Hewlett Packard Enterprise

HPE iLO 5 1.20 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た HPE ProLiant Gen10 サーバーおよび HPE Synergy コンピュートモジュールの構成、更新、および操作に関する情報を提供します。本書は、iLO 5 を含む Hewlett Packard Enterprise サーバーの設定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: 880740-193
発行: 2018 年 2 月
版数: 1

© Copyright 2012-2018 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。

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。

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。

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。

改訂履歴

部品番号	出版日付	版数	変更の概要
880740-193	2018 年 2 月	1	HTML5 リモートコンソール サポートされる管理ツールのシステムリカバリイベント 共有ネットワークポート IPv6 および iLO 連携のサポート ファームウェアとソフトウェアアップデートインターフェイスの機能強化 SNMPv3 Inform 通知および最大 8 個の SNMP トラップの宛先のサポート
880740-002a (英語版のみ)	2018 年 1 月	2	Linux ドライバー名の修正

表は続く

部品番号	出版日付	版数	変更の概要
880740-002	2017 年 9 月	1	iLO バックアップと復元 複数の宛先メールアドレスのアラートメールのサポート
880740-191	2017 年 7 月	1	初回リリース

目次

iLO 18
iLO の主な機能 18
ROM ベースの構成ユーティリティ 19
iLO Mobile 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 20
iLO Amplifier Pack 20

iLO のセットアップ 21
iLO をセットアップするための準備 21
iLO ネットワーク接続オプション 21
共有ネットワークポート構成による NIC チーミング 22
iLO IP アドレスの取得 23
iLO アクセスセキュリティ 24
iLO 構成ツール 24
その他の iLO 構成ツール 24
初期セットアップ手順：プロセスの概要 25
iLO ネットワークに接続する 25
iLO 5 構成ユーティリティを使用した iLO のセットアップ 26
静的 IP アドレスの構成（iLO 5 構成ユーティリティ） 26
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 27
iLO に初めてログインする方法 29
iLO デフォルト認証情報 29
iLO ライセンスが必要な機能 30
iLO ドライバーのサポート 30
iLO ドライバーのインストール 31

iLO の Web インターフェイスの使用 32
iLO Web インターフェイス 32
ブラウザーの要件 32
サポートされるブラウザー 32
Internet Explorer JavaScript 設定の構成 32
iLO Web インターフェイスへのログイン 33
ブラウザーインスタンスと iLO の間での Cookie の共有 33
iLO Web インターフェイスの概要 35
iLO 制御の使用 35
ログインページからのリモート管理ツールの起動 36
ログインページからの言語の変更 37

iLO 情報およびログの表示 38
iLO の概要情報の表示 38
システム情報の詳細 38
システムステータスの詳細 39
HPE への接続ステータス 40
iLO セッションの管理 40

セッションリストの詳細....40
iLO イベントログ....41
イベントログの表示....41
CSV ファイルへのイベントログの保存....43
イベントログのクリア....43
インテグレーテッドマネジメントログ....43
IML の表示....44
IML エントリーの修正済みへの変更....46
IML にメンテナンスノートを追加する....47
CSV ファイルへの IML の保存....47
IML のクリア....47
Active Health System....48
Active Health System のデータ収集....48
Active Health System ログ....48
Active Health System ログのダウンロード方法....48
日付範囲を指定した Active Health System ログのダウンロード....49
Active Health System ログ全体のダウンロード....50
curl を使用した Active Health System ログの抽出....50
Active Health System ログの消去....52
iLO セルフテスト結果の表示....53
iLO セルフテスト....53

全般的なシステム情報の表示....55
ヘルスサマリー情報の表示....55
冗長ステータス....55
サブシステムおよびデバイスのステータス....55
サブシステムおよびデバイスステータスの値....55
プロセッサー情報の表示....56
プロセッサーの詳細....56
メモリ情報の表示....57
アドバンストメモリプロテクションの詳細....57
メモリの概要....59
物理メモリ詳細....60
論理メモリ詳細....60
メモリ詳細ペイン....61
ネットワーク情報の表示....63
物理ネットワークアダプター....64
論理ネットワークアダプター....65
デバイスインベントリの表示....65
デバイスインベントリの詳細....66
スロットの詳細ペイン....66
デバイスステータスの値....67
MCTP 検出の構成....68
MCTP 工場出荷時リセットの開始....69
ストレージ情報の表示....69
サポート対象のストレージコンポーネント....70
Smart アレイの詳細....70
直接接続ストレージの詳細....72

ファームウェアおよびソフトウェアの表示および管理....74
ファームウェアの更新....74
オンラインでのファームウェアアップデート....74
オンラインでのファームウェアアップデート方法....74
オフラインでのファームウェアの更新....75

オフラインでのファームウェア更新方法.....75
ファームウェアおよびソフトウェアの表示およびアップデート.....76
インストール済みファームウェア情報の表示.....77
冗長なシステム ROM でアクティブなシステム ROM を交換.....78
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更新.....78
ソフトウェア情報の表示.....81
iLO レポジトリ.....82
iLO レポジトリからコンポーネントをインストールする.....82
iLO レポジトリからのコンポーネントの削除.....83
iLO レポジトリからすべてのコンポーネントを削除する.....84
iLO レポジトリの概要とコンポーネントの詳細の表示.....84
iLO レポジトリにアップロードペインの使用.....85
インストールセット.....86
インストールセットのインストール.....86
インストールセットを削除する.....87
すべてのインストールセットを削除する.....87
インストールセットの表示.....88
システムリカバリセット.....89
インストールキュー.....89
インストールキューの表示.....90
インストールキューからのタスクの削除.....91
インストールキューからのすべてのタスクの削除.....91
キューに追加ペインの使用.....91

iLO 連携の構成と使用.....94
iLO 連携.....94
iLO 連携の構成.....94
iLO 連携機能を使用するための前提条件.....94
iLO 連携のネットワーク要件.....95
一度につき 1 つの iLO システム用にマルチキャストオプションを構成.....95
iLO 連携グループ.....96
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）.....98
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）.....100
エンクロージャー iLO 連携サポートの設定.....103
iLO 連携機能の使用.....104
選択されたグループのリスト.....104
iLO 連携情報を CSV ファイルにエクスポートする方法.....105
iLO 連携マルチシステムビュー.....106
iLO 連携マルチシステムマップの表示.....107
iLO 連携グループ仮想メディア.....108
iLO 連携グループ電力.....110
グループ消費電力上限の構成.....112
iLO 連携グループのファームウェアアップデート.....114
ライセンスキーのインストール（iLO 連携グループ）.....116

iLO リモートコンソール.....119
内蔵リモートコンソールの起動.....120
HTML5 IRC の起動.....120
概要ページからの HTML5 IRC の起動.....121
.NET IRC の起動.....121
概要ページからの.NET IRC の起動.....122
Java IRC の起動（Oracle JRE）.....123
Java IRC の起動（OpenJDK JRE）.....124

概要ページからの Java IRC（Oracle JRE）の起動 124
リモートコンソールの取得 125
共有リモートコンソールセッションへの参加（.NET IRC 専用） 126
.NET IRC 要件 127
Microsoft .NET Framework 127
Microsoft ClickOnce 127
リモートコンソール機能の使用 127
リモートコンソールを使用したキーボード操作の送信 127
リモートコンソール仮想メディア 128
リモートコンソールの仮想電源スイッチの使用 132
コンソールの取得（.NET IRC 専用） 134
リモートコンソールのホットキー 136
ホットキーの作成 137
リモートコンソールのコンピューターロックキーとホットキーを設定するためのキー 137
ホットキーのリセット 138
リモートコンソールの構成済みホットキーの表示（Java IRC のみ） 138
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 139
リモートコンソールのコンピューターロックのオプション 139
統合リモートコンソールの信頼設定（.NET IRC）の設定 139

テキストベースのリモートコンソールの使用 141
iLO 仮想シリアルポートの使用 141
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設定 142
iLO 仮想シリアルポートを使用するための Linux の設定 142
iLO 仮想シリアルポート搭載の Windows EMS コンソール 145
iLO 仮想シリアルポートを使用するための Windows の設定 145
iLO 仮想シリアルポートセッションの開始 146
iLO 仮想シリアルポートログの表示 146
テキストベースのリモートコンソール（Textcons） 147
テキストベースのリモートコンソールのカスタマイズ 147
テキストベースのリモートコンソールの使用 148
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 の使用 149

iLO 仮想メディアの使用 150
iLO 仮想メディア 150
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 151
オペレーティングシステムの USB 要件 151
Windows 7 で iLO 仮想メディアを使用するための Windows 7 の設定 151
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 152
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 153
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 153
iLO Web インターフェイスからの仮想メディアの使用 154
仮想メディアのステータスおよびポート構成の表示 154
接続されているローカルメディアの表示 154
ローカル仮想メディアデバイスの取り出し 155
URL ベースのメディアの接続 155
接続されている URL ベースのメディアの表示 156
URL ベースの仮想メディアデバイスの取り出し 157
リモートコンソールからの iLO 仮想メディアの使用 157
スクリプト仮想メディア用 IIS のセットアップ 157
IIS の設定 157
読み出し/書き込みアクセス用の IIS の設定 158
ヘルパーアプリケーションによる仮想メディアの挿入 159

仮想メディアヘルパーアプリケーションのサンプル.....159

電力および温度機能の使用.....161

サーバーの電源オン.....161
電圧低下からの復旧.....161
正常なシャットダウン.....162
電力効率.....162
電源投入時の保護.....162
電力割り当て（ブレードサーバーおよび Compute Module）.....163
サーバー電力の管理.....163
仮想電源ボタンのオプション.....164
システム電源リストアの設定.....164
自動電源オン.....165
電源オン遅延.....165
サーバー電力使用量の表示.....165
電力メーターグラフの表示オプション.....166
現在の電源状態の表示.....167
サーバー電力履歴の表示.....168
電力設定.....168
パワーレギュレーターの設定.....169
消費電力上限の構成.....170
バッテリバックアップユニット設定の構成.....171
電力しきい値設定超過の SNMP アラートの構成.....172
マウスとキーボードの持続接続の構成.....173
電力情報の表示.....173
電源装置概要の詳細.....174
電源装置のリスト.....175
Power Discovery Services iPDU 概要.....176
電力読み取り値.....177
パワーマイクロコントローラー.....177
バッテリバックアップユニットの詳細.....178
Smart ストレージバッテリのリスト.....178
電力監視.....178
高効率モード.....179
ファン情報の表示.....179
ファンの詳細.....179
ファン.....179
温度情報.....180
温度グラフの表示.....180
温度センサーデータの表示.....181
温度の監視.....181

iLO ネットワーク設定の構成.....183

iLO ネットワーク設定.....183
ネットワーク構成の概要の表示.....183
ネットワーク構成の概要の詳細.....183
IPv4 概要の詳細.....184
IPv6 概要の詳細.....184
ネットワーク共通設定.....185
iLO ホスト名の設定.....185
NIC 設定.....186
IPv4 設定の構成.....188
IPv4 設定.....189
IPv6 設定の構成.....190

IPv6 設定 191
IPv6 をサポートしている iLO の機能 193
iLO SNTP 設定の構成 193
SNTP オプション 194
iLO のクロック同期 195
DHCP NTP アドレスの選択 195
iLO NIC 自動選択 195
NIC 自動選択のサポート 196
NIC 自動選択が有効になっている場合の iLO 起動時の動作 196
iLO NIC 自動選択の有効化 197
NIC フェイルオーバーの構成 197
Windows ネットワークフォルダー内の iLO システムの表示 197

リモートサポートの管理 199
HPE 内蔵リモートサポート 199
デバイスサポート 200
HPE リモートサポートにより収集されるデータ 200
HPE プロアクティブケアサービス 201
リモートサポートの登録に関する前提条件 201
サポートされるブラウザー 202
リモートサポート登録用の ProLiant サーバーのセットアップ 203
Insight Online Direct Connect のネットワーク要件 204
Insight Remote Support Central Connect 環境のセットアップ 205
Insight Online へのアクセスの確認 206
Insight Online Direct Connect の登録 206
Insight Online Direct Connect の登録（手順 1） 207
Insight Online Direct Connect の登録（手順 2） 207
登録が完了したことの確認（iLOWeb インターフェイス） 208
登録後の手順（オプション）の完了 208
Web プロキシ設定の編集（Insight Online Direct Connect のみ） 208
Insight Remote Support Central Connect の登録 209
Insight Online Direct Connect からの登録の解除 209
Insight Remote Support Central Connect の登録解除 210
リモートサポートサービスイベント 210
サービスイベントの送信 210
メンテナンスモードの使用 211
iLO を使用したテストサービスイベントの送信 211
サービスイベントログの表示 212
サービスイベントログの消去 214
リモートサポートのデータ収集 214
データ収集情報の送信 214
Active Health System レポート情報の送信 215
iLO でのデータ収集ステータスの表示 215
iLO での Active Health System レポートステータスの表示 216
Insight Online でのデータ収集ステータスの表示 216
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 216
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 217
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 217
サポートされるデバイスの Central Connect から Direct Connect への変更 218
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 218

iLO の管理機能の使用 219

iLO ユーザーアカウント 219
ローカル ユーザー アカウントの追加 219
ローカル ユーザー アカウントの編集 220
ユーザーアカウントの削除 221
iLO ユーザーアカウントオプション 221
iLO ユーザー権限 221
パスワードに関するガイドライン 222
IPMI/DCMI ユーザー 223
ユーザーアカウントの表示 223
iLO ディレクトリグループ 224
ディレクトリグループの追加 224
ディレクトリグループの編集 225
ディレクトリグループの削除 225
ディレクトリグループのオプション 226
ディレクトリグループ権限 226
ディレクトリグループの表示 227
ブート順序 227
サーバーブートモードの設定 227
サーバーブート順序の構成 228
ワンタイムブートステータスの変更 229
ROM ベースユーティリティを次回のリセット時に起動 230
ブラウザーを使用したライセンスキーのインストール 230
ライセンス情報の表示 231
失われたライセンスキーの復旧 231
iLO ライセンス 231
Enterprise Secure Key Manager を iLO で使用する 232
キーマネージャーサーバーの構成 233
キーマネージャー構成の詳細の追加 233
ESKM 構成のテスト 234
ESKM イベントの表示 235
ESKM ログのクリア 235
言語パック 236
言語パックのインストール 236
言語パックの選択 237
デフォルト言語設定の構成 237
現在の iLO Web インターフェイスセッション言語の構成 238
言語パックのアンインストール 238
iLO がセッションの言語を決定する方法 238
ファームウェア検証 238
ファームウェア検証設定の構成 239
ファームウェア検証スキャンの実行 240
ファームウェアヘルスステータスの表示 240
フルシステムリカバリの開始 241
iLO バックアップとリストア 242
リストアされる情報 243
iLO 構成のバックアップ 243
iLO 構成のリストア 244
システムボード交換後の iLO 構成のリストア 244

iLO のセキュリティ機能の使用 246
iLO セキュリティ 246
iLO アクセス設定 247
iLO サービス設定の構成 247
iLO アクセスオプションの構成 249
SSH クライアントによる iLO ログイン 253

iLO サービスポート 254
iLO サービスポート経由での Active Health System ログのダウンロード 254
iLO サービスポートを介した iLO へのクライアントの接続 255
iLO サービスポート設定の構成 256
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 257
iLO サービスポートのサポート対象デバイス 257
iLO サービスポート経由で Active Health System ログをダウンロードするためのサンプルテキストファイル 258
SSH キーの管理 259
Web インターフェイスを使用した新しい SSH キーの認証 259
CLI を使用した新しい SSH キーの認証 260
SSH キーの削除 260
HPE SIM サーバーから SSH キーを承認するための要件 261
SSH キー 261
サポートされている SSH キー形式の例 262
CAC Smartcard 認証 262
CAC Smartcard 認証設定の構成 263
CAC Smartcard 認証用の信頼済み証明書の管理 264
証明書マッピング 266
SSL 証明書の管理 267
SSL 証明書情報の表示 268
SSL 証明書の取得とインポート 268
ディレクトリの認証と認可 270
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 271
iLO での Kerberos 認証設定の構成 271
iLO におけるスキーマフリーディレクトリ設定の構成 272
iLO における HPE 拡張スキーマディレクトリの構成 273
ディレクトリユーザーコンテキスト 275
ディレクトリサーバー CA 証明書 275
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 276
ディレクトリテストの実行 276
暗号化の設定 279
製品または高度なセキュリティのセキュリティ状態の有効化 279
FIPS および CNSA セキュリティ状態を有効にする 280
高いセキュリティ状態を使用する場合の iLO への接続 281
iLO による FIPS 承認済み環境の構成 282
FIPS モードの無効化 282
CNSA モードの無効化 283
iLO セキュリティ状態 283
SSH 暗号、キー交換、および MAC のサポート 285
SSL 暗号および MAC のサポート 285
HPE SSO 287
HPE SSO 用の iLO の設定 287
信頼済み証明書の追加 289
HPE SMS SSO 証明書の取得 289
直接 DNS 名のインポート 290
信頼済み証明書とレコードの表示 290
信頼済み証明書とレコードの削除 291
ログインセキュリティバナーの設定 291
システムメンテナンススイッチを使用した iLO セキュリティ 292

iLO 管理設定の構成 294
Agentless Management と AMS 294
Agentless Management Service 295
AMS のインストール 295

AMS のインストールの確認....296
AMS の再起動....297
System Management Assistant....298
SNMP 設定の構成....302
SNMP オプション....302
SNMPv3 認証....303
SNMP アラート送信先の構成....303
SNMP アラート送信先オプション....304
SNMP アラート送信先の削除....304
SNMPv3 ユーザーの構成....304
SNMPv3 ユーザーオプション....305
SNMPv3 ユーザーの削除....306
SNMPv3 設定の構成....306
SNMPv3 の設定オプション....307
SNMP アラートの構成....307
SNMP アラートの構成....307
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）....308
SNMP トラップ....308
iLO アラートメール....317
アラートメールを有効にする....317
アラートメールを無効にする....318
リモート Syslog....318
iLO リモート Syslog の有効化....318
iLO リモート Syslog の無効化....319

エンクロージャー、フレーム、およびシャーシの操作....320
アクティブ Onboard Administrator の使用....320
OA 情報の表示....320
OA GUI の起動....320
エンクロージャー UID LED の切り替え....321
iLO オプション....321
フレーム情報の表示....322
フレームの詳細....322
フレームの UID LED の切り替え....323
サーバーの詳細....323
サーバーの UID LED の切り替え....323
シャーシ情報の表示....323
シャーシ情報....323
電源装置のリスト....324
各電源装置の詳細....324
インテリジェント PDU の詳細....326
Smart ストレージバッテリのリスト....326
各バッテリの詳細....326
パワーレギュレーション....327
電力レギュレーターモード設定の構成....327
グローバルパワーレギュレーション設定の構成....328
ゾーンマッピングの構成....329
ゾーンの優先度設定の構成....330
消費電力上限値設定の構成....331
電力較正の構成....332

iLO と他のソフトウェア製品およびツールとの使用....334
iLO およびリモート管理ツール....334

リモート管理ツールの iLO からの起動.....334
リモートマネージャー設定の削除.....334
HPE OneView での iLO の使用.....335
Always On Intelligent Provisioning.....336
iLO からの Intelligent Provisioning の起動.....336
IPMI サーバー管理.....336
Linux 環境での IPMI ツールの高度な使用方法.....337
HPE SIM での iLO の使用.....337
HPE SIM の機能.....338
HPE SIM での SSO の確立.....338
iLO の識別および関連付け.....338
HPE SIM での SNMP アラートの受信.....339
同じ HTTP ポートを使用するための iLO と HPE SIM の設定.....339
HPE SIM での iLO ライセンス情報の確認.....340
HPE Insight Control サーバープロビジョニングでの iLO の使用.....340

Kerberos 認証とディレクトリサービス.....341
iLO での Kerberos 認証.....341
Kerberos 認証の設定.....341
Kerberos 認証用の iLO ホスト名とドメイン名の設定.....341
ドメインコントローラーでの Kerberos サポートの準備.....342
Windows 環境での iLO 用キータブファルの生成.....342
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.....344
iLO での Kerberos サポートの設定.....345
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.....345
ディレクトリの統合.....347
iLO で使用するディレクトリ構成の選択.....348
スキーマフリーディレクトリ認証.....348
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.....350
プロセスの概要：スキーマフリーのディレクトリ統合のための iLO の設定.....350
スキーマフリーの入れ子型グループ（Active Directory のみ）.....350
HPE 拡張スキーマディレクトリ認証.....350
プロセスの概要：Active Directory を使用した HPE 拡張スキーマの設定.....351
HPE 拡張スキーマの設定を使用して Active Directory を設定するための前提条件.....352
ディレクトリサービスのサポート.....352
iLO ディレクトリサポートソフトウェアのインストール.....352
Schema Extender の実行.....354
ディレクトリサービスオブジェクト.....355
Active Directory スナップインでのロールおよびオブジェクトの管理.....356
構成例：Active Directory と HPE 拡張スキーマ.....359
ディレクトリ対応リモート管理（HPE 拡張スキーマ構成）.....362
組織構造に基づいたロール.....362
ロールアクセス制限の適用方法.....363
ユーザーアクセス制限.....364
ロールのアクセス制限.....365
一度に複数の iLO システムを構成するためのツール.....367
ディレクトリサービスによるユーザーログイン.....368
ProLiant 管理プロセッサー用のディレクトリサポート（HPLOMIG）.....368
HPLOMIG によるディレクトリ認証の設定.....370
管理プロセッサーの検出.....370
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）.....372
ディレクトリ構成オプションの選択.....373
管理プロセッサーの命名（HPE 拡張スキーマのみ）.....375
HPE 拡張スキーマを選択したときのディレクトリの設定.....376
管理プロセッサーの設定（スキーマフリー構成のみ）.....379

ディレクトリ用の管理プロセッサーのセットアップ.....380
LDAP CA 証明書のインポート.....381
HPLOMIG を使用したディレクトリテストの実行（オプション）..... 382
ディレクトリサービススキーマ.....384
HPE Management コア LDAP OID クラスおよび属性..... 384
コアクラスの定義.....385
コア属性の定義.....386
Lights-Out Management 固有の LDAP OID クラスおよび属性.....389
Lights-Out Management 属性.....389
Lights-Out Management クラスの定義..... 389
Lights-Out Management 属性の定義.....390

iLO の再起動、工場出荷時リセット、および NMI の管理..... 392
iLO の再起動（リセット）.....392
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）..... 392
iLO 5 構成ユーティリティを使用した iLO のリブート（リセット）..... 392
サーバーの UID ボタンを使用した iLO の再起動（リセット）..... 393
iLO の工場出荷時デフォルト設定へのリセット..... 394
工場出荷時のデフォルト設定への iLO のリセット（iLO 5 構成ユーティリティ）.....394
NMI の生成.....395

トラブルシューティング.....396
Windbg での iLO 仮想シリアルポートの使用..... 396
サーバーヘルスサマリーの使用.....397
サーバーヘルス概要の詳細..... 398
イベントログのエントリー.....399
iLO イベントログエントリーのタイムスタンプが正しくない.....399
iLO サービスポートに接続された USB キーのマウントが失敗する..... 399
iLO 共有ネットワークポートを使用するサーバーでの仮想メディアデバイスからの OS インストールに失敗する.....400
IML のトラブルシューティングのリンク.....400
Intelligent Provisioning が iLO ナビゲーションペインにない..... 400
ログインと iLO アクセスの問題.....401
iLO ファームウェアのログイン名とパスワードが受け付けられない 401
名前を使用して iLO マネジメントポートにアクセスできない.....401
iLO ログインページにアクセスできない 402
ネットワーク設定の変更後 iLO に接続できなくなった.....402
iLO のリセット後に iLO ログインページに戻れない 403
iLO ファームウェアの更新後に iLO 接続エラーが発生する 403
NIC を用いて iLO プロセッサーに接続できない 403
iLO の証明書のインストール後 iLO にログインできない 403
iLO の IP アドレスに接続できない 404
iLO TCP/IP 通信が失敗する 404
Firefox を使用して iLO に接続するときのセキュアな接続の失敗エラー..... 404
Internet Explorer を使用して iLO の Web インターフェイスに移動するときの証明書エラー.....405
Chrome を使用して iLO の Web インターフェイスに移動するときの証明書エラー.... 406
Firefox を使用して iLO の Web インターフェイスに移動するときの証明書エラー..... 406
iLO ログインページに「Web サイトは不明な機関で認証されています」メッセージが表示される.....407
HPEOneView によって管理されるサーバー上で iLO にアクセスできない 407
iOS モバイルアプリケーションで iLO システムに接続できない.....408
iLO が ping に断続的に応答するか、または応答しない..... 408
iLO を使用した XML スクリプトの実行に失敗する.....409

ディレクトリの問題.....409
Kerberos 認証による iLO へのログインが失敗する.....409
Kerberos ログインの試行中に iLO 認証情報プロンプトが表示される 410
名前による Kerberos ログインの試行中に iLO 認証情報プロンプトが表示される 411
iLO へのディレクトリ接続が途中で終了する 411
構成されているディレクトリユーザーコンテキストが iLO ログインで動作しない 411
ディレクトリタイムアウトになった後も iLO ディレクトリユーザーアカウントがログアウトしない 412
iLO Zero サインイン構成用の Kerberos キータブファイルの生成の失敗..... 412
iLOKerberos 構成での `Setspn` の実行中のエラー 412
OpenLDAP 認証は、入れ子型グループまたは posixgroups で構成されている場合に失敗します。.....413
ドメインコントローラー OS の再インストール後に iLO Zero サインインが失敗する 413
Active Directory の認証情報での iLO ログインに失敗する 413
Directory Server DNS Name テストで失敗が報告される.....414
ディレクトリサーバーへの Ping テストが失敗を報告する.....414
Connect to Directory Server テストで失敗が報告される.....415
Connect using SSL テストで失敗が報告される..... 415
Bind to Directory Server テストで失敗が報告される.....415
Directory Administrator Login テストで失敗が報告される.....416
ユーザー認証テストで失敗が報告される.....416
ユーザー承認テストで失敗が報告される.....416
ディレクトリユーザーコンテキストテストで失敗が報告される.....416
LOM Object Exists テストで失敗が報告される..... 417
リモートコンソールの問題.....417
Linux クライアントで Firefox を使用して Java IRC を実行すると、iLO Java IRC に赤色の X が表示される 417
iLO Java IRC が起動しない 418
カーソルが iLO のリモートコンソールウィンドウの隅にアクセスできない 418
iLO リモートコンソールのテキストウィンドウが正しく更新されない..... 418
iLO .NET IRC または Java IRC（Java Web Start）でマウスやキーボードを使用できない.....419
iLO Java IRC（Java Applet）でマウスやキーボードを使用できない.....419
iLO .NET IRC がウィンドウの切り替え後に継続して文字を送信する 420
iLO Java IRC のディスケットおよび USB キーデバイス情報の表示が誤っている 420
iLO と Java IRC の間で Caps Lock が同期しない 421
iLO と共有リモートコンソールの間で Num Lock が同期しない 421
iLO リモートコンソールセッション中に意図しないキーストロークが繰り返される...421
iLO .NET IRC が再生モードにあるとき、セッションリーダーが接続要求を受信しない 422
iLO リモートコンソールのキーボード LED が正しく動作しない 422
iLO .NET IRC が非アクティブになるか切断される.....423
iLO .NET IRC がサーバーに接続できない 423
サーバーから iLO 仮想メディア USB キーにファイルをコピーした後にファイルが表示されない 424
iLO .NET IRC はアプリケーション要件を確認するのに長い時間がかかる 425
iLO .NET IRC が起動しない 425
iLO .NET IRC を共有できません 425
iLO .NET IRC が Firefox で起動しない 426
iLO .NET IRC が Google Chrome で起動しない 426
iLO リモートコンソールを使用してマウントされた USB キーを使用して DOS からブートできない.....427
SSH の問題.....427
iLO との PuTTY の初期接続時の入力が緩慢である 427
iLO 共有ネットワークポートを使用する場合、PuTTY クライアントが応答しない..... 428

iLO への SSH 接続を使用する場合にテキストが正しく表示されない.....428
SSH セッションが起動に失敗する、または予期せず終了する.....428
テキストベースのリモートコンソールの問題.....429
テキストベースのリモートコンソールで Linux インストーラーを表示できない.....429
SSH ターミナル経由でデータを送信できない.....429
シリアルタイムアウト時間内の VSP 主導の選択によって、出力が VSP ではなく BIOS リダイレクトに送信される.....429
スクロールとテキストが、BIOS リダイレクト中にイレギュラーに見える.....430
リモートサポートの問題.....430
Insight RS 登録中の SSL Bio エラー.....430
Insight Online または Insight RS でサーバー名によってサーバーが識別されない.....431
サーバーの OS 名とバージョンが Insight RS または Insight Online に表示されない... 431
Insight Online Direct Connect に登録中の接続エラー.....432
iLO Insight Online Direct Connect 登録中に iLO セッションが予期せず終了する.....432
Insight RS または Insight Online でサーバーのヘルスステータスが赤色になる..... 432
Insight Online または Insight RS でサーバー名によってサーバーが識別されない.....433
リモートサポートデータが Hewlett Packard Enterprise に送信されたときにサーバー情報が上書きされる..... 433
OS 情報が Insight Online に正しく表示されない.....434
システムボードを交換したサーバーで、Insight Online Direct Connect が動作を停止する.....434
Central Connect デバイスの重複レコードが Insight Online に存在する..... 434
デバイスの無償保証が Insight RS に期限切れとして不正に表示される..... 435
サービスイベントおよび収集が Insight RS Console に不正なタイムスタンプを表示する.....435
iLO 連携の問題.....436
iLO 連携ページでクエリエラーが発生する.....436
iLO のマルチシステムマップページにタイムアウトエラーが表示される 436
iLO マルチシステムマップページに 502 エラーが表示される 437
iLO マルチシステムマップページに 403 エラーが表示される 437
iLO ピアが iLO 連携ページに表示されない..... 438
iLO のピアが、IPv4 ネットワーク上で IPv6 アドレスで表示される.....438
ファームウェアの問題.....438
iLO ファームウェアの更新が失敗する 438
iLO ファームウェア更新エラー 439
iLO ファームウェアアップデートが終了しない 439
iLO ネットワークのフラッシュエラーリカバリ..... 440
iLO によるシステム ROM（BIOS）失敗のレポート..... 441
iLO による無効なファームウェアコンポーネントの検出.....441
ライセンス問題.....442
ライセンスキーインストールエラー.....442
仮想メディアまたはグラフィックリモートコンソールにアクセスできない.....443
iLO ライセンスキーのリカバリ.....444
Agentless Management、AMS、および SNMP の問題..... 444
AMS がインストールされているのに、iLO で使用できない 444
HPE SIM から SNMP 情報を取得できない.....445
iLO から HPE SIM のアラーム（SNMP トラップ）を受信できない.....445

Web サイト.....446

サポートと他のリソース.....448
Hewlett Packard Enterprise サポートへのアクセス.....448
アップデートへのアクセス.....448
カスタマーセルフリペア（CSR）.....449

リモートサポート（HPE 通報サービス）..... 449
保証情報..... 449
規定に関する情報..... 450
ドキュメントに関するご意見、ご指摘..... 450

iLO

iLO 5 は、HPE ProLiant サーバーおよび Synergy 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、更新、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（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。

サーバー管理者の生産性を向上させる機能および追加のセキュリティ機能がライセンス付与されています。詳しくは、**http://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 の主な機能

- **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。iLO は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と、システムボードにインストールされているファン、メモリ、ネットワーク、プロセッサー、電源装置、ストレージ、デバイスのステータスも監視します。
- **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。
- **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。
- **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。
- **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。
- **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。
- **内蔵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。
- **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。
- **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。
- **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。
- **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。
- **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。
- **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。
- **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。
- **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 Premium Security Edition のライセンスが必要です。

- **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。
- **iLO 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、製品セキュリティ状態（デフォルト）や、高度なセキュリティ、FIPS、CNSA などの高セキュリティ状態をサポートしています。
- **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できます。
- **ファームウェア管理** - コンポーネントを iLO レポジトリに保存し、SUM を使用してインストールセットを設定し、インストールキューを管理します。
- **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すすめします。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。
- **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。
- **iLO RESTful API と RESTful インターフェイスツール（iLOREST）** - iLO 5 には、Redfish API に準拠した iLO RESTful API が含まれます。
- **iLO バックアップと復元** - 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。
- **Intelligent System Tuning** - Intelligent System Tuning for Gen10 サーバーは、サーバーのパフォーマンスを向上させるいくつかの機能から構成されています。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。ワークロードが一致すると、設定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ます。コアブートは選択されたインテルプロセッサーを使用して、複数のプロセッサーコアのパフォーマンスを向上させることができます。詳しくは、*HPE Gen10 Servers Intelligent System Tuning* ホワイトペーパーを参照してください。

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。

iLO Mobile アプリケーション

iLO Mobile アプリケーションは、モバイルデバイスからご使用のサーバーへのアクセスを提供します。Mobile アプリケーションは、iLO プロセッサーと直接やり取りし、サーバーが接続されている限り常に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、空のハードディスク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。

iLO Mobile アプリケーションについて詳しくは、**http://www.hpe.com/jp/servers/ilo** を参照してください。

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構成、インベントリ、および監視タスクを実行するために使用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（**http://www.hpe.com/info/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、**http://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。

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。**http://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、iLO Advanced の機能を活用して迅速な検出、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更新を可能にする、高度なサーバーインベントリとファームウェアおよびドライバーの更新ソリューションです。iLO Amplifier Pack は、ファームウェアとドライバーの大規模更新を目的として、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 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

通常、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します。

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。

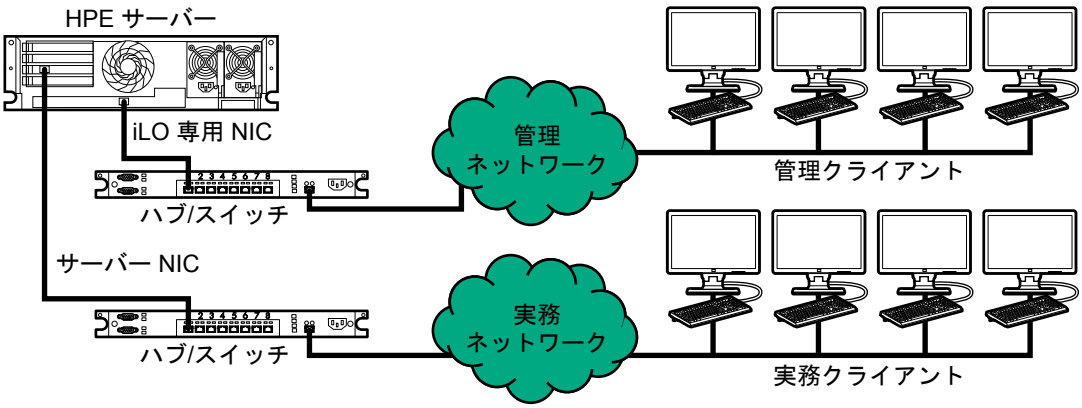


図 1: 専用管理ネットワーク

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 にアクセスできるため、iLO をサポートするために必要なネットワーキングハードウェアと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。
- サーバーのブートプロセス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 の通信がリストアされ、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。

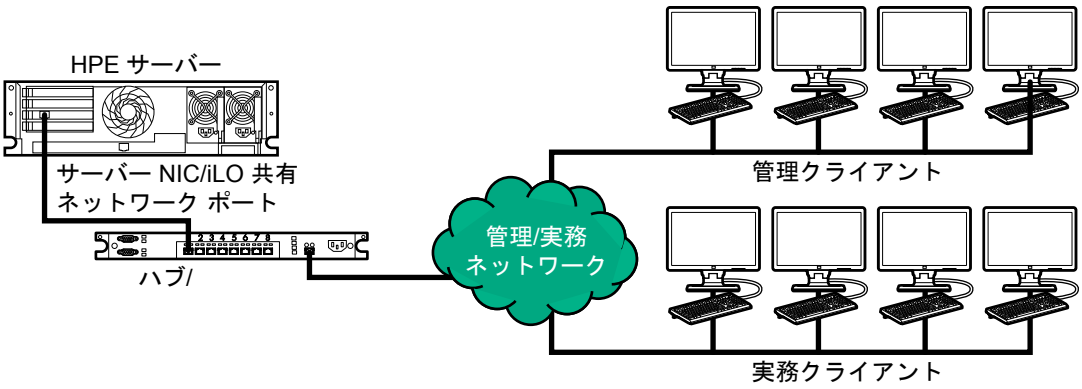


図 2: 共有ネットワーク接続

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。

詳しくは、**ProLiant ネットワークアダプターチーミングサポートドキュメント**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

iLO では、最大 6 つのディレクトリグループを設定することができます。ディレクトリサービスを使用して iLO アクセスの認証や権限付与を行います。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 Smartcard 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。

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。このガイドでは、次のインターフェイスについて説明します。

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、その他に以下の 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 Web インターフェイス経由で 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。
http://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。

  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は、Linux 用 HPONCFG のみがサポートされます。

- 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。**http://www.hpe.com/support/ilo5**

初期セットアップ手順：プロセスの概要

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 をネットワークに接続します**。
2. 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**。
3. 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**。
4. オプション：**iLO ライセンスをインストールします**。
5. **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(21 ページ)

iLO 5 構成ユーティリティを使用した iLO のセットアップ

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。

注記:

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 を構成することもできます。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。

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、**Yes - Save Changes** 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、**Yes - Save Changes** 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 ユーザー権限(221 ページ)
iLO ユーザーアカウントオプション(221 ページ)

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**を更新します。
7. **パスワード**を更新します。

   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。

   設定の構成権限は 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更新し、**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、**Yes - Save Changes** 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 ユーザー権限(221 ページ)
iLO ユーザーアカウントオプション(221 ページ)

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. 変更の確認を求めるメッセージが表示されたら、**Yes - Save Changes** 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。

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。

iLO デフォルト認証情報

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 管理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** - 無作為に選んだ 8 文字の文字列
- **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すすめします。

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、**http://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。

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 チャネルインターフェイスドライバー 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 自動サーバーリカバリドライバー - このドライバーは自動サーバーリカバリをサポートしています。

Linux

iLO で Linux を使用する場合は、`hpilo` 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` は以下の Linux カーネルに含まれます。

- SUSE Linux Enterprise Server 12 SP2 以降
- SUSE Linux Enterprise Server 11 SP4 SUSE Installation Kit 以降
- Red Hat Enterprise Linux 7.4 以降
- Red Hat Enterprise Linux 7.3 errata kernel-3.10.0-514.6.1.el7
- Red Hat Enterprise Linux 6.9 以降
- Ubuntu 16.04.3/HWE カーネル以降

`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 ドライバーを入手するには、ProLiant のサービスパックをダウンロードするか、Hewlett Packard Enterprise の Web サイトからドライバーをダウンロードします。

   Red Hat Enterprise Linux、SUSE Linux Enterprise Server、および Ubuntu 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。

   - **Windows の場合** - SPP を使用して、iLO ドライバーをインストールするか、**http://www.hpe.com/support/hpesc** の Hewlett Packard Enterprise サポートセンターからダウンロードします。

     SPP の使用については、以下の Web サイトを参照してください。

     - SPP のドキュメント：**http://www.hpe.com/info/spp/documentation**
     - SPP カスタムダウンロードホスティングサービス：**http://www.hpe.com/servers/spp/custom**

   - **VMware の場合** - Software Delivery Repository の Web サイト **http://www.hpe.com/support/SDR-Linux** の **vibsdepot** セクションから iLO ドライバーをダウンロードします。

     ソフトウェアに付属のインストール手順を実行します。

iLO の Web インターフェイスの使用

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 iLO を管理できます。また、リモートコンソール、XML 構成および制御スクリプト、SMASH CLP、または iLO RESTful API を使用することもできます。

