムの **Home**（Windows）キーをタップすると、**スタート**メニューが開きます。
- **?123** をタップすると、次のキーが使用可能になります。
  - 数字と記号
  - カーソルの制御キー
  - **ESC**
  - **DEL**

  標準キーボードに戻るには、**FN** をタップしてから、**ABC** をタップします。
- **?123** をタップしてから **FN** をタップすると、次のキーが使用可能になります。
  - ファンクションキー
  - **SysRq**

標準キーボードに戻るには、**ABC** をタップします。

- 標準キーボードで使用できない特殊キーコマンドを入力するには、モバイルアプリのキーボードを使用します。

  たとえば、**?123** をタップして拡張キーボードにアクセスしてから、**Ctrl**、**Alt**、および **DEL** キーをタップして **Ctrl+Alt+Del** を入力します。

サポートされるリモートコンソールのジェスチャー

- **クリックまたは左クリック** - タップします。
- **マウスの左ボタンをダブルクリック** - ダブルタップします。
- **右クリック** - 1 秒間押し続けます。
- **選択してドラッグ** - タッチしたまま、選択した項目をドラッグします。
- **ズームインまたはズームアウト** - 画面をピンチします。
- **パン** - 2 本の指でドラッグします。

Web サーバーに保存されたスクリプトの起動

手順

1. **iLO を選択**ページで iLO システムをタップします。
2. **スクリプトの起動**をタップします。

   保存されたスクリプトは、 **スクリプトの選択**ウィンドウにリストされます。
3. （オプション）スクリプトを追加します。

   a. **スクリプトの追加**をタップします。

      iLO RIBCL スクリプトの完全な URL の入力を求められます。

   b. URL を入力してから、**OK** をタップして**スクリプトの選択**ページに戻ります。

4. **スクリプトの選択**ページで、リスト内のスクリプト URL をタップします。

   システムをモバイルアプリに追加したときに iLO ログイン情報を保存した場合、アプリは保存された認証情報を使用します。iLO ログイン認証情報を保存しなかった場合、アプリは XML スクリプトで提供されるログイン認証情報を使用します。

   スクリプトの進行状況と結果が表示されます。

iLO Web インターフェイスの起動

手順

1. **iLO を選択**ページで iLO システムをタップします。
2. **iLO Web インターフェイス**をタップします。
3. Web インターフェイスの使用が終了したら、**< iLO** をタップして iLO リストページに戻ります。

iLO モバイルアプリの履歴のクリア

手順

1. **履歴**をタップすると、モバイルアプリからアクセスされた iLO システムのリストが表示されます。
2. **クリア**をタップします。
3. 要求を確認するメッセージが表示されたら、**OK** をタップします。

iOS デバイスでの iLO モバイルアプリの使用

モバイルアプリへの iLO システムの追加

手順

1. iLO リストページでのプラス記号（+）アイコンをタップします。
2. **iLO ネットワークアドレス**を入力します。

   iLO の DNS 名または IP アドレスを使用できます。
3. （オプション）モバイルアプリ内でこの iLO システム用に使用する**表示名**を入力します。
4. （オプション）表示名を使用するには、**Use display name** オプションを有効にします。

   デフォルト設定はオフです。
5. iLO ユーザーアカウントの**ログイン名**と**パスワード**を入力します。
6. （オプション）ログイン認証情報を保存するには、 **ログイン情報を保存**のオン/オフスイッチをタップします。

   デフォルト設定はオフです。

   ログイン認証情報は、iLO との接続が成功する場合のみ保存されます。
7. （オプション）この iLO をお気に入りリストに追加するかどうかを指定するには、**お気に入り**のオン/オフスイッチをタップします。

   このデフォルト設定は、on です。
8. **保存**をタップしてこの iLO を保存し、リストページに戻ります。
   リストに iLO システムが表示されます。接続が成功すると、表示名またはネットワークアドレスの下にシステムの説明が表示されます。

QR コードのスキャンによるモバイルアプリへの iLO システムの追加

手順

1. QR コードジェネレーターをダウンロードしてインストールします。
2. コードタイプを**テキスト**に設定した QR コードを作成します。
3. **address;login_name;password** のフォーマットで iLO のネットワークアドレス、ログイン名、およびパスワードを入力します。
4. QR コードイメージを保存します。
5. iLO モバイルアプリを起動します。

6. iLO リストページでのプラス記号（+）アイコンをタップします。
7. **スキャン**をタップします。
8. デバイスのカメラを使用して QR コードをスキャンします。

   QR コードのネットワークアドレス、ログイン名、パスワードがモバイルアプリに表示されます。
9. **保存**をタップして、iLO システムの詳細を保存します。

   リストに iLO システムが表示されます。接続が成功すると、表示名またはネットワークアドレスの下にシステムの説明が表示されます。

iLO システムのリストの編集

手順

1. iLO リストページで**編集**をタップします。
2. 編集する iLO システムの行にある情報（i）アイコンをタップします。

   iLO の編集ウィンドウが開きます。
3. iLO の詳細をアップデートしてから、**保存**をクリックします。
4. **完了**をクリックして、iLO システムのリストに戻ります。

リストからの iLO システムの削除

手順

1. **編集**をタップします。
2. 削除する各 iLO システムの行をタップします。
3. ウィンドウの左下にあるごみ箱アイコンをタップします。

   アプリから要求を確認するように求められます。
4. **削除**をタップします。
5. **完了**をタップして、iLO システムのリストに戻ります。

iLO システムのリストの表示

手順

1. iLO モバイルアプリを開きます。

   表示されているすべての iLO システムのリスト。
2. （オプション）**お気に入り**リストの iLO システムのみを表示するには、**お気に入り**をタップします。
3. （オプション）アクセスしたことのある iLO システムを表示するには、**履歴**をタップします
4. （オプション）リストの順序を変更するには、**編集**をタップしてから、水平バーアイコンをドラッグします。

リモートコンソールの起動

前提条件

リモートコンソールが使用中ではありません。

手順

1. **iLO を選択**ページで iLO システムをタップします。
2. **リモートコンソール**をタップします。
3. プロンプトが表示されたら、iLO のログイン認証情報を入力します。

リモートコンソールの使用方法

iLO モバイルアプリは、全画面モードで仮想マウスとキーボードのあるサーバーコンソールを表示します。

リモートコンソール機能は、ステータスバーアイコンから使用できます。2 本の指で一度タップすると、ステータスバーの表示/非表示を切り替えることができます。

- キーボードにアクセスするには、キーボードアイコンをタップします。
- iLO Web インターフェイスにアクセスするには、サーバーヘルスアイコンをタップします。このアイコンは、灰色、緑色、黄色、または赤色でサーバーヘルスを表します。

  Web インターフェイスを開始するとき、追加のログインは不要です。

  リモートコンソールに戻るには、**X** をタップします。
- 仮想メディア機能にアクセスするには、CD/DVD-ROM アイコンをタップします。
- 仮想電源スイッチにアクセスするには、電源ボタンアイコンをタップします。
- iLO から切断するには、**X** をタップします。

  一定時間にわたって何も実行しないと、iLO はセッションを切断します。この時間は、iLO Web インターフェイスで設定できます。

詳しくは

iLO アクセス設定の構成
サブシステムおよびデバイスステータスの値

モバイルアプリのキーボードの使用方法

- 以下のキーをタップすると、キーを押し続けるのと同じ効果があります。**Ctrl**、**Alt**、**Shift**。
- Windows システムの **Home**（Windows）キーをタップすると、**スタート**メニューが開きます。
- 標準キーボードで使用できない特殊キーコマンドを入力するには、iLO モバイルアプリのキーボード機能を使用します。

  たとえば、**Ctrl+Alt+Del** と入力するには、**Ctrl** と **Alt** をタップしてから、**Del** をタップします。

サポートされるリモートコンソールのジェスチャー

- **クリックまたは左クリック** - タップします。
- **ステータスバーの表示/非表示** - 2 本の指で一度タップします。
- **マウスの左ボタンをダブルクリック** - ダブルタップします。
- **右クリック** - 1 秒間押し続けます。
- **選択してドラッグ** - タッチしたまま、選択した項目をドラッグします。
- **ズームインまたはズームアウト** - 画面をピンチします。
- **パン** - 2 本の指でドラッグします。