詳しくは、次の Web サイトにある iLO および iLO RESTful API のドキュメントを参照してください。
http://www.hpe.com/support/ilo-docs

ブラウザーの要件

iLO Web インターフェイスでは、以下の要件を満たすブラウザーが必要です。

- **JavaScript** - iLO Web インターフェイスは、クライアント側 JavaScript を頻繁に使用します。

  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 JavaScript 設定の構成**(32 ページ)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** - iLO Web インターフェイス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。

サポートされるブラウザー

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。

- Microsoft Edge
- Mozilla Firefox
- Google Chrome モバイルおよびデスクトップ
- Microsoft Internet Explorer 11

Internet Explorer JavaScript 設定の構成

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**が設定されている場合、バナーテキストが**通知**セクションに表示されます。

2. 次のいずれかを実行します。

   - 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。
   - **Zero サインイン**ボタ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。

   - スマートカードを接続して、**Smartcard でログイン**ボタンをクリックします。

     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。

     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 デフォルト認証情報(29 ページ)

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**ボタンをクリック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**をクリックすると、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 セッションを閉じるには、**ログアウト**ボタンをクリックします。

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､左ペインのナビゲーションツリーに編成されています。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。

サーバータイプや設定でサポートしている場合のみ、ナビゲーションツリーに、以下のブランチが表示されます。

- また、ProLiant サーバーブレードがある場合は、**BL c-Class** ブランチが表示されます。
- Synergy Compute Module がある場合は、**Synergy フレーム**ブランチが表示されます。
- ProLiant XL サーバーがある場合は、**シャーシ**ブランチが表示されます。
- 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>**ブランチが含まれています。

iLO 制御の使用

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。

- **電源アイコン** - 仮想電源ボタン機能にアクセスするには、このアイコンをクリックします。
- **UID アイコン** - UID LED をオンまたはオフに切り替えるには、このアイコンをクリックします。

- **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、このアイコンをクリックします。

  言語設定を表示または変更するには、言語アイコンをクリックし、**設定**を選択します。

- **ヘルスアイコン** - サーバーのファン、温度センサー、および他の監視対象サブシステムの全体的なヘルスステータスを表示するには、このアイコンをクリックします。Agentless Management Service（AMS）以外のコンポーネントでは、コンポーネントをクリックすると追加情報が表示されます。
- **ユーザーアイコン** - このアイコンは、以下の場合にクリックします。
  - 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するには、ユーザーアイコンをクリックし、**ログアウト**を選択します。
  - アクティブな iLO セッションを表示するには、ユーザーアイコンをクリックし、**セッション**を選択します。
  - iLO ユーザーアカウントを表示または変更するには、ユーザーアイコンをクリックし、**設定**を選択します。
- **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、このアイコンをクリックします。
- **省略記号アイコン** - 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。**ファームウェアアップデート**および **iLO レポジトリにアップロード**オプションにアクセスするには、このアイコンをクリックします。これらのオプションは、**ファームウェア & OS ソフトウェア**のすべてのタブで利用可能です。

iLO ナビゲーションペイン

iLO には、各ページからアクセス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の表示/非表示を切り替えるには、iLO Web インターフェイスの左上隅にあるアイコンをクリックします。

- ナビゲーションペインを非表示にするには、X アイコンをクリックします。
- ナビゲーションペインを表示するには、iLO Web インターフェイスの左上隅にあるアイコンをクリックします。
- 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。
- モニターを備えたサーバーの場合：スリープモードになっているモニターを起動するには、ナビゲーションペインで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**を選択します。

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、リモート管理システムの動作に影響を及ぼす可能性があります。

2. リモート管理ツールの名前はリンクになっています。このリンクをクリックして、リモート管理ツールを起動してください。

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。

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 の更新に失敗した場合や、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。
- **内蔵リモートコンソール** - サーバーコンソールとのリモートのアウトオブバンド通信用に HTML5 IRC、.NET IRC、または Java IRC アプリケーションを起動するためのリンクを提供します。リモートコンソールの使用可能なオプションについては、**iLO リモートコンソール**(119 ページ)を参照してください。

- **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。
- **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。**ファームウェアアップデート**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。

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。**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。
- **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。
- **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 インターフェイスウィンドウの上部にある UID 制御をクリックするか、サーバーシャーシにある 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。

- **TPM ステータス**または **TM ステータス** - TPM または TM 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、iLO RESTful API、CLP、および XML インターフェイスに渡します。

- **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。
- **SD カードステータス** - 内蔵 SD カードのステータス。SD カードが存在する場合、SD カードのブロック数が表示されます。
- **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、シャーシ侵入検知コネクターを持つサーバー、および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。

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。

- **Remote Support 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。

iLO セッションの管理

前提条件

ユーザーアカウント管理特権

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 : 1 つまたは複数のセッションを切断するには、切断する各セッション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。

セッションリストの詳細

iLO では、**現在のセッション**および**セッションリスト**テーブルに以下の詳細が表示されます。

- **ユーザー** - iLO ユーザーアカウント名。
- **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。

- **ログイン時刻** - 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**。

iLO イベントログ

このイベントログは、iLO ファームウェアが記録した重大なイベントの記録です。

記録されるイベントには、サーバーの電源障害やサーバーリセットのような重大なサーバーイベントと、無許可ログイン試行のような iLO イベントが含まれます。また、他に成功または失敗したブラウザーログインおよびリモートコンソールログイン、仮想電源および電源の再投入イベント、ログのクリア、ならびにユーザーの作成や削除のような設定変更も含まれます。

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、およびすべてのログイン失敗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：イベントログのソート、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。

   記録されたイベントの合計数がフィルターアイコンの上に常に表示されます。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。
3. 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。

イベントログの詳細

- **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、イベントログは ID でソートされ、最新のイベントが先頭になります。
- **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、記録されるイベントのコンポーネントと詳細な特性が特定されます。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更新するか、イベントログをクリアすることによって解決できます。
- **最終更新** - 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。

イベントが更新された日時を iLO ファームウェアが認識しなかった場合は、「未セット」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イベントログエントリーを生成します。これらのイベントが 1 つのイベント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 つのイベントログエントリーにまとめられ、**回数**および**最終更新**の値が更新されます。各イベントタイプは特定の間隔を備えており、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

iLO は、以下のアイコンを使用してイベントの重要度を示します。

- **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。
- **警戒** - 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。
- **不明** - イベントの重要度を判断できませんでした。

イベントログイベントペインの詳細

- **初期更新** - 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、未セットと表示されます。

- **イベントコード** - 特定のイベントクラス内のイベントの一意の識別子。16 進数で表示されます。

イベントログのビューのカスタマイズ

イベントのソート

列の見出しをクリックすると、その列でイベントログテーブルをソートします。

表示の昇順と降順を切り替えるには、列の見出しを再度クリックします。

イベントフィルター

イベント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、**Severity** メニューから深刻度レベルを選択します。
- イベント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。

- 最終更新日でフィルタリングするには、**最終更新**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。

CSV ファイルへのイベントログの保存

サポート対象のブラウザーを使用して、イベントログを CSV ファイルにエクスポートします。

手順

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

イベントログのクリア

前提条件

iLO 設定の構成特権

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。
3. 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。

   以前に記録されたすべての情報のイベントログが消去されて、イベントが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 に記録される情報の種類の例は、次のとおりです。

- Fan inserted（ファンが取り付けられた）
- Fan removed（ファンが取り外された）
- Fan failure（ファンが故障した）
- Fan degraded（ファンの機能が低下した）
- Fan repaired（ファンが修復した）
- Fan redundancy lost（ファンの冗長性が失われた）
- Fans redundant（ファンは冗長）
- Power supply inserted（電源装置が取り付けられた）
- Power supply removed（電源装置が取り外された）
- Power supply failure（電源装置が故障した）
- Power supplies redundancy lost（電源装置の冗長性が失われた）
- Power supplies redundant（電源装置冗長化）
- Temperature over threshold（温度のしきい値は異常）
- Temperature normal（温度は正常）
- Automatic shutdown started（自動シャットダウンが開始した）
- Automatic shutdown cancelled（自動シャットダウンが取り消された）
- Drive failure（ドライブ障害）

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：IML のソート、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。

   記録されたイベントの合計数がフィルターアイコンの上に常に表示されます。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。
3. 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 の詳細

- 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を使用して、修復済みとしてマークするイベントを選択します。
- **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、IML 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、記録されるイベントのコンポーネントと詳細な特性が特定されます。

  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更新するか、ログをクリアすることによって解決できます。

- **最終更新** - 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。

  イベントが更新された日時を iLO が認識しなかった場合は、「未セット」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 IML エントリーを生成します。これらのイベントが 1 つのイベント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 IML エントリーにまとめられ、**回数**および**最終更新**値が更新されます。各イベントタイプは特定の間隔を備えており、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

iLO は、以下のアイコンを使用して IML イベントの重要度を示します。

- **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。
- **不明** - イベントの重要度を判断できませんでした。

IML イベントペインの詳細

- **初期更新** - 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、「未セット」と表示されます。

- **イベントコード** - 特定のイベントクラス内のイベントの一意の識別子（16 進数で表示されます）。
- **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。

IML ビューのカスタマイズ

イベントのソート

列の見出しをクリックすると、その列で IML テーブルをソートします。

表示の昇順と降順を切り替えるには、列見出しの横にある矢印をクリックします。

イベントフィルター

イベント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**リストから深刻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。
- イベント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。
- **最終更新**日付でフィルタリングするには、**最終更新**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、をクリックして検索ボックスにテキストを入力します。

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 の設定の構成

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

アップグレード、システムバックアップ、定期的システムメンテナンス、ソフトウェアインストールなどのメンテナンス作業に関するログエントリーを作成するには、メンテナンスノート機能を使用します。

前提条件

iLO の設定の構成

手順

1. ナビゲーションツリーで**情報**をクリックして、**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。

   Maintenance クラスの **Informational** 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

サポート対象のブラウザーを使用して、IML を CSV ファイルにエクスポートします。

手順

1. ナビゲーションツリーで**情報**をクリックし、**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. CSV アイコンをクリックします。
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。

IML のクリア

前提条件

iLO 設定の構成特権

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。
3. 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。

以前に記録されたすべての情報の IML が消去されて、イベントが IML 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。

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、Privacy Statement（**http://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（**http://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。

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。

- **iLOWeb インターフェイス**
- **iLO サービスポート** - 詳しくは、**iLO サービスポート**(254 ページ)を参照してください。
- **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。
- **Active Health System ダウンロード CLI** - 手順については、サーバーのトラブルシューティングガイドを参照してください。
- **UEFI システムユーティリティ** - 手順については、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。
- **`curl` ユーティリティ**
- **iLO RESTful API** - 詳しくは、**http://www.hpe.com/support/restfulinterface/docs** を参照してください。

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。

   Intelligent Provisioning、iLO サービスポート、または Active Health System ダウンロード CLI ツールで Active Health System ログが使用されている場合、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、**リセット**アイコン↺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 Privacy Statement 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、**http://www.hpe.com/servers/ahsv** をご覧ください。

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。

   Intelligent Provisioning、iLO サービスポート、または Active Health System ダウンロード CLI ツールで Active Health System ログが使用されている場合、Active Health System ログにアクセスできません。

2. **アドバンス設定を表示**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 Privacy Statement 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、**http://www.hpe.com/servers/ahsv** をご覧ください。

curl を使用した Active Health System ログの抽出

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. 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
```

5. ファイルは指定したパスに保存されます。
6. コマンドウィンドウを閉じます。

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

指定すると HTTPS 警告が無視されます。

-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、次の手順を使用して Active Health System ログを消去してください。

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**をクリックして、**Active Health System ログ**タブをクリックします。

   Intelligent Provisioning、Active Health System ダウンロード CLI ツール、または iLO サービスポートで Active Health System ログが使用されている場合、Active Health System ログにアクセスできません。

2. **アドバンス設定を表示**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、**OK** 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 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、内部 iLO 診断テストの結果やテスト名、ステータス、ノートなどが表示されます。

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

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。

iLO セルフテスト

セルフテストの詳細

セルフテスト

テスト済みの関数。

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。
- **障害** - 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更新、またはサービスが必要になる場合があります。
- **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。

注意事項

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。
- **Embedded Flash** - 構成、プロビジョニング、およびサービスの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。

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更新されます。

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、列見出しの右側にある矢印アイコンをクリックします。

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**
- **電源ステータス**

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 バッテリステータス**（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

ヘルスサマリーページでは、次のステータスの値を使用します。

- **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。ただし、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**と表示されます。

- **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に関するデータを受信していません。iLO をリセットしたときにサーバーの電源が切れていた場合、サーバーの電源が切れているとステータスを更新できないため、一部のサブシステムでは、**不明**のステータスが表示されます。
- **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更新されます。

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更新されます。

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
   - 論理メモリ

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。空のメモリソケットを表示するには、**空白のソケットを表示**をクリックします。空のメモリソケットが表示されている場合、それらを非表示にするには、**空白のソケットを隠す**をクリックします。
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、列見出しの右側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 Online Spare Rank 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 Online Spare Channel 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 Online Spare Rank 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 Online Spare Channel 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。

ソケット数

現在のメモリモジュールソケット数。

トータルメモリ

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。

速度

メモリモジュールの速度。

電圧

メモリが動作する電圧。

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。

位置

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。

サイズ

メモリモジュールのサイズ（MB）。

速度

メモリモジュールの速度。

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** - 存在しません。
- **同期**
- **RDIMM**
- **UDIMM**
- **LRDIMM**
- **NVDIMM**
- **NVDIMM-N**
- **R-NVDIMM**

論理メモリ詳細

このセクションには、構成済みであり、POST 実行時に正常に動作した HPE スケーラブル永続性メモリデバイスが表示されます。

位置

論理デバイスのプロセッサーまたは領域。例：**プロセッサー 1、2: スパン論理 NVDIMM**、**プロセッサー 1: 論理 NVDIMM 1**

ステータス

論理メモリのステータス。

サイズ

論理メモリのサイズ（MB）。

速度

論理メモリの速度。

テクノロジー

論理メモリテクノロジー。表示される可能性がある値は、以下のとおりです。

- **NVDIMM**
- **NVDIMM-N**
- **R-NVDIMM**

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 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、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。

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** - メモリの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。

最小電圧

メモリモジュールが動作可能な最小電圧。

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。

スロット

メモリモジュールのスロット番号。

ソケット

メモリモジュールのソケット番号。

状態

メモリの状態。

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。

メディア寿命

メディアの残りの寿命の割合。

論理メモリ

名前

メモリモジュールの製品名。

製造元

メモリモジュールの製造元。

パワーバックアップユニットベイ

論理 DIMM にバックアップ電源を提供するバッテリバックアップユニットのベイの数。

タイプ

搭載されたメモリのタイプ。

論理メモリの唯一の可能な値は**論理**です。

最小電圧

メモリモジュールが動作可能な最小電圧。

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）。

Memory Media

メモリモジュールの独自のメディアソース。例：**NAND**、**Proprietary**

状態

メモリの状態。

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。

メディア寿命

メディアの残りの寿命の割合。

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、この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更新されます。

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更新されます。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、列見出しの右側にある矢印アイコンをクリックします。
3. オプション：このページでデータを展開するには**すべてを展開**をクリックし、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。

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たことがない場合、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が現在は接続されていない場合、iLO はステータスを**リンクダウン**と表示します。

  - 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**アップ**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。

  - VMware サーバー：

    iLO が NIC ポートと通信できない場合、ステータスは**不明**と表示されます。

    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**アップ**と表示します。

- **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。
- **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、ブートの進行状況とブートターゲットに関する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更新されます。

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：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、列見出しの右側にある矢印アイコンをクリックします。

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。

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。

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。これを実行すると、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 Array、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。

前提条件

iLO 設定の構成特権

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 設定の構成特権

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サーバーとすべてのアダプターで 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 検出がサーバーとすべてのアダプターで有効になります。

ストレージ情報の表示

サーバーの電源がオフの場合、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更新されます。

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、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：データを展開するには**すべてを展開**をクリックし、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. Smart アレイコントローラーのみ：表示するコントローラーに対して、次のオプションのいずれかを選択します。

   - **論理ビュー** - 設定されている論理ドライブと、関連付けられた物理ドライブを表示します。このビューには、アレイの一部またはスペアドライブとして構成されていない物理ドライブは表示されません。
   - **物理ビュー** - 物理ドライブを表示します。このビューには論理ドライブは表示されません。

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 Array コントローラ、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。
- 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。

  iLO 5 は次の製品をサポートします。

  - 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

このページには、最初に Smart Array コントローラが表示され、続いて他の 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が表示されます。

Smart アレイの詳細

iLO では、コントローラー、エンクロージャー、論理ドライブ、および物理ドライブの情報が表示されます。

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。

コントローラー

このセクションには、Smart アレイコントローラーごとに以下の詳細が表示されます。

- コントローラー位置 - スロット番号またはシステムボード
- 最上位のコントローラーステータス（コントローラーの場所の左側に表示される） - コントローラーのハードウェアステータスと、キャッシュモジュール、エンクロージャー、物理ドライブ、論理ドライブ、およびそのコントローラーと関連付けられたスペアドライブのステータスとの組み合わせです。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、障害の種類によって、**メジャー警告**、または**劣化**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**障害**の場合、最上位のコントローラーステータスは**障害**です。
- **コントローラーステータス** - コントローラーハードウェアステータス（**OK** または**障害**）
- **シリアル番号**
- **モデル**
- **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。

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。

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設定できます。

ドライブエンクロージャー

このセクションには、Smart アレイコントローラーに接続されているドライブエンクロージャーに関する以下の情報が表示されます。

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

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なく、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ありません。

論理ドライブ

論理ビューオプションを選択すると、Smart アレイコントローラーに接続されている論理ドライブについて以下の情報が表示されます。

- 論理ドライブ番号
- **ステータス**
- **容量**
- **フォールトトレランス**
- **論理ドライブのタイプ**
- **暗号化ステータス**

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

物理ドライブ

このセクションで示される情報は、**論理ビュー**オプションと**物理ビュー**オプションのうちどちらが選択されているかによって異なります。 **論理ビュー**では、アレイの一部として構成されている物理ドライブが表示されます。 **物理ビュー**では、すべての物理ドライブが表示されます。

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。

Smart アレイコントローラーに接続されている物理ドライブについて、次の情報が一覧で表示されます。

- 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**
- **シリアル番号**
- **モデル**
- **メディアタイプ**
- **容量**
- **位置**
- **ファームウェアバージョン**
- **ドライブの構成**
- **暗号化ステータス**

直接接続ストレージの詳細

コントローラー

このセクションには、直接接続ストレージを管理する Hewlett Packard Enterprise および他社製のストレージコントローラーに関する以下の情報が表示されます。

- コントローラー情報
- 最上位のコントローラーステータス - 最上位のコントローラーステータス（コントローラーの場所の左側に表示される）は、コントローラーのハードウェアステータスと、エンクロージャー、物理ドライブ、およびそのコントローラーと関連付けられたスペアドライブのステータスとの組み合わせです。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、障害の種類によって、**メジャー警告**、または**劣化**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**障害**の場合、最上位のコントローラーステータスは**障害**です。
- **コントローラーステータス** - コントローラーハードウェアステータス（**OK** または**障害**）
- **シリアル番号**
- **モデル**
- **ファームウェアバージョン**
- **コントローラータイプ**

物理ドライブ

このセクションでは、Hewlett Packard Enterprise および他社製のストレージコントローラーに接続された物理ドライブに関する情報が表示されます。

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。

- 物理ドライブの位置
- **ステータス**
- **シリアル番号**
- **モデル**
- **メディアタイプ**
- **容量**
- **位置**
- **ファームウェアバージョン**
- **ドライブの構成**
- **暗号化ステータス**

ファームウェアおよびソフトウェアの表示および管理

ファームウェアの更新

ファームウェアの更新では、新機能、改良、およびセキュリティ更新によりサーバーと 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更新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更新する場合、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更新を実行できます。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特権は確認されません。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、高度なセキュリティ、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。

iLO 5 1.20 以降を搭載した HPONCFG バージョン 5.2.0 以降を使用する際に必要なユーザーの権限を持っていない場合、HPONCFG はエラーメッセージを表示します。

オンラインによるインバンドのファームウェアアップデート方法の例として、iLO オンライン ROM フラッシュコンポーネントや HPONCFG があります。

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 設定の構成特権を持つユーザーは、アウトオブバンド方式を使用してファームウェアを更新できます。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更新できます。

オンラインでのアウトオブバンドのファームウェアアップデート方法の例として、iLO Web インターフェイス、HPQLOCFG、HPLOMIG、iLO RESTful API、LOCFG.PL および SMASH CLP があります。

詳しくは

iLO ドライバーのインストール(31 ページ)

オンラインでのファームウェアアップデート方法

インバンドのファームウェアアップデート

- **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更新します。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。

Web サイト **http://www.hpe.com/support/ilo5** で、iLO およびサーバーファームウェア向けオンライン ROM フラッシュコンポーネントをダウンロードすることができます。

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更新します。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。

  サンプルスクリプトは **http://www.hpe.com/support/ilo5** から入手できます。スクリプティングについて詳しくは、iLO スクリプティング/CLI ガイドを参照してください。

  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は、Linux 用 HPONCFG のみがサポートされます。

アウトオブバンドのファームウェアアップデート

- **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更新できます。
- **iLO RESTful API** - iLO RESTful API および RESTful インタフェースツールなどの REST クライアントを使用して、ファームウェアを更新します。

  詳しくは、**http://www.hpe.com/info/restfulinterface/docs** を参照してください。

- **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更新します。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。

  サンプルスクリプトは **http://www.hpe.com/support/ilo5** から入手できます。スクリプティングについて詳しくは、iLO スクリプティング/CLI ガイドを参照してください。

- **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ぶ） - 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更新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、ファームウェアを更新します。

  SMASH CLP 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。

オフラインでのファームウェアの更新

ファームウェアの更新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の更新方法の例として、SPP、SUM、Scripting Toolkit for Windows、および Scripting Toolkit for Linux があります。

オフラインでのファームウェア更新方法

以下のオフラインファームウェア更新方法を使用できます。

SPP

SPP を使用して、ファームウェアをインストールします。詳しくは、次の Web サイトを参照してください。**http://www.hpe.com/info/spp/documentation**

SUM

SUM は、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のためのツールです。

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、ファームウェアを更新したりします。この方法は、複数のサーバーを展開する場合に便利です。手順については、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。

ファームウェアおよびソフトウェアの表示およびアップデート

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。
- アクティブなシステム ROM および冗長化システム ROM を**スワッピング**する。
- **インストールされているソフトウェア**を表示する。
- **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。

- **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 レポジトリに**コンポーネントをアップロード**する。
  - **iLO レポジトリ**を管理し、保存されているコンポーネントをインストールキューに追加する。
  - **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。

  - インストールキューに**コンポーネントを追加**する。
  - **インストールキュー**のコンポーネントを表示および削除する。

    インストールキューの管理には SUM を使用することをおすすめします。iLO Web インターフェイスを使用すると、個々のコンポーネントを追加または削除することによってキューを更新できます。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。

インストール済みファームウェア情報の表示

手順

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更新されます。

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 ストレージバッテリ
- 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
- イノベーションエンジン（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

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

- サーバーは冗長なシステム ROM をサポートしています。
- 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**ファームウェア & OS ソフトウェア**をクリックします。
2. **インストールされたファームウェア**ページで、**冗長化システム ROM** の詳細の横にあるスワップアイコン🔁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. **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。

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更新

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更新できます。署名済みファイルが必要です。

iLO レポジトリページから iLO またはサーバーのファームウェアアップデートを開始することもできます。

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 設定の構成特権が必要です。
- 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、リカバリセット特権が必要です。
- **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. **iLO ファームウェア**または**サーバーファームウェア**のファイルを入手します。
2. 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**をクリックします。

   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。
3. **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。
4. 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。

- **ローカルバイナリファイル**ボックスで、**参照**（Internet Explorer または Firefox）あるいは**ファイルを選択**（Chrome）をクリックしてから、ファームウェアコンポーネントの場所を指定します。
- **リモートのバイナリファイル 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。

5. 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。
6. 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して、既存のコンポーネントを選択したコンポーネントに置き換えます。

   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か、必要な特権が与えられていない場合は、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、**同様に、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。
7. TPM または TM がサーバーにインストールされている場合は、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 のオーバーライドを確認する**チェックボックスを選択します。

   注意:
   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。
8. **フラッシュ**をクリックして、更新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 ファームウェアを更新すると、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。
9. **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 ファームウェアを更新すると、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。
10. iLO ファームウェアアップデートのみ : 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。
11. サーバーファームウェアアップデートのみ : 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。詳しくは、ファームウェアの更新を有効にするための要件(80 ページ)を参照してください。
12. 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。

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、さまざまなタイプのファームウェアアップデートがサポートされます。この中には以下のタイプが含まれます。

- iLO
- システム ROM/BIOS
- シャーシ
- 電源管理コントローラー
- プログラマブルロジック（CPLD）
- バックプレーン
- 言語パック

ファームウェアの更新を有効にするための要件

- iLO ファームウェアまたは言語パック ー iLO のリセットが必要です。これは自動的にトリガーされます。
- 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。

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 iLO 連携グループ内の 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 ROM 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。**http://www.hpe.com/support/hpesc**
2. 画面の指示に従って iLO オンライン ROM 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。
  - `#sh ./CP00XXXX.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。**http://www.hpe.com/support/hpesc**
2. 画面の指示に従ってオンライン ROM 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. 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。
4. 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。

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 を更新する場合、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。

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更新するには、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 では最終更新の日時が表示されます。ページの更新から 5 分以上が経過している場合は、をクリックしてページを最新情報に更新します。

製品関連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 を使用してインストールされた、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。

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。このフラッシュメモリは、iLONAND 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、サポートされるサーバーに適用できます。SUM を使用して保存されているコンポーネントをインストールセットに整理し、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 が連携してソフトウェアとファームウェアを管理する方法については、SUM ドキュメントを参照してください。

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、キューの末尾に追加されます。キューに入れられた他の項目が完了した後、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。

キューにすでに入れられているタスク内のコンポーネントが開始または終了を待機している場合、キューに入れられた新しいコンポーネント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アップデートがサーバーの POST 中に UEFI BIOS によって検出されるまで待機する必要があり、サーバーが再起動されていない場合、キュー内のその後のアップデートはインストールされません。

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**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にある、コンポーネントのインストールアイコンをクリックします。

   iLO は、コンポーネントがインストールキューの末尾に追加されることを通知し、要求を確認するプロンプトを表示します。
3. **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。

iLO レポジトリからのコンポーネントの削除

前提条件

- iLO の設定の構成
- コンポーネントはインストールセットに含まれていない。
- コンポーネントはキュー内の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. コンポーネントの削除アイコンをクリックします。

   iLO によって要求を確認するように求められます。
3. **はい、削除**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 設定の構成特権
- 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 : 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 レポジトリの詳細

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 **Contents** 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の一部かどうか

iLO レポジトリにアップロードペインの使用

iLO レポジトリにアップロードペインを使用して、iLO レポジトリにアップロードの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。

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。

iLO レポジトへのコンポーネントの追加

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 設定の構成特権が必要です。
- 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、リカバリセット特権が必要です。
- **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。
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。
   - **ローカルバイナリファイル**ボックスで、**参照**（Internet Explorer または Firefox）あるいは**ファイルを選択**（Chrome）をクリックしてから、ファームウェアコンポーネントの場所を指定します。
   - **リモートのバイナリファイル 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. 前の手順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。

   - **ローカルコンポーネント署名ファイル**ボックスで、**参照**（Internet Explorer または Firefox）あるいは**ファイルを選択**（Chrome）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。
   - **リモートのコンポーネント署名ファイル 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、既存のコンポーネントを選択したコンポーネントに置き換えます。

   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か、必要な特権が与えられていない場合は、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。

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 を使用してインストールセットを作成します。iLO を使用して既存のインストールセットを iLO Web インターフェイスに表示できます。

SUM から展開する際に、インストールセットを保存すると、iLO システム上にすべてのコンポーネントが保持されるので、元の SPP を検索することなく、後ですぐに使用して、コンポーネントバージョンを復元したり、ロールバックしたりできます。

iLO、SUM、および BIOS 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インストールキューの末尾に追加します。キューに入れられた他の項目が完了した後、各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、インストールセットの内容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、コンポーネントの詳細を確認してください。

キューにすでに入れられているタスク内のコンポーネントが開始または終了を待機している場合、キューに入れられた新しいコンポーネント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アップデートがサーバーの POST 中に UEFI BIOS によって検出されるまで待機する必要があり、サーバーが再起動されていない場合、キュー内のその後のアップデートはインストールされません。

前提条件

- iLO 設定の構成権限
- 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にあるインストールアイコンをクリックします。

   iLO は、インストールセットの内容がインストールキューの末尾に追加されることを通知し、要求を確認するプロンプトを表示します。
3. **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 がインストールセットでアップデートを開始できる場合、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。

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 設定の構成特権。
- 保護されたインストールセットを削除するための iLO 設定の構成特権とリカバリセット特権。

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. インストールセットの削除アイコン 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。

   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

この手順を使用して、すべてのインストールセットを削除します。

システムリカバリセットが存在し、リカバリセットの特権を持たない場合は、このアクションによってリカバリセットは削除されません。システムリカバリセットが存在し、リカバリセット特権を持っている場合は、リカバリセットを削除または保存することができます。

前提条件

- iLO 設定の構成特権
- リカバリセットの特権（システムリカバリセットが存在する場合）

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. システムリカバリセットが存在し、リカバリセット特権を持っている場合、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する**チェックボックスを選択します。
4. **はい、すべて削除します**をクリックします。

   インストールセットが削除されます。

インストールセットの表示

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、**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：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詳細

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。

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**したりします。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。

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。
- **システムリカバリセット?** - インストールセットを編集または削除できるかどうかを示します。このステータスは**システムリカバリセット**で使用します。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。

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

デフォルトのシステムリカバリセットが削除された場合、**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、SUM ユーザーガイドを参照してください。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の順序付けされたリストです。コンポーネントは、次の方法を使用してインストールキューに追加できます。

- SUM を使用する。
- iLO の**キューに追加**ペインを使用する。
- iLO リポジトリページで、コンポーネントのインストールアイコンをクリックする。

コンポーネントをインストールキューに追加すると、キューの末尾に追加されます。キューに入れられた他の項目が完了した後、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。

キューにすでに入れられているタスク内のコンポーネントが開始または終了を待機している場合、キューに入れられた新しいコンポーネント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アップデートがサーバーの POST 中に UEFI BIOS によって検出されるまで待機する必要があり、サーバーが再起動されていない場合、キュー内のその後のアップデートはインストールされません。

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。

インストールキューの表示

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、**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の詳細

タスクの概要の詳細

インストールキュータブには、各タスクに関する以下の詳細が表示されます。

状態

タスクのステータス。値には、以下のものがあります。

- **進行中** - タスクは処理されています。
- **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。
- **完了** - タスクが正常に完了しました。
- **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。

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、ステータスは**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）。

個々のタスクの詳細

個々のタスクをクリックすると、以下の詳細が表示されます。

- **名前** - タスク名。
- **状態** - タスクの状態。
- **結果** - タスクの結果（ある場合）。
- **Installable by** - 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。
- **開始時刻** - 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、ステータスは**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）。

インストールキューからのタスクの削除

前提条件

iLO の設定の構成

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 によって要求を確認するように求められます。
3. **はい、削除**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 設定の構成特権
- 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。

キューに追加ペインの使用

キューに追加ペインを使用して、コンポーネント、インストールセット、またはインストールキューへのコマンドの追加を行います。

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。

インストールキューへのコンポーネントの追加

前提条件

- インストールキューにコンポーネントを追加するには、iLO 設定の構成特権が必要です。
- 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、リカバリセット特権が必要です。
- **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、**キューに追加**をクリックします。
2. タスク名を入力します。
3. **コンポーネント**ボックスで値を選択します。

   リストには、iLO レポジトリに格納されているコンポーネントが含まれます。
4. オプション：キューに入れられたコンポーネントの開始および終了時刻を指定します。

   a. **時間枠を指定してください**チェックボックスを選択します。

   b. **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。

   c. カレンダーで範囲の開始日を選択します。

   d. **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。

   e. カレンダーで範囲の終了日を選択します。終了日はタスクの有効期限（日付と時刻）を設定します。
5. 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、既存のコンポーネントを選択したコンポーネントに置き換えます。

   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か、必要な特権が与えられていない場合は、このオプションは表示されません。
6. TPM または TM がサーバーにインストールされている場合は、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 のオーバーライドを確認する**チェックボックスを選択します。

   △ **注意:**
   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。
7. **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。

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。

指定された期間内にアップデートが開始されない場合は、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、iLO RESTful API を使用して、スケジュールを更新します。

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、アップデートが開始され、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。

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 連携ページがロードされると、Web インターフェイスを実行する iLO システムから iLO 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 - iLO 連携グループ内のサーバー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 - iLO 連携グループ内のサーバーの電源ステータスを管理します。
- グループ消費電力上限 - iLO 連携グループ内のサーバー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 - iLO 連携グループ内のサーバーのファームウェアを更新します。
- 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、iLO 連携グループ内のサーバー上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。

一度につき 1 つの iLO システム用にマルチキャストオプションを構成

以下の手順を実行して、iLO 連携グループに追加される各 iLO システムのマルチキャストオプションを構成する必要があります。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。

複数の iLO システムに対して、iLO RESTful API または RIBCL スクリプトを使用してマルチキャストオプションを表示および構成できます。

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 **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）** - iLO システムがネットワーク上で自身を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。
- **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。デフォルト値は 5 です。

iLO 連携グループ

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。

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。

iLO 連携グループの権限

iLO 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。
- **リモートコンソール** - グループのメンバーは、ビデオ、キーボード、マウスの制御を含めて、管理対象サーバーのリモートコンソールにリモートにアクセスできます。
- **仮想電源およびリセット** - グループのメンバーは、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。ここに示した作業は、システム可用性に割り込みます。
- **仮想メディア** - グループのメンバーは、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。
- **ホスト BIOS 構成** - グループのメンバーは、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。
- **iLO 設定を構成** - グループのメンバーは、セキュリティ設定を含むほとんどの iLO 設定を行い、リモートでファームウェアを更新することができます。
- **ユーザーアカウント管理** - グループのメンバーは、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** - グループのメンバーはホスト NIC 設定を構成できます。
- **ホストストレージ構成** - グループのメンバーは、ホストストレージ設定を構成できます。
- **リカバリセット** - グループのメンバーはリカバリインストールセットを管理できます。

  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。

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。

- iLO システムは最大で 10 の iLO 連携グループのメンバーとなることができます。
- グループの中にある 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 の設定の構成が必要です。
- 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に対して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、次の Web サイトにある iLO RESTful API のドキュメントを参照してください。**http://www.hpe.com/support/restfulinterface/docs**

- 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すすめします。

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 設定の構成権限

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. **グループへの参加**をクリックします。
3. 次の情報を入力します。

   - **グループ名** - グループ名は 1～31 文字で指定できます。
   - **グループキー** - グループのパスワードは、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。
   - **グループキーの確認** - グループのパスワードの確認。

   既存のグループの名前とキーを入力すると、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すると、グループが作成され、ローカル iLO システムが新しいグループに追加されます。

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 設定の構成**
- **ユーザーアカウント管理**
- **ホスト NIC**
- **ホストストレージ**
- **リカバリセット**

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。

5. **グループへの参加**をクリックします。

iLO 連携グループメンバーシップの編集

前提条件

iLO の設定の構成

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。

5. 更新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。

   使用可能な権限について詳しくは、**iLO 連携グループの権限**(97 ページ)を参照してください。

6. **グループの更新**をクリックします。
7. グループ名またはグループキーを更新した場合は、それらを他のシステムの影響を受けるグループで更新します。

iLO 連携グループからのローカル iLO システムの削除

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 **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を表示する（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。

グループに関する情報を表示するのに RIBCL スクリプトを使用することもできます。詳しくは、iLO 連携ユーザーガイドを参照してください。

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。

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、iLO 連携グループの追加

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 iLO 連携グループを作成します。たとえば、DEFAULT グループと同じシステムを含むが、権限が異なるグループを作成する必要があるとします。

前提条件

- iLO 設定の構成権限
- 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、次の web サイトにあるライセンス文書を参照してください。
  http://www.hpe.com/support/ilo-docs

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。

   iLO 連携グループが存在しない場合、このページには、構成済みのグループはありませんというメッセージが表示されます。iLO 連携**セットアップ**ページを使用してグループを作成します。

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、このページで作成したグループに追加されます。

3. 次の情報を入力します。

- **グループ名** - グループ名は 1～31 文字で指定できます。
- **グループキー** - グループのパスワードは、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。
- **グループキーの確認** - グループのパスワードの確認。

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。

4. 次の権限のいずれかを選択します。

   - **ユーザーアカウント管理**
   - **リモートコンソールアクセス**
   - **仮想電源およびリセット**
   - **仮想メディア**
   - **iLO 設定の構成**
   - **ログイン権限**

   この手順では、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定義します。

5. 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。

   選択したグループが、管理するリモートシステム上の iLO 設定の構成権限を持っていない場合は、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。

6. **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。

サーバーのフィルターされたセットからのグループの作成

この手順を使用して、フィルターされたサーバーのリストから iLO 連携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。

フィルターされたサーバーのリストからグループを作成すると、グループの作成時に**影響するシステム**リストに記載されているサーバーだけがグループに追加されます。グループの作成後に、フィルターの条件に適合するサーバーを構成しても、それらのサーバーはグループに追加されません。

前提条件

- iLO 設定の構成権限
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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。

   システムのセットを作成するときに適用するフィルターは、ページの上部に表示されます。フィルターを削除するには、フィルターの名前をクリックします。

   iLO 連携グループが存在しない場合、このページには、構成済みのグループはありませんというメッセージが表示されます。**セットアップ**ページを使用してグループを作成します。
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. 次の情報を入力します。

   - **グループ名** - グループ名は 1～31 文字で指定できます。
   - **グループキー** - グループのパスワードは、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。
   - **グループキーの確認** - グループのパスワードの確認。
5. 次の権限のいずれかを選択します。

   - **ユーザーアカウント管理**
   - **リモートコンソールアクセス**
   - **仮想電源およびリセット**
   - **仮想メディア**
   - **iLO 設定の構成**
   - **ログイン権限**

   この手順では、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定義します。
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。

   選択したグループが、管理するリモートシステム上の iLO 設定の構成権限を持っていない場合は、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。

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(105 ページ)

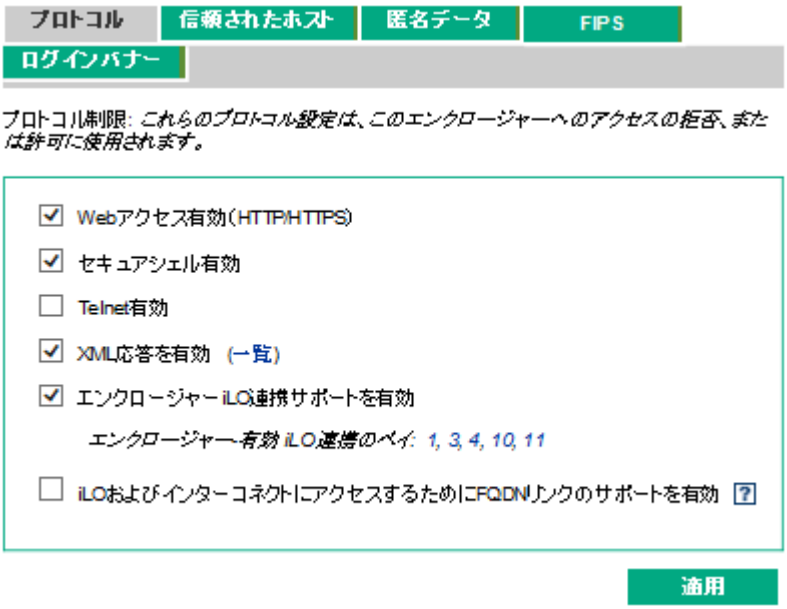
エンクロージャー iLO 連携サポートの設定

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。

管理プロセッサー情報	
名前	[illegible]
アドレス	[illegible]
MACアドレス	[illegible]
モデル	iLO5
ファームウェアバージョン	1.10 Jun 07 2017
iLO連携機能	対応

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。
- 選択したグループは cookie に保存され、iLO からログアウトしても永続的に残ります。

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 からログアウトしても永続的に残ります。

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**
- **マルチシステムマップ**
- **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**
- **グループ構成**

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 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 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。

iLO 連携情報のエクスポートオプション

次の情報を **iLO 連携**ページからエクスポートできます。

クリティカルまたは劣化ステータスのシステム

マルチシステムビューページから、このリストをエクスポートします。

iLO ピアリスト

マルチシステムマップページから、このリストをエクスポートします。

影響するシステムリスト

次のページでの iLO 連携操作によって影響を受けたシステムのリストをエクスポートします。

- **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**
- **グループ構成**

エクスポート機能は、**グループ電力設定**ページではサポートされていません。

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

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。

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。

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

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 連携情報を CSV ファイルにエクスポートする方法(105 ページ)

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** - 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。iLO の 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。

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 連携ページがロードされると、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に、およびそれらのピアから他のピアに、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のリクエストが送信されます。

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 連携情報を CSV ファイルにエクスポートする方法(105 ページ)

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。

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、iLO 連携グループ内のサーバー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。

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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- 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。

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. **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。

グループの URL ベースの仮想メディアのステータス表示

手順

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。

URL ベースのメディアの詳細

URL ベースのメディアが iLO 連携グループ内のシステムに接続している場合、**仮想フロッピーステータス**セクションと**仮想 CD/DVD-ROM ステータス**セクションに、次の詳細が示されます。

- **メディアが挿入されました** - 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指し示す URL。

メディアが接続されている場合にのみ、**仮想フロッピーステータス**および**仮想 CD/DVD-ROM ステータス**セクションが表示されます。

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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- 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。

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。

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(105 ページ)

iLO 連携グループ電力

グループ電力機能では、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電力を管理することができます。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**情報を更新するには、ブラウザーの更新機能を使用します。

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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- 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。

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。

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。

   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。

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。

  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。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、Hewlett Packard Enterprise はシステムコマンドを使用して適切なオペレーティングシステムシャットダウンを完了することをおすすめします。

- **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の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。

- **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。
- **コールドブート** - 選択したグループ内のサーバーの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。

仮想電源ボタン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(105 ページ)

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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- 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。

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. **電力消費上限値**を W、BTU/時、または%で入力します。

%は、最大電力値と最小電力値の差です。消費電力上限の値は、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。

グループ消費電力上限の注意事項

グループ電力設定機能では、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。設定可能な最大消費電力上限です。
  - **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。
- 一部のサーバーの消費電力上限設定は、iLO Web インターフェイスの外部で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、**http://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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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 W で表示されているときは、**値を BTU/時で表示**をクリックして表示を BTU/時に変更します。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**値をワットで表示**をクリックします。

消費電力上限の詳細

- **HPE 自動グループ電力消費上限の設定** - このセクションには、以下の詳細が表示されます。
  - **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** - このセクションには、以下の詳細が含まれています。
  - **現在の電力読み取り値** - 選択されたグループの現在の電力読み取り値。
  - **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が一覧表示されます。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 連携グループの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参照したり、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更新したりできます。次のファームウェアタイプが iLO 連携で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
- 言語パック

複数のサーバーのファームウェアの更新

前提条件

- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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（**http://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すべての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、ファームウェアの更新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. **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。

   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が更新され、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**セクションが更新されます。

   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(80 ページ)
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(81 ページ)

グループ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 **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。

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。

- サポート対象の各 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。

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、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(105 ページ)

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 設定の構成権限
- 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。
- 選択したサーバーの数に対するライセンスキーが付与されている。

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、ライセンスタイプまたはステータスリンクをクリックします。
3. オプション: 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。
4. **アクティベーションキー**ボックスにライセンスキーを入力します。
5. **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。
6. **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。
7. **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**セクションが更新され、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 ライセンス(231 ページ)

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(105 ページ)

ライセンス情報の表示

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。

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）機能が有効化されています。

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。オペレーティングシステム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（使用許諾されている場合）、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。

ブレードサーバーでは、内蔵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 の起動後に内蔵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。

アクセスオプション

iLO Web インターフェイスから、以下のリモートコンソールオプションにアクセスできます。

- **HTML5 内蔵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 内蔵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 または ClickOnce アドオンを使用している Windows クライアント用。
- **Java 内蔵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 内蔵リモートコンソール（Applet）** - 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。

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。

- **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通過せずに、Windows デスクトップからすべての iLO 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 IRC と同じです。HPLOCONS は、Web サイト **http://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 Mobile 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。

  Mobile 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（**http://www.hpe.com/support/ilo-docs**）の Mobile アプリケーションのドキュメントを参照してください。

一般的な使用方法とヒント

- 内蔵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。
- iLO プロセッサーを搭載しているサーバー上のホストオペレーティングシステムから内蔵リモートコンソールを実行しないでください。
- Hewlett Packard Enterprise は､内蔵リモートコンソールを通じてサーバーにログインするユーザーに、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。
- 内蔵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。

- 内蔵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、内蔵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、この値は内蔵リモートコンソールセッションに影響を与えません。
- 内蔵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します。

内蔵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特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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 内蔵リモートコンソール**セクションで**起動**ボタンをクリックします。

   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。

HTML5 IRC のコントロール

HTML5 IRC には 3 つの異なるモードがあり、各モードには固有の制御オプションがあります。

Windowed モード

Windowed モードを使用する場合、リモートコンソールはセカンダリウィンドウに表示されます。

- 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には、キーボードアイコンをクリックします。**CTRL+ALT+DEL**、**Num Lock**、または **Caps Lock**。
- URL ベースの仮想メディア機能にアクセスするには、CD/DVD アイコンをクリックします。
- Windowed モードから固定モードに変更するには、をクリックします。
- 固定モードからフルスクリーンモードに変更するには、をクリックします。
- リモートコンソールセッションを切断するには、をクリックします。

固定モード（ナビゲーションペインのサムネイル）

- 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には、キーボードアイコンをクリックします。**CTRL+ALT+DEL**、**Num Lock**、または **Caps Lock**。
- URL ベースの仮想メディア機能にアクセスするには、CD/DVD アイコンをクリックします。
- 固定モードからセカンダリウィンドウに変更するには、をクリックします。
- 固定モードからフルスクリーンモードに変更するには、をクリックします。
- リモートコンソールセッションを切断するには、をクリックします。

フルスクリーンモード

フルスクリーンモードを使用すると、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。

- フルスクリーンモードを終了するには、**Esc** キーを押します。
- （それを固定するオプション）のメニューを表示するには、画面の一番上にカーソルを移動します。

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特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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. **HTML5** リンクをクリックします。

   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。

.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。

Chrome では、.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、このコンソールは Google Chrome 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オプションを選択するか、別のブラウザーを使用します。

前提条件

- リモートコンソール特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- Internet Explorer の場合：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。
- Mozilla Firefox の場合：ClickOnce アドオン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. **起動**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

.NET IRC 要件(127 ページ)

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。

Chrome では、.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、このコンソールは Google Chrome 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オプションを選択するか、別のブラウザーを使用します。

前提条件

- リモートコンソール特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- Internet Explorer の場合：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。
- Mozilla Firefox の場合：ClickOnce アドオン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

.NET IRC 要件(127 ページ)

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特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- Oracle JRE 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. **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. 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。
5. **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。

   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。

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特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- 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カー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。

概要ページからの 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。

OpenJDK の環境では、**Java IRC の起動（OpenJDK JRE）**(124 ページ)を参照してください。

前提条件

- リモートコンソール特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- Oracle JRE 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**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. 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。
5. **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。

   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。

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特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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。

他のユーザーが要求を承認した場合、または 10 秒以内に応答しなかった場合は、許可が付与され、リモートコンソールが起動します。

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特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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 リモートコンソール(.NET IRC)**セクションで**起動**をクリックします。

   .NET IRC 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. **共有**をクリックします。

   セッションリーダーは、.NET IRC セッションへの参加のリクエストを受信します。

   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.NET IRC 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。

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により、同じサーバーで複数のセッションの接続が可能です。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に各アクセス要求用のダイアログボックスが表示され、要求者のユーザー名と DNS 名（使用できる場合）または IP アドレスを識別します。セッションリーダーは、アクセスを許可または拒否することができます。応答がない場合、アクセスは拒否されます。

共有リモートコンソールは、セッションリーダー指定を別のユーザーに渡したり、障害後にユーザーを再接続したりしません。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します。

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が、他のすべて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。サテライトクライアントは、仮想電源や仮想メディアを制御できません。

まず、iLO がクライアントを認証することで共有リモートコンソールセッションを暗号化し、次に、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ます。

.NET IRC 要件

Microsoft .NET Framework

.NET IRC は、.NET Framework の次のバージョンのいずれかを必要とします。

- .NET Framework 3.5 Full（SP1 を推奨）
- .NET Framework 4.0 Full
- .NET Framework 4.5
- .NET Framework 4.6

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、OS 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。

.NET Framework バージョン 3.5 および 4.0 には、デプロイメントオプションの Full と Client Profile があります。Client Profile は、Full フレームワークの一部にあたります。.NET IRC は、Full フレームワークを使用する場合にのみサポートされます。Client Profile はサポートされません。.NET Framework のバージョン 4.5 以降には、Client Profile オプションはありません。

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。

- Mozilla Firefox では、.NET アプリケーションを起動するためにアドオンが必要です。Microsoft .NET Framework Assistant のような ClickOnce アドオンがあると、Mozilla Firefox のサポートされるバージョンから.NET IRC を起動できます。.NET Framework Assistant は、**http://addons.mozilla.org/**からダウンロードできます。
- Google Chrome の以前のバージョンでは、ClickOnce をサポートする NPAPI プラグインを使用して.NET IRC を実行できました。Google Chrome バージョン 42 以降では、NPAPI ベースのプラグインがサポートされません。

  回避策として、以下のいずれかを使用してください。

  - 別のブラウザーの.NET IRC
  - スタンドアロン.NET IRC
  - Java IRC。
  - iLO Mobile アプリケーション。

リモートコンソール機能の使用

リモートコンソールを使用したキーボード操作の送信

リモートコンソールからサーバーに以下のキーボード操作を送信できます。

- **CTRL+ALT+DEL**
- **Num Lock**
- **Caps Lock**

前提条件

- リモートコンソール特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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. 以下のいずれかを実行します。
   - .NET IRC と Java IRC を使用する場合は、リモートコンソールの**キーボード**メニューからキーボード操作を選択します。
   - HTML5 IRC を使用する場合は、キーボードアイコンをクリックし、キーボード操作を選択します。

リモートコンソール仮想メディア

ホストサーバー上の仮想メディアには、リモートコンソール、iLO の Web インターフェイス、XML 構成および制御スクリプト、iLO RESTful API および CLP を使用してアクセスできます。このセクションでは、仮想メディア機能で.NET IRC または Java IRC を使用する方法を説明します。

仮想ドライブ

仮想ドライブ機能は、物理フロッピーディスクまたは CD/DVD-ROM、USB キードライブ、イメージファイル、あるいは URL ベースのイメージファイルの使用をサポートします。

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特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- 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 管理者特権を有している。

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/DVD-ROM、または USB キードライブのドライブ文字を選択します。

   仮想ドライブの動作 LED は、仮想ドライブのアクティビティを表示します。

仮想ドライブ（ローカル IMG または ISO）の使用

前提条件

- リモートコンソール特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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て、**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。

   .NET IRC または Java IRC からディスクイメージを選択するように求められます。

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するか、イメージファイルの位置に移動して**開く**をクリックします。

   仮想ドライブの動作 LED は、仮想ドライブのアクティビティを表示します。

仮想ドライブ（IIS/Apache での URL 経由のイメージファイル）の使用

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特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- 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. リモートコンソールを起動します。
3. 以下のいずれかを実行します。

   - .NET IRC、Java IRC、およびスタンドアロンのリモートコンソールの場合は、**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/DVD-ROM**（ISO ファイル）を選択します。
   - HTML5 IRC の場合は、CD/DVD アイコンをクリックし、**フロッピー** > **仮想メディア URL**（IMG ファイル）または **CD/DVD** > **仮想メディア URL**（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。

   仮想ドライブの動作 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

スクリプト仮想メディア用 IIS のセットアップ(157 ページ)

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。

Java IRC を使用したディスクイメージファイルの作成

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。
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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-ROM 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。

Java IRC を使用した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

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。IMG ディスクイメージファイルのみがサポートされます。CD-ROM 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
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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。

   ディスクの作成が完了すると、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。

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
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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 Folder** という名前でサーバーにマウントされます。

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。

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。

リモートコンソールの仮想電源スイッチの使用

リモートコンソールの電源スイッチメニューを使用して、iLO 仮想電源ボタン機能にアクセスします。

前提条件

- リモートコンソール特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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. リモートコンソールの**電源スイッチ**メニューから次のいずれかのオプションを選択します。

   - **瞬間的に押す**
   - **押し続ける**
   - **コールドブート**
   - **リセット**

   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。

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すすめします。

- **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。

コンソールの取得（.NET IRC 専用）

コンソールの取得は、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障害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るリモートコンソール機能です。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取得します。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取得されません。
- 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、取得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たときに取得を開始し、容量が不足したときに停止します。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一杯になったときに取得を開始し、iLO が ASR イベントを検出したときに停止します。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。
- コンソールの取得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。

  以下の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。

  カーソルをコントロール上で動かすと各ボタンを確認できます。

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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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。

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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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。

リモートコンソールを使用したビデオファイルの取得

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取得します。

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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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。

   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。

保存した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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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取得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。

リモートコンソールのホットキー

プログラムリモートコンソール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、ホットキーを押すとホストサーバーへ送信される最大 5 つのキーの組み合わせを表します。ホットキーは、.NET IRC、Java IRC、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。

ホットキーの作成

前提条件

iLO の設定の構成

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目的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のコンピューターロックキーとホットキーを設定するためのキー**(137 ページ)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更新されたことを確認します。

リモートコンソールのコンピューターロックキーとホットキーを設定するためのキー

リモートコンソールのホットキーとリモートコンソールのコンピューターロックキーを設定する場合、次のキーがサポートされます。

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

表は続く

END	F10	[	r
PG UP	F11	\	s
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 設定の構成特権

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 のみ）

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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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。

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。この機能が設定されているときに NET IRC または Java IRC ウィンドウを開いた場合、ウィンドウを閉じるときにオペレーティングシステムがロックされます。

前提条件

iLO の設定の構成

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. コンピューターロックの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。

リモートコンソールのコンピューターロックのオプション

- **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します。iLO 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できます。iLO 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オペレーティングシステム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オペレーティングシステム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キーとホットキーを設定するためのキー(137 ページ)

統合リモートコンソールの信頼設定（.NET IRC）の設定

.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する**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する**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 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、**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する**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。

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 管理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、は、画面フレームバッファーを使用してテキスト情報の変更を検出し、変更を暗号化し、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の使用**(141 ページ)
- **テキストベースのリモートコンソール（Textcons）**(147 ページ)

iLO 仮想シリアルポートの使用

標準ライセンスと iLO 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。

iLO 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。

iLO 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。サーバーがプレオペレーティングシステム状態にあるとき、iLO はこの情報を SSH クライアントを通して表示するので、ライセンスのない iLO システムが POST 処理中にサーバーを確認して通信できるようになります。

iLO 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、iLO 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。
- iLO 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。

詳しくは

iLO 仮想シリアルポートを使用するための Windows の設定(145 ページ)
iLO 仮想シリアルポートを使用するための Linux の設定(142 ページ)
iLO 仮想シリアルポート搭載の Windows EMS コンソール(145 ページ)

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設定

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、物理的 UART を使用していないため、**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、**Yes - Save Changes** 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 Linux 6 の設定

手順

1. 次の設定例に基づいて GRUB を設定します。

   注記:

   次の設定例では、ttyS0 と unit 0 は com1 用で、ttyS1 と unit 1 は com2 用です。

   次の設定例では Red Hat Enterprise Linux 6 および com1 を使用しています。

   ```
   serial -unit=0 -speed=115200
   terminal -timeout=10 serial console
   default=0
   timeout=10
   #splashimage=(hd0,2)/grub/splash.xpm.gz
   title Red Hat Linux (2. 6.18-164.e15)
   root (hd0,2)
   9
   kernel /vmlinux-2.6.18-164.e15 ro root=/dev/sda9 console=tty0 console=ttyS0,115200
   initrd /initrd-2.6.18-164.e15.img
   ```

   com2 を選択した場合、構成の例は次のようになります。

   ```
   serial -unit=1 -speed=115200
   terminal -timeout=10 serial console
   default=0
   timeout=10
   #splashimage=(hd0,2)/grub/splash.xpm.gz
   title Red Hat Linux (2. 6.18-164.e15)
   root (hd0,2)
   9
   kernel /vmlinux-2.6.18-164.e15 ro root=/dev/sda9 console=tty0 console=ttyS1,115200
   initrd /initrd-2.6.18-164.e15.img
   ```

   Linux が完全にブートすると、ログインコンソールをシリアルポートにリダイレクションできます。

   `/dev/ttyS0` および`/dev/ttyS1` デバイスが設定されている場合、これらのデバイスにより、iLO 仮想シリアルポートを通じてシリアル TTY セッションを取得できます。

2. 設定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
   ```

   次の例は、`dev/ttys1:`でログインコンソールを開始します。

   ```
   S1:2345:respawn:/sbin/agetty 115200 ttyS1 vt100
   ```

3. 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を使用するための Red Hat Enterprise Linux 7 の設定

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_CMD_LINELINUX 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。

   次に例を示します。

   systemctl enable serial-getty@ttyS0.service

4. シリアルポートで getty をリッスンします。

   次に例を示します。

   systemctl start getty@ttyS0.service

5. 設定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 ファイルを更新するには、次のコマンドを入力します。

   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：

- iLO 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、iLO 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、iLO リモートコンソールと同時に使用できます。
- `SAC>`プロンプトが表示されるようにするには、iLO 仮想シリアルポートを介して接続した後で、**Enter** キーを押す必要がある場合があります。

詳しくは

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設定(142 ページ)

iLO 仮想シリアルポートを使用するための Windows の設定

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。

詳しくは

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設定(142 ページ)

iLO 仮想シリアルポートセッションの開始

前提条件

- iLO 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、iLO 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

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設定(142 ページ)
iLO 仮想シリアルポートを使用するための Windows の設定(145 ページ)
iLO 仮想シリアルポート搭載の Windows EMS コンソール(145 ページ)

iLO 仮想シリアルポートログの表示

iLO 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 iLO 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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、iLO 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. iLO 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 アクセスオプションの構成(249 ページ)

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。UEFI 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、使用するクライアントによって異なります。クライアントは、iLO と互換性のある標準の SSH クライアントならどれでもかまいません。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

詳しくは

ブート順序(227 ページ)

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更新します。

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。例：

```
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

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。

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 の使用

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。

iLO 仮想メディアの使用

iLO 仮想メディア

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。

- 一部の形式の仮想メディアを使用するには、iLO ライセンスキーが必要です。
- この機能を使用するには、仮想メディア特権が必要です。
- 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も依存します。
- オペレーティングシステムでは、iLO の仮想ディスケット/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。iLO を初めて使用する場合、ホストオペレーティングシステムが、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が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オペレーティングシステム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オペレーティングシステムの展開、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。
  - ホストサーバーのオペレーティングシステムの実行中に、仮想フロッピー/USB キーを使用して、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を行うことができます。
  - 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。
- ホストサーバーのオペレーティングシステムが USB の大容量記憶装置をサポートする場合、ホストサーバーのオペレーティングシステムをロードした後にも、iLO 仮想 CD/DVD-ROM を使用できます。

- ホストサーバーのオペレーティングシステムの実行中に、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。

- .NET IRC を使用すると、仮想フォルダーをマウントして、クライアントと管理対象サーバーの間でファイルにアクセスし、コピーすることができます。
- 仮想フロッピー/USB キーまたは仮想 CD/DVD-ROM 機能が有効になっている場合、通常、クライアントオペレーティングシステム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 iLO 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 での Java IRC のみの場合：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、Java IRC で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。

Windows 7 で iLO 仮想メディアを使用するための Windows 7 の設定

デフォルトで、Windows 7 は、起動時に有効になったり、接続されたりする仮想メディアデバイスがないと、iLO 仮想ハブの電源を切ります。

この設定を変更するには、以下の手順を使用します。

手順

1. **デバイスマネージャー**を開きます。
2. **表示** > **デバイス（接続別）**の順に選択します。
3. **標準ユニバーサル PCI to USB ホストコントローラ**を展開し、汎用 USB ハブを含む USB デバイスを表示します。

   汎用 USB ハブオプションは、iLO 仮想 USB ハブコントローラーです。
4. **汎用 USB ハブ**を右クリックし、**プロパティ**を選択します。
5. **電源管理**タブをクリックします。
6. **電力の節約のために、コンピューターでこのデバイスの電源をオフにできるようにする**チェックボックスをクリアします。

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

- **起動プロセスおよび DOS セッション** - 起動プロセスと DOS セッションの実行中、仮想ディスケットデバイスは標準の 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ディスケットドライブを同時に使用することはできません。
- **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ケットとして使用するには、ホスト RBSU の内蔵ディスケットドライブを無効にし、仮想ディスケットがドライブ A であるかのようにしてください。

  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すすめします。

- **Windows Vista** - 保護モードを有効にして Internet Explorer 7 を使用すると、仮想メディアは正しく動作しません。プロテクトモードが有効のときに仮想メディアを使用しようとすると、さまざまなエラーメッセージが表示されます。仮想メディアを使用するには、**ツール** > **インターネットオプション** > **セキュリティ**の順に選択して、**保護モードを有効にする**のチェックマークを外し、**適用**をクリックします。保護モードを無効にしたら、開いているすべてのブラウザーインスタンスを終了してブラウザーを再起動します。
- **Red Hat Enterprise Linux および SuSE Linux Enterprise Server** - Linux は、USB ディスケットおよびキードライブの使用をサポートします。

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。iLO の仮想ディスケット/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

Red Hat Enterprise Linux および SuSE Linux Enterprise Server の要件は以下のとおりです。

- **Red Hat Enterprise Linux** - CD/DVD-ROM ドライブがローカル接続されているサーバーでは、`/dev/cdrom1` で仮想 CD/DVD-ROM デバイスにアクセスできます。ただし、CD/DVD-ROM ドライブがローカル接続されていないサーバー（BL c-Class ブレードシステムなど）では、仮想 CD/DVD-ROM は、`/dev/cdrom` でアクセスできる最初の CD/DVD-ROM です。

  仮想 CD/DVD-ROM は、通常の CD/DVD-ROM デバイスと同じように、次のコマンドを使用してマウントできます。

  ```
  mount /mnt/cdrom1
  ```

- **SuSE Linux Enterprise Server** - USB で接続されたローカルの CD/DVD-ROM がない場合、仮想 CD/DVD-ROM は`/dev/scd0` にあります。その場合、仮想 CD/DVD-ROM は`/dev/scd1` を使用します。

  仮想 CD/DVD-ROM は、通常の CD/DVD-ROM デバイスと同じように、次のコマンドを使用してマウントできます。