Web サーバーに保存されたスクリプトの起動

手順

1. iLO リストページで iLO システムをタップします。
2. **スクリプティング**をタップします。

   保存されたスクリプトは、 **スクリプトの選択**ウィンドウにリストされます。
3. （オプション）スクリプトを追加します。

   a. プラス記号（+）アイコンをタップします。

      iLO RIBCL スクリプトの完全な URL の入力を求められます。

   b. URL を入力してから、**完了**をタップして**スクリプトの選択**ページに戻ります。
4. **スクリプトの選択**ページで、リスト内のスクリプト URL をタップします。

   システムをモバイルアプリに追加したときに iLO ログイン情報を保存した場合、アプリは保存された認証情報を使用します。iLO ログイン認証情報を保存しなかった場合、アプリは XML スクリプトで提供されるログイン認証情報を使用します。

   スクリプトを実行することの確認が求められます。
5. **実行**をタップします。

   スクリプトの進行状況と結果が表示されます。

iLO Web インターフェイスの起動

手順

1. iLO リストページで iLO システムをタップします。
2. **ホームページ**をタップします。
3. Web インターフェイスの使用が終了したら、**戻る**ボタンをタップして iLO から切断します。

iLO モバイルアプリの履歴のクリア

手順

1. **履歴**をタップすると、モバイルアプリからアクセスされた iLO システムのリストが表示されます。
2. **クリア**をタップします。
3. 要求を確認するメッセージが表示されたら、**はい**をタップします。

iLO モバイルアプリのフィードバック

iLO モバイルアプリについてのフィードバックを **iLO@hpe.com** に送信します。

Web サイト

全般的な Web サイト

Hewlett Packard Enterprise Information Library

https://www.hpe.com/info/EIL

上記以外の Web サイトについては、**サポートと他のリソース**を参照してください。

製品の Web サイト

iLO

https://www.hpe.com/info/ilo

iLO 5 Information Library

https://www.hpe.com/support/ilo-docs

iLO サポート

https://www.hpe.com/support/ilo5

iLO の役立つリンクとリソース

https://www.hpe.com/support/ilo-resource-ref-en

HPE iLO の無料オンライントレーニング

https://www.hpe.com/ww/iloBundle

Active Health System Viewer

https://www.hpe.com/servers/ahsv

HPE ProLiant のトレーニング

https://www.hpe.com/ww/learnproliant

HPE Synergy

https://www.hpe.com/info/synergy-docs

UEFI システムユーティリティ

https://www.hpe.com/info/ProLiantUEFI/docs

SUM

https://www.hpe.com/info/sut-docs

SPP

https://www.hpe.com/info/spp/documentation

Intelligent Provisioning

https://www.hpe.com/info/intelligentprovisioning/docs

iLO RESTful API および RESTful インターフェイスツール

https://www.hpe.com/support/restfulinterface/docs

リモートサポート

https://www.hpe.com/info/insightremotesupport/docs

HPE InfoSight for Servers

https://www.hpe.com/servers/infosight

iLO Amplifier Pack

https://www.hpe.com/servers/iloamplifierpack

HPE OneView

https://www.hpe.com/info/oneview/docs

HPE SIM

https://www.hpe.com/info/insightmanagement/sim/docs

サポートと他のリソース

Hewlett Packard Enterprise サポートへのアクセス

- ライブアシスタンスについては、Contact Hewlett Packard Enterprise Worldwide の Web サイトにアクセスします。

  https://www.hpe.com/info/assistance

- ドキュメントとサポートサービスにアクセスするには、Hewlett Packard Enterprise サポートセンターの Web サイトにアクセスします。

  https://www.hpe.com/support/hpesc

ご用意いただく情報

- テクニカルサポートの登録番号（該当する場合）
- 製品名、モデルまたはバージョン、シリアル番号
- オペレーティングシステム名およびバージョン
- ファームウェアバージョン
- エラーメッセージ
- 製品固有のレポートおよびログ
- アドオン製品またはコンポーネント
- 他社製品またはコンポーネント

アップデートへのアクセス

- 一部のソフトウェア製品では、その製品のインターフェイスを介してソフトウェアアップデートにアクセスするためのメカニズムが提供されます。ご使用の製品のドキュメントで、ソフトウェアの推奨されるソフトウェアアップデート方法を確認してください。
- 製品のアップデートをダウンロードするには、以下のいずれかにアクセスします。