  ```
  mount /dev/scd0 /media/cdrom1
  ```

Linux システムで USB 仮想メディア CD/DVD-ROM をマウントする

手順

1. Web インターフェイス経由で iLO 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. 使用する CD/DVD-ROM を選択します。
5. 以下のコマンドを使用して、ドライブをマウントします。

   - Red Hat Enterprise Linux の場合

     ```
     mount /dev/cdrom1  /mnt/cdrom1
     ```

   - SuSE Linux Enterprise Server の場合：

     ```
     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 インターフェイスからの仮想メディアの使用

仮想メディアページでは、以下のタスクを実行できます。

- ローカルに保存されたイメージファイル、フロッピーディスク、USB キー、CD/DVD-ROM、および仮想フォルダーのようなローカルメディアを表示する、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。

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ステータスおよびポート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。

   仮想メディア機能のステータスと構成されている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。

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。

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

- **メディアが挿入されました** - 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。

- **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。

仮想 CD/DVD-ROM ステータス

- **メディアが挿入されました** - 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。

- **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。

ローカル仮想メディアデバイスの取り出し

前提条件

- 仮想メディア特権
- 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。

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。他の仮想メディアタイプを接続するには、.NET IRC または Java IRC、RIBCL/XML、あるいは iLO CLI を使用します。 **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

- 仮想メディア特権
- 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. **メディアの挿入**をクリックします。
5. 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。

接続されている URL ベースのメディアの表示

前提条件

- 仮想メディア特権
- 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。

URL ベースのメディアの詳細

URL ベースの仮想メディアが接続されている場合、**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、次の詳細情報が示されます。

- **メディアが挿入されました** - 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

- 仮想メディア特権
- 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特権を付与する iLO ライセンスがないサーバーブレードの場合、URL ベースの仮想メディアイメージでは**メディアの強制イジェクト**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。

リモートコンソールからの iLO 仮想メディアの使用

リモートコンソールから仮想メディア機能を使用する手順については、**リモートコンソール仮想メディア** (128 ページ)を参照してください。

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。

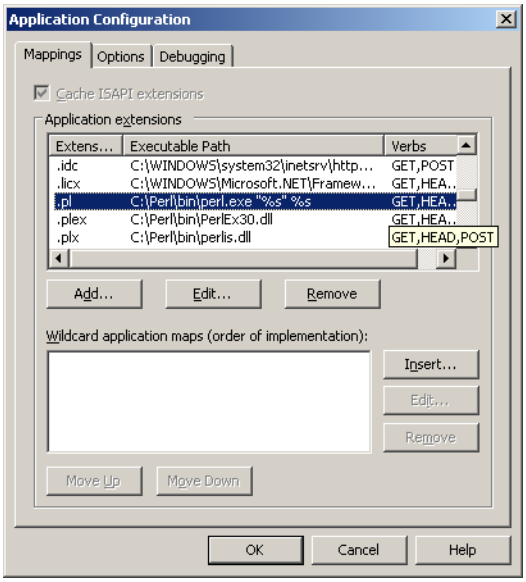


図 3: Perl 設定の例

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

仮想メディアヘルパーアプリケーションのサンプル(159 ページ)

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、iLO スクリプティングおよび CLI 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 Premium Security Edition 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、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は、サーバーが起動しません。

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 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 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。

詳しくは

iLO ネットワークのフラッシュエラーリカバリ(440 ページ)

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。

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(295 ページ)

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。

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 Compute Module 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。

電力割り当て（ブレードサーバーおよび Compute Module）

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 Compute Module）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 Compute Module 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 Compute Module 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すすめします。

- **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。

システム電源リストアの設定

システム電力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。POST 実行中に UEFI システムユーティリティを使用して、これらの設定を構成することもできます。

前提条件

iLO の設定の構成

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、この値は選択できません。

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。サーバーブレードでは使用できません。

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、ブレードサーバーではサポートされません。

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、仮想電源ボタンによる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クリアされますが、瞬間的に押す操作または押し続ける操作ではデータはクリアされません。

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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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、**電力メーター**タブをクリックします。
2. **グラフタイプ**メニューでグラフの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。

   測定値のデータを表示するには、グラフ内でカーソルを左右に移動します。
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**
   - **最小**
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。

   デフォルトでは、ページを開いた後はページのデータは更新されません。

   - ページをただちに更新するには、更新アイコンをクリックします。
   - ページの自動更新を開始するには、更新アイコンの横にある三角形のアイコンをクリックします。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、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。
5. オプション：電力読み取り値をワットまたは BTU/時に変更するには、**電力単位**メニューで値を選択します。
6. オプション：表示されるデータをグラフ上の特定のポイントにロックするには、目的のポイントにカーソルを移動してクリックします。

   カーソルのロックを解除するには、グラフをもう一度クリックするか、またはロックアイコンをクリックします。

電力メーターグラフの表示オプション

グラフタイプ

- **直近 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。
- **直近 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 分ごとに更新します。

グラフデータ

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。

- **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。消費電力上限データは電力メーターグラフに赤色で表示されます。
  - 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設定すると、システムの性能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。最大電力データは電力メーターグラフに紫色で表示されます。
- **平均** - サンプル中の電力測定値の平均。平均電力データは、電力メーターグラフに青色で表示されます。
- **最小** - ある測定期間で観測された最小値。20 分間のグラフでは、10 秒ごとの平均測定値の最小値が表示されます。24 時間のグラフでは、5 分間の平均値より低い最小値が表示されます。最小電力データは電力メーターグラフにグレーで表示されます。

電力メーターグラフの更新

- ページをただちに更新するには、更新アイコン↻をクリックします。
- ページの自動更新を開始するには、更新アイコンの横にある開始アイコン▷をクリックします。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。

電力単位の表示

電力読み取り値をワットまたは BTU/時に変更するには、**電力単位**リストで値を選択します。

電力メーターロックアイコン

- 自動更新が実行されていない場合、ロックアイコンをクリックするか、グラフ上の任意のポイントをクリックすると、グラフ上の特定のポイントで表示がロックされます。
- 自動更新が実行されている場合、ロック機能を使用すると、x 軸に沿った特定の履歴ポイントに対応するデータポイントが表示されます。たとえば、20 分間のグラフでは、-10 分で表示をロックすると、グラフが更新されるたびに 10 分前の値が表示されます。

現在の電源状態の表示

手順

ナビゲーションツリーで**電力管理**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。

- **現在の電力読み取り値** - サーバーからの現在の電力読み取り値。

  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。

- **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**(168 ページ)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

手順

ナビゲーションツリーで**電力管理**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 つの期間で電力読み取り値を表示します。

- **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。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。

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 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. 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の場合、iLO は、パワーレギュレーターの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。
- **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 設定の構成特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- 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。iLO が出荷時のデフォルト設定になっている場合、ROM ベースのシステムユーティリティの消費電力上限値管理機能は無効になっており、この機能を使用するには、これを再度有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**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. **手動の消費電力上限を有効**チェックボックスを選択します。
3. **消費電力上限値**を W、BTU/時、または%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 W で表示されているときは、**値を BTU/時で表示**をクリックして表示を BTU/時に変更します。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、**http://www.hpe.com/info/qs** でサーバーの仕様書を参照してください。

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（**http://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 の設定の構成

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構成

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。

この機能を有効にすると、iLO 仮想キーボードとマウスが、iLO UHCI USB コントローラーに常時接続されます。この機能を無効にすると、リモートコンソールアプリケーションが開いて iLO に接続している場合にのみ、iLO 仮想キーボードとマウスが 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ことで、サーバー OS がアイドル状態で、接続されている仮想 USB キーボードおよびマウスがない場合に、サーバーによっては消費電力を 15 ワット削減できます。

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。

前提条件

iLO 設定の構成特権

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**を有効にします。

   マウス、キーボードの持続接続機能は、デフォルトでは無効になっています。

   設定が変更されたことが iLO によって通知されます。

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 バッテリ**
- **電力読み取り値**
- **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更新されます。

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。

現在の電力読み取り値

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読み取り値が表示されます。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。詳しくは、**サーバー電力使用量の表示**(165 ページ)を参照してください。

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。

電力情報

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**電力情報**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、**電力情報**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。

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 分かかる場合があります。
  - iPDU モジュールにネットワーク（または IP）アドレスがない。

製品番号

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。

電力読み取り値

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。

現在の電力読み取り値

サーバーからの最新の電力読み取り値。

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**(165 ページ)を参照してください。

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 ストレージバッテリのリスト

シャーシ情報ページには、Smart ストレージバッテリ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

バッテリの索引番号。

設置

バッテリのインストールステータス。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

バッテリステータス。指定できる値は、**OK**、**劣化**、**障害**、または**その他**です。

容量

バッテリ容量。

ファームウェア

搭載されているバッテリのファームウェアバージョン。

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。このような状況が発生すると、冗長電源装置が構成されている場合は冗長性を失ったり、冗長電源装置を使用していない場合は動作しなくなったりする可能性があります。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、サーバーの外部入力電源の冗長ステータスおよび個々（内部）の電源装置のステータスがインテリジェントに報告されます。

詳しくは、次の Web サイトを参照してください。**http://www.hpe.com/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更新されます。

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 : 冷却ファンの冗長性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。

- **ステータス** - ファンのヘルスステータス。
- **速度** - ファン速度（%）。

ファン

iLO ファームウェアは、ハードウェアとの組み合わせで、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。**仮想**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

温度情報ページは、温度グラフとテーブルを含みます。このテーブルは、サーバーシャーシ内の温度センサーの位置、ステータス、温度、およびしきい値設定を表示します。

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更新されます。

温度グラフの表示

手順

1. ナビゲーションツリーで**電力管理**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。センサーの温度が上がると、グラフの色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**電力管理**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。

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、冷却機能を最大化するためのファンの回転速度の増加、IML の温度イベントのログ記録、LED インジケーターを使用したイベントの視覚

的な表示、データの破損を防ぐためのオペレーティングシステムの適切なシャットダウンの開始が含まれます。

温度超過状態の修正後は、ファンの回転速度を通常に回復、IML へのイベントの記録、LED インジケーターの消灯、シャットダウンを実行中の場合はその停止などの追加のポリシーが実施されます。

iLO ネットワーク設定の構成

iLO ネットワーク設定

iLO 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（ラベルは **iLO**）を使用します。
- **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が、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。

  このオプションは、非ブレードサーバーでのみサポートされます。

- **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が、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。

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。

ネットワーク構成の概要の詳細

- **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。

- **リンク状態** - 選択している iLO ネットワークインターフェイスの現在のリンク速度。デフォルト値はオートネゴシエートです。
- **デュプレックスオプション** - 選択している iLO ネットワークインターフェイスの現在のリンクデュプレックス設定。デフォルト値はオートネゴシエートです。

iLO ホスト名および NIC 設定は、**ネットワーク共通設定**ページで設定できます。

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。
- **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** - アドレスタイプ。
  - **IPv6** - IPv6 アドレス。
  - **プレフィックス長** - アドレスのプレフィックスの長さ。
  - **ステータス** - アドレスステータス。表示される可能性のある値は、**アクティブ**（このアドレスは iLO が使用しています）、**保留中**（重複アドレス検出が進行中です）、**障害**（重複アドレス検出に失敗したため、iLO はこのアドレスを使用していません）です。
- **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 **固定デフォルトゲートウェイ**設定を元に生成されます。

  固定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 設定の構成権限

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 が設定されていない場合は、iLO **ドメイン名**を入力します。

   iLO 専用ネットワークポートを選択しているときに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。

   iLO 共有ネットワークポートを選択しているときに静的ドメイン名を使用するには、**IPv4 設定**ページで **DHCPv4 が提供するドメイン名を使用**の設定を無効にします。
5. 変更を保存するには、**適用**をクリックします。
6. **共通**、**IPv4**、**IPv6**、および **SNTP** タブで iLO ネットワークの設定が完了したら、**リセット**をクリックして iLO プロセッサーを再起動します。

   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 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
  - IP アドレスと DNS/WINS 名で iLO プロセッサーに PING できることを確認する
  - NSLOOKUP が iLO ネットワークアドレスを正しく解決し、名前空間の競合が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
- 名前空間を変更した場合は DNS 名を更新する

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 設定の構成権限

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. **リンク状態**を選択します。

   リンク状態設定は、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。

   この設定は、サーバーブレードでは使用できません。
6. 変更を保存するには、**適用**をクリックします。
7. **共通**、**IPv4**、**IPv6**、および **SNTP** タブで iLO ネットワークの設定が完了したら、**リセット**をクリックして iLO を再起動します。

   接続が再確立されるまでに、数分かかることがあります。

リンク状態の値

iLO 専用ネットワークポートを有効にする場合、次の**リンク状態**の値から選択します。

- **自動**（デフォルト） - iLO は、ネットワークに接続するときに、サポートされる最高のリンク速度とデュプレックス設定をネゴシエーションできます。
- **1000BaseT, フルデュプレックス** - 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）。
- **1000BaseT, ハーフデュプレックス** - 半二重を使用した 1 Gb 接続を強制します（サポートされるサーバーのみ）。

  1000BaseT、ハーフデュプレックスは標準の設定ではなく、ほとんどのスイッチがサポートしていません。この設定を使用する場合、1000BaseT、ハーフデュプレックスをサポートするようにスイッチが構成されていることを確認します。
- **100BaseT, フルデュプレックス** - 全二重を使用した 100 Mb 接続を強制します。
- **100BaseT, ハーフデュプレックス** - 半二重を使用した 100 Mb 接続を強制します。

- **10BaseT, フルデュプレックス** - 全二重を使用した 10 Mb 接続を強制します。
- **10BaseT, ハーフデュプレックス** - 半二重を使用した 10 Mb 接続を強制します。

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 設定の構成権限

手順

1. 共有ネットワークポート LOM または FlexibleLOM 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。
4. サーバーの構成に応じて、**LOM** または **FlexibleLOM** を選択します。
5. **ポート**メニューから値を選択します。

   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。
6. VLAN を使用するには、**VLAN 有効**オプションを有効にします。

   共有ネットワークポートがアクティブで VLAN が有効な場合、iLO 共有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 VLAN 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。
7. VLAN を有効にした場合は、**VLAN タグ**を入力します。相互に通信するネットワークデバイスすべてが、同じ VLAN タグを持つ必要があります。VLAN タグは、1～4094 の任意の番号です。
8. 変更を保存するには、**適用**をクリックします。
9. **共通**、**IPv4**、**IPv6**、および **SNTP** タブで iLO ネットワークの設定が完了したら、**リセット**をクリックして iLO を再起動します。

   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 または FlexibleLOM ポート経由で転送されるようになります。

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（ラベルは **iLO**）を使用します。
- **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が、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** - 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が、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。**http://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 または FlexibleLOM 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を使用しないサーバーでは、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、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ことをおすすめします。

  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、リンク状態やデュプレックス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。

IPv4 設定の構成

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 **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. **IPv4 設定**ページで行った変更を保存するには、**適用**をクリックします。
9. **共通**、**IPv4**、**IPv6**、および **SNTP** タブで iLO ネットワークの設定が完了したら、**リセット**をクリックして iLO を再起動します。

   接続が再確立されるまでに、数分かかることがあります。

IPv4 設定

DHCPv4 構成設定

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。

Use DHCPv4 Supplied WINS Servers（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。

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 を使用しない場合は、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 を使用する場合、サブネットマスクは自動的に提供されます。DHCP を使用しない場合は、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。

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。

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。

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、スタティックルートの値を入力してください。

その他の設定

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。

IPv6 設定の構成

iLO 専用ネットワークポートの **IPv6 設定**ページを使用して、iLO の IPv6 を設定します。

前提条件

iLO 設定の構成特権

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. **IPv6 設定**ページで行った変更を保存するには、**適用**をクリックします。
9. **共通**、**IPv4**、**IPv6**、および **SNTP** タブで iLO ネットワーク設定が完了したら、**リセット**をクリックして iLO を再起動します。

   接続が再確立されるまでに、数分かかることがあります。

IPv6 設定

グローバル IPv6 構成

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。

ステートレスアドレス自動構成（SLAAC）を有効

iLO がルーター通知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。

DHCP の構成設定

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。

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。

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。

- **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。
- **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。
- **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。

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。

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。

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通知メッセージが存在し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。

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インプリメンテーションを導入することで両方のプロトコルの同時使用をサポートしています。

以下の機能が IPv6 の使用をサポートします

- 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
- 内蔵リモートコンソール
- Onboard Administrator シングルサインオン
- HPE 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

iLO SNTP 設定の構成

前提条件

- iLO 設定の構成特権
- 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. **SNTP 設定**ページで行なった変更を保存するには、**適用**をクリックします。
7. **共通**、**IPv4**、**IPv6**、および **SNTP** タブで iLO ネットワーク設定が完了したら、**リセット**をクリックして iLO を再起動します。

   接続が再確立されるまでに、数分かかることがあります。

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。

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。

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。

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 イベントログと IML 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、iLO イベントログおよび IML 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 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(197 ページ)

NIC 自動選択のサポート

- ProLiant Gen10 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 `oemhp_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、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。

3. 必要に応じてサーバーのケーブルを配線してから、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。

NIC フェイルオーバーの構成

手順

1. iLO NIC 自動選択を設定します。
2. 次のいずれかを実行します。

   a. CLI コマンド `oemhp_nicfailover` を使用して、NIC フェイルオーバーを設定します。

   b. NIC フェイルオーバー機能を設定するには、MOD_NETWORK_SETTINGS スクリプトに ILO_NIC_FAIL_OVER タグを追加します。

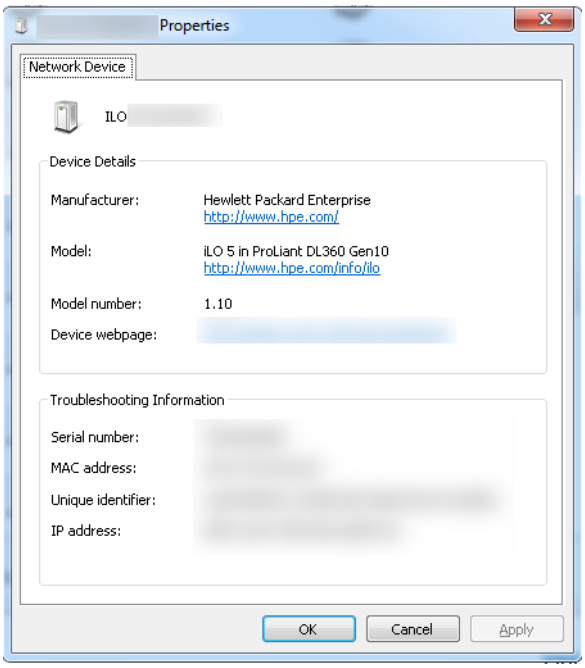
   詳しくは、iLO スクリプティング/CLI ガイドを参照してください。

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

HPEiLO 5 には、Embedded Remote Support の機能が含まれ、この機能により、HPE ProLiant Gen10 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 Hewlett Packard Enterprise のプライバシー声明に従って管理されます。この声明は Web サイト **http://www.hpe.com/info/privacy** で参照できます。

内蔵リモートサポート機能を使用する場合は、次の構成オプションから選択します。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。

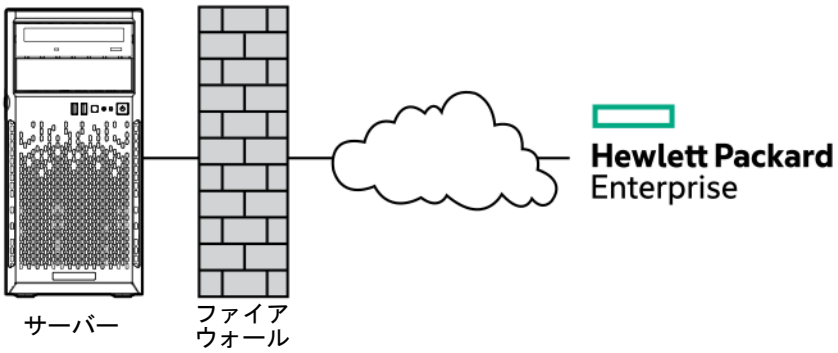


図 4: Insight Online Direct Connect とサーバー

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。

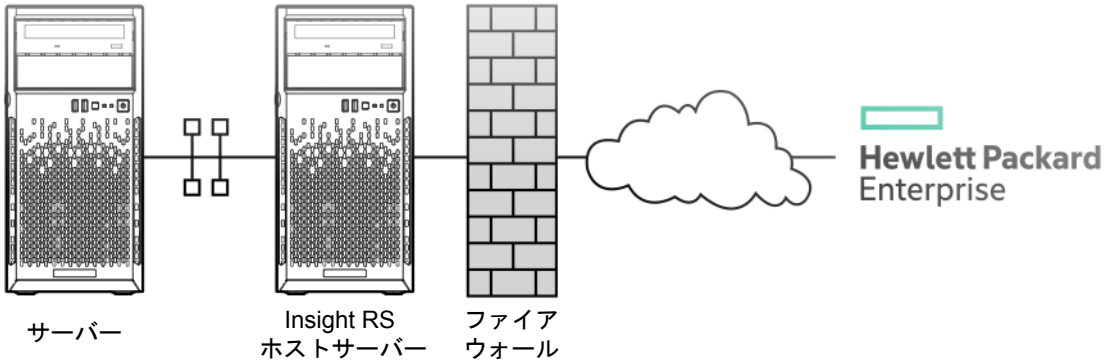


図 5: Insight Remote Support とサーバーの Central Connect

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

ProLiant Gen10 サーバー

Insight Remote Support Central Connect

ProLiant Gen10 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閉ループ品質分析に使用されます。

詳しくは

Active Health System(48 ページ)
リモートサポートのデータ収集(214 ページ)
リモートサポートサービスイベント(210 ページ)

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。**http://www.hpe.com/services/proactivecarecentral**

リモートサポートの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 **http://www.hpe.com/info/insightonline-ja** 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 **http://www.hpe.com/info/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. 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する以下の情報を収集します。
   - 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. 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。
6. **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。
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。**

サポートされるブラウザー

HPE Embedded Remote Support ソリューションでは、以下のブラウザーをサポートします。

iLO

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。

- Microsoft Edge
- Mozilla Firefox
- Google Chrome モバイルおよびデスクトップ
- Microsoft Internet Explorer 11

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更新するために必要なファイルがあることを確認します。構成に応じて、以下のファイルが必要です。

- **Service Pack for ProLiant（Ubuntu を除く、サポートされているすべての OS）** - SPP には、iLO ファームウェア、ドライバー、および AMS が含まれています。SPP は、Web サイト（**http://www.hpe.com/servers/spp**）からダウンロードしてください。

  一部の各コンポーネントは個別にダウンロードできます。

  - **iLO 5 チャネルインターフェイスドライバー** - iLO 5 チャネルインターフェイスドライバー for Windows は、Web サイト（**http://www.hpe.com/info/hpesc**）からダウンロードしてください。
  - **iLO ファームウェア** - iLO ファームウェアは、Web サイト（**http://www.hpe.com/support/ilo5**）からダウンロードしてください。
  - **Agentless Management Service** - AMS は、次の Web サイトからダウンロードしてください。Hewlett Packard Enterprise サポートセンター：**http://www.hpe.com/info/hpesc**

- **Management Component Pack（Ubuntu）** - AMS は MCP に含まれていますが、iLO ファームウェアや iLO ドライバーは含まれていません。MCP は次の Web サイトからダウンロードしてください。**http://www.hpe.com/support/SDR-Linux**

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、初期のサーバーのセットアップタスクを実行します。

   このプロセス中にハードウェアの設定を構成し、オペレーティングシステムをインストールし、iLO 設定を構成できます。iLO を構成する場合は、iLO の IP アドレスを記録します。
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すすめします。

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。

Intelligent Provisioning の**推奨**インストール方法で Windows をインストールすると、AMS は自動的にインストールされます。

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. **iLO ドライバー**がまだインストールされていない場合は、インストールします。

   Intelligent Provisioning の**推奨**インストール方法で Windows をインストールすると、iLO 5 チャネルインターフェイスドライバー for Windows が自動的にインストールされます。

   Red Hat Enterprise Linux、SUSE Linux Enterprise Server、および Ubuntu 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. 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。

8. 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。

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 **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。

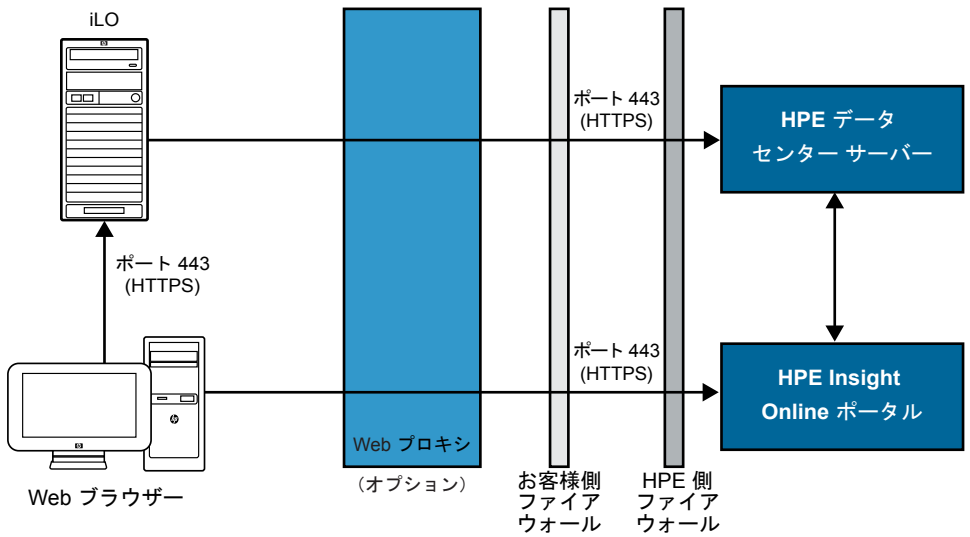


図 6: Insight Online Direct Connect のネットワーク要件

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。

   注記:

   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 **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。

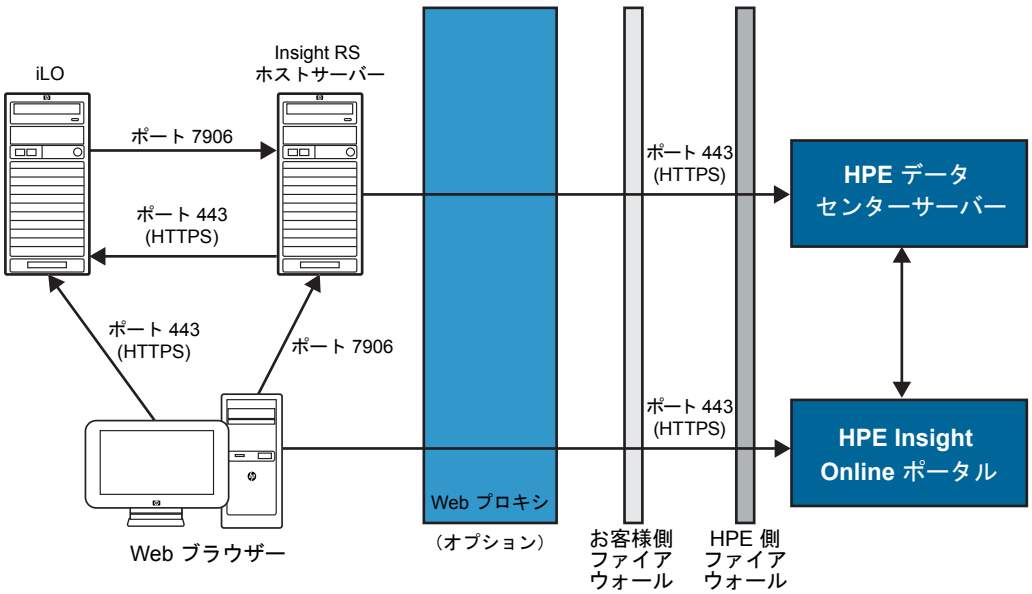


図 7: Insight Remote Support Central Connect のネットワーク要件

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。**http://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 アダプターを構成します。

   詳しくは、Web サイト（**http://www.hpe.com/info/insightremotesupport/docs**）にある Insight Remote Support インストール/コンフィギュレーションガイドを参照してください。

4. Insight RS ホストサーバーで、Web ブラウザーを使用して、次の Web サイトに移動し、Insight RS ホストサーバーとリモートサポート Web サービス間の通信を確認します。**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（たとえば、`17.1.0.354`）のバージョンが表示されます。

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。**http://www.hpe.com/info/insightonline-ja**
2. HPE パスポートのユーザー ID とパスワードを入力して、**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

- ご使用の環境が組み込みリモートサポート登録の前提条件を満たしている。
- ご使用の iLO ユーザーアカウントが iLO 設定の構成特権を有している。
- HPE パスポートアカウントがある。詳しくは、**http://www.hpe.com/info/insightonline-ja** 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

リモートサポートの登録に関する前提条件(201 ページ)
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(217 ページ)

Insight Online Direct Connect の登録（手順 1）

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。**http://www.hpe.com/info/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。**http://www.hpe.com/info/insightonline-ja**
2. HPE パスポートの認証情報を入力してログインします。
3. **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 個のデバイスの登録を完了できます。
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、**登録の送信**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）

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、**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場合は、**アラートメールを構成します**。

Web プロキシ設定の編集（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更新します。

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、次の設定を更新します。

- **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

- ご使用の環境が組み込みリモートサポート登録の前提条件を満たしている。
- iLO 設定の構成特権。

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 リモートサポート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。
   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

リモートサポートの登録に関する前提条件(201 ページ)

Insight Online Direct Connect からの登録の解除

前提条件

iLO 設定の構成特権。

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

サービスイベントを監視し、テストイベントを送信し、メンテナンスモードを設定するには、**サービスイベント**ページを使用します。

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。リモートサポートにサーバーを登録すると、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、イベントは Insight Online（Direct Connect）または Insight RS ホストサーバー（Central Connect）に直接送信され、そこから 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）。

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使用

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では、Insight RS または Insight Online に送信されるすべてのイベントまたはメッセージに、イベントの処置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 の設定の構成

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に設定**チェックボックスを選択します。
3. **失効**メニューから時間を選択します。
4. **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。

   ヒント:

   メンテナンスモードを早目に終了するには、**メンテナンスモードをクリアする**チェックボックスを選択し、**適用**をクリックします。

   指定した時間が経過すると、メンテナンスモードは自動的に終了します。メンテナンスモードがクリアされると、iLO によって通知されます。

iLO を使用した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 設定の構成特権。

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。

Insight Online を使用したテストサービスイベントの表示

手順

1. 次の Web サイトに移動します。**http://www.hpe.com/info/insightonline-ja**
2. HPE パスポートの認証情報を入力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 コンソールを使用したテストサービスイベントの表示（Insight Remote Support Central Connect のみ）

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

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。この列には、設定された 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	パワーサプライ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

サービスイベントログの消去

前提条件

iLO 設定の構成特権

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、Remote Support 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

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。

Active Health System レポート

Insight Online Direct Connect または Insight Remote Support Central Connect のどちらを使用するかに応じて、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および閉ループ品質分析に使用されます。

- 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。

データ収集情報の送信

前提条件

iLO 設定の構成特権。

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**が更新されます。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。

Active Health System レポート情報の送信

前提条件

iLO 設定の構成特権。

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**が更新されます。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。

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（**http://www.hpe.com/info/insightonline-ja**）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：ProLiant サーバー上の Insight RS Console で以前に監視されていたデバイスを、新しいホストサーバーで監視するよう構成する場合は、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。
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. iLO または Intelligent Provisioning を使用して、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。

   この手順における Insight RS のタスクの詳細は、Insight Remote Support 監視対象デバイスコンフィギュレーションガイドと、Insight Remote Support のインストール/コンフィギュレーションガイドを参照してください。

詳しくは

Insight Remote Support Central Connect の登録解除(210 ページ)
Insight Online Direct Connect の登録(206 ページ)

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 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、Insight Remote Support Central Connect から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パリ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、パリで現地時間午後 5 時に Insight Remote Support Central Connect から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、再登録されたデバイスは Insight Online に表示されません。
3. Insight Online Direct Connect にデバイスを登録します。

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、Insight Online Direct Connect から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パリ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、パリで現地時間午後 5 時に Insight Online Direct Connect から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、再登録されたデバイスは Insight Online（有効な場合）に表示されません。
3. Insight Remote Support Central Connect にデバイスを登録します。

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。特権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 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。

12 個を超えるユーザーアカウントをサポートするには、ディレクトリを使用できます。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

ディレクトリの認証と認可(270 ページ)

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特権

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. 次の特権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 設定の構成**
   - **ユーザーアカウント管理**

- **ホスト NIC**
- **ホストストレージ**
- **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。

5. 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。

6. 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。

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特権

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**ローカルユーザーの追加/編集**ページに入力します。

   - **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**の値を更新します。
5. 次の特権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 の構成**
   - **ユーザーアカウント管理**
   - **ホスト NIC**
   - **ホストストレージ**
   - **リカバリセット**

6. 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。
7. ユーザーアカウントの変更を保存するには、**ユーザーの更新**をクリックします。

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 ユーザーアカウントオプション

- **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。
- **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、印字可能な文字を使用する必要があります。
- **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。
- **サービスアカウント** - サービスアカウントとして、アカウントを指定します。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。

iLO ユーザー権限

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設定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** - ホストプラットフォー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。
- **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 ファームウェアを更新することができます。この権限では、ローカルユーザーアカウントは管理できません。

  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、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** - 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。
- **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。
- **リカバリセット** - リカバリインストール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 Administrator 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。

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、ホストストレージ、リカバリセット、ホスト BIOS、およびログイン。

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を介して使用できません。ログイン、およびリカバリセット。

ホスト BIOS、ホスト NIC、およびホストストレージの各権限は、ホストベースのユーティリティを使用した構成に影響しません。

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編集する場合に、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すすめします。

- パスワードを使用する場合：
  - パスワードを書き留めたり記録したりしないでください。
  - 他のユーザーとパスワードを共有しないでください。
  - 辞書にあるような単語で構成されたパスワードを使用しないでください。
  - 会社名、製品名、ユーザー名、ログイン名のような推測しやすい単語が含まれるパスワードを使用しないでください。
- 少なくとも以下の 3 つの特性を持つパスワードを使用してください。

- 1 文字以上の数字
- 1 文字以上の特殊文字
- 1 文字以上の小文字
- 1 文字以上の大文字

- iLO 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。デフォルトの**最小パスワード長**は、8 文字です。

重要:

Hewlett Packard Enterprise では、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 文字未満に設定することはおすすめできません。

詳しくは

iLO アクセスオプションの構成(249 ページ)

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、同等の 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。オペレーターレベルを満たさない権限の任意の組み合わせは、IPMI ユーザーです。

- **オペレーター** - オペレーターは、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。

  IPMI オペレーター権限については、リモートコンソールアクセス、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。管理者レベルを満たさないオペレーター以上の権限の任意の組み合わせは、IPMI ユーザーです。

- **管理者** - 管理者は、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 管理者権限については、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特権が表示されます。

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特権が表示されます。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：特権の名前を表示るには、カーソルを特権アイコン上に移動します。

iLO ディレクトリグループ

iLO では、ディレクトリグループアカウントを管理できます。MMC または ConsoleOne を使用して、ディレクトリベースのユーザーアカウントを管理します。

ディレクトリグループの追加

前提条件

- iLO 設定の構成権限
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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 設定の構成**
   - **ユーザーアカウント管理**
   - **ホスト NIC**
   - **ホストストレージ**
   - **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。

ディレクトリグループの編集

前提条件

- iLO 設定の構成権限
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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**
   - **iLO 設定の構成**
   - **ユーザーアカウント管理**
   - **ホスト NIC**
   - **ホストストレージ**
   - **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、**グループの更新**をクリックします。

ディレクトリグループの削除

前提条件

- iLO 設定の構成特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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。

ディレクトリグループ権限

次の権限は、ディレクトリグループに適用されます。

- **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設定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。

- **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 ファームウェアを更新することができます。この権限では、ローカルユーザーアカウントは管理できません。

  iLO を構成したら、iLO Web インターフェイス、iLO RESTful API、HPQLOCFG、または CLI を使用して、すべてのユーザーからこの権限を取り消して、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。

- **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。

- **リカバリセット** - ディレクトリユーザーがクリティカルリカバリインストール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 Administrator 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。

ホスト BIOS、ホスト NIC、およびホストストレージの各権限は、ホストベースのユーティリティを使用した構成に影響しません。

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、構成された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。

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。

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 または従来の BIOS を選択できます。

前提条件

iLO の設定の構成

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** を選択します。
3. **適用**をクリックします。

   変更を確認するよう iLO により求められます。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。
4. **OK** をクリックします。
5. 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 設定の構成特権

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 iLO 仮想メディアデバイスでサポートされていますが、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更新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。

前提条件

iLO の設定の構成

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

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。

   以下のオプションを使用できます。

   - **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 <番号>**。サーバー Ethernet カードはネットワークデバイス 1、追加の NIC/FlexibleLOM カードはネットワークデバイス 2、3 などになります。
   - **Intelligent Provisioning**
   - **内蔵 UEFI シェル** - このオプションを選択した場合、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ブートします。

   注記:

   フロッピードライブは iLO 仮想メディアデバイスでサポートされていますが、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 は、ワンタイムブートオプションが正常に更新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更新され、選択内容が示されます。

UEFI モードでのワンタイムブートステータスの変更

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。

   以下のオプションを使用できます。

- **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<番号>**。サーバー Ethernet カードはネットワークデバイス 1、追加の NIC/FlexibleLOM カードはネットワークデバイス 2、3 などになります。
- **Intelligent Provisioning**
- **HTTP ブート** - このオプションを選択すると、HTTP ブート機能が有効でありブート可能イメージの URI が ROM ベース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。
- **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** - このオプションを選択した場合、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ブートします。

注記:

フロッピードライブは iLO 仮想メディアデバイスでサポートされていますが、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. **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、ブート可能パーティションが 2 つあるハードディスクドライブを所有している場合、このオプションを使用して、次回のサーバーリセットで使用するブート可能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更新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更新され、選択内容が示されます。

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 の設定の構成

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。

ブラウザーを使用したライセンスキーのインストール

前提条件

iLO 設定の構成特権

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。

   セグメント間を移動するには、**Tab** キーを押すか、**アクティブ化キー**ボックスのセグメントの内側をクリックします。**アクティブ化キー**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。
3. **Install** 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

失われたライセンスキーの復旧

iLO のライセンスキーが失われた場合、以下のメールアドレスのいずれかに交換要求とお客様の購入の証明を送信してください。

- 南北アメリカ：**licensing.ams@hpe.com**
- 欧州、中東、およびアフリカ：**licensing.emea@hpe.com**
- アジア太平洋地域および日本：**licensing.apj@hpe.com**

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、サーバーセットアップ、サーバーヘルスの監視、電力と温度制御の監視、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。

iLO ライセンスを登録する理由

- 登録により、一意の HPE サポート契約 ID（SAID）が有効になります。SAID はユーザーとユーザーが使用する製品を識別します。
- SAID を使用すると、より迅速な HPE サポートサービスが得られます。

- HPE サポートセンターにアクセスできます。
- HPE アップデートセンターでソフトウェアアップデートにアクセスできます。
- 重要な製品アラートを受信します。
- HPE ライセンスポータルを使用して 1 つの場所で HPE 製品ライセンスキーを追跡します。

iLO ライセンスを登録する方法

1. **ライセンス権利証明書**または**ライセンスの確認メール**で権利注文番号（EON）を探します。
2. HPE **ライセンスポータル**で EON を入力します。

ライセンスキー情報

- 無料の iLO トライアルライセンスの取得、またはライセンスキーの購入、登録、および取得については、**http://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。
- 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。
- 別のサーバータイプを意味するライセンスキーを使用してサーバーにライセンスを適用することはできません。
- 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。
- ライセンスキーを無くした場合、無くなったライセンスキーに対する手順に従います。

Enterprise Secure Key Manager を iLO で使用する

iLO 5 では、Enterprise Secure Key Manager（ESKM）3.1 以降がサポートされており、HPE Smart Array Secure Encryption と組み合わせて使用することができます。

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。

CNSA セキュリティ状態が有効になっている場合、ESKM はサポートされません。

- HPE Smart Array Secure Encryption は、HPE Smart アレイコントローラをサポートし、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。
- ESKM 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 は、ESKM と Smart アレイコントローラ間のキー交換を管理します。iLO は、ESKM 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、管理者特権を持つ、ESKM 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、HPE Smart Array Secure Encryption インストール/ユーザーガイドを参照してください。

HPE Smart Array Secure Encryption と ESKM について詳しくは、HPE Smart Array Secure Encryption インストール/ユーザーガイドを参照してください。

キーマネージャーサーバーの構成

前提条件

- iLO 設定の構成権限
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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. 次の情報を入力します。
   - **プライマリキーサーバー** - 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、およびポート。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** - 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、およびポート。この文字列の最大長は 79 文字です。
3. 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の場合、**冗長化が必要**オプションを有効にして、サーバーの冗長化を確認します。

   Hewlett Packard Enterprise では、このオプションを有効にすることをおすすめします。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。
4. **適用**をクリックします。

キーマネージャー構成の詳細の追加

前提条件

- iLO 設定の構成権限
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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。

   ESKM 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 の MAC アドレス>**です。アカウント名は読み取り専用で、iLO が ESKM と通信するときに使用されます。
2. 次の情報を **ESKM 上の iLO アカウント**セクションに入力します。
   - **Group**
   - **ESKM ローカル CA 証明書名**（オプション）
3. 次の情報を **ESKM 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**

4. **ESKM をアップデート**をクリックします。

   iLO は、ESKM に存在する **ilo-<iLO の MAC アドレス >**という名前のアカウントを確認します。

   アカウントが存在する場合は、iLO はアカウントのパスワードが正しいことを確認します。iLO はこのパスワードを自動的に生成します。パスワードが正しくない場合は、iLO はパスワードを更新します。iLO が出荷時のデフォルト設定に戻った場合、パスワードは正しくない可能性があります。アカウントが存在しない場合は、iLO がアカウントを作成します。

   iLO が ESKM ローカルグループのメンバーでない場合は、要求された名前のグループを作成しようとします。iLO は、すでに ESKM ローカルグループのメンバーになっている場合、ステップ 2 で入力されたグループを無視し、ESKM に存在する既存のグループ割り当てを使用します。iLO でグループを変更しても、ESKM に設定されている現在のキーのグループアクセス権には影響しません。新しいグループの割り当てが必要な場合は、iLO 設定を更新する前に ESKM を更新します。

   ステップ 2 で **ESKM ローカル CA 証明書名**を入力した場合、ESKM 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

- **グループ** - iLO ユーザーアカウントと、iLO が ESKM にインポートするキーで使用するために、ESKM 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。

- **ESKM ローカル CA 証明書名**（オプション） - iLO を信頼済み ESKM サーバーと確実に通信させるために、ESKM 内のローカル認証機関証明書の名前を入力します。通常、**Local CA** という名前が付けられ、ESKM のローカル CA の下に一覧表示されています。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 ESKM 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** - ESKM に構成された管理者アクセス権を持つローカルのユーザー名。このユーザー名は ESKM デプロイメントユーザーです。

  iLO でキーマネージャー構成の詳細を追加する前に、展開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** - ESKM に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のパスワード。

ESKM 構成のテスト

ESKM 接続のテスト機能を使用して、構成設定を確認します。テストは、HPE セキュア暗号化のキー管理サービスを提供するために iLO および ESKM サーバーが設定されているかを確認します。

テスト中、iLO は次のタスクを試みます。

- TLS を使用してプライマリ ESKM サーバー（および構成されている場合はセカンダリ ESKM）に接続する。
- 構成済みの認証情報およびアカウントを使用して、ESKM への認証を試みる。
- ESKM 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。

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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- 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. **ESKM 接続のテスト**をクリックします。

   テスト結果は、**Enterprise Secure Key Manager イベント**テーブルに表示されます。

ESKM 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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. **Enterprise Secure Key Manager 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。

ESKM ログのクリア

前提条件

- iLO 設定の構成特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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. **ESKM ログのクリア**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、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 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、.NET IRC、および Java IRC の翻訳を提供しています。

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。

- Java IRC および.NET IRC 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 ファームウェアを更新する場合は、言語パックの内容が iLO Web インターフェイスに対応するように、Hewlett Packard Enterprise は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。

言語パックのインストール

前提条件

iLO の設定の構成

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。**http://www.hpe.com/support/ilo5**
2. 内容を解凍するには、ダウンロードしたファイルをダブルクリックします。

   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**をクリックします。

   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. **参照**（Internet Explorer または Firefox）または**ファイルを選択**（Chrome）をクリックします。
5. 言語パックを選択し、**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 は、選択された言語パックをインストールし、再起動して、ブラウザー接続を終了します。

   接続が再確立されるまでに、数分かかることがあります。

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 設定の構成特権
- 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。

現在の iLO Web インターフェイスセッション言語の構成

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。

言語パックのアンインストール

前提条件

iLO の設定の構成

手順

1. 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。
2. 削除する言語の横にあるゴミ箱アイコンをクリックします。
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。

   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。iLO

   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 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。詳しくは、**デフォルト言語設定の構成**(237 ページ)を参照してください。

ファームウェア検証

ファームウェア検証ページでは、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応するには、結果を記録するのか、それとも結果を記録してリカバリインストールセットを使用する修復アクションを開始するのかを選択します。

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
- 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。

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 設定の構成特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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）** - バックグラウンドスキャン頻度（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(89 ページ)

ファームウェア検証スキャンの実行

前提条件

- iLO 設定の構成特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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更新され、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。詳しくは、iLO のユーザーガイドを参照してください。

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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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。

フルシステムリカバリの開始

iLO は、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 設定の構成特権
- 仮想メディア特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- 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。）

iLO バックアップとリストア

バックアップとリストア機能を使用すると、バックアップ元のシステムと同じハードウェア構成を持つシステムに iLO 構成をリストアできます。この機能は、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。

一般に、iLO のリストア操作をユーザーが実行する必要があることは予期されていません。ただし、構成のバックアップを取っておくことで、通常の動作環境に容易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 ファームウェアを更新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。

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、工場出荷時のデフォルト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。

システムボードの取り付け

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。

失われたライセンスキー

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。

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、ユーザーデータベース、ライセンスキーなど、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。

リストアされない情報

情報によってはリストアの対象として適していないものがあります。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時間または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時間または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。

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 構成のバックアップ

前提条件

iLO 設定の構成特権

手順

1. ナビゲーションツリーで**管理**をクリックし、**バックアップと復元**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 設定の構成特権
- iLO ユーザーアカウント管理特権
- iLO 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。

  FIPS および CNSA の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更新時に削除されます。

手順

1. ナビゲーションツリーで**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。

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 設定の構成特権
- iLO ユーザーアカウント管理特権
- iLO 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。

  FIPS および CNSA の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更新時に削除されます。

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。**

iLO のセキュリティ機能の使用

iLO セキュリティ

iLO Web インターフェイスを使用して、設定できるセキュリティ機能にアクセスするには、ナビゲーションツリーの**セキュリティ**をクリックします。

iLO のセキュリティについて詳しくは、*HPE Gen10 セキュリティリファレンスガイド*を参照してください。

セキュリティに関する一般的なガイドライン

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。

- 別個の管理ネットワーク上に iLO を構成します。
- iLO は、インターネットに直接接続しないでください。
- SSL 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のパスワードを変更します。
- 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。
- 使用しないプロトコル（SNMP や IPMI over LAN など）を無効にします。
- 使用しない機能（リモートコンソールや仮想メディアなど）を無効にします。
- 統合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、**リモートコンソール&メディア**ページの**セキュリティ**タブで **IRC は iLO 内の信頼された証明書を要求します**を有効にします。

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セキュリティ保護します。

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の製品レベル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。

詳しくは

SSL 証明書の管理(267 ページ)
ディレクトリの認証と認可(270 ページ)
iLO アクセス設定(247 ページ)
iLO ネットワークに接続する(25 ページ)
ローカル ユーザー アカウントの編集(220 ページ)
暗号化の設定(279 ページ)
統合リモートコンソールの信頼設定（.NET IRC）の設定(139 ページ)

iLO アクセス設定

サービスの設定やアクセスオプションを含めて、iLO アクセス設定を変更することができます。

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。

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。

このページで、ポート、iLO インターフェイスとフィーチャアクセス、パスワード長、および iLO ログインセキュリティなどの iLO セキュリティ機能を設定できます。

iLO サービス設定の構成

iLO が使用する TCP/IP ポートは設定可能であり、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。

iLO の機能を有効または無効にするには、**アクセス設定**ページの**サービス**セクションを使用します。

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。これらの設定を変更すると、変更を有効にするために iLO のリセットが必要になります。

前提条件

iLO 設定の構成特権

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. 必要に応じて、サービス設定を更新します。

   サービス設定を無効にするとき、iLO によって、変更を適用するとこのサービス設定に依存する機能を使用できなくなることが通知されます。

3. **適用**をクリックします。

   変更を適用して iLO をリセットすることを確認するように iLO が要求します。

4. 今すぐ変更を適用して iLO をリセットするには、**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。

サービス設定

アクセス設定ページの**サービス**セクションでは、以下の設定を構成できます。

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、暗号化された iLO CLP への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 22 です。

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。

この値を無効に設定した場合、iLO は、Web サーバー非 SSL ポートまたは Web サーバー SSL ポート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。RIBCL、iLO RESTful API、リモートコンソール、iLO 連携、および iLO Web インターフェイス。

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 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 443 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、HTML5 IRC、.NET IRC、Java IRC、スタンドアロンリモートコンソール、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 17990 です。

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、ローカルおよび URL ベースの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 17988 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更新されます。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が使用できなくなり、入力できなくなります。

SNMP ポート

SNMP ポートを設定します。SNMP アクセス用の業界標準（デフォルト）の SNMP ポートは、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 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）用の業界標準（デフォルト）の SNMP ポートは、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。

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。

IPMI/DCMI over LAN が無効になっている場合、iLO は LAN 経由の 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。

IPMI/DCMI over LAN 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。

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 623 です。

iLO アクセスオプションの構成

前提条件

iLO 設定の構成特権

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、**アクセス設定**タブをクリックします。
2. 必要に応じて、アクセスオプションを更新します。
3. **適用**をクリックします。

   リセットを必要としない値を変更した場合、iLO は変更を完了して、ページを更新します。

   リセットを反映する必要がある値を変更した場合、iLO は変更を保存して、iLO のリセットを確認するよう求めます。
4. iLO がリセットするよう求めたら、**はい、リセットします**をクリックしてブラウザー接続を終了し、iLO をリセットします。

   iLO のリセットが完了すると、変更が反映されます。

アクセスオプション

アクセス設定ページの**アクセスオプション**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）

ここで指定した時間が経過してもユーザーの操作がない場合、iLO Web インターフェイスセッションまたはリモートコンソールセッションは自動的に終了します。

各接続は別個のセッションであるため、iLO Web インターフェイスまたはリモートコンソールは、アイドル時間を別々に追跡します。仮想メディアデバイスが接続されている場合、この設定はリモートコンソールセッションに影響を与えません。

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

iLO の機能が使用可能かどうかを指定します。

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 機能を再度有効にするには、UEFI システムユーティリティを使用します。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。

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。

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。

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>
```

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。

このオプションは、UEFI システムユーティリティでは **iLO 5 構成ユーティリティ**と呼ばれています。

iLO 5 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、ユーザー認証情報プロンプトを表示する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。

FIPS および CNSA のセキュリティ状態が有効になっている場合、iLO は、このオプションが無効な場合でもユーザー認証情報プロンプトを表示します。

このオプションは、UEFI システムユーティリティでは **Require user login and configuration privilege for iLO 5 Configuration** と呼ばれます。

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。

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。

XML 応答

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、ネットワーク上の iLO システムを他のソフトウェアが検出して識別することが許可されます。iLO が提供する XML 応答を表示するには、**表示**をクリックします。

このオプションが無効になっている場合、iLO は空の XML オブジェクトで要求に応答します。

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。

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：この値を必ず 9600 に設定してください。別の値を使用した場合、Synergy コンソールおよびコンポーザーの CLI からシリアルコマンドラインインターフェイスにアクセスできません。

- **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。

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。

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。
- ブラウザーの更新を強制して新しい値を表示するには、この設定を保存して **F5** キーを押します。

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。
- ブラウザーの更新を強制して新しい値を表示するには、この設定を保存して **F5** キーを押します。

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**— 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。

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。

遅延の前の認証エラー

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 1、3、5 回、または各ログイン試行の失敗時です。

デフォルト設定は 1 です。これは、2 度目に試したログインが失敗するまでログイン遅延は課せられないことを意味します。

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、ProLiant Gen10 サーバーおよび Synergy Gen10 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。

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 Ethernet 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、iLO Web インターフェイス、リモートコンソール、CLI、iLO RESTful API、またはスクリプトにアクセスします。

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。

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ます。

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更新の進行中などの別の状態を示して点滅します。
5. オプション：Active Health System Viewer にファイルをアップロードします。

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

iLO サービスポートを介した iLO へのクライアントの接続

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 Ethernet 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. ブラウザー、CLI、またはスクリプティングユーティリティで以下の IPv4 アドレスを使用して、iLO に接続します。**`169.254.1.2`**。

   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更新の進行中などの状態を示して点滅します。

iLO サービスポート設定の構成

前提条件

iLO の設定の構成

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、**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 Ethernet アダプタ**
3. **適用**をクリックします。

   更新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 ユーザー名とパスワードを `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 Ethernet アダプター** - USB Ethernet 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 イーサネットアダプターをサポートします。

- AX88772
- AX88772A
- AX88772B
- AX88772C

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すすめします。

iLO サービスポート経由で Active Health System ログをダウンロードするため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` - ダウンロードの範囲を制御します。日付範囲に対応する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 iLO 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

セキュアシェルキー（SSH）ページには、各ユーザーに関連付けられた SSH パブリックキーのハッシュが表示されます。各ユーザーに割り当てられるキーは 1 つだけです。SSH キーを表示、追加、または削除するには、このページを使用します。

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特権

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` ファイルを生成します。
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、**セキュアシェルキー**タブをクリックします。
4. SSH キーを追加するユーザーの名前の左にあるチェックボックスを選択します。
5. **新しいキーの認証**をクリックします。
6. パブリックキーをコピーして**パブリックキーインポートデータ**ボックスに貼り付けます。

   キーは、2,048 ビットの DSA キーまたは RSA キーでなければなりません。

7. **パブリックキーのインポート**をクリックします。

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特権

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. ディレクトリを切り替えます（`cd /Map1/Config1`）。
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 でなければなりません。
   - hostname と filename の値は必須です。
   - username:password と port の値はオプションです。
   - `oemhpe_loadSSHkey` は、大文字と小文字が区別されます。

   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（SSH）**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。

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 SSH キーを承認するための要件

`mxagentconfig` ユーティリティを使用すると、SSH キーを HPE SIM サーバーから承認できます。

- `mxagentconfig` を使用してキーを承認する前に、iLO で SSH を有効にする必要があります。
- `mxagentconfig` に入力するユーザー名とパスワードは、iLO の設定の構成を持つ iLO ユーザー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 で承認され、`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 キー

iLO に SSH キーを追加する場合、SSH キーファイルを iLO に貼り付けて、そのファイルにユーザーが生成したパブリックキーが含まれる必要があります。iLO ファームウェアは、選択したローカル ユーザーアカウントに各キーを関連付けます。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、同じ特権を持ちます。
- iLO ファームウェアは、1,366 バイト以下の長さの SSH キーをインポートすることができます。キーが 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 ボディで提供されます。
- 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。

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
ZtzF0VInP5x2VFVYmIvdVjSupD92CTlxxAtarOPON2qUqoOajKRtBWLmxcfqsLCTCRLF
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
AAAAB3NzaC1kc3MAAACAYjEd8Rk8HLCLqDI1I+RkA1UXjVS28hNSk8YDljTaJpw1VOlBirrLGPdSt0avN
Sz0DNQuU7gTPfjj/8cXyHe3y95Oa3Rics1fARyLiNFGqFjr7w2ByQuoYUaXBzzghIYMQcmpc/W/kDMC0d
VOf2XnfcLpcVDIm3ahVPRkxFV9WKkAAAAVAI3J61F+oVKrbNovhoHh8pFfUa9LAAAAgA8pU5/M9F0s5Qx
qkEWPD6+FVz9cZ0GfwIbiuAI/9ARsizkbwRtpAlxAp6eDZKFvj3ZIyNjcQODeYYqOvVU45AkSkLBMGjpF
05cVtnWEGEvrW7mAvtG2zwMEDFSREw/V526/jR9TKzSNXTH/wqRtTc/oLotHeyV2jFZFGpxDOvNWAAAAg
Ff6pvWaco3CDELmH0jT3yUkRSaDztpqtoo4D7ev7VrNPPjnKKKmpzHPmAKRxz3g5S80SfWSnWM3n/pekB
a9QI9lH1r3Lx4JoOVwTpkbwb0by4eZ2cqDw20KQ0A5J84iQE9TbPNecJ0HJtZH/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----- CRLF
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 CRLF
-----END SSH KEY-----CRLF
```

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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- オプション : LDAP サーバー CA 証明書をディレクトリ統合のためにインストールする。
- オプション : LDAP ディレクトリ統合を、ディレクトリ統合のための**ディレクトリデフォルトスキーマ**モードで構成します。

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、**CAC Smartcard 認証**タブをクリックします。
2. **信頼済み CA 証明書をインストールします**。

   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（ディレクトリ統合のため）: **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。
5. **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**ボタンをクリックします。
6. オプション : 証明書失効リスト（CRL）をインポートするには、**失効リストの URL** ボックスに URL を入力して、**適用**をクリックします。

   この手順により、以前に発行されて、失効した証明書を無効にできます。

   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。

7. オプション：オンライン証明書ステータスプロトコルを使用してユーザー証明書を確認するには、HTTP または HTTPS URL を入力して、**適用**をクリックします。
8. **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）。

CAC Smartcard 認証の設定

認証オプション

CAC Smartcard 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 は接続時に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

ユーザー証明書の一部分を選択して、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

OCSP URL

設定されている場合、認証用に入力されたユーザー証明書は、オンライン証明書ステータスプロトコルを使用して確認されます。

HTTP および HTTPS URL のみ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 設定の構成権限
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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。

   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。
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 設定の構成権限
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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。

   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。

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 設定の構成権限
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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。

   CRL が**証明書失効リスト（CRL）**セクションに追加され、CRL の説明とシリアル番号が表示されます。

   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。

証明書失効リストの削除

前提条件

- iLO 設定の構成権限
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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。

証明書マッピング

証明書マップページには、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他の CAC

  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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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、**証明書インポートデータ**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。
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**

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. 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。

SSL 証明書の管理

SSL 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 ユーザー認証情報を保護することをお勧めします。

SSL 証明書情報の表示

手順

証明書情報を表示するには、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。
- **発行元** - 証明書を発行した CA。
- **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** - CA によって割り当てられた証明書のシリアル番号。

SSL 証明書の取得とインポート

iLO では、信頼された SSL 証明書を取得するために認証機関に送信できる証明書署名要求を作成して、iLO にインポートできます。

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た場合、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 が生成された場合、証明書は動作しません。その場合には、新しい CSR を生成し、この CSR を使用して CA から新しい証明書を取得する必要があります。

前提条件

iLO の設定の構成

手順

1. **認証機関（CA）から信頼済み証明書を取得します。**
2. **信頼済み証明書を 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 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. **証明書のカスタマイズ**をクリックします。
3. **SSL 証明書カスタマイズ**ページで、次のように入力します。
   - **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. iLO IP アドレスを CSR に含める場合、**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。

   一部の CA はこの入力を使用できないため、このオプションはデフォルトでは無効です。

   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 の作成**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 の作成**を再度クリックします。

   CSR が表示されます。

   CSR には、クライアントのブラウザーと 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。最大 2,048 ビットのキーサイズをサポートします。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。
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。

   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。
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。一部の CA はこの入力を使用できないため、このオプションはデフォルトでは無効です。

信頼済みの証明書のインポート

前提条件

iLO の設定の構成

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 は、最大 3 KB（プライベートキーで使用されるバイト数を含む。つまり 1,024 ビット証明書の場合は 609 バイト、2,048 ビット証明書の場合は 1,187 バイトを含む）の SSL 証明書をサポートします。
5. iLO をリセットします。

ディレクトリの認証と認可

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、スキーマフリーオプションや HPE 拡張スキーマを使用することができます。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。

スキーマフリーおよび HPE 拡張スキーマのディレクトリサーバー証明書検証オプションは、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。

認証およびディレクトリサーバーの設定は、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。

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 iLO 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。
4. Kerberos キータブファイルが利用可能である（Kerberos 認証のみ）。

iLO での Kerberos 認証設定の構成

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. **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場合は、**ブラウズ**（Iternet Explorer または Firefox）もしくは**ファイルを選択**（Chrome）をクリックしてから、画面上の指示に従ってください。
8. **設定の適用**をクリックします。

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。この文字列は最大 128 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。この文字列は最大 128 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 証明書を置換します。

   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 間の通信をテストするには、**設定のテスト**をクリックします。
13. ディレクトリグループを設定するには、**グループ管理**をクリックして**ディレクトリグループ**ページに移動します。

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。アクセスを無効にするには、**無効**を選択します。

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** ー 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** ー 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。ディレクトリユーザーコンテキストは最大 128 文字です。
- **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 証明書を置換します。

   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

ディレクトリテストの実行(276 ページ)
iLO ディレクトリグループ(224 ページ)

HPE 拡張スキーマディレクトリの設定

- **iLO 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。アクセスを無効にするには、**無効**を選択します。

  この構成では、Active Directory をサポートしています。

- **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。

- **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（たとえば、`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、ユーザー検索コンテキストは iLO オブジェクト DN には適用されません。

- **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。ディレクトリユーザーコンテキストは最大 128 文字です。
- **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。

詳しくは

ディレクトリテストの実行(276 ページ)
iLO ディレクトリグループ(224 ページ)

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

ディレクトリまたは Kerberos 認証を使用するように iLO を構成した場合、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。
- ディレクトリサポートが無効になってる場合や、iLO ライセンスが取り消された場合に、ローカルユーザーアカウントを使用するアクセスが有効になります。

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

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更新するには、**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更新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。テストの実行が終了したとき、テストが失敗して先に進めないとき、またはテストを停止したとき、結果は停止します。テスト結果を示します。

- **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、すぐには入手できない情報（ディレクトリサーバーの証明書のサブジェクトや、どのロールの評価が成功したかなど）によって更新されます。

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、構成された 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 アドレスで設定されている場合、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、構成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。

テストが失敗する場合、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 接続のネゴシエーションを試みます。

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、ネゴシエーション、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 ハンドシェークとネゴシエーションが成功した場合、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、ディレクトリサーバーに対して、指定されたユーザー名とパスワードを認証します。

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 **LOM 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。

暗号化の設定

製品または高度なセキュリティのセキュリティ状態の有効化

この手順を使用して、iLO が**セキュリティ状態**として **製品**を使用するか**高度なセキュリティ**を使用するかを設定します。

iLO が **FIPS** および **CNSA** セキュリティ状態を使用するように構成するには、**FIPS および CNSA セキュリティ状態を有効にする**(280 ページ)を参照してください。

前提条件

iLO 設定の構成特権

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**製品**または**高度なセキュリティ**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 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。

FIPS および CNSA セキュリティ状態を有効にする

この手順を使用して、iLO が **FIPS** および **CNSA** セキュリティ状態を使用するように構成します。iLO が**製品**または**高度なセキュリティ**セキュリティ状態を使用するように構成するには、**製品または高度なセキュリティのセキュリティ状態の有効化**(279 ページ)を参照してください。

iLO を FIPS 承認済み環境に設定するには、**iLO による FIPS 承認済み環境の構成**(282 ページ)を参照してください。

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。

FIPS または 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 は構成されているセキュリティ状態で引き続き動作しますが、期限切れになった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。

前提条件

- iLO 設定の構成特権
- 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 iLO 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：iLO バックアップ機能または HPONCFG を使用して、iLO の現在の設定を取得します。

   詳しくは、**iLO バックアップと復元**または iLO スクリプティング/CLI ガイドを参照してください。

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。すべての iLO 設定とユーザーデータ、ほとんどの構成設定、ログが消去されます。インストールした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には、**はい、適用してリセットします**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** を有効にする要求を確認するには、**はい、適用してリセットします**をクリックします。

      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。

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**と **SNMP アクセス**が無効になっていることを確認します。

   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。

9. オプション：iLO 復元機能または HPONCFG を使用して、iLO 構成を復元します。

   HPONCFG を使用して構成を復元するときは、ユーザーの権限が必要です。必要なユーザーの権限を持っていない場合は、エラーメッセージが表示されます。

   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、Windows 用 HPONCFG はサポートされません。

   詳しくは、**iLO バックアップと復元**または iLO スクリプティング/CLI ガイドを参照してください。

10. オプション：構成を復元した場合は、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て、**アクセス設定**ページで **IPMI/DCMI over LAN** アクセスと **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、構成を復元するとリセットされる可能性があります。

11. 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。

高いセキュリティ状態を使用する場合の iLO への接続

デフォルト値よりも高いセキュリティ状態（**製品**）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、高度なセキュリティ、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を持っていない場合は、エラーメッセージが表示されます。
- CNSA セキュリティ状態が有効になっている場合は、Windows 用 HPONCFG はサポートされません。

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**(280 ページ)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 に関する情報を確認するには、iLO というキーワードを *Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules* ドキュメントで検索してください。

FIPS モードの無効化

手順

1. iLO の FIPS モードを無効にするには（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、iLO のユーザーデータ、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。

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。

CNSA モードの無効化

手順

1. CNSA モードを無効にするには、次のいずれかの操作を行います。

   - CNSA モードを無効にして、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 モードと FIPS 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、iLO のユーザーデータ、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。

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。

iLO セキュリティ状態

製品（デフォルト）

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。

高度なセキュリティ

iLO がこのセキュリティ状態に設定されている場合：

- iLO は、ブラウザー、SSH ポート、iLO RESTful API、および RIBCL 経由の安全な 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。**高度なセキュリティ**が有効になっている場合、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 に接続する必要があります。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。
- このセキュリティ状態を使用するように iLO が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。
- 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

iLO がこのセキュリティ状態に設定されている場合：

- 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。

  詳しくは、**iLO による FIPS 承認済み環境の構成**(282 ページ)を参照してください。

- iLO は、ブラウザー、SSH ポート、iLO RESTful API、および RIBCL 経由の安全な 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。**FIPS** が有効になっている場合、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 に接続する必要があります。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。
- このセキュリティ状態を使用するように iLO が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。
- 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。

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 により定義された CNSA 要件への準拠を目的とするほか、米国政府機密として分類されたデータを保持するために使用するシステムを保護すること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。

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 HighSecurity

- 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

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、ESKM 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。

設定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 HighSecurity

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

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 準拠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 設定の構成特権

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 特権は、**シングルサインオン設定**セクションで設定します。
4. SSO 設定を保存するには、**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、 **信頼済み証明書の追加**(289 ページ)または**直接 DNS 名のインポート**(290 ページ)を参照してください。

6. iLO で SSO を設定後、HPE SSO 準拠アプリケーションにログインして iLO にアクセスします。

   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。

   システムが信頼済みサーバーとして登録されていても、現在の信頼モードや証明書のステータスによって SSO が拒否されることもあります。たとえば、SSO が拒否されるのは次のようなときです。

   - サーバーが信頼済みサーバーとして登録されていて、証明書がインポートされておらず、信頼モードが**証明書による信頼**に設定されている。
   - サーバー証明書がインポートされているが、失効している。
   - インストールされている証明書は iLO のセキュリティ要件を満たしていません。
     - HighSecurity または FIPS セキュリティ状態が有効な場合、2048 ビット証明書が必要です。
     - CNSA セキュリティ状態が有効な場合は、3072 ビット RSA キーまたは NIST P-384 曲線の 384 ビット ECDSA キーを含む証明書が必要です。

   信頼済みサーバーのリストは、SSO が無効になっているときは使用されません。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のオプション

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照合することで、HPE SSO 準拠アプリケーションからの 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 名と照合することで、HPE SSO 準拠アプリケーションからの SSO 接続を有効にします。
- **すべて信頼**（最も安全性が低い） - HPE SSO 準拠アプリケーションから開始されたすべての SSO 接続を受け入れます。

SSO ユーザー権限

ユーザーは、HPE SSO 準拠アプリケーションにログインすると、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証されます。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。

HPE SSO 準拠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 準拠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 の設定の構成

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、**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 名または IP アドレスを **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 準拠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 SMS 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** > **HPE Systems Insight Manager Server Certificate** の順に選択して、**Export** をクリックします。

直接 DNS 名のインポート

前提条件

iLO の設定の構成

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. **DNS 名から直接インポート**セクションに DNS 名または IP アドレスを入力し、**適用**をクリックします。

信頼済み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 を使用するように設定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。
  - 証明書は設定されている 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**有効開始日**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）。

信頼済み証明書とレコードの削除

前提条件

iLO の設定の構成

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。

   選択した証明書またはレコードを削除することを確認するプロンプトが表示されます。iLO

   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場合に正常に機能しないことがあります。
4. **はい**をクリックします。

ログインセキュリティバナーの設定

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 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。

ヒント:

デフォルトのテキストを復元するには、**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を使用した iLO セキュリティ

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。セキュリティを無効にすると、iLO が**製品**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に、すべての特権によるユーザー ID とパスワードを使用しないログインアクセスを許可します。

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。iLO セキュリティを有効または無効に設定し、サーバーの電源を投入します。システムメンテナンススイッチを使用して iLO セキュリティを有効および無効にする方法については、サーバーのメンテナンス&サービスガイドを参照してください。

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理由

- ユーザーアカウント管理特権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 NIC がオフになっていて、ROM ベースの構成ユーティリティを実行してオンにし直すことが不可能かまたは不便である。
- ユーザー名が 1 つだけ設定され、パスワードを忘れた。

iLO セキュリティの無効化の影響

iLO が本番環境セキュリティ状態を使用するように設定されており、iLO セキュリティを無効にしている場合、次のようになります。

- すべてのセキュリティ認証確認が無効になる。
- ホストサーバーがリセットされると、ROM ベースの構成ユーティリティが実行される。
- iLO が無効化されず、設定に従って、ネットワーク上で表示できる。
- iLO 機能が無効にされても、サーバーの電源を切って再度投入するまで、iLO は、ユーザーをログアウトしたり無効化プロセスを実行したりしない。
- 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 アラート送信先が設定されている場合、システムメンテナンススイッチを使用して iLO セキュリティを有効または無効にしてから iLO を開始すると、SNMP アラートが送信される。
- この特権を持つ既存のアカウントのユーザー認証情報を入力した場合でも、システムリカバリ特権が必要なアクションはどれも実行できない。

  セキュリティが無効なときに 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。

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。

表 2: 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 Array • SMART ドライブ監視（Smart Array に接続） • Smart Array に接続されている内蔵および外付けドライブ • Smart ストレージバッテリ監視（サポート対象のサーバーのみ）	• SMART ドライブ監視（Smart Array、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 • VLAN 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 Linux での [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] AMS ベースの OS ログ記録（Red Hat および SUSE Linux Enterprise Server では/var/log/messages、VMware では/var/log/syslog）。

[2] Smart Array のログ記録をサポートします。

Agentless Management Service

- Windows インストールの場合に Intelligent Provisioning の**推奨**インストール方法を使用すると、AMS は自動的にインストールされます。
- 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

iLO ドライバーのインストール(31 ページ)

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 Web サイト **http://www.hpe.com/servers/spp.**からダウンロードします。
- **http://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 **http://www.hpe.com/support/SDR-Linux**（VMware）（英語）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。

  また、AMS は、Hewlett Packard Enterprise Software Depot（**http://www.hpe.com/support/SDR-Linux**）でリリースされるカスタマイズされた Hewlett Packard Enterprise VMware ISO イメージに含まれています。

- Linux Management Component Pack に登録します（Ubuntu）。詳しくは、**http://www.hpe.com/support/SDR-Linux** を参照してください。

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、**http://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 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、次のコマンドのいずれかを入力します。
   - **SuSE Linux Enterprise Server 12 および Red Hat Enterprise Linux 7** - **`systemctl status smad; systemctl status amsd`**。
   - **SuSE Linux Enterprise Server 11 および Red Hat Enterprise Linux 6** - **`service smad status; service amsd status`**。

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 ステータスの確認：Ubuntu

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 **`dpkg -l amsd`** を入力します。
2. AMS が実行されていることを確認するには、コマンド **`service smad status; service amsd 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 12 および Red Hat Enterprise Linux 7** - コマンドとして `systemctl restart smad; systemctl restart amsd` を入力します。
- **SuSE Linux Enterprise Server 11 および Red Hat Enterprise Linux 6** - コマンドとして **`service smad restart; service amsd restart`** 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。
- **Ubuntu 16.04.3/HWE カーネル以降** - コマンド`sudo service smad restart; sudo service amsd restart`を入力します。

System Management Assistant

Gen10 サーバー プラットフォームのリリースでは、iLO で OS ベースの SNMP エージェントがサポートされなくなりました。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 12 および Red Hat Enterprise Linux 7** - コマンドとして `systemctl enable smad_rev; systemctl start smad_rev` を入力します。
   - **SuSE Linux Enterprise Server 11 および Red Hat Enterprise Linux 6** - コマンドとして `service smad_rev start` を入力します。
   - **Ubuntu 16.04.3/HWE カーネル以降** - コマンド **`sudo service smad_rev start`** 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 12 および Red Hat Enterprise Linux 7** - コマンドとして **`systemctl enable amsd_rev; systemctl start amsd_rev`** を入力します。
   - **SuSE Linux Enterprise Server 11 および Red Hat Enterprise Linux 6** - コマンドとして **`service amsd_rev start`** を入力します。
   - **Ubuntu 16.04.3/HWE カーネル以降** - コマンド **`sudo service amsd_rev start`** 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 設定の構成特権

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**
   - **システム担当者**
   - **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(298 ページ)

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。
- **システム担当者** - 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。

- **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 アラート送信先の構成

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 設定の構成特権

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、次のいずれかを実行します。

   - 新しいアラート送信先を追加するには、**新規**をクリックします。
   - 構成済みのアラート送信先を編集するには、アラート送信先の横にある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。

- **SNMP アラートの送信先**
- **トラップコミュニティ**
- **SNMP プロトコル**
- **SNMPv3 ユーザー**

4. アラート送信先を保存するには、次のいずれかを実行します。
   - 新しいアラート送信先を保存するには、**追加**をクリックします。
   - 編集したアラート送信先を保存するには、**更新**をクリックします。

SNMP アラート送信先オプション

- **SNMP アラート送信先** - 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。

  FQDN を使用して SNMP アラート送信先を構成し、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**）。
- **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 アラート送信先の削除

前提条件

iLO 設定の構成特権

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 設定の構成特権

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、**更新**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** または **SHA** を選択します。
- **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。
- **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 設定の構成特権

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 設定の構成特権

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 6〜32 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`）

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 設定の構成特権

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. 次のアラートタイプを構成します。

   - **iLO SNMP アラート**
   - **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 アラートの構成

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 の構成要素であり、ハードディスク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 アラート送信先に送信されません。

コールドスタートトラップブロードキャスト

このオプションが有効になっている場合、有効なトラップの宛先が構成されていないと、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。

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ブロードキャストされます。

- **SNMP アラート送信先**が構成されていない。
- **SNMP アラート送信先**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または修理済みに変更された場合）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 設定を更新します。
4. オプション : テストアラートを生成し、**トラップ先**ボックス内の TCP/IP アドレスに送信するには、**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

SNMP トラップには、iLO 5 を使用して生成できる SNMP トラップおよびサポートされている ProLiant サーバーと Synergy コンピュートモジュールを一覧表示します。

表 3: SNMP トラップ

トラップ番号	トラップ名	説明
0	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。
4	Authentication Failure Trap	SNMP が認証失敗を検出しました。
1006	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。
1010	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。
1011	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。
1012	cpqSeUSBStorageDeviceRedundancyLost	USB ストレージデバイスの冗長性が失われました。
1013	cpqSeUSBStorageDeviceRedundancyRestored	USB ストレージデバイスの冗長性が回復しました。
1014	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。
1015	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。
1016	cpqSePCIeDiskTemperatureOk	PCIe ディスクの温度は正常です。
1017	cpqSePCIeDiskConditionChange	PCIe ディスクのステータスが変化しました。
1018	cpqSePCIeDiskWearStatusChange	PCIe ディスク消耗ステータスが変化しました。
1019	cpqSePciDeviceAddedOrPoweredOn	PCI デバイスが追加されたか、電源がオンになりました。
1020	cpqSePciDeviceRemovedOrPoweredOff	PCI デバイスが削除されたか、電源がオフになりました。
2014	cpqSiIntrusionInstalled	システム侵入ハードウェアが取り付けられました。
2015	cpqSiIntrusionRemoved	システム侵入ハードウェアが取り外されました。
2016	cpqSiHoodReplaced	システムフードが交換されました。

表は続く

トラップ番号	トラップ名	説明
2017	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。
3033	cpqDa6CntlrStatusChange	Smart Array コントローラのステータスの変化が検出されました。
3034	cpqDa6LogDrvStatusChange	Smart Array 論理ドライブのステータスの変化が検出されました。
3038	cpqDa6AccelStatusChange	Smart Array 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。
3039	cpqDa6AccelBadDataTrap	Smart Array 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。
3040	cpqDa6AccelBatteryFailed	Smart Array 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。
3046	cpqDa7PhyDrvStatusChange	Smart Array 物理ドライブのステータスの変化が検出されました。
3047	cpqDa7SpareStatusChange	Smart Array スペアドライブのステータスの変化が検出されました。
3049	cpqDaPhyDrvSSDWearStatusChange	Smart Array 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。
5022	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。
5026	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。
6026	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、現在は稼動しています。
6027	cpqHe3PostError	1 つまたは複数の POST エラーが発生しました。
6032	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。
6033	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。
6034	cpqHe3FltTolPowerSupplyRemoved	フォールトトレラント電源装置が取り外されました。

表は続く

トラップ番号	トラップ名	説明
6035	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。
6036	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。
6037	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。
6038	cpqHe3FltTolFanInserted	フォールトトレラントファンが取り付けられました。
6039	cpqHe3FltTolFanRemoved	フォールトトレラントファンが取り外されました。
6040	cpqHe3TemperatureFailed	サーバーの温度を超えました。
6041	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。
6042	cpqHe3TemperatureOk	温度ステータスが、**OK** に設定されました。
6048	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。
6049	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。
6050	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。
6051	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。
6054	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。
6055	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。
6061	cpqHeManagementProcInReset	管理プロセッサーはリセット中です。
6062	cpqHeManagementProcReady	管理プロセッサーは使用可能です。

表は続く

トラップ番号	トラップ名	説明
6064	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。
6069	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。
6070	cpqHeSysBatteryFailed	HPE Smart ストレージバッテリーが故障しました。
6071	cpqHeSysBatteryRemoved	HPE Smart ストレージバッテリーが取り外されました。
6072	cpqHeSysPwrAllocationNotOptimized	iLO は所要電力を特定できませんでした。サーバーの電力割当てが最適化されていません。
6073	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。
6074	cpqHePowerFailureError	デバイスの電源障害が検出されました。
6075	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。
6076	cpqHeNvdimmBackupError	NVDIMM バックアップエラーが検出されました。
6077	cpqHeNvdimmRestoreError	NVDIMM の復元エラーが検出されました。
6078	cpqHeNvdimmUncorrectableMemoryError	訂正不能なメモリエラーが検出されました。
6079	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。
6080	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。
6081	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。
6082	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。

表は続く

トラップ番号	トラップ名	説明
6083	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。
6084	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。
6085	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。
6086	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。
6087	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。
6088	cpqHeNvdimmEventNotifyError	この NVDIMM のイベント通知を設定できません。
6089	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。
6090	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。
6091	cpqHeNvdimmLifecycleWarning	NVDIMM ライフサイクルの警告 - NVDIMM の寿命に達しました。
6092	cpqHeNvdimmLogicalNvdimmError	論理 NVDIMM のエラーが発生しました。
6093	cpqHeNvdimmConfigurationError	NVDIMM 構成エラーが発生しました。
6094	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。
6095	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。

表は続く

トラップ番号	トラップ名	説明
6096	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。
6097	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。
6098	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。
6099	cpqHePwrSupplyError	システム電源装置のエラーが発生しました。
6100	cpqHePwrSupplyErrorRepaired	システム電源装置のエラーが修復されました。
6101	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。
6102	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。
6103	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。
6104	cpqHePowerProtectionFault	システムボードの電源保護障害が発生しました。
8029	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。
8030	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。
8031	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。
8032	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。
9001	cpqSm2ServerReset	サーバー電源がリセットされました。
9003	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。
9005	cpqSm2SelfTestError	iLO 5 がセルフテストエラーを検出しました。

表は続く

トラップ番号	トラップ名	説明
9012	cpqSm2SecurityOverrideEngaged	iLO 5 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。
9013	cpqSm2SecurityOverrideDisengaged	iLO 5 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。
9017	cpqSm2ServerPowerOn	サーバーの電源が入れられました。
9018	cpqSm2ServerPowerOff	サーバーの電源が切られました。
9019	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。
9020	cpqSm2IrsCommFailure	Insight Remote Support または Insight Online との通信に失敗しました。
9021	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）。
9022	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。
9023	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。
9024	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。
9025	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。
9026	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。
9027	cpqSm2SecurityStateChange	iLO セキュリティ状態が変更されました。
11003	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。
11018	cpqHo2PowerThresholdTrap	電力しきい値を超えました。

表は続く

トラップ番号	トラップ名	説明
11020	cpqHoMibHealthStatusArrayChangeTrap	サーバーのヘルスステータスが変化しました。
14004	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。
16028	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。
18011	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。
18012	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。
18013	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。
18014	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。
169001	cpqiScsiLinkUp	iSCSI リンクがアップしています。
169002	cpqiScsiLinkDown	iSCSI リンクがダウンしています。

これらの SNMP トラップについて詳しくは、HPE SIM 用の Insight Management MIB 更新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
`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

表は続く

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

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、指定したメールアドレスに送信するように iLO を設定することができます。iLO メールアラートには、主要なホストシステムイベントが含まれます。

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。iLO により生成されたメッセージの受信が、これらのツールによってブロックされる場合があります。このようなメールサービスは iLO アラートメールメッセージの受信に適していません。

アラートメールを有効にする

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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- iLO 設定の構成権限

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、**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。
   - **電子メールアドレス**
   - **送信ドメイン**
   - **SMTP ポート**
   - **SMTP サーバー**
4. オプション：設定した電子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。
5. 変更を保存するには、**適用**をクリックします。

アラートメールのオプション

- **メールアドレス** - iLO メールアラートの宛先メールアドレス。この文字列は最大 63 文字であり、標準のメールアドレス形式でなければなりません。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。
- **送信ドメイン** - 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。
- **SMTP ポート** - SMTP サーバーが非認証 SMTP 接続に使用するポート。デフォルト値は 25 です。
- **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。この文字列は最大 63 文字です。

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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- iLO 設定の構成権限

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、**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

- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- iLO 設定の構成権限

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**オプションを有効に設定します。
3. 次の情報を入力します。
   - **リモート Syslog サーバー**
   - **リモート Syslog ポート**
4. オプション：設定した 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。
5. 変更を保存するには、**適用**をクリックします。

リモート syslog のオプション

- **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。サーバーあたり最大 63 文字、合計 127 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。iLO 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上に Syslog サーバーを設定することができます。iLO で 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。

- **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。

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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- iLO 設定の構成権限

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。

エンクロージャー、フレーム、およびシャーシの操作

アクティブ Onboard Administrator の使用

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、エンクロージャー情報を表示したり、OA の Web インターフェイスを起動したり、エンクロージャーの UID LED を切り替えたりできます。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

ナビゲーションツリーで **BL c-Class** をクリックします。

このページには、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表示されます。

OA の詳細

- **MAC アドレス** - アクティブな OA の MAC アドレス。
- **システムヘルス** - 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。

- **ブレードロケーション** - 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）。
- **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。
- **ラック名** - アクティブな OA が管理しているエンクロージャーを含むラック。この値は、OA を通じて変更できます。

OA GUI 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. OA が複数のアドレスをサポートする場合は、**Onboard Administrator アドレス選択**テーブルのオプションから使用するアドレスを選択します。

   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）**

3. **起動**をクリックします。

   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。

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。

   現在の UID LED ステータスが横にリストされている、**エンクロージャー UID ランプ**アイコン。

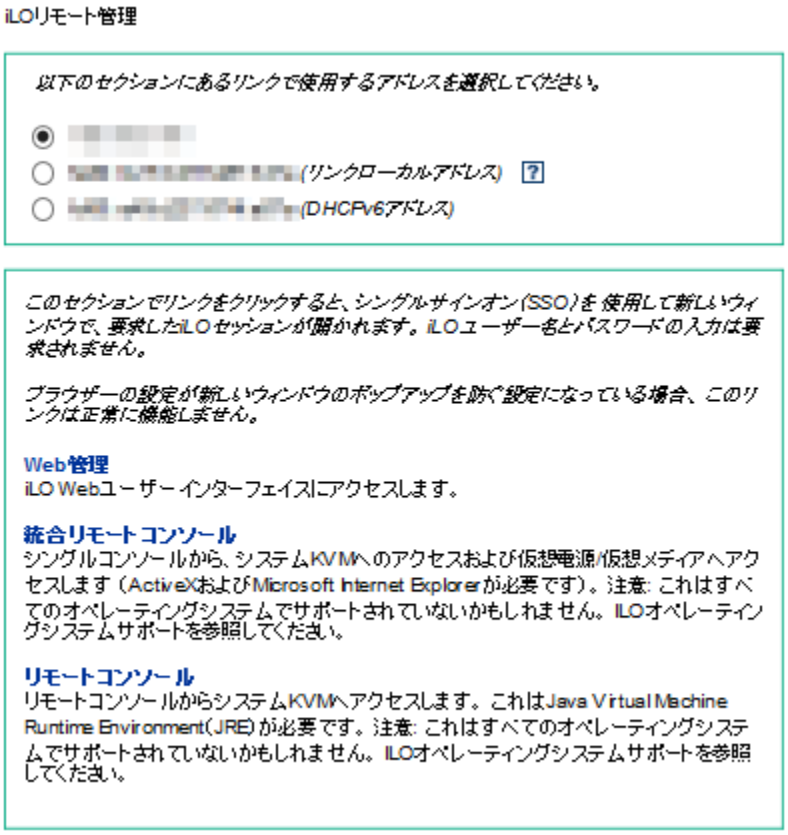
2. iLO が配置されているエンクロージャーの UID LED の状態を切り替えるには、**UID 切り替え**ボタンまたは UID アイコンをクリックします。

   アクティブ Onboard Administrator ページの UID LED ステータスは、iLO ページがロードされたときのエンクロージャー UID LED ステータスを示します。ステータスを更新するには、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

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。

   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。

2. オプション：サーバーの詳細を表示するには、フレーム図の上にカーソルを移動します。

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。

- **エンクロージャー 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。

  このステータス値は、iLO ページがロードされたときのフレームの UID LED ステータスを示します。ステータスを更新するには、ページを更新します。

  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** - フレーム内のサーバーのベイ番号。
- **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。

フレームの UID LED の切り替え

このページの UID LED ステータスは、UID LED のステータスが変化したときに最大 30 秒の遅延で自動的に更新されます。ステータスをすぐに更新するには、ページを更新します。

手順

フレームの UID LED の状態を変更するには、フレーム図にあるフレーム UID アイコンをクリックします。

サーバーの詳細

サーバー上にカーソルを移動すると、フレーム図に以下の詳細が表示されます。

- サーバーのヘルスステータス
- サーバーホスト名
- サーバーモデル
- サーバーの UID ステータス

サーバーの UID LED の切り替え

手順

サーバーの UID LED の状態を変更するには、フレーム図にあるサーバー UID アイコンをクリックします。

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 ストレージバッテリ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。

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 Vaux 警告**
- **低 Vaux 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 Vaux 警告**
- **低 Vaux 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 ストレージバッテリのリスト

シャーシ情報ページには、Smart ストレージバッテリ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

バッテリの索引番号。

設置

バッテリのインストールステータス。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

バッテリステータス。指定できる値は、**OK**、**劣化**、**障害**、または**その他**です。

容量

バッテリ容量。

ファームウェア

搭載されているバッテリのファームウェアバージョン。

各バッテリの詳細

Smart ストレージバッテリ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。

現在

バッテリのインストールステータス。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

バッテリステータス。指定できる値は、**OK**、**劣化**、**障害**、または**その他**です。

容量

バッテリ容量。

ファームウェア

搭載されているバッテリのファームウェアバージョン。

モデル

バッテリのモデル番号。

スペア

スペアバッテリの部品番号。

シリアル番号

バッテリのシリアル番号。

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 設定の構成特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- 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. 以下の電力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**
   - **フル AC/DC 冗長モード**
   - **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更新されました。）

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。
- **フル AC/DC 冗長モード** - 消費電力上限機能は、システムの電源が N+1 の冗長性を持つように強化されています。このモードでは、使用可能な電源装置の 1 台を予備として確保できるようにノードがシステムで調整されます。1 台の電源装置しか使用できない場合は、その電源装置の容量を完全に使用できるようにノードがシステムで調整されます。
- **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。上限には、最小より低い値または最大より大きい値を設定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。
- **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、電力供給の損失が検出された場合に、ノードが完全な停止状態になるようにシステムが完全に調整されます。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 設定の構成特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- 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/復元を有効化**

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/復元有効** - 電源情報は EEPROM に保存され、復元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 設定の構成特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- **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更新されました。）
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、リフレッシュアイコン ↻ 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開始アイコン ▷ をクリックします。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、**スロットル**および**警告ステータス**の値は自動的に更新されます。

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 設定の構成特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- 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更新されました。）

消費電力上限値設定の構成

前提条件

- iLO 設定の構成特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- 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、構成が更新されるまで消費電力上限値設定が更新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。）

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 設定の構成特権
- 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、次の web サイトにあるライセンス文書を参照してください。**http://www.hpe.com/support/ilo-docs**
- 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**
   - **操作**
   - **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更新されました。）

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。

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、
  リモート管理システムの動作に影響を及ぼす可能性があります。

- **<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。

リモートマネージャー設定の削除

ご使用のネットワークでリモート管理ツールの使用を中止する場合は、ツールと iLO の関連付けを削除できます。

この機能は、Synergy Compute Module ではサポートされません。

重要:

iLO でリモートマネージャー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すすめします。ネットワーク上で使用されており、現在の iLO システムを含むサーバーを管理しているツールに関するリモートマネージャー構成は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。

4. iLO のナビゲーションツリーから、**<リモート管理ツールの名前>**ページが削除されます。

HPE OneView での iLO の使用

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 は次の 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更新されます。詳しくは、HPE OneView 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。
- Remote Support の登録

重要:

HPE OneView を iLO 5 と併用するときに最高のパフォーマンスを得るには、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または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 Compute Module のみ）

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、**http://www.hpe.com/support/restfulinterface/docs** を参照してください。

Always On Intelligent Provisioning

Always On Intelligent Provisioning は、オペレーティングシステム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特権
- ホスト BIOS 構成特権
- 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で **Intelligent Provisioning** をクリックします。

   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. Intelligent Provisioning を起動するには、**常時稼動**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。

   Intelligent Provisioning の使用方法については、Intelligent Provisioning のオンラインヘルプ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。
3. 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 **XML 応答**値を有効にします。

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. iLO が SNMP トラップを送信できるようにするには、**マネジメント - SNMP 設定**ページに移動し、SNMP および SNMP アラート通知を構成します。**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。

同じ HTTP ポートを使用するための iLO と HPE SIM の設定

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。ポートは変更できます。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、**セキュリティ - アクセス設定**ページに移動し、**Web サーバー非 SSL ポート**ボックスに新しいポート番号を入力します。
- 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

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。

HPE Insight Control サーバープロビジョニングでの iLO の使用

HPE Insight Control サーバープロビジョニングを iLO と統合することにより、OS やハードウェアの状態にかかわらず、リモートサーバーの管理やリモートコンソールの操作を実行できるようになります。

デプロイメントサーバーでは、iLO の電源管理機能を使用して、ターゲットサーバーの電源を入れたり、切ったり、入れなおしたりすることができます。サーバーがデプロイメントサーバーに接続されるたびに、デプロイメントサーバーは、ターゲットサーバーをポーリングして、iLO デバイスが取り付けられていることを確認します。取り付けられている場合、サーバーは、DNS 名、IP アドレス、ユーザーのログイン名などの情報を収集します。セキュリティは、ユーザー名に対応する正しいパスワードの入力をユーザーに求めることによって、維持されます。

HPE Insight Control サーバープロビジョニングについて詳しくは、HPE Insight Control の Web サイト **http://www.hpe.com/jp/insightcontrol** を参照してください。

Kerberos 認証とディレクトリサービス

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 サポートを設定します**
7. **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設定

使用したいドメイン名または DNS サーバーが DHCP サーバーによって供給されない場合：

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）**を更新します。
8. **ドメイン名**を更新します。
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。

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。

Windows Vista の場合のみ：Microsoft ホットフィックス KB960830 を参照し、`Ktpass.exe` バージョン 6.0.6001.22331 以降を使用します。

2. オプション：`Setspn` コマンドを使用して、Kerberos SPN を iLO システムに割り当てます。
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。

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 `knvo` 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

iLO での Kerberos サポートの設定

手順

1. **iLO Kerberos 固有のパラメーターを設定します**。
2. **ディレクトリグループを設定します**。

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。

Internet Explorer でのシングルサインオンの有効化

以下の手順は、Internet Explorer 11 に基づいています。その他のバージョンのブラウザーでは、手順が異なる場合があります。

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. **詳細設定**タブをクリックします。
   c. **セキュリティ**セクションまでスクロールします。
   d. **統合 Windows 認証を有効にする**が選択されていることを確認します。
   e. **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。

g. 企業ネットワークでは、`*.example.net` で十分です。

h. **追加**をクリックします。

i. **閉じる**をクリックします。

j. **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。

k. **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**セクションまでスクロールします。

   f. **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。

   g. **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。

   h. **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。

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。

   動作保証対象外になります!というメッセージが表示される場合があります。

2. **動作保証対象外になります!**というメッセージが表示された場合は、**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. 設定をテストします。詳しくは、シングルサインオン（Zero サインイン）設定の確認(347 ページ)を参照してください。

Chrome でのシングルサインオン

Chrome 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。

ディレクトリの統合

iLO でディレクトリを使用すると、以下の利点があります。

- **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 拡張スキーマ構成） - 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を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 拡張スキーマ構成） - 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 拡張スキーマ構成） - 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する必要があります。

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。

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オプションを使用すると、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 内に保存されている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。何も設定しない場合、ディレクトリは、既存のユーザーと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 という名前のドメイン管理者がいる場合、ドメイン管理者セキュリティグループの DN を iLO

にコピーして完全な権限を付与することができます。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、同時に多数の iLO システムを構成できるツールを提供しています。

スキーマフリー構成オプション

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=HPE,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=HPE,DC=COM` が構成されている場合は、iLO で `CN=JOHN.SMITH,CN=USERS,DC=HPE,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。

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**。

プロセスの概要：スキーマフリーのディレクトリ統合のための iLO の設定

手順

1. **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。**
2. **ディレクトリグループを設定します。**

スキーマフリーの入れ子型グループ（Active Directory 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、構成を更新できます。

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。

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。

プロセスの概要：Active Directory を使用した HPE 拡張スキーマの設定

手順

1. **計画**

   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**
   - **ディレクトリサービススキーマ**
   - **HPE 拡張スキーマの設定のための Active Directory の要件**

2. **インストール**

   a. **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**。

   b. **ProLiant 管理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**。

   スキーマエクステンダー、スナップイン、および ProLiant 管理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。

   c. **スキーマエクステンダーを実行してスキーマを拡張します。**

   d. **ご使用のディレクトリサービスに適したスナップインを 1 台または複数の管理ワークステーションにインストールします**。

3. **更新**

   iLO の Web インターフェイスのページで、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。

   ProLiant 管理プロセッサー用のディレクトリサポートを使用してこの手順を実行することもできます。

4. **ロールとオブジェクトの管理**

   a. スナップインを使用して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、ロールをマネジメント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。

5. **例外の取り扱い**

   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ロール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必要がある場合があります。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、一度に複数の iLO システムを構成するためのツール(367 ページ)を参照してください。

HPE 拡張スキーマの設定を使用して 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. Active directory のスナップインとスキーマをインストールする前に、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*

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。

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 管理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 **http://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 管理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**をクリックしてください。
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。

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 管理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(354 ページ)
ProLiant 管理プロセッサー用のディレクトリサポート（HPLOMIG）(368 ページ)
Active Directory スナップインでのロールおよびオブジェクトの管理(356 ページ)

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

- **スキーマエクステンダー** - スキーマエクステンダー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。

詳しくは

Schema Extender の実行(354 ページ)
ProLiant 管理プロセッサー用のディレクトリサポート（HPLOMIG）(368 ページ)
Active Directory スナップインでのロールおよびオブジェクトの管理(356 ページ)

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。
   - Windows 7 および Windows Server 2008 - Windows メニューをクリックし、**すべてのプログラム** > **Hewlett-Packard Enterprise** > **Management Devices Schema Extender** の順にクリックします。
   - Windows 8 および Windows Server 2012 - Windows メニューをクリックし、**Management Devices Schema Extender** を検索します。
   - Windows 10 - Windows メニューをクリックし、**すべてのアプリ** > **Hewlett-Packard Enterprise** > **Management Devices Schema Extender** の順にクリックします。
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、どの属性が変更されたかなど、インストールの結果が表示されます。

スキーマエクステンダーで必要な情報

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。ユーザーは、Active Directory Users and Computers ツールを使用して次の作業を行います。

- 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

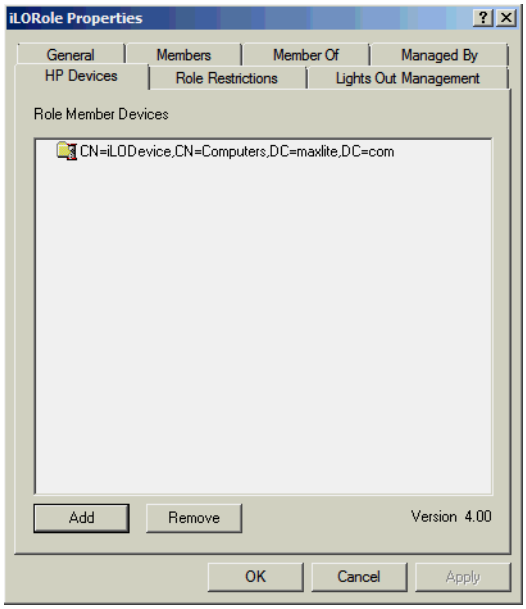
注記:

スナップインがインストールされた後、新しいエントリーを表示するには、ConsoleOne および MMC を再起動します。

Active Directory スナップインでのロールおよびオブジェクトの管理

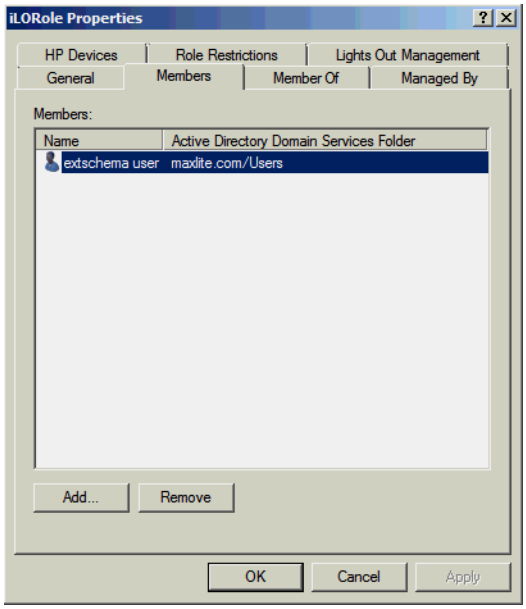
Hewlett Packard Enterprise スナップインをインストールした後、Active Directory ユーザーとコンピューターで次の管理オプションが使用できるようになります。

HP Devices タブ



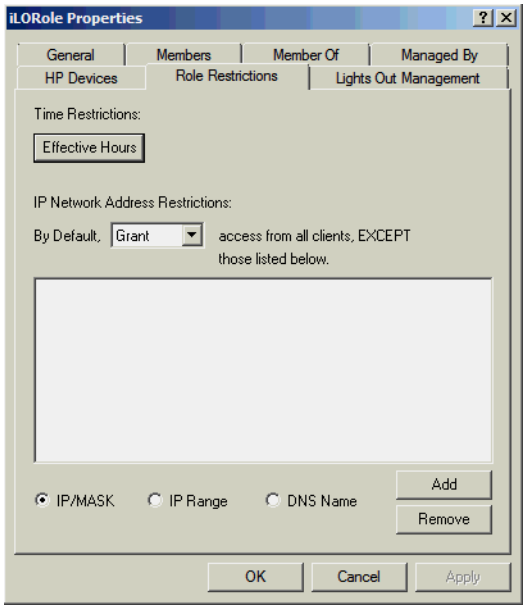
このタブでは、ロール内で管理する Hewlett Packard Enterprise デバイスを追加できます。**Add** をクリックすると、デバイスにアクセスして、そのデバイスをメンバーデバイスのリストに追加することができます。既存のデバイスを選択して、**Remove** をクリックすると、そのデバイスは有効なメンバーのデバイスリストから削除されます。

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。

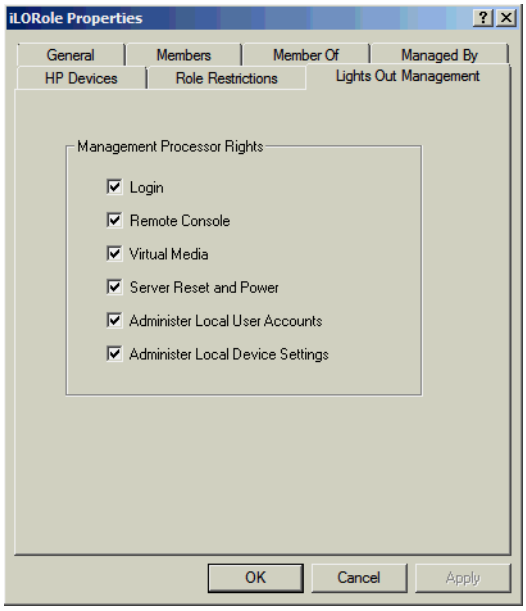
Role Restrictions タブ



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。連続した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、変更する各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(360 ページ)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:

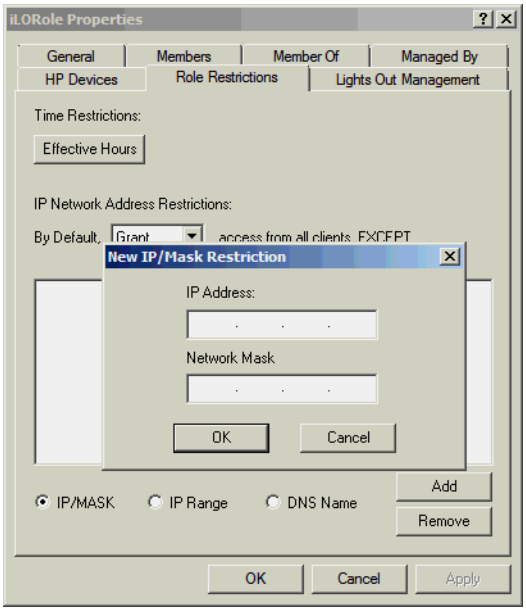
システムリカバリ、ホスト NIC、ホストストレージ、およびホスト BIOS 権限は、スキーマエクステンダーで使用できません。

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。

構成例：Active Directory と HPE 拡張スキーマ

以下の各項では、iLO を使用して Active Directory を構成する方法の例を示します。

設定プロセスの概要

手順

1. Active Directory および DNS をインストールします。
2. ルート CA をインストールします。
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. **最新の 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します。**
5. **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。**
6. **Hewlett Packard Enterprise LDAP コンポーネントスナップインをインストールします。**
7. Hewlett Packard Enterprise デバイスおよびロールを作成します。
8. iLO にログインし、**ディレクトリ**ページで、ディレクトリ設定およびディレクトリユーザーコンテキストを入力します。
9. **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**。

スナップインのインストールと Active Directory 用の初期設定

手順

1. スナップインインストーラーを実行します。
2. ディレクトリサービスを設定して、ディレクトリサービスが iLO マネジメント用の適切なオブジェクトおよび関連を所有するようにします。

   少なくとも、次のオブジェクトを作成する必要があります。

   - 1 人以上のユーザーと 1 つ以上の iLO オブジェクトを含む Role オブジェクトを 1 つ
   - ディレクトリを使用する iLO 管理プロセッサーごとに 1 つの iLO オブジェクト

   a. Hewlett Packard Enterprise が提供するマネジメントスナップインを使用して、iLO ロールおよび User Role オブジェクトを作成します。
   b. Hewlett Packard Enterprise が提供するマネジメントスナップインを使用して、iLO オブジェクトとロールオブジェクトの関連を作成します。
   c. iLO オブジェクトが Admin オブジェクトと User Role オブジェクトを指し示すようにします（Admin オブジェクトと User Role オブジェクトは、自動的に iLO オブジェクトを指し示します）。

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 が提供する Active Directory Users and Computers スナップインを使用して完了します。

Active Directory スナップインの使用について詳しくは、**Active Directory スナップインでのロールおよびオブジェクトの管理**(356 ページ)を参照してください。

手順

プロセスの概要：

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**。
4. **iLO を構成し、Lights-Out Management オブジェクトと関連付けます**。

iLOs 組織単位の作成および 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 組織単位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** をクリックします。
5. **適用**をクリックします。
6. **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。
7. **OK** をクリックします。
8. **適用**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。
9. **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。
10. 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。
11. **OK** をクリックします。
12. **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 の設定および 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
```