  Hewlett Packard Enterprise サポートセンター

  https://www.hpe.com/support/hpesc

  Hewlett Packard Enterprise サポートセンター：ソフトウェアのダウンロード

  https://www.hpe.com/support/downloads

  My HPE Software Center

  https://www.hpe.com/software/hpesoftwarecenter

- eNewsletters およびアラートをサブスクライブするには、以下にアクセスします。

  https://www.hpe.com/support/e-updates-ja

- お客様の資格を表示、アップデート、または契約や保証をお客様のプロファイルにリンクするには、Hewlett Packard Enterprise サポートセンターの **More Information on Access to Support Materials** ページに移動します。

https://www.hpe.com/support/AccessToSupportMaterials

重要: 一部のアップデートにアクセスするには、Hewlett Packard Enterprise サポートセンターからアクセスするときに製品資格が必要になる場合があります。関連する資格を使って HPE パスポートをセットアップしておく必要があります。

リモートサポート（HPE 通報サービス）

リモートサポートは、保証またはサポート契約の一部としてサポートデバイスでご利用いただけます。リモートサポートは、インテリジェントなイベント診断を提供し、ハードウェアイベントを Hewlett Packard Enterprise に安全な方法で自動通知します。これにより、ご使用の製品のサービスレベルに基づいて、迅速かつ正確な解決が行われます。ご使用のデバイスをリモートサポートに登録することを強くおすすめします。

ご使用の製品にリモートサポートの追加詳細情報が含まれる場合は、検索を使用してその情報を見つけてください。

リモートサポートおよびプロアクティブケア情報

HPE 通報サービス

http://www.hpe.com/jp/hpalert

HPE プロアクティブケアサービス

http://www.hpe.com/services/proactivecare-ja

HPE データセンターケアサービス

http://www.hpe.com/services/datacentercare

HPE プロアクティブケアサービス：サポートされている製品のリスト

http://www.hpe.com/services/proactivecaresupportedproducts

HPE プロアクティブケアアドバンストサービス：サポートされている製品のリスト

https://www.hpe.com/jp/ja/services/proactive-care-central.html

保証情報

ご使用の製品の保証情報を確認するには、以下のリンクを参照してください。

HPE ProLiant と IA-32 サーバーおよびオプション

https://www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise および Cloudline サーバー

https://www.hpe.com/support/EnterpriseServers-Warranties

HPE ストレージ製品

https://www.hpe.com/support/Storage-Warranties

HPE ネットワーク製品

https://www.hpe.com/support/Networking-Warranties

規定に関する情報

安全、環境、および規定に関する情報については、Hewlett Packard Enterprise サポートセンターからサーバー、ストレージ、電源、ネットワーク、およびラック製品の安全と準拠に関する情報を参照してください。

https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts

規定に関する追加情報

Hewlett Packard Enterprise は、REACH（欧州議会と欧州理事会の規則 EC No 1907/2006）のような法的な要求事項に準拠する必要に応じて、弊社製品の含有化学物質に関する情報をお客様に提供することに全力で取り組んでいます。この製品の含有化学物質情報レポートは、次を参照してください。

https://www.hpe.com/info/reach

RoHS、REACH を含む Hewlett Packard Enterprise 製品の環境と安全に関する情報と準拠のデータについては、次を参照してください。

https://www.hpe.com/info/ecodata

社内プログラム、製品のリサイクル、エネルギー効率などの Hewlett Packard Enterprise の環境に関する情報については、次を参照してください。

https://www.hpe.com/info/environment

ドキュメントに関するご意見、ご指摘

Hewlett Packard Enterprise では、お客様により良いドキュメントを提供するように努めています。ドキュメントを改善するために役立てさせていただきますので、何らかの誤り、提案、コメントなどがございましたら、ドキュメントフィードバック担当（**docsfeedback@hpe.com**）へお寄せください。このメールには、ドキュメントのタイトル、部品番号、版数、およびドキュメントの表紙に記載されている刊行日をご記載ください。オンラインヘルプの内容に関するフィードバックの場合は、製品名、製品のバージョン、ヘルプの版数、およびご利用規約ページに記載されている刊行日もお知らせください。