ディレクトリ対応リモート管理（HPE 拡張スキーマ構成）

この項は、ディレクトリサービスと iLO 製品に習熟し、iLO 用の HPE スキーマディレクトリ統合オプションを使用したい管理者を対象にしています。

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。

LOM デバイスには、意味のある名前（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）を付けることをおすすめします。

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 アドレスもしくは DNS 名、またはマルチホスト DNS 名（冗長性を高くする場合）です。

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。

複数の（重複する）ロールには、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。

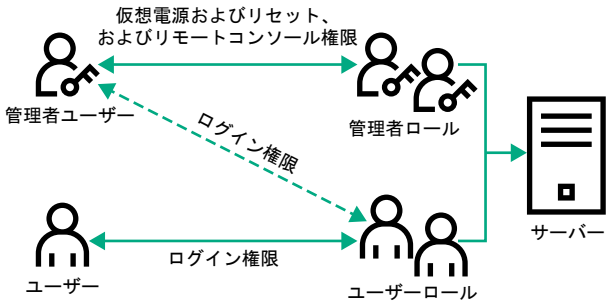


図 8: 複数の（重複する）ロール

重複するロールを使用しない場合は、複数の（独立した）ロールに示すように、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。

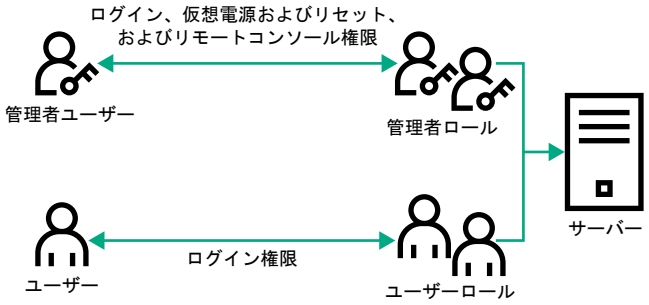


図 9: 複数の（独立した）ロール

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。

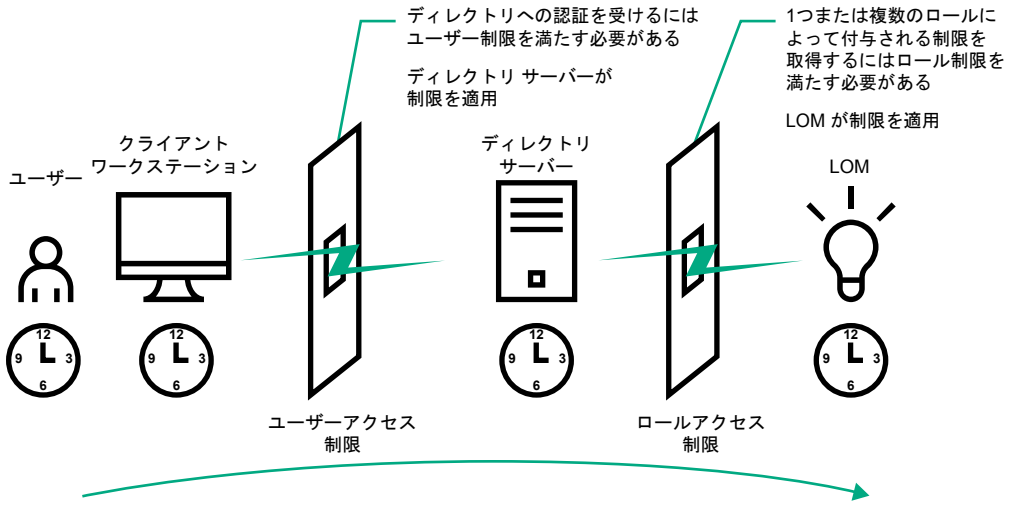


図 10: ディレクトリのログイン制限

ユーザーアクセス制限

ユーザーのアドレス制限

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。

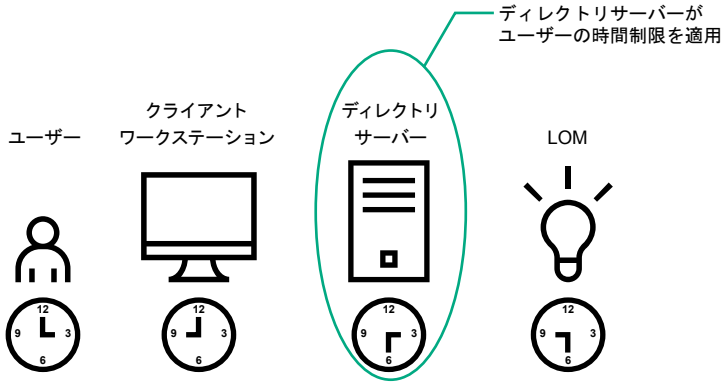


図 11: ユーザーの時間制限

ロールのアクセス制限

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。これにより、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。

<u>制限およびロールの作成</u>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。

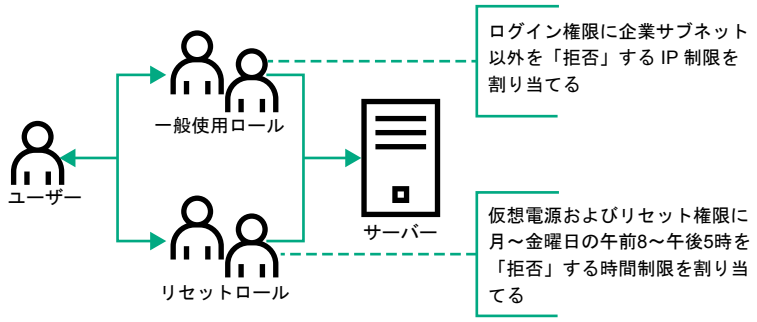


図 12: 制限およびロールの作成

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。

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。**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。

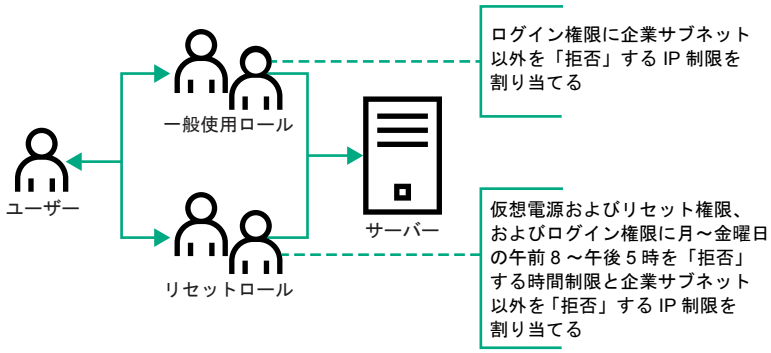


図 13: リセットロールと一般使用ロールの制限

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(384 ページ)
ProLiant 管理プロセッサー用のディレクトリサポート（HPLOMIG）(368 ページ)

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。

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。**http://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 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista

要件

拡張セキュリティ機能（**FIPS**、**CNSA**、または**高度なセキュリティ**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 で高度なセキュリティ、FIPS、または CNSA セキュリティ状態が有効になっている HPLOMIG。
Windows Vista[1] 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

表は続く

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 で高度なセキュリティ、FIPS、または CNSA セキュリティ状態が有効になっている HPLOMIG。
Windows 8 Windows 8.1 Windows 10 Windows Server 2012 Windows Server 2012 R2 Microsoft Windows Server 2016	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 Vista および 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：管理プロセッサーで iLO ファームウェアを更新します。
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. 管理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管理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。

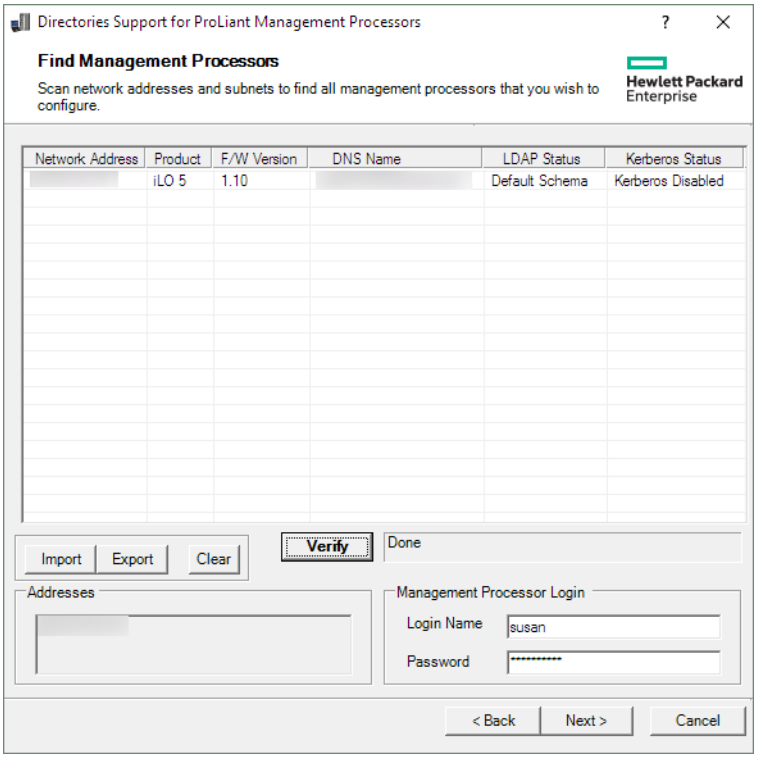
ヒント:

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 管理プロセッサーのインポートリストの要件

各行に 1 つの管理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 ステータス
- 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
```

セキュリティに関する理由によって、ユーザー名とパスワードを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:

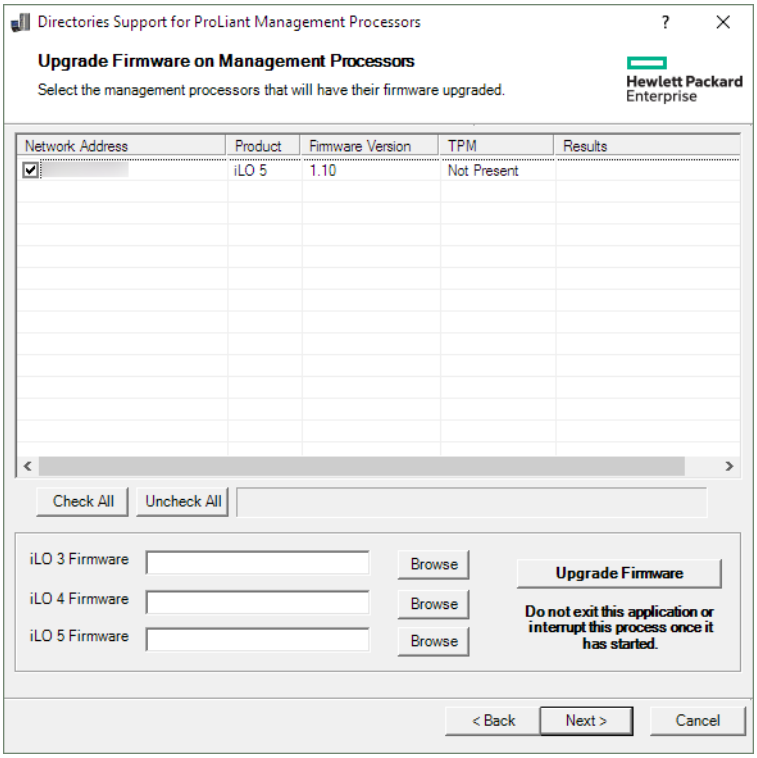
Hewlett Packard Enterprise は、本番環境ネットワークで HPLOMIG を実行する前に、テスト環境でアップグレードプロセスをテストし、結果を確認することをおすすめします。管理プロセッサーへのファームウェアイメージの不完全な転送によって、管理プロセッサーをローカルで再プログラミングしなければならなくなる場合があります。

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 **http://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管理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。

   選択した管理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。

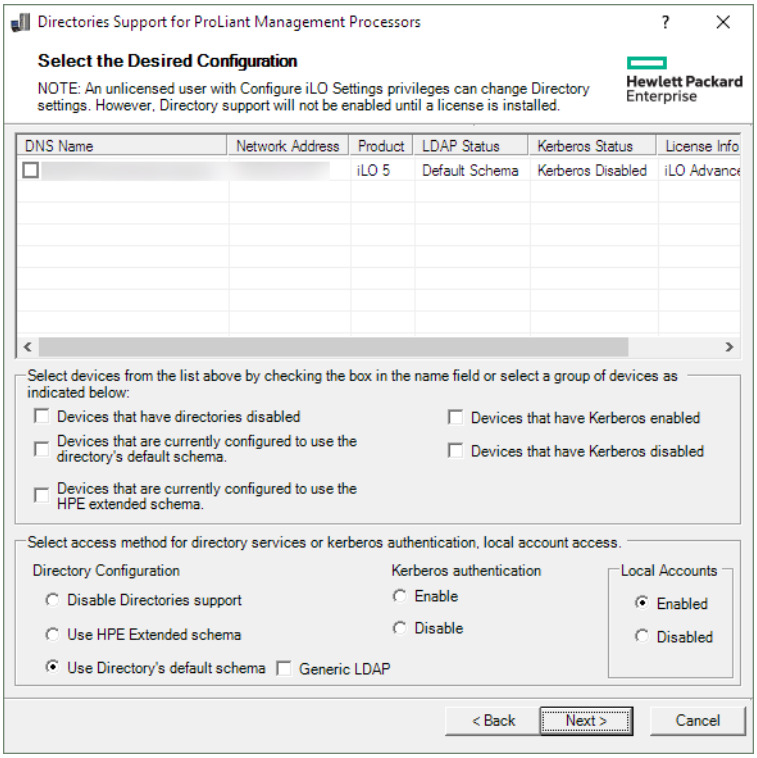
   アップグレードに失敗すると、**Results** 欄にメッセージが表示され、ユーティリティは、選択された他の管理プロセッサーのアップグレードを継続します。
5. アップグレードが完了したら、**Next** をクリックします。

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。

   この選択は、すでに HPE スキーマ用に構成された iLO や、ディレクトリが無効にされている iLO の不慮の上書きを防止するのに役立ちます。

3. **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。

4. **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。

5. 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）**(379 ページ)に進みます。HPE 拡張スキーマ構成を選択した場合は、**管理プロセッサーの命名（HPE 拡張スキーマのみ）**(375 ページ)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。

管理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。

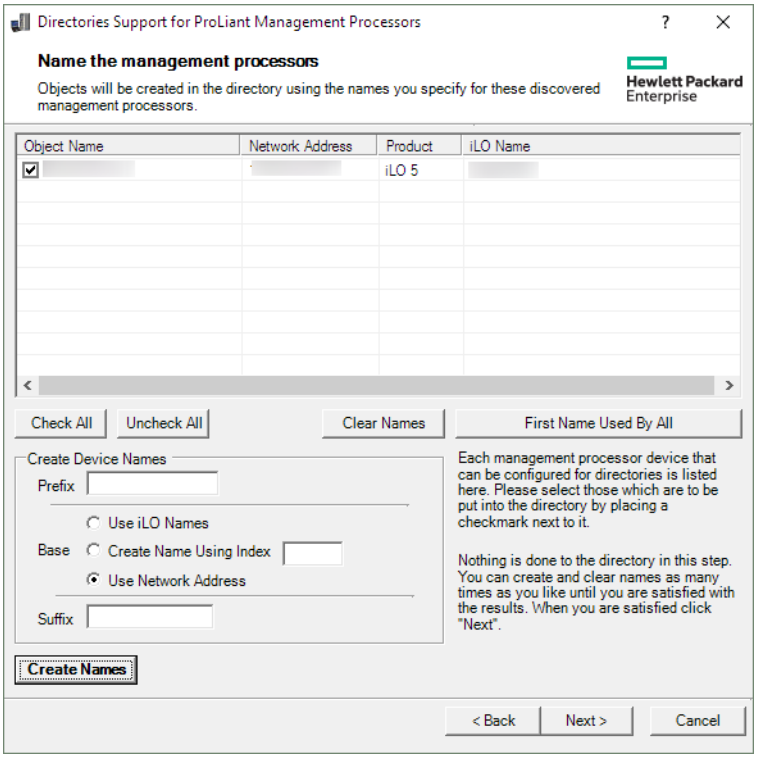
以下の 1 つまたは複数のコンポーネントを使用して名前を作成できます。

- 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

管理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、ディレクトリや管理プロセッサーに書き込まれていません。名前は、次の ProLiant 管理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。

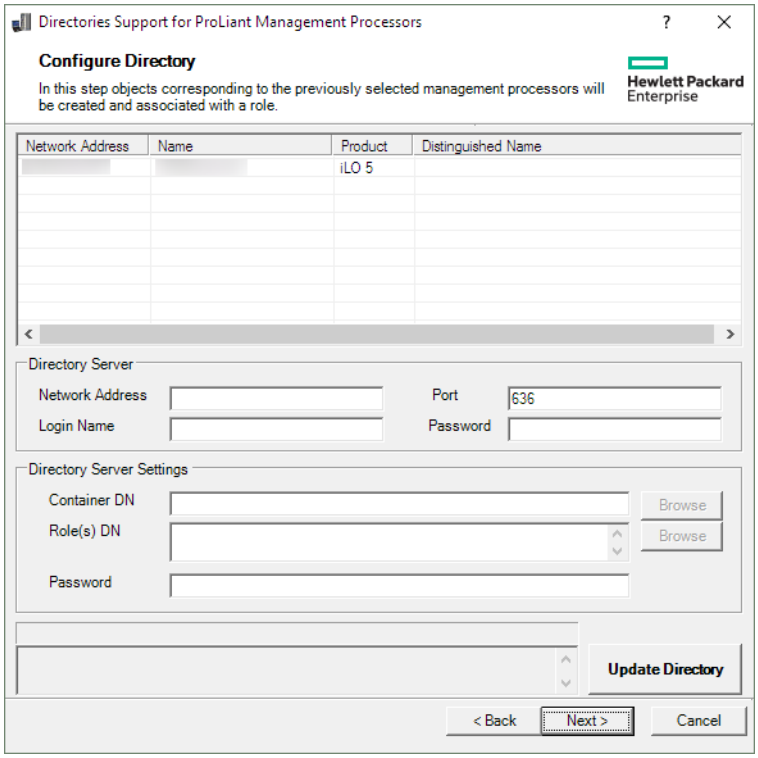
4. オプション：名前を変更するには、**Clear Names** をクリックして管理プロセッサーの名前を修正します。

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**(376 ページ)に進みます。

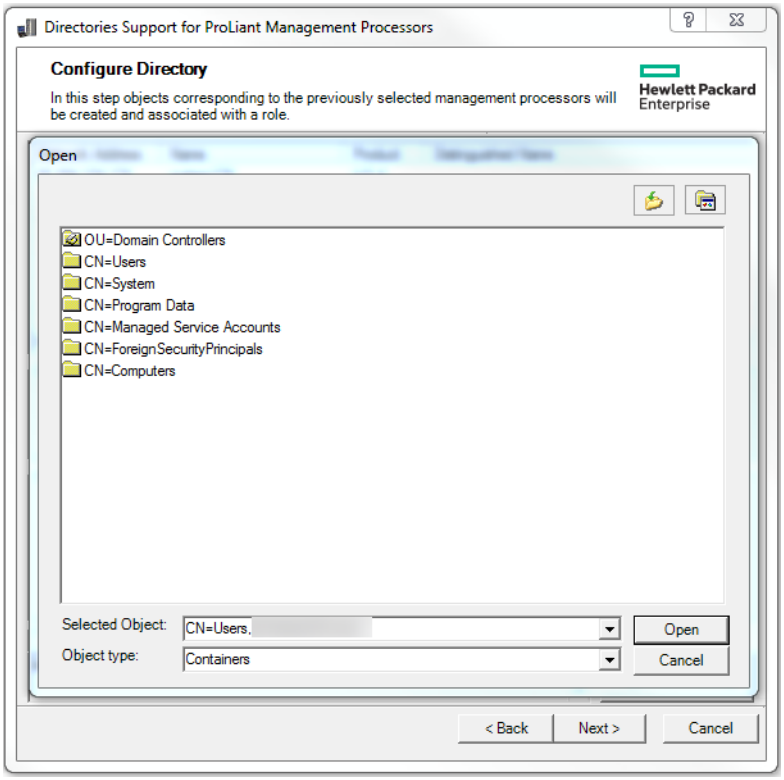
HPE 拡張スキーマを選択したときのディレクトリの設定

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。

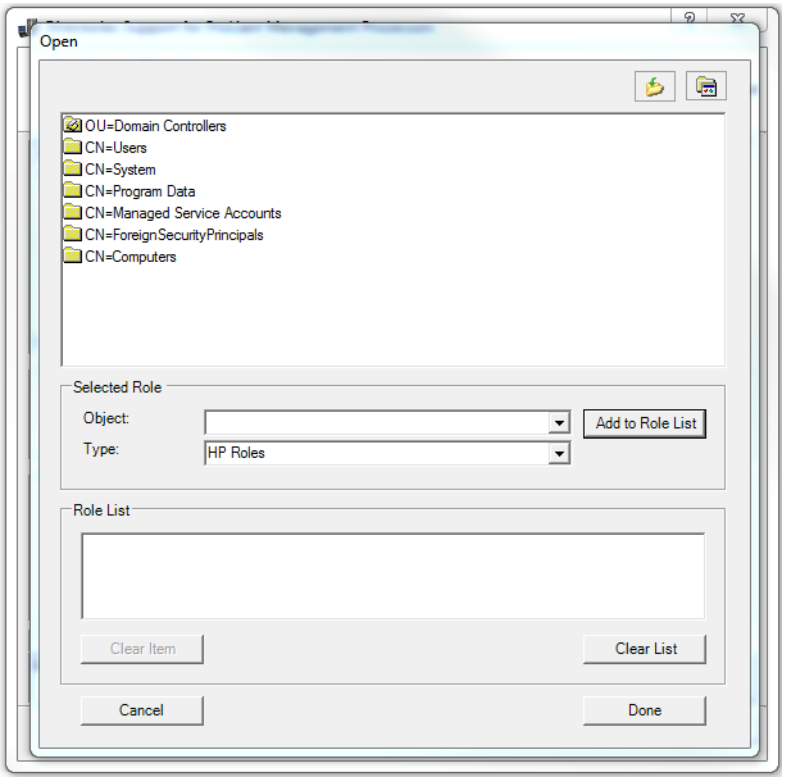


手順

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。

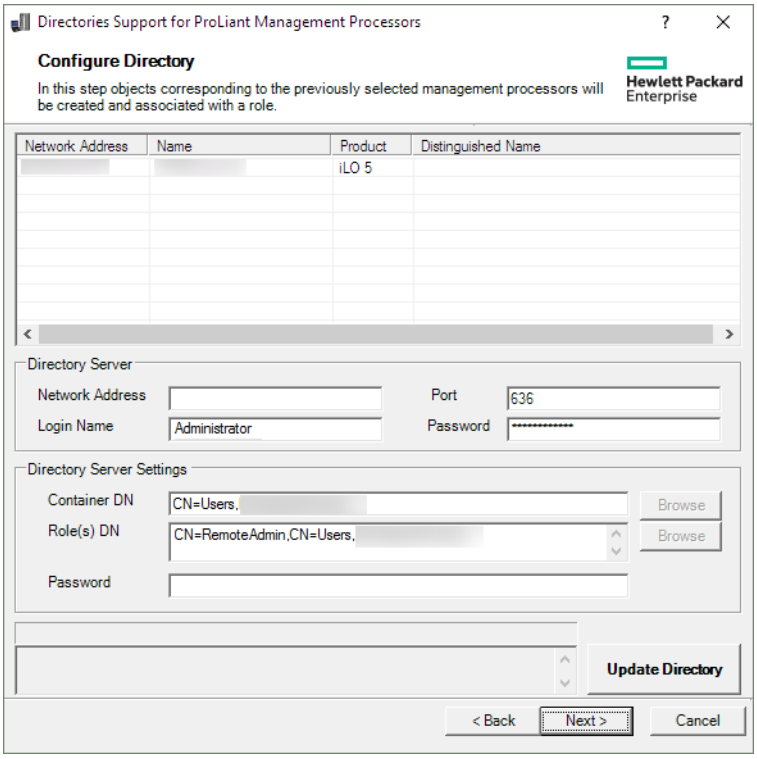


4. **Update Directory** をクリックします。

   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(380 ページ)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。

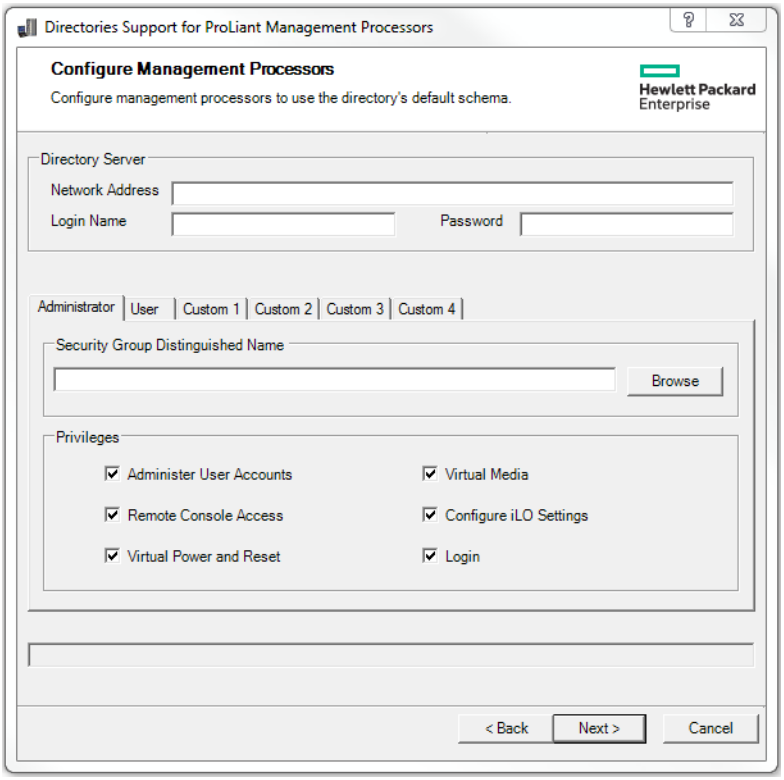
- **Network Address** - ディレクトリサーバーのネットワークアドレス（有効な DNS 名または IP アドレス）です。
- **Port** - ディレクトリへの SSL ポートです。デフォルトポートは 636 です。管理プロセッサーは、SSL を使用してのみディレクトリと通信できます。
- **Login Name** および **Password** - ディレクトリへのドメイン管理者アクセスを持つアカウントのログイン名とパスワードを入力します。
- **Container DN** - ネットワークアドレス、ポート、およびログイン情報を入力したら、**Browse** 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管理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。

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(380 ページ)に進みます。

管理プロセッサー設定

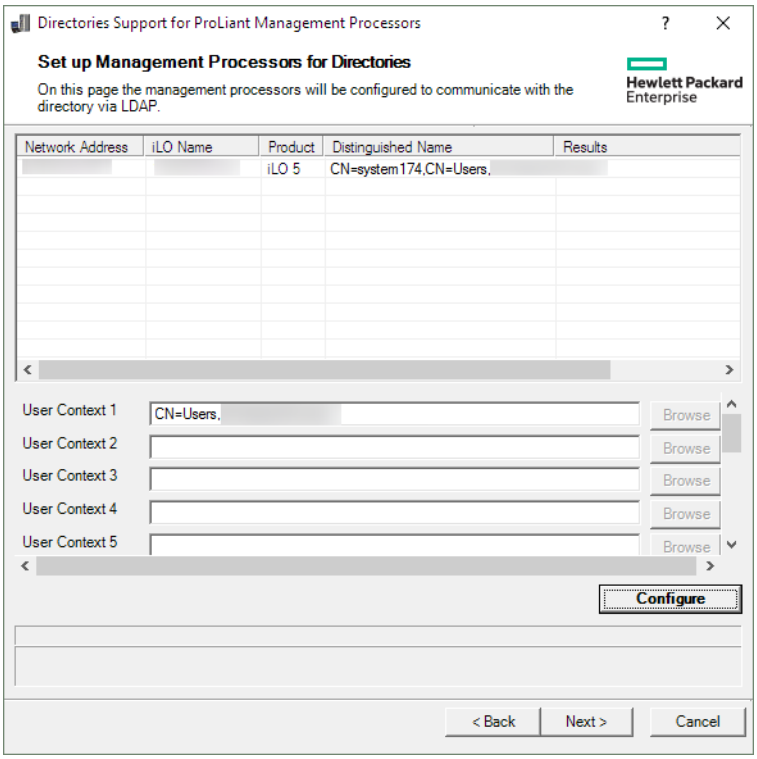
- **Network Address** - ディレクトリサーバーのネットワークアドレス（有効な DNS 名または IP アドレス）です。
- **Login Name** および **Password** - ディレクトリへのドメイン管理者アクセスを持つアカウントのログイン名（DN）とパスワードを入力します。
- **Security Group Distinguished Name** - 共通の権限を持つ一連の iLO ユーザーを含むディレクトリ内のグループの DN です。ディレクトリ名、ログイン名、およびパスワードが正しい場合は、**Browse** をクリックしてグループにアクセスし、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。

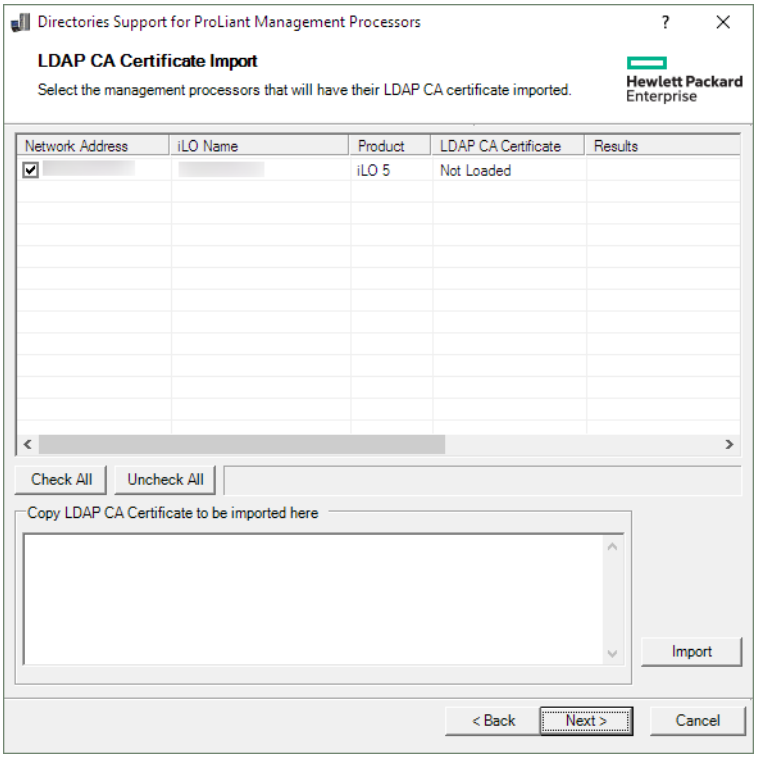
   LDAP CA Certificate Import ウィンドウが開きます。
5. LDAP CA 証明書のインポート(381 ページ)に進みます。

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 iLO システムを選択し、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。
3. 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。

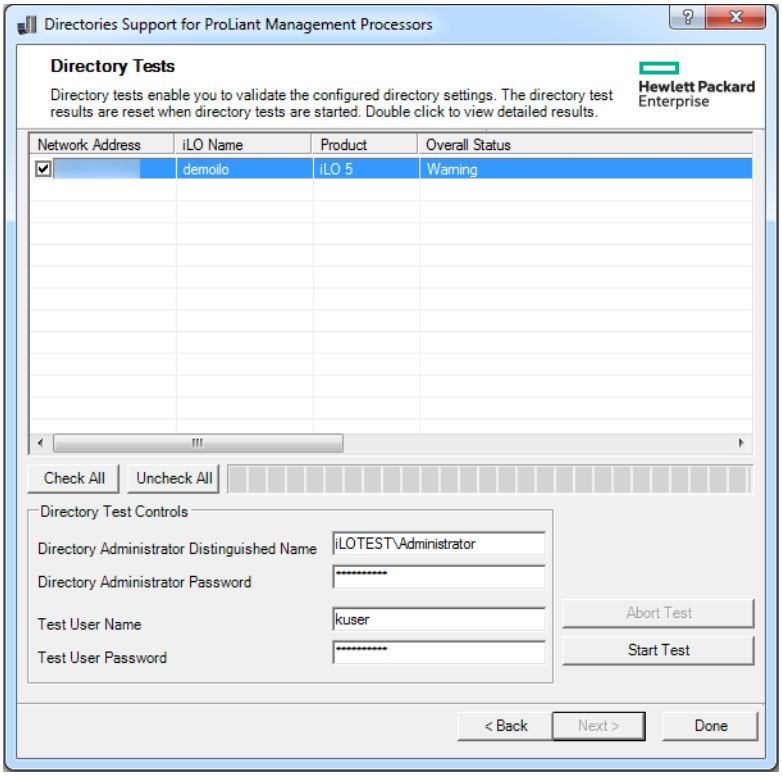
   ディレクトリテストウィンドウが開きます。
4. **HPLOMIG を使用したディレクトリテストの実行（オプション）**(382 ページ)に進みます。

HPLOMIG を使用したディレクトリテストの実行（オプション）

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 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。

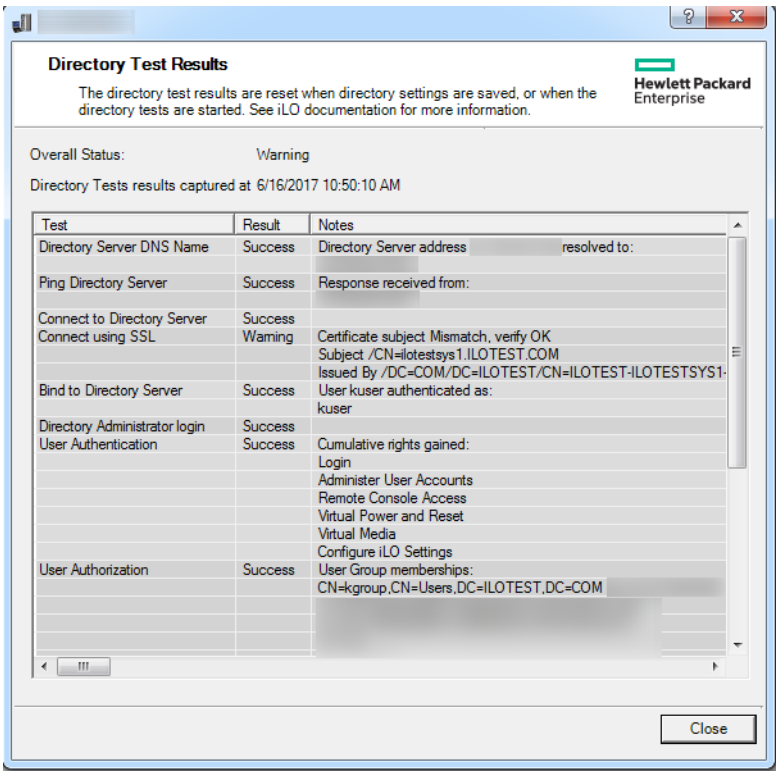
      - **テストユーザー名**および**テストユーザーパスワード** - iLO へのログインとアクセス権をテストします。ユーザー検索コンテキストを適用できるため、ユーザー名は完全修飾である必要はありません。このユーザーは、この iLO のロールに関連付けられている必要があります。

        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(276 ページ)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

この付録では、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
スーパークラス	group

表は続く

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。
構文	オクテット文字列 - 1.3.6.1.4.1.1466.115.121.1.40

表は続く

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 4: 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 5: 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。
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 の再起動、工場出荷時リセット、および NMI の管理

iLO の再起動（リセット）

場合によっては、iLO をリセット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を使用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。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。

iLO のリセット方法

- iLO の Web インターフェイスの**診断**ページで、**リセット**をクリックします。
- CLI または HPONCFG を使用します。手順については、iLO スクリプティング/CLI ガイドを参照してください。
- iLO 5 構成ユーティリティを使用します。
- サポートされているサーバーでサーバー UID ボタンを使用します。
- iLO RESTful API を使用します。詳しくは、**http://www.hpe.com/info/restfulapi** を参照してください。
- IPMI を使用します。詳しくは、iLO IPMI のユーザーガイドを参照してください。

これらのどの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、電源装置を切断する必要があります。

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 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、**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。
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。

   iLO がリセットされ、ブラウザー接続が閉じます。

iLO 5 構成ユーティリティを使用した iLO のリブート（リセット）

前提条件

iLO 設定権限の構成

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に、リセット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 ボタンを使用した iLO の再起動（リセット）

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

UID ボタンについて詳しくは、サーバーのユーザーガイドを参照してください。

サーバーの UID ボタンで、正常な iLO のリブートを実行します。

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

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。

詳しくは

iLO ネットワークのフラッシュエラーリカバリ(440 ページ)
サーバーの電源オン(161 ページ)

iLO の工場出荷時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する必要があることがあります。たとえば、FIPS モードを無効にすると、iLO をデフォルト設定にリセットする必要があります。このタスクは、iLO 5 構成ユーティリティ、iLO RESTful API、または RIBCL スクリプトを使用して実行できます。

- iLO 5 構成ユーティリティの使用方法については、**工場出荷時のデフォルト設定への iLO のリセット（iLO 5 構成ユーティリティ）**(394 ページ)を参照してください。
- iLO RESTful API の使用方法については、Web サイト（**http://www.hpe.com/info/restfulapi**）にある iLO RESTful API のドキュメントを参照してください。
- RIBCL スクリプトの使用方法については、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。

工場出荷時のデフォルト設定への iLO 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 のユーザーデータ、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。

NMI の生成

システムに 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。

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。**システムに 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**をクリックして、**診断**タブをクリックします。
2. **システムに NMI を生成**をクリックします。
3. NMI をシステムに生成するとデータが消失する可能性があるという警告が iLO から出された場合、**OK** をクリックして確認するか、**キャンセル**をクリックします。

   OK をクリックすると、iLO は NMI が送信されたことを確認します。

トラブルシューティング

Windbg での iLO 仮想シリアルポートの使用

サーバーをデバッグする場合は、ローカルのテストシステムで動作している Windows `Windbg` カーネルデバッガとともに、iLO 仮想シリアルポート機能を使用できます。

前提条件

PuTTY がローカルテストシステムにインストールされている。PuTTY は Web サイト **http://www.putty.org/**からダウンロードできます。

手順

1. カーネル問題が発生したサーバー上の iLO Web インターフェイスから、**セキュリティ - アクセス設定**ページに移動して、**シリアルコマンドラインインターフェイス速度**を構成します。

   デフォルト値は 9600 です。

2. Windows でデバッグオプションを設定します（シリアル接続の `boot.ini` パラメーター）。

   `debugport = com2` を使用して、構成された**シリアルコマンドラインインターフェイス速度**と一致するようにボーレートを設定します。

3. サーバーを起動または再起動します。

4. サーバーの POST 画面で **F9** キーを押します。

   ROM ベースの構成ユーティリティが起動します。

5. 以下の設定を行います。

   - EMS および BIOS シリアルコンソールを無効にします。
   - 仮想シリアルポートを `COM 2` に設定します。

6. Windows のデバッグブートオプションの選択メニューにアクセスするには、サーバーを再起動します。

7. ローカルテストシステムから、PuTTY を使用して iLO に接続し、ログインします。

8. セッションホスト名の IP アドレスを入力します。SSH セッションのデフォルト設定を使用します。

   PuTTY iLO CLI セッションが開くと、ユーザーログインウィンドウが開きます（プライベートキーを使用するように PuTTY セッションを設定していない場合）。

   プロンプトが表示されるまでに少し時間がかかる場合があります。

9. `</>hpiLO->`プロンプトで、コマンド `windbg_enable` を入力します。

   このコマンドにより、ポート 3002 で仮想シリアルポートへのソケットが開きます。

10. Windows のデバッガーを起動するには、コマンド `windbg -k com:port=<IP-address>,ipport=3002` を入力します。

    `<IP-address>`は iLO の IP アドレス、「`3002`」は接続するソケット（3002 は iLO の Raw シリアルデータソケット）です。

    `ipport` パラメーターは省略可能です。デフォルトのポートは、3002 です。

必要に応じて、その他の `windbg` コマンドラインパラメーターを追加することができます。Hewlett Packard Enterprise は、初期ブレークポイントのための`-b` パラメーターを使用することをおすすめします。

11. サーバーコンソール（または iLO リモートコンソール）にアクセスし、**Enter** キーを押して、OS ロードメニューでデバッグ選択を起動します。

    この手順には、数分かかる場合があります。

12. ホストサーバーのデバッグを完了したら、PuTTY を使用して CLI に接続し、仮想シリアルポートへのデバッグソケットをオフにします。その後、コマンド `windbg_disable` を入力します。

    iLO デバッグソケットが有効になっているかぎり、Windows デバッガーへの接続の切断および再接続が可能です。

サーバーヘルスサマリーの使用

iLO を使用すると、サーバーの電源をオンまたはオフにしたときに外部モニターにサーバーヘルスサマリーを表示できます。この機能は、サーバーが起動しないときのトラブルシューティングに役立ちます。この機能を使用すると、サーバーの IP アドレスやその他のヘルス情報を表示できます。

前提条件

- サーバーには UID ボタンがあります。
- 外部モニターが接続されています。

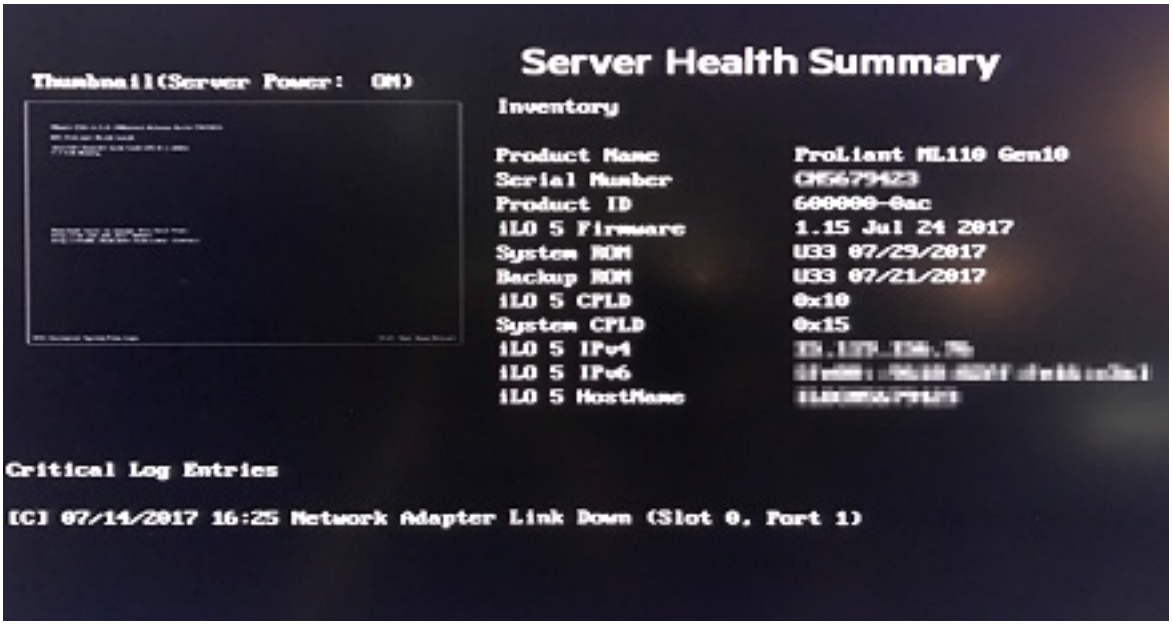
手順

1. サーバー上の UID ボタンを押します。

   注意:

   UID ボタンを押して放します。5 秒以上押しつづけると、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。

   外部モニターにサーバーヘルスサマリー画面が表示されます。



2. 再度 UID ボタンを押して、サーバーヘルスサマリー画面を閉じます。

サーバーヘルス概要の詳細

サーバー画面のサムネイル

サーバー画面のサムネイルイメージ。

サーバー電源

サーバーの電源ステータス。

製品名

サーバーのモデル。

シリアル番号

サーバーのシリアル番号。

製品 ID

この iLO プロセッサーを統合する製品。

iLO ファームウェア

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。

システム ROM

インストールされているシステム ROM のバージョン。

バックアップ ROM

バックアップシステム ROM のバージョン。

iLOCPLD

インストールされている iLO CPLD のバージョン。

システム CPLD

インストールされているシステム CPLD のバージョン。

内蔵 Smart アレイ

インストールされている Smart アレイファームウェアのバージョン。この値は、最後の補助電源サイクル以降にサーバー POST が正常に完了した場合にのみ表示されます。

iLOIPv4

iLO の IPv4 アドレス。この値は、**アクセス設定**ページ上で **POST 実行中に iLO IP を表示**が有効になっている場合にのみ表示されます。

iLOIPv6

iLO の IPv6 アドレス。この値は、**アクセス設定**ページ上で **POST 実行中に iLO IP を表示**が有効になっている場合にのみ表示されます。

iLO ホスト名

iLO のホスト名。

クリティカルログエントリ

IML からの最新の**クリティカル**イベントが表示されます。最新のイベントが最初に表示されます。

イベントログのエントリー

iLO 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、次の Web サイト（**http://www.hpe.com/info/EIL**）で、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。

iLO イベントログエントリーのタイムスタンプが正しくない

症状

iLO イベントログエントリーの日付または時刻が正しくありません。

原因

NTP サーバーアドレスまたはタイムゾーンが正しく設定されていません。

アクション

SNTP 設定が正しく構成されていることを確認します。

iLO サービスポートに接続された USB キーのマウントが失敗する

症状

iLO サービスポートに接続された USB キーのマウントが失敗する

原因

USB キーは、FAT32 フォーマットでフォーマットされていないか、無効なパーティションテーブルがあります。

アクション

- USB キーが FAT32 にフォーマットされていることを確認します。フォーマットされていない場合、USB キーを再フォーマットします。
- USB キーが FAT32 にフォーマットされており、かつマウントされない場合、Microsoft DiskPart などのユーティリティを使用してそのパーティションを削除して再作成します。

iLO 共有ネットワークポートを使用するサーバーでの仮想メディアデバイスからの OS インストールに失敗する

症状

仮想メディアデバイスを使用して、共有ネットワークポートを使用するサーバーに OS をインストールすると、OS インストールに失敗する。

原因

共有ネットワークポートが有効な場合、iLO ネットワーク接続はサーバー NIC に依存します。サーバーのブートプロセス時および OS 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 の通信がリストアされ、iLO がネットワークトラフィックに応答します。iLO への到達不能時間は、NIC ファームウェアに依存します。到達不能な状態が長すぎる場合、仮想メディアクライアントは iLO との通信の試行を停止し、セッションを切断します。

アクション

- インストールを再試行します。
- サーバーに直接接続されている物理メディアから OS をインストールします。

IML のトラブルシューティングのリンク

選択した IML イベントのトラブルシューティング情報を入手できます。サポートされているイベントは、IML イベントのペインに**さらに詳しくは**リンクとして表示されます。

Intelligent Provisioning が iLO ナビゲーションペインにない

症状

Intelligent Provisioning オプションを iLO ナビゲーションペインで選択できない。

原因

Intelligent Provisioning がインストールされていないか、インストールしたバージョンに問題があります。

アクション

1. 最新バージョンの Intelligent Provisioning をインストールします。
2. iLO からログアウトします。
3. iLO にもう一度ログインして、Intelligent Provisioning にアクセスします。

ログインと iLO アクセスの問題

iLO ファームウェアのログイン名とパスワードが受け付けられない

症状

iLO ファームウェアのログインに失敗します。

原因

入力されたユーザーアカウント情報が誤っています。

アクション

1. 正しいユーザーアカウント情報を入力します。
   - パスワードでは大文字と小文字が区別されます。
   - ユーザー名は、大文字と小文字が区別されません。大文字と小文字は同一として扱われます（例：Administrator は administrator と同一として扱われます）。

名前を使用して iLO マネジメントポートにアクセスできない

症状

名前を使用して iLO マネジメントポートにアクセスできません。

原因

iLO マネジメントポートは、WINS サーバーまたは DDNS サーバーを使用して、iLO マネジメントポートに名前でアクセスするために必要な名前-IP アドレス解決を提供することができます。名前を使用して iLO マネジメントポートにアクセスできるように環境が構成されていません。

アクション

1. 環境が以下の要件を満たすことを確認します。
   - iLO マネジメントポートの電源を入れる前に、WINS サーバーまたは DDNS サーバーが稼働している必要があります。
   - iLO マネジメントポートは､WINS サーバーまたは DDNS サーバーの IP アドレスを使用して構成されます。DHCP を使用して、必要な IP アドレスを構成できます。
   - iLO マネジメントポートは、WINS サーバーまたは DDNS サーバーへの有効な経路を持っている必要があります。
   - iLO マネジメントポートにアクセスするために使用するクライアントは、マネジメントポートの IP アドレスが登録された DDNS サーバーを使用するように構成されます。

WINS サーバーと動的でない DNS サーバーを使用する場合は、DNS サーバーが名前解決用に WINS サーバーを使用するように設定すると、iLO マネジメントポートアクセスを高速化させることができます。詳しくは、Microsoft のドキュメントを参照してください。

iLO ログインページにアクセスできない

症状

iLO Web インターフェイスのログインページがロードされません。

解決方法 1

原因

ブラウザーの SSL 暗号化レベルが 128 ビット以上に設定されていません。

iLO の SSL 暗号化レベルは 128 ビット以上に設定されており、変更することはできません。ブラウザーと iLO の暗号化レベルは一致していなければなりません。

アクション

ブラウザーの SSL 暗号化レベルを 128 ビット以上に設定します。

解決方法 2

原因

iLO は共有ネットワークポートを使用するように構成され、その共有ネットワークポートが使用する NIC に対する NIC チーミングが有効になっています。この構成では、次の場合にネットワーク通信がブロックされる可能性があります。

- 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。
- 選択した 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る以外の NIC/ポートに送信されます。

アクション

共有ネットワークポート構成が、iLO NIC チーミングガイドラインに従うことを確認します。

ネットワーク設定の変更後 iLO に接続できなくなった

症状

ネットワーク設定を変更した後、iLO にアクセスできません。

原因

NIC とスイッチの設定が同じではありません。

アクション

接続の両端（NIC およびスイッチ）で、トランシーバー速度の自動選択、速度、およびデュプレックスについて同じ設定が行われていることを確認してください。

たとえば、一方の側で接続が自動選択されるように設定されている場合、もう一方の側でも同じ設定を使用してください。

iLO のリセット後に iLO ログインページに戻れない

症状

iLO のリセット後に iLO ログインページが開きません。

アクション

ブラウザーのキャッシュをクリアし、ブラウザーを再起動します。

iLO ファームウェアの更新後に iLO 接続エラーが発生する

症状

ファームウェアの更新後に、Web インターフェイスを使用して iLO に接続できません。

アクション

ブラウザーのキャッシュをクリアして、再試行します。

NIC を用いて iLO プロセッサーに接続できない

症状

NIC 経由で iLO プロセッサーにアクセスできません。

アクション

- ROM ベースのシステムユーティリティを使用して NIC が有効になっていることを確認し、割り当てられた IP アドレスとサブネットマスクを確認します。

  詳しくは、ROM ベースの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。
- ネットワーク上の別のワークステーションから、その NIC の IP アドレスを ping します。
- ブラウザーで、NIC の IP アドレスを URL として入力して、NIC との接続を試みます。このアドレスで、iLO のログインページを表示できます。
- iLO をリセットします。ネットワーク接続が確立した場合、DHCP サーバー要求を最大 90 秒待つ必要がある場合があります。

iLO の証明書のインストール後 iLO にログインできない

症状

iLO の自己署名証明書をブラウザーの証明書ストアにインストールした後、iLO にアクセスできません。

原因

iLO を工場出荷時のデフォルト設定にリセットするか、iLO ホスト名を変更すると、新しい自己署名証明書が生成されます。一部のブラウザーでは、自己署名証明書を永久的にインストールすると、新しい自己署名証明書を生成した後で iLO にログインできないことがあります。

アクション

自己署名証明書をブラウザーの証明書ストアから削除します。

自己署名証明書の証明書名は iLO で、**発行元**値には**デフォルトの発行元**というテキストが含まれています。

iLO の自己署名証明書をブラウザーの証明書ストアにインストールしないでください。証明書をインストールする場合は、CA に永久的な証明書を要求し、iLO にインポートします。

証明書の使用について詳しくは、ブラウザーのドキュメントを参照してください。

iLO の IP アドレスに接続できない

症状

iLO の IP アドレスを使用して iLO に接続できません。

原因

プロキシサーバーを使用するように Web ブラウザーが構成されています。

アクション

プロキシサーバーを使用せずに iLO に接続するには、プロキシサーバーの例外リストに iLO を追加します。

手順については、ブラウザーのドキュメントを参照してください。

iLO TCP/IP 通信が失敗する

症状

iLO 通信が失敗します。

原因

1 つまたは複数の TCP/IP ポートを介した iLO 通信をファイアウォールが防げていす。

アクション

iLO が使用するポートでの通信を許可するようにファイアウォールを構成します。

Firefox を使用して iLO に接続するときのセキュアな接続の失敗エラー

症状

Firefox 使用して iLO に接続しようとするときに、次のエラーが発生します：`sec_error_reused_issuer_and_serial`。

解決方法 1

原因

インストールされている証明書には、認証機関によって発行された別の証明書と同じシリアル番号が含まれています。

アクション

1. メニューボタンをクリックし、**オプション**を選択します。
2. **詳細設定**をクリックします。
3. **証明書**をクリックします。
4. **証明書の表示**をクリックします。
5. **サーバー**タブをクリックし、iLO に関係する証明書をすべて削除します。
6. **その他**タブをクリックし、iLO に関係する証明書をすべて削除します。
7. **OK** をクリックします。
8. Firefox を起動し、iLO に接続します。

解決方法 2

原因

インストールされている証明書には、認証機関によって発行された別の証明書と同じシリアル番号が含まれています。

アクション

1. Firefox を閉じます。
2. Firefox の `AppData` フォルダーに移動して、すべての Firefox ディレクトリにある`*.db` ファイルをすべて削除します。

   `AppData` フォルダーは通常次の場所にあります。`C:\\Users\<`ユーザー名`>\AppData\Local\Mozilla\Firefox\`

Internet Explorer を使用して iLO の Web インターフェイスに移動するときの証明書エラー

症状

Internet Explorer を使用して iLO Web インターフェイスに移動すると、証明書のエラーが表示されます。

解決方法 1

アクション

1. **このサイトの閲覧を続行する（推奨されません）。**リンクをクリックします。
2. iLO にログインします。

解決方法 2

アクション

1. **管理** > **セキュリティ** > **SSL 証明書情報**ページに移動します。
2. SSL 証明書を取得してインポートします。
3. iLO をリセットします。

Chrome を使用して iLO の Web インターフェイスに移動するときの証明書エラー

症状

Chrome を使用して iLO Web インターフェイスに移動すると、証明書のエラーが表示されます。

解決方法 1

アクション

1. **詳細設定**をクリックします。
2. **（iLO のホスト名または 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。
3. iLO にログインします。

解決方法 2

アクション

1. **管理** > **セキュリティ** > **SSL 証明書情報**ページに移動します。
2. SSL 証明書を取得してインポートします。
3. iLO をリセットします。

Firefox を使用して iLO の Web インターフェイスに移動するときの証明書エラー

症状

Firefox を使用して iLO Web インターフェイスに移動すると、証明書のエラーが表示されます。

解決方法 1

アクション

1. **危険性を理解した上で接続するには**をクリックし、**例外を追加**をクリックします。
2. **セキュリティ例外の追加**ダイアログボックスで、**場所**ボックスに `https://<iLO ホスト名または IP アドレス>`と入力します。
3. **セキュリティ例外を承認**をクリックします。

セキュリティ例外が保存され、iLO ログイン画面が表示されます。

4. iLO にログインします。

解決方法 2

アクション

1. **管理** > **セキュリティ** > **SSL 証明書情報**ページに移動します。
2. SSL 証明書を取得してインポートします。
3. iLO をリセットします。

iLO ログインページに「Web サイトは不明な機関で認証されています」メッセージが表示される

原因

iLO ログインページに移動すると、「`Web` サイトは不明な機関で認証されています」というメッセージが表示されます。

アクション

1. 証明書を表示して、（にせのサーバーでなく）正しいマネジメントサーバーにアクセスしていることを確認します。
   a. **発行先**の名前がマネジメントサーバーであることを確認します。必要と思われる手順を実行して、マネジメントサーバーの識別情報を確認します。
   b. これが正しいマネジメントサーバーかどうか確信が持てない場合は、先に進まないでください。にせのサーバーにアクセスしている可能性があり、ログインするときにログイン認証情報をにせのサーバーに渡すおそれがあります。管理者に連絡してください。接続を取り消すには、証明書ウィンドウを終了し、**いいえ**または**キャンセル**をクリックします。
2. 前のステップの項目を確認した後、次のオプションを選択します。
   - このセッションのために一時的に証明書を受け入れる。
   - 永久的に証明書を受け入れる。
   - いったん中止し、管理者から提供されたファイルからブラウザーに証明書をインポートする。

HPEOneView によって管理されるサーバー上で iLO にアクセスできない

症状

HPEOneView が管理するサーバー上で iLO にアクセスできません。

原因

サーバー署名が変更され、HPE OneView はサーバーの再検出および構成を実行していません。

アクション

HPE OneView を使用して、サーバーを含むフレームを更新します。

iOS モバイルアプリケーションで iLO システムに接続できない

症状

iOS モバイルアプリケーションを使用して iLO システムに接続しようとすると、接続に失敗する。

解決方法 1

原因

iLO の構成が間違っているか、ローカルネットワークに問題があります。

アクション

この原因を確認するために、iLO と同じネットワークにあるノートパソコンまたはデスクトップコンピューターを使用して、iLO との接続を試みてください。接続に失敗した場合、iLO とネットワーク構成を確認してください。

解決方法 2

原因

iOS デバイスと iLO の間にファイアウォールがあります。この原因を確認するために、iOS デバイスの Safari ブラウザーから iLO への接続を試みてください。

アクション

- iLO Web サーバー SSL ポート（HTTPS）とリモートコンソールポートの例外を許可するようファイアウォールを構成します。デフォルトでは、Web サーバー SSL ポートはポート 443 を使用して、リモートコンソールポートはポート 17990 を使用します。
- ほとんどのファイアウォールで許可されている例外で動作するように iLO を構成します。通常、ファイアウォールは、ポート 80 と 443 のアドレスの例外を許可します。iLO Web サーバー非 SSL ポートをデフォルト値（80）から別の値に変更し、ポート 80 を使用するようにリモートコンソールポートを構成します。

  iLO ポートの値は、iLO の Web インターフェイスの**アクセス設定**ページで構成できます。
- iOS デバイスをネットワークに接続するには、VPN 接続を使用します。

  VPN 接続を使用する場合は、通常、Oath トークンまたは同等のものおよびアカウントを IT 部門から取得する必要があります。デバイスで VPN を構成した後で、一時パスワードを生成し、使用する iLO を含むネットワークにログインします。

  iOS デバイスで VPN をセットアップする方法については、IT 管理者にお問い合わせください。

iLO が ping に断続的に応答するか、または応答しない

症状

iLO は、ping に断続的に応答するか、または応答しません。

原因

iLO は共有ネットワークポートを使用するように構成され、その共有ネットワークポートが使用する NIC に対する NIC チーミングが有効になっています。この構成では、次の場合にネットワーク通信がブロックされる可能性があります。

- 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。
- 選択した 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る以外の NIC/ポートに送信されます。

アクション

共有ネットワークポート構成が NIC チーミングガイドラインに従っていることを確認します。

iLO を使用した XML スクリプトの実行に失敗する

症状

iLO に対して XML スクリプトを実行すると、セッションが開始されないか、または突然終了します。

原因

iLO は共有ネットワークポートを使用するように構成され、その共有ネットワークポートが使用する NIC に対する NIC チーミングが有効になっています。この構成では、次の場合にネットワーク通信がブロックされる可能性があります。

- 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。
- 選択した 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る以外の NIC/ポートに送信されます。

アクション

共有ネットワークポート構成が NIC チーミングガイドラインに従っていることを確認します。

ディレクトリの問題

Kerberos 認証による iLO へのログインが失敗する

症状

Kerberos へのログインを試みて失敗しました。

解決方法 1

原因

クライアントにチケットがないか、チケットが無効である。

アクション

クライアント PC をロックして新しいチケットを取得するには、**Ctrl+Alt+Del** を押します。

解決方法 2

原因

Kerberos ログインの設定が誤っています。考えられる原因は、以下のとおりです。

- クライアント PC がログインしている Kerberos レルムが、iLO が設定されている Kerberos レルムと一致しない。
- iLO に保存されている Kerberos キータブファイル内のキーが、Active Directory のキーと一致しない。
- iLO が不正な KDC サーバーアドレス用に構成されている。
- クライアント PC、KDC サーバー、および iLO の間で、日時が一致しない。これらのシステム上の日時を同じ値に設定します。これらのシステム上の日時は 5 分以上異なっていてはいけません。

アクション

ご使用の環境が、Kerberos サポートの要件を満たしていることを確認します。

解決方法 3

原因

ディレクトリユーザーアカウントに関わる問題があります。次のような問題が考えられます。

- iLO コンピューターアカウントが Active Directory 内に存在しないか、アカウントが無効になっている。
- クライアント PC にログインしているユーザーが、iLO アクセスを認可された（汎用またはグローバルな）ディレクトリグループのメンバーでない。

アクション

DNS サーバーを修復します。

Kerberos ログインの試行中に iLO 認証情報プロンプトが表示される

症状

ユーザーが **Zero Sign In** ボタンをクリックしたとき、認証情報プロンプトが表示されます。

原因

ブラウザーが Kerberos ログイン用に正しく構成されていません。

アクション

Kerberos ログインをサポートするようにブラウザーを構成します。

名前による Kerberos ログインの試行中に iLO 認証情報プロンプトが表示される

症状

ユーザーが Kerberos SPN 形式のユーザー名および関連付けられているドメインパスワードを使用して iLO にログインしようとするときに、認証情報プロンプトが表示されます。

原因

iLO 用のコンピューターアカウントは子ドメインの一部であり、Kerberos 構成パラメーターは親ドメインを参照します。

アクション

以下の Kerberos パラメーターが正しく構成されていることを確認します。**Kerberos Realm**、**Kerberos KDC Server Address**、**Kerberos KDC Server Port**。

iLO へのディレクトリ接続が途中で終了する

症状

アクティブディレクトリセッションが途中で終了します。

原因

ネットワークエラーによって、iLO は、ディレクトリ接続が無効になったと判断することがあります。iLO がディレクトリを検出できない場合、iLO は、ディレクトリ接続を終了します。終了された接続を使用して作業の継続を試みても、ブラウザーは、ログインページに転送されます。

この問題は、以下の状況で発生する可能性があります。

- ネットワーク接続が切断された。
- ディレクトリサーバーがシャットダウンした。

アクション

ログインしなおして iLO の使用を継続します。

ディレクトリサーバーを使用できない場合は、ローカルユーザーアカウントを使用してログインします。

構成されているディレクトリユーザーコンテキストが iLO ログインで動作しない

症状

ディレクトリユーザーコンテキストが構成されていますが、ディレクトリユーザーコンテキストが提供するログインオプションが機能しません。

原因

ディレクトリまたはユーザーコンテキスト内のユーザーオブジェクトが正しく構成されていません。

アクション

- ユーザーオブジェクトの完全な DN がディレクトリに存在することを確認します。

  この情報は DN の最初の `CN=`の後にあります。

- DN の残りの部分はユーザーコンテキストとして追加されていることを確認します。

  ユーザーコンテキストは、大文字と小文字を区別しません。また、それ以外の文字は、空白も含めて、ユーザーコンテキストの一部です。

ディレクトリタイムアウトになった後も iLO ディレクトリユーザーアカウントがログアウトしない

症状

ディレクトリユーザーは、ディレクトリログインタイムアウトのために構成された時間だけアイドル状態になった後、ログアウトされません。

原因

iLO の **Idle Connection Timeout** 値が**無限**に設定されています。この構成の場合、リモートコンソールは、定期的に iLO ファームウェアの ping を実行して、接続が存在することを確認します。リモートコンソールが iLO に ping を送信すると、iLO ファームウェアは、ユーザー権限についてディレクトリにクエリを実行します。この定期的なクエリによりディレクトリ接続がアクティブであり続け、ディレクトリタイムアウト設定に基づくユーザーのログアウトが行われなくなります。

アクション

Idle Connection Timeout 設定を変更します。

iLO Zero サインイン構成用の Kerberos キータブファイルの生成の失敗

症状

`ktpass` を使用してキータブファイルを生成しようとしたときにプロセスが失敗します。

原因

`ktpass` コマンドの書式が正しくありませんでした。

アクション

もう一度実行し、`ktpass` コマンド内のプリンシパル名の書式が正しいことを確認してください。

iLOKerberos 構成での `Setspn` の実行中のエラー

症状

`Setspn` コマンドの実行中にエラーが発生しました。

アクション

1. `ADSIEdit` スナップインを備えた MMC を使用し、iLO のコンピューターオブジェクトを検索します。
2. `DNSHostName` プロパティを iLO の DNS 名に設定します。
   例：`cn=iloname,ou=us,ou=clients,dc=example,dc=net`

OpenLDAP 認証は、入れ子型グループまたは posixgroups で構成されている場合に失敗します。

症状

OpenLDAP 認証は、ディレクトリが入れ子型グループまたは posixgroups ディレクトリで構成されている場合に失敗します。

原因

iLO では、OpenLDAP での入れ子型グループまたは posixgroups をサポートしません。

アクション

iLO に LDAP ユーザーがダイレクトメンバーシップを持つグループを構成します。OpenLDAP ディレクトリグループがタイプ groupOfNames の objectClass を持つことを確認します。

ドメインコントローラー OS の再インストール後に iLO Zero サインインが失敗する

症状

ドメインコントローラー OS を再インストールした後に iLO Web インターフェイスの **Zero Sign In** オプションが動作しません。

原因

ドメインコントローラー OS が再インストールされると、キーバージョン番号がリセットされます。

アクション

新しい Kerberos キータブファイルを生成してインストールします。

Active Directory の認証情報での iLO ログインに失敗する

症状

Active Directory を使用するように iLO が構成されている場合にユーザー認証に失敗します。

原因

証明書の問題があります。

- Active Directory サーバーに SSL 証明書がインストールされていません。
- Active Directory サーバー上の古い SSL 証明書は、現在の証明書の CA と同じ名前の以前の信頼済み CA を指しています。これは、証明書サービスが追加された後削除され、再度、追加された場合に発生することがあります。

Directory Tests ページの SSL 接続テスト結果を確認することによって、この原因を確認できます。

アクション

1. MMC を起動します。
2. 証明書スナップインを追加します。
3. プロンプトが表示されたら、表示する証明書のタイプとして**コンピューターアカウント**を選択します。
4. 証明書スナップインに戻るために、**OK** をクリックします。
5. **個人** > **証明書**フォルダーを選択します。
6. フォルダーを右クリックして、**新しい証明書の要求**を選択します。
7. **証明書の種類**がドメインコントローラーになっていることを確認したら、証明書が発行されるようになるまで**次へ**をクリックします。

Directory Server DNS Name テストで失敗が報告される

症状

Directory Server DNS Name テストで、ステータス**失敗**が報告されます。

原因

iLO は、ディレクトリサーバーの IP アドレスを取得できません。

アクション

- iLO に設定されている DNS サーバーが正しいことを確認します。
- ディレクトリサーバーの FQDN が正しいことを確認します。
- トラブルシューティングツールとして、FQDN の代わりに IP アドレスを使用します。
- 問題がなくならない場合は、DNS サーバーの記録とネットワークルーティングをチェックします。

ディレクトリサーバーへの Ping テストが失敗を報告する

症状

ディレクトリサーバーへの Ping テストが**失敗**ステータスを報告します。

原因

iLO は、ディレクトリサーバーを Ping し、応答を受信しませんでした。

アクション

- ディレクトリサーバーでファイアウォールが有効かどうかをチェックします。
- ネットワークルーティング問題をチェックします。

Connect to Directory Server テストで失敗が報告される

症状

Connect to Directory Server テストで、ステータス**失敗**が報告されます。

原因

指定したディレクトリサーバーとの LDAP 接続を iLO が開始できませんでした。

アクション

- 構成されたディレクトリサーバーが正しいホストであることを確認します。
- （iLO とディレクトリサーバー間のすべてのルーターやファイアウォールを考慮して）iLO がポート 636 経由でディレクトリサーバーとのクリアな通信パスを持っていることを確認します。
- ディレクトリサーバー上のローカルファイアウォールが有効になっており、ポート 636 経由で通信できることを確認します。

Connect using SSL テストで失敗が報告される

症状

Connect using SSL テストで、ステータス**失敗**が報告されます。

原因

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失敗しました。

アクション

- ディレクトリサーバーで SSL 交渉を有効にします。
- Microsoft Active Directory を使用する場合は、Active Directory 証明書サービスがインストールされていることを確認します。

Bind to Directory Server テストで失敗が報告される

症状

Bind to Directory Server テストで、ステータス**失敗**が報告されます。

原因

iLO は、指定されたユーザー名との接続のバインドまたは匿名バインドに失敗しました。

アクション

- ディレクトリサーバーが匿名バインドを許可することを確認します。
- テストボックスにユーザー名を入力した場合は、認証情報が正しいことを確認します。
- ユーザー名が正しいことを確認した場合は、`user@domain.com`、`DOMAIN\username`、`username`（Active Directory の表示名）、または `userlogin` のような他のユーザー名フォーマットを使用してみてください。
- 指定したユーザーがログインを許可され、有効であることを確認します。

Directory Administrator Login テストで失敗が報告される

症状

Directory Administrator Login テストで、ステータス**失敗**が報告されます。

原因

オプションの**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**ボックスに値を入力しましたが、ディレクトリサーバーへのログインが失敗しました。

アクション

ディレクトリ管理者の認証情報が正しく入力されていることを確認します。

ユーザー認証テストで失敗が報告される

症状

ユーザー認証テストで**失敗**ステータスが報告されます。

原因

入力されたユーザー名とパスワードを使用した認証に失敗しました。

アクション

- ユーザー認証情報が正しく入力されていることを確認してください。
- `user@domain.com`、`DOMAIN\username`、`username`（Active Directory の表示名）、または `userlogin` のような他のユーザー名形式を使用してみてください。
- 指定したユーザーがログインを許可され、有効であることを確認します。
- 指定したユーザーアカウントにアクセス制限が構成されているかどうかを確認します。

ユーザー承認テストで失敗が報告される

症状

ユーザー承認テストで**失敗**ステータスが報告されます。

原因

入力されたユーザー名とパスワードを使用した承認に失敗しました。

アクション

- 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することを確認します。
- 指定したユーザーアカウントにアクセス制限が構成されているかどうかを確認します。

ディレクトリユーザーコンテキストテストで失敗が報告される

症状

ディレクトリユーザーコンテキストテストで、ステータス**失敗**が報告されます。

原因

iLO が、指定された**ディレクトリ管理者識別名**を使用して、指定されたユーザーコンテキストを検索するときに、ディレクトリでコンテナーが見つかりませんでした。

アクション

検索コンテキストが正しく入力されていることを確認します。

LOM Object Exists テストで失敗が報告される

症状

LOM Object Exists テストでステータス**失敗**が報告されます。

原因

iLO は、**セキュリティ - ディレクトリ**ページに設定されている **iLO オブジェクト識別名**で指定されたディレクトリオブジェクトを見つけられませんでした。

アクション

- iLO オブジェクトの LDAP FQDN が正しいことを確認します。
- HPLOMIG ソフトウェアを更新して、ディレクトリサーバー内の HPE 拡張スキーマとスナップインを更新してみてください。

リモートコンソールの問題

以下の各項では、リモートコンソールの問題のトラブルシューティングについて説明します。

重要:

新しいウィンドウの自動起動を防止するポップアップブロックアプリケーションを使用すると、リモートコンソールを実行できなくなります。この場合、ポップアップブロックプログラムを無効にしてから、リモートコンソールを起動してください。

Linux クライアントで Firefox を使用して Java IRC を実行すると、iLO Java IRC に赤色の X が表示される

症状

Linux システム上で Java IRC を実行すると、Java IRC に赤色の X アイコンが表示されます。

原因

Firefox が cookie を受け入れる設定になっていません。

アクション

cookie を受け入れるように Firefox を構成します。

iLO Java IRC が起動しない

症状

セキュリティ警告を受け入れずに、アプリケーションを実行することを確認した場合、Java IRC は起動しません。

原因

セキュリティ警告を受け入れてアプリケーションを実行することを確認することなく Java IRC を起動することはできません。

アクション

1. **Java コンソール**ウィンドウの**クリア**ボタンをクリックします。
2. **Java コンソール**ウィンドウの**閉じる**ボタンをクリックします。
3. iLO をリセットします。
4. ブラウザーのキャッシュをクリアします。
5. ブラウザーを閉じて、新しいブラウザーウィンドウを開きます。
6. iLO にログインして、Java IRC を起動し、証明書を受け入れます。

カーソルが iLO のリモートコンソールウィンドウの隅にアクセスできない

症状

マウスカーソルをリモートコンソールウィンドウの隅に移動できません。

アクション

マウスカーソルを右クリックしてリモートコンソールウィンドウの外側にドラッグしてから、内側にドラッグして戻してください。

iLO リモートコンソールのテキストウィンドウが正しく更新されない

症状

リモートコンソールを使用して、高速でスクロールするテキストウィンドウを表示する場合、テキストウィンドウが正しく更新されないことがあります。

原因

この問題は、iLO のファームウェアの検出/表示速度よりもビデオの更新速度のほうが速いときに発生することがあります。通常、テキストウィンドウの左上隅だけが更新され、残りの部分の表示は更新されません。

アクション

テキストウィンドウのスクロールが停止した後、**更新**をクリックしてリモートコンソールウィンドウを更新します。

iLO .NET IRC または Java IRC（Java Web Start）でマウスやキーボードを使用できない

症状

.NET IRC または Java IRC（Java Web Start オプション）でマウスやキーボードを使用できません。

解決方法 1

アクション

1. .NET IRC または Java IRC を閉じます。
2. **電力設定**ページに移動します。
3. **マウス、キーボードの持続接続**チェックボックスをクリアし、**適用**をクリックします。
4. .NET IRC または Java IRC を再び起動します。

解決方法 2

アクション

マウスカーソルを右クリックしてリモートコンソールウィンドウの外側にドラッグしてから、内側にドラッグして戻してください。

iLO Java IRC（Java Applet）でマウスやキーボードを使用できない

症状

Java IRC（Java Applet オプション）でマウスやキーボードを使用できません。

解決方法 1

アクション

1. Java IRC を閉じます。
2. **電力設定**ページに移動します。
3. **マウス、キーボードの持続接続**チェックボックスをクリアし、**適用**をクリックします。
4. Java IRC を再び起動します。

解決方法 2

アクション

マウスカーソルを右クリックしてリモートコンソールウィンドウの外側にドラッグしてから、内側にドラッグして戻してください。

解決方法 3

アクション

1. ブラウザーウィンドウを閉じて、新しいブラウザーを開きます。
2. Java コントロールパネルを開きます。
3. **Java Runtime Environment 設定**ダイアログボックスに移動します。
4. 次のランタイムパラメーターを追加します。`-Dsun.java2d.d3d=false`。
5. **OK** をクリックして **Java Runtime Environment 設定**ウィンドウを閉じます。
6. **適用**をクリックし、**了解**をクリックして Java コントロールパネルを閉じます。

   適用をクリックする前に変更内容を表示すると、**ランタイムパラメーター**ダイアログボックスがリセットされ、編集内容が失われることがあります。
7. ブラウザーを起動して、iLO にログインします。
8. Java IRC を再び起動します。

iLO .NET IRC がウィンドウの切り替え後に継続して文字を送信する

症状

別のウィンドウに切り替えると、.NET IRC は継続的に文字を送信します。

原因

.NET IRC セッション時にキーを押して、ウィンドウを切り替えた場合、キーはセッション中に押されたままの状態になります。これにより、文字が継続的に繰り返されることになります。

アクション

.NET IRC ウィンドウをクリックして、デスクトップの前面にリモートコンソールウィンドウを移動させます。

iLO Java IRC のディスケットおよび USB キーデバイス情報の表示が誤っている

症状

Firefox ブラウザーを使用する場合、Java IRC が表示するディスケットドライブおよび USB キーデバイス情報が誤っている可能性があります。

原因

クライアント OS または Java ソフトウェアが期限切れの場合があります。

アクション

1. Red Hat Enterprise Linux 6 以降がローカルクライアントシステムにインストールされていることを確認します。
2. 最新バージョンの Java をインストールし、Firefox ブラウザーで接続するように Java を設定します。
3. iLO Web インターフェイスにログインします。
4. USB キーまたはディスケットをローカルクライアントシステムに挿入します。
5. USB キーまたはディスケットにアクセスできることを確認します。
6. Java IRC セッションを開きます。
7. **仮想ドライブ** > **イメージファイルリムーバルメディア**の順に選択します。

   ディスクイメージファイルを選択してくださいダイアログボックスが開きます。
8. クライアントに挿入した USB キーまたはディスケットのパス（`/dev/disk`）を入力または選択します。

   USB キーまたはディスケットを by-label でマウントすることもできます。
9. **OK** をクリックします。

iLO と Java IRC の間で Caps Lock が同期しない

症状

Java IRC にログインすると、iLO と Java IRC の間で **Caps Lock** 設定が同期しない場合があります。

アクション

Caps Lock 設定を同期させるには、Java IRC で**キーボード** > **Caps Lock** の順に選択して、Caps Lock 設定を同期させます。

iLO と共有リモートコンソールの間で Num Lock が同期しない

症状

共有リモートコンソールセッションにログインすると、iLO と一部のリモートコンソールセッションの間で **Num Lock** 設定が同期しない場合があります。

アクション

Num Lock 設定を同期させるには、リモートコンソールで**キーボード** > **Num Lock** の順に選択します。

iLO リモートコンソールセッション中に意図しないキーストロークが繰り返される

症状

リモートコンソールセッション中に意図しないキーストロークが繰り返されます。

解決方法 1

原因

ネットワークの問題がネットワーク遅延を引き起こしている可能性があります。

アクション

ネットワーク遅延を引き起こす場合がある問題を特定し、解決します。

解決方法 2

原因

リモートシステムの設定により遅延が生じています。

アクション

1. リモートマシンで以下の設定を調整します。

   - **Increase the typematic delay** - この設定は、キーボードのキーを押したままにしたときに文字を繰り返す前の遅延を制御します。
   - **Decrease the typematic rate** - この設定は、キーボードのキーを押したままにしたときに文字を繰り返す速度を制御します。

   これらの設定の正式名称は、使用している OS によって異なります。キーリピート遅延と速度の変更について詳しくは、OS のドキュメントを参照してください。

iLO .NET IRC が再生モードにあるとき、セッションリーダーが接続要求を受信しない

症状

リモートコンソールセッションリーダーがキャプチャされたビデオデータを再生する場合、別のユーザーが.NET IRC へのアクセスまたは共有を要求するときにプロンプトが表示されません。

原因

.NET IRC をアクセスまたは共有する要求がタイムアウトしました。

アクション

他のユーザーに連絡するか、リモートコンソール取得機能を使用して.NET IRC を制御します。

iLO リモートコンソールのキーボード LED が正しく動作しない

症状

クライアントのキーボード LED は、リモートコンソールキーボードの状態を反映しません。

原因

クライアントのキーボード LED は、リモートコンソールキーボードの実際の状態を反映しません。リモートコンソールでキーボードオプションを使用すると、**Caps Lock**、**Num Lock**、および **Scroll Lock** キーは完全に機能します。

アクション

操作は必要ありません。

iLO .NET IRC が非アクティブになるか切断される

症状

iLO .NET IRC は、稼働率が高くなると非アクティブになったり、切断されたりします。.NET IRC は非アクティブになる前に、動作が遅くなります。非アクティブな.NET IRC の症状には以下のものがあります。

- .NET IRC の画面が更新されない。
- キーボードおよびマウスの動作が記録されない。
- 共有リモートコンソール要求が登録されない。
- キャプチャされたビデオファイルを再生することはできますが、他の.NET IRC 機能が非アクティブのままです。

解決方法 1

原因

複数のユーザーが iLO にログインしています。

アクション

- 同時 iLO ユーザーセッション数を減らします。
- iLO をリセットします。

解決方法 2

原因

接続されている仮想メディアセッションは、継続したコピー動作の実行に使用されています。継続したコピー動作が優先されるため、.NET IRC の同期が失われます。やがて仮想メディア接続が何度かリセットされ、OS が仮想メディアクライアントとの同期を失います。

アクション

- .NET IRC と仮想メディアを接続しなおします。
- iLO をリセットします。

iLO .NET IRC がサーバーに接続できない

症状

iLO は.NET IRC セッションの確立時に `Failed to connect to server` というメッセージを表示します。

解決方法 1

原因

ネットワークの応答が遅延している。iLO .NET IRC クライアントは、iLO との接続が確立されるまで、指定された時間待ちます。クライアントサーバーは、この時間内に応答を受信しない場合、エラーメッセージを表示します。

アクション

ネットワーク遅延を修正して、.NET IRC 接続を再試行します。

解決方法 2

原因

共有リモートコンソールセッションが要求されたが、セッションリーダーの受諾または拒否のメッセージ送信が遅延している。iLO .NET IRC クライアントは、iLO との接続が確立されるまで、指定された時間待ちます。クライアントサーバーは、この時間内に応答を受信しない場合、エラーメッセージを表示します。

アクション

.NET IRC セッションリーダーに問い合わせて要求の再試行を行うか、リモートコンソール取得機能を使用してください。

サーバーから iLO 仮想メディア USB キーにファイルをコピーした後にファイルが表示されない

症状

ファイルをターゲットサーバーから iLO 仮想ドライブにコピーした場合、ファイルがクライアントコンピューター上の Windows エクスプローラーに表示されません。

原因

iLO 仮想メディア USB キー上のファイルの変更を、クライアントコンピューターのユーザーが Windows エクスプローラーで表示するこ Virtual Drives とはできません。

Windows エクスプローラーでは、ファイルのキャッシュされたコピーを USB キー上に保持します。USB キーがファイルの変更によって更新されたとき、iLO リモートコンソールは Windows シェルに通知しません。エクスプローラーウィンドウを更新すると、キャッシュされた情報が USB キーに送り返されるため、変更された情報を表示することはできません。

アクション

1. Windows クライアントコンピューターに USB キーを接続します。
2. .NET IRC を起動し、USB キーを**仮想ドライブ**メニューで選択することによって USB キーを接続します。
3. 接続したデバイス上のファイルを変更（コピー、削除など）します。
4. デバイス上のすべてのデータが更新されたことを確認するには、ターゲットサーバーからデバイスをアンマウントします。
5. .NET IRC の **Virtual Devices** メニューを使用して、デバイスを切断します。

USB キーの内容の更新に、Windows エクスプローラーを使用しないでください。

6. **ハードウェアの安全な取り外し**機能を使用して、クライアントコンピューターからデバイスを取り出します。
7. クライアントコンピューターからデバイスを取り外します。

   USB キーをコンピューターに接続すると、Windows エクスプローラーでファイルの変更を確認できます。

iLO .NET IRC はアプリケーション要件を確認するのに長い時間がかかる

症状

.NET IRC を iLO Web インターフェイスから起動すると、**アプリケーションの起動中**ダイアログボックスが表示され、その画面が長い間表示されます。

アクション

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。

   インターネットオプションウィンドウが開きます。
3. **接続**タブをクリックし、**LAN の設定**ボタンをクリックします。

   ローカルエリアネットワーク（LAN）の設定ウィンドウが開きます。
4. **設定を自動的に検出する**チェックボックスの選択を解除します。
5. オプション：必要に応じてプロキシサーバーの設定を行います。
6. すべてのブラウザーウィンドウを閉じます。
7. ブラウザーを再起動し、.NET IRC を起動します。

iLO .NET IRC が起動しない

症状

.NET IRC を起動すると、**アプリケーションを起動できませんでした。**ダイアログボックスが表示され、`Application cannot be started` のメッセージが表示されます。アプリケーションベンダーにお問い合わせください。

アクション

Windows コマンドプロンプトから次のコマンドを入力して、ClickOnce アプリケーションキャッシュをクリアします。**`rundll32 %windir%\system32\dfshim.dll CleanOnlineAppCache`**

iLO .NET IRC を共有できません

症状

共有.NET IRC セッションに参加しようとしたときに、**接続できません**ダイアログボックスが表示され、`Unable to connect to shared IRC` というメッセージが表示されます。これは `17990` ポートをブロックするファイアウォールが原因かもしれません。

アクション

- セッションリーダーの.NET IRC クライアントと各共有.NET IRC クライアントの間に通信パスが存在することを確認します。
- すべてのクライアントのファイアウォール設定が、リモートコンソールポート（デフォルトポートは17990）へのインバウンド接続を許可していることを確認します。

iLO .NET IRC が Firefox で起動しない

症状

Mozilla Firefox で.NET IRC を起動すると、アプリケーションが起動に失敗する場合があります。

原因

iLO システムがデフォルトの iLO SSL 証明書（署名されている信頼済み証明書ではない）を使用している場合、iLO Web インターフェイスは、HTTPS ではなく HTTP を使用して、.NET IRC を起動します。iLO Web インターフェイスは HTTPS を使用し、Web インターフェイスは HTTP を使用してリモートコンソールを起動するため、ブラウザーに警告が表示されます。

アクション

- iLO に SSL 証明書をインポートし、**iLO 統合リモートコンソール**ページの **IRC は iLO 内の信頼された証明書を要求します**設定を有効にします。この構成が最も安全な解決方法です。
- アドレスバーの盾アイコンをクリックし、 **オプション** > **Disable protection for now** を選択します。
- 別のブラウザーを使用します。
- スタンドアロンの IRC を使用します。

  スタンドアロンの IRC を次の Web サイトからダウンロードできます。**http://www.hpe.com/support/hpesc**
- iLO Mobile アプリケーションを使用します。

  詳しくは、**http://www.hpe.com/info/ilo/mobileapp** を参照してください。

iLO .NET IRC が Google Chrome で起動しない

症状

Google Chrome で.NET IRC を起動すると、アプリケーションが起動に失敗します。

原因

Google Chrome の以前のバージョンでは、ClickOnce をサポートする NPAPI プラグインを使用して.NET IRC を実行できました。Google Chrome バージョン 42 以降では、NPAPI ベースのプラグインがサポートされません。

アクション

- 別のブラウザーを使用します。
- Java IRC を使用します。
- スタンドアロンの IRC を使用します。

スタンドアロンの IRC を次の Web サイトからダウンロードできます。**http://www.hpe.com/support/hpesc**

- iLO Mobile アプリケーションを使用します。

  詳しくは、**http://www.hpe.com/info/ilo/mobileapp** を参照してください。

iLO リモートコンソールを使用してマウントされた USB キーを使用して DOS からブートできない

症状

iLO リモートコンソールを使用して、マウントされている DOS ブート可能な USB キーから起動しようとすると、エラーが発生します。

USB キーの容量が 2 GB 以下の場合は、次のメッセージが表示されます。

```
Attempting Boot from CD-ROM
Attempting Boot from USB DriveKey (C:)
Cannot load DOS! Any key to retry
```

USB キーの容量が 2 GB を超える場合は、次のメッセージが表示され、サーバーがその時点で操作を停止します。

```
Attempting Boot from USB DriveKey (C:)Boot from Drive
Operating system load error
```

原因

リモートコンソールが USB キーのブートセクタにアクセスするための十分な特権を持っていません。

アクション

- Internet Explorer を右クリックし、**管理者として実行**を選択します。iLO の Web インターフェイスを起動し、リモートコンソールを起動してから、USB キーからブートします。
- USB キーをサーバーに挿入します。

SSH の問題

iLO との PuTTY の初期接続時の入力が緩慢である

症状

PuTTY クライアントを使用して初めて iLO に接続を行う際、入力の受け付けが緩慢（約 5 秒間）になります。

アクション

- クライアントの構成オプションが正しいことを確認します。
- Low-level TCP connection options の **Disable Nagle's algorithm** チェックボックスの選択を解除してください。

iLO 共有ネットワークポートを使用する場合、PuTTY クライアントが応答しない

症状

共有ネットワークポートで PuTTY クライアントを使用する場合、PuTTY セッションが応答しなくなります。

原因

大量のデータが転送されているか、仮想シリアルポートとリモートコンソールを使用しています。

アクション

PuTTY クライアントを終了して、セッションを再開してください。

iLO への SSH 接続を使用する場合にテキストが正しく表示されない

症状

80 文字×25 行を超える拡張テキスト構成は、SSH を使用する場合は、正しく表示されません。

原因

テキストベースのリモートコンソールからの SSH アクセスでは、標準の 80 文字×25 行構成のテキスト画面がサポートされます。このモードは、ほとんどのテキストモードインターフェイスで、テキストベースのリモートコンソール に対する互換性を備えています。

アクション

Hewlett Packard Enterprise は、テキストアプリケーションを 80 文字×25 行モードで設定するか、グラフィックリモートコンソールを使用することをお勧めします。

SSH セッションが起動に失敗する、または予期せず終了する

症状

SSH セッションが起動に失敗する、または予期せず終了します。

原因

iLO は共有ネットワークポートを使用するように構成され、その共有ネットワークポートが使用する NIC に対する NIC チーミングが有効になっています。この構成では、次の場合にネットワーク通信がブロックされる可能性があります。

- 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。
- 選択した 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る以外の NIC/ポートに送信されます。

アクション

共有ネットワークポート構成が、**NIC チーミングガイドライン**に従うことを確認します。

テキストベースのリモートコンソールの問題

テキストベースのリモートコンソールで Linux インストーラーを表示できない

症状

テキストベースのリモートコンソールから Linux をインストールすると、Linux インストーラー画面が表示されません。

原因

画面はグラフィックモードで表示されます。

アクション

- ほとんどのバージョンの Linux では、`linux text nofb` と入力します。

  入力する文字は表示されません。

  コマンドを入力すると、画面がグラフィックモードからテキストモードに変更され、画面が表示されます。
- SuSE Linux Enterprise Server の場合は、テキストコンソールで **F2** キーと下向きの矢印キーを押します。テキストモードが選択され、画面が表示されます。

SSH ターミナル経由でデータを送信できない

症状

SSH ターミナルからテキストベースのリモートコンソールにキーストロークデータが送信されません。

原因

SSH ターミナルを使用してテキストコンソールにアクセスする場合、SSH によってキーストロークデータの送信が阻止され、操作がテキストベースのリモートコンソールに伝わらないことがあります。この動作が発生すると、キーストロークが機能していないように見えます。

アクション

SSH ターミナルのショートカットを無効にします。

シリアルタイムアウト時間内の VSP 主導の選択によって、出力が VSP ではなく BIOS リダイレクトに送信される

症状

シリアルタイムアウト時間内の VSP 主導の選択によって、出力が VSP ではなく BIOS リダイレクトに送信されます。

原因

`/etc/grub.conf` ファイルには、シリアルタイムアウト時間のオプションが含まれています（`terminal --timeout=10 serial console`）。このオプションは、VSP または VGA コンソールでキーストロークを選択する際の制限時間を指定し、対応するデバイスにメニューが出力されます。BIOS シリアルリダイレクトは、このタイムアウト時間内に VSP キーストロークをインターセプトします。

アクション

10 秒のタイムアウト時間内に VSP 主導の選択のキーを押さないようにするか、または VSP への BIOS リダイレクトを無効にします。

スクロールとテキストが、BIOS リダイレクト中にイレギュラーに見える

症状

BIOS リダイレクト中にスクロールとテキストが正しく表示されません。ROM ベースのユーティリティでコマンドを入力すると、そのテキストがターミナルウィンドウの最下行で上書きされることがあります。

原因

BIOS は、固定長の 80x24 文字ウィンドウを予期して制御します。シリアルポートにリダイレクトした場合も、BIOS は依然として固定長の 80x24 文字ウィンドウを予期して制御します。VSP クライアント（SSH、HyperTerminal、または他のターミナルエミュレーター）がウィンドウのサイズを 80x24 以外に変更できる場合は、スクロール機能で混乱が生じ、出力が正しく表示されません。

アクション

ターミナルエミュレーターのウィンドウサイズを正確に 80x24 文字に構成してください。

リモートサポートの問題

Insight RS 登録中の SSL Bio エラー

症状

サーバーを Insight Remote Support Central Connect に登録しようとすると、「`SSL Bio Error`」というエラーが発生する場合があります。

アクション

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。

   リセットを使用しても構成は変化しませんが、iLO とのアクティブな接続が終了し、実行中のファームウェア更新が完了します。iLO をリセットするには、iLO 設定権限が必要です。
3. リセットが終了したら、iLO の Web インターフェイスにログインし、登録手順を再実行します。

Insight Online または Insight RS でサーバー名によってサーバーが識別されない

症状

Insight Online または Insight RS でサーバーが<サーバー名>として識別されない。ただし、Insight Online では<製品名>_<シリアル番号>として、Insight RS では<シリアル番号>として識別される。

原因

iLO がサーバー名を検出する前に、サーバーがリモートサポートに登録されていました。

アクション

1. 次のいずれかを実行します。
   - AMS が有効であり、オペレーティングシステムが実行されていることを確認します。
   - iLO Web インターフェイスの**アクセス設定**ページで、サーバー名を更新します。
   - Windows システムのみ : 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。
2. 手順 1 を実行したときにアクティブな Insight Online セッションがあった場合は、更新ボタンをクリックして Insight Online の表示をそのサーバーの情報に更新します。

サーバーの OS 名とバージョンが Insight RS または Insight Online に表示されない

症状

サーバーの OS 名とバージョンが Insight RS または Insight Online に表示されません。

原因

OS および AMS が実行されていないときにサーバーがリモートサポートに登録されました。このような状況では、iLO はどの OS がインストールされているかを判別できません。OS 情報を更新するには、iLO は AMS から OS 情報を取得する必要があります。

アクション

1. 以下の点を確認します。

- AMS が有効であり、OS が実行されている。
- Insight Remote Support Central Connect のみ : Insight RS のサポートされるバージョンがホストサーバーにインストールされている。詳しくは、**http://www.hpe.com/support/InsightRS-Support-Matrix** を参照してください。
- Insight Remote Support Central Connect のみ：サーバーの RIBCL 認証情報が Insight RS Console で入力され、ProLiant サーバーに関連付けられている。

2. iLO Web インターフェイスの**データ収集**ページで、データ収集プロセスを開始します。手順については、データ収集情報の送信(214 ページ)を参照してください。データ収集プロセスで、OS 名とバージョンが Insight RS と Insight Online に転送されます。
3. 前の手順を実行したときにアクティブな Insight Online セッションがあった場合は、更新ボタンをクリックします。

   AMS がインストールされていて、最新のデータ収集送信中に OS が実行されていた場合は、OS 名とバージョンが Insight Online の**デバイス構成の詳細**ページに表示されます。

Insight Online Direct Connect に登録中の接続エラー

症状

サーバーを Insight Online Direct Connect に登録しようとすると、次のエラーが発生します。`Cannot connect to remote host.`（リモートホストに接続できません。）

原因

iLO で DNS 設定が正しく構成されていません。

アクション

iLO で DNS 情報が正しく構成されていることを確認します。

iLO Insight Online Direct Connect 登録中に iLO セッションが予期せず終了する

症状

サーバーを Insight Online Direct Connect に登録しようとすると、セッションが失効しましたのエラーが発生して、iLO Web インターフェイスセッションが予期せず終了します。

原因

iLO で DNS 設定が正しく構成されていません。

アクション

DNS 設定が正しく構成されていることを確認します。

Insight RS または Insight Online でサーバーのヘルスステータスが赤色になる

症状

Insight RS または Insight Online では、リモートサポートに登録されているサーバーが赤色のステータスで表示されます。

原因

サーバー保証の期限が切れています。

アクション

リモートサポートを受けるには、有効な契約または保証が必要です。

保証の期限が切れた後でも、引き続き iLO の機能を使用してサーバーを監視および管理できます。

Insight Online または Insight RS でサーバー名によってサーバーが識別されない

症状

Insight Online または Insight RS でサーバーが<サーバー名>として識別されない。ただし、Insight Online では<製品名>_<シリアル番号>として、Insight RS では<シリアル番号>として識別される。

原因

iLO がサーバー名を検出する前に、サーバーがリモートサポートに登録されていました。

アクション

1. 次のいずれかを実行します。
   - AMS が有効であり、オペレーティングシステムが実行されていることを確認します。
   - iLO Web インターフェイスの**アクセス設定**ページで、サーバー名を更新します。
   - Windows システムのみ : 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。
2. 手順 1 を実行したときにアクティブな Insight Online セッションがあった場合は、更新ボタンをクリックして Insight Online の表示をそのサーバーの情報に更新します。

リモートサポートデータが Hewlett Packard Enterprise に送信されたときにサーバー情報が上書きされる

症状

データが Hewlett Packard Enterprise に送信されたときに Insight RS と Insight Online でサーバー情報が上書きされます。

原因

サーバーが Central Connect と Direct Connect の両方のリモートサポートに登録されており、データ収集情報が 2 つの異なる通信パスから Hewlett Packard Enterprise に送信されています。

アクション

- Insight Remote Support Central Connect を引き続き使用するには、Insight Online Direct Connect からサーバーを登録解除し、Insight RS ホストサーバーでサーバーを再検出します。
- Insight Online Direct Connect を引き続き使用するには、Insight Remote Support 管理対象デバイス構成ガイドに説明されているとおりに、Insight Remote Suport Central Connect からサーバーを登録解除します。

詳しくは

Insight Online Direct Connect からの登録の解除(209 ページ)
Insight Remote Support Central Connect の登録解除(210 ページ)

OS 情報が Insight Online に正しく表示されない

症状

OS 情報が Insight Online デバイスページの上部に表示されますが、デバイスの**設定**セクションには**不明**として表示されます。

アクション

Insight Online の更新ボタンをクリックします。

システムボードを交換したサーバーで、Insight Online Direct Connect が動作を停止する

症状

Insight Online Direct Connect に登録されたサーバーのシステムボードを交換したら、リモートサポート接続が動作しなくなります。

原因

サーバーのシステムボードが交換され、サーバーが Insight Online で認識されなくなっています。

アクション

1. サーバーを再登録します。
   a. システム RBSU または UEFI システムユーティリティを使用してシステム製品番号とシリアル番号を SMBIOS にプログラムします。

      詳しくは、ROM ベースの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。
   b. 新しいリモートサポート登録の場合と同様にサーバーを登録します。

Central Connect デバイスの重複レコードが Insight Online に存在する

症状

同じ Central Connect デバイスが 2 回検出されると、Insight Online に重複レコードが作成されます。

原因

以下の場合に、Insight Online にデバイスの重複レコードが作成される可能性があります。

- Insight RS がデバイスについて、以下のような不完全な詳細を検出しました。OS とネットワークの情報は検出されたましたが、シリアル番号または製品番号が検出されませんでした。Insight RS がデバイスを再検出すると、そのデバイスに関する情報の完全なセットが取得されます。
- デバイスの SNMP トラップ転送がホストサーバーに設定されていて、Insight RS がデバイスを検出する前に、ホストサーバーがイベントを受信しました。

アクション

なし。この時点では、重複したレコードを削除できません。

デバイスの無償保証が Insight RS に期限切れとして不正に表示される

症状

有効な無償保証を備えたデバイスが Insight RS で期限切れの保証として表示されます。

解決方法 1

原因

ホスティングデバイスセットアップウィザードの**サイト情報**ページで、無効な情報が入力されました。

アクション

サイト情報ページで有効な情報を入力したことを確認します。

解決方法 2

原因

HPE パスポートアカウントに国名/地域名が入力されていません。

アクション

国名/地域名を含めるように HPE パスポートアカウントを更新します。

サービスイベントおよび収集が Insight RS Console に不正なタイムスタンプを表示する

症状

イベント時間とイベント処理時間との間に矛盾があります。

原因

監視対象デバイスの時間またはタイムゾーンの設定が正しくありません。

Insight RS Console でサービスイベントおよび収集を表示すると、表示されている時間はブラウザーに設定されているタイムゾーンに変換されます。この機能により、ユーザーは自身のローカルタイムゾーンを使用してイベントのタイミングを参照することができます。

アクション

監視対象デバイスの時間およびタイムゾーンの設定を確認します。タイムゾーンがタイムサーバーまたは DHCP を使用して設定されている場合は、そのタイムサーバーまたは DHCP が正しく構成されていて、適切な時間に設定されていることを確認します。

ホストサーバーの時間は参照として使用されるため、この問題は Hewlett Packard Enterprise または Hewlett Packard Enterprise 認定サービスパートナーによって提供されるサービスには影響しません。

iLO 連携の問題

iLO 連携ページでクエリエラーが発生する

症状

iLO 連携ページを開いたときに、iLO ピアおよび関連付けられたデータがページに表示されないことがあり、次のエラーが表示されます。

```
Errors occurred during query, returned data may be incomplete or inconsistent.
```

原因

このエラーはネットワーク通信エラー、構成の問題、または障害が発生した iLO システムによって、iLO 連携グループ内のすべてのシステムからデータを取得できないときに発生することがあります。

アクション

- 構成済みの**マルチキャストアナウンスメント間隔**の 2 倍待ってから、iLO 連携ページを更新します。

  iLO システムが再構成され、ローカル iLO システムと通信できない場合は、期限が切れた後でピア関係から削除されます。

- **マルチシステムマップ**ページのエラーを確認します。

  このページでは、iLO ピア間の通信の問題を識別することができます。

- BladeSystem 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 Web インターフェイスの**エンクロージャー設定** > **ネットワークアクセス** > **プロトコル**ページで、**エンクロージャー iLO 連携サポート**が構成されているか確認します。

  Onboard Administrator 4.11 以降では、この設定を構成していなければなりません。

  これは、エンクロージャー内のサーバーブレード間でのピアツーピア通信を許可するために必要です。

- ネットワーク内のスイッチが iLO ピア間で通信できるように構成されていることを確認します。

- iLO ピアのネットワークルート、サブネットマスク、IP アドレス、または HTTP ポートを変更した場合、ピアがローカル iLO システムへの通信パスを持っていることを確認します。

- ローカルの iLO システムとエラーが発生したピアとの間に通信パスが存在することを確認します。

  中間のファイアウォール、または iLO ネットワーク構成や HTTP ポート設定の変更により、ローカルの iLO システムとピア間の通信がブロックされる可能性があります。

iLO のマルチシステムマップページにタイムアウトエラーが表示される

症状

マルチシステムマップページに、ローカル iLO システムのピアに対する `Timed Out` エラーが表示されます。

原因

このエラーは、次の状況で発生する可能性があります。

- ローカル iLO システムのピアに障害のあるピアがある。
- 中間のファイアウォールによってローカル iLO システムとピア間の通信が妨害されている。
- ネットワーク構成の変更によってローカル iLO システムとピア間の通信が妨害されている。
- ピアが搭載されているエンクロージャーが、iLO 連携をサポートするように構成されていない。

アクション

- 障害が発生したピアを削除するか修復します。
- ネットワークが iLO ピアの間で通信できるように構成されていることを確認します。
- Onboard Administrator Web インターフェイスの**エンクロージャー設定** > **ネットワークアクセス** > **プロトコル**ページで、iLO サーバーブレードピアを含むエンクロージャーが iLO 連携サポートに構成されていることを確認します。

  Onboard Administrator 4.11 以降では、この設定を構成していなければなりません。これは、エンクロージャー内のサーバーブレード間でのピアツーピア通信を許可するために必要です。

iLO マルチシステムマップページに 502 エラーが表示される

症状

マルチシステムマップページで 502 エラーが表示されます。

原因

一覧表示されているピアがローカル iLO システムからの要求を拒否しました。

アクション

ローカルの iLO システムとエラーが発生したピアとの間に通信パスが存在することを確認します。

中間のファイアウォール、または iLO ネットワーク構成や HTTP ポート設定の変更により、ローカルの iLO システムとピア間の通信がブロックされる可能性があります。

iLO マルチシステムマップページに 403 エラーが表示される

症状

マルチシステムマップページで 403 禁止/認証エラーが表示されます。

原因

ローカル iLO システムのグループキーとピア iLO システムのグループキーが一致しません。

アクション

選択したグループのメンバーになっているすべての iLO システムのグループキーが一致することを確認してください。

iLO ピアが iLO 連携ページに表示されない

症状

iLO ピア（ローカル iLO システムと同じグループ内のシステム）が iLO 連携ページに表示されていません。

アクション

- 選択したグループのメンバーになっているすべての iLO システムのグループキーが一致することを確認してください。
- 構成済みのマルチキャスト間隔の 2 倍待ってから、iLO 連携ページを更新します。

  iLO システムが再構成され、ローカル iLO システムと通信できない場合は、期限が切れた後でピア関係から削除されます。
- 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 Web インターフェイスの**エンクロージャー設定** > **ネットワークアクセス** > **プロトコル**ページで、**エンクロージャー iLO 連携サポート**が構成されているか確認します。

  Onboard Administrator 4.11 以降では、この設定を構成していなければなりません。これは、エンクロージャー内のサーバーブレード間でのピアツーピア通信を許可するために必要です。
- ネットワーク内のスイッチが iLO ピア間で通信できるように構成されていることを確認します。
- ローカルの iLO システムとエラーが発生したピアとの間に通信パスが存在することを確認します。

  中間のファイアウォール、または iLO ネットワーク構成や HTTP ポート設定の変更により、ローカルの iLO システムとピア間の通信がブロックされる可能性があります。

iLO のピアが、IPv4 ネットワーク上で IPv6 アドレスで表示される

症状

IPv4 ネットワーク上の iLO ピアが iLO 連携ページに IPv6 アドレスで表示されます。

アクション

iLO 専用ネットワークポート IPv6 ページまたは **iLO 共有ネットワーク 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**チェックボックスが選択されていないことを確認します。

ファームウェアの問題

iLO ファームウェアの更新が失敗する

症状

iLO ファームウェアを更新しようとすると次の問題が発生します。

- iLO ファームウェアが応答していません。
- iLO がファームウェア更新要求を受け入れませんでした。
- iLO ファームウェアの更新は、更新が完了する前に停止しました。

解決方法 1

原因

通信またはネットワークの問題が発生しました。

アクション

1. iLO に Web ブラウザー経由で接続を試みます。接続できない場合は、通信に問題があります。
2. iLO に対して ping を実行します。成功する場合、ネットワークは動作しています。
3. ファームウェアアップデートを再度実行してください。

解決方法 2

アクション

別のファームウェアアップデート方法を試してください。

iLO ファームウェア更新エラー

症状

iLO は、ファームウェアを更新する最後の試行が失敗したことを通知します。

原因

iLO ファームウェアの更新で間違ったファイルを使用しました。

アクション

フラッシュプロセスをリセットするには、🗑をクリックして正しいファームウェアファイルでファームウェアの更新を再び実行します。

エラーをクリアしないと、正しいファームウェアファイルを使用しても、同じエラーが発生する場合があります。

iLO ファームウェアアップデートが終了しない

症状

iLO ファームウェアアップデートが 1%完了のままで終了しません。

原因

iLO Web インターフェイスが応答を停止しました。

アクション

1. ブラウザーウィンドウを更新します。
2. iLO ファームウェアアップデートを再度実行してください。

iLO ネットワークのフラッシュエラーリカバリ

ほとんどのファームウェアアップグレードは、正常に終了します。万一、iLO ファームウェアのアップグレード時にサーバーの電源が切れた場合でも、iLO は、電源が再投入されたときに復旧することができます。

iLO が起動すると、起動コードは、メインイメージのイメージ検証を実行します。イメージが破損しているか不完全で、セキュアリカバリ機能で自動的に復元できない場合、iLO はフラッシュエラーリカバリモードになります。フラッシュエラーリカバリにより、iLO 内の FTP サーバーがアクティブになります。この FTP サーバーを使用すると、プログラミングのためにイメージを iLO に送信できます。FTP サーバーは、他のサービスを提供しません。

この機能は、iLO が製品セキュリティ状態または FIPS 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にのみ使用できます。

ネットワーククライアントは、FTP サーバーに接続できます。接続のためのユーザー名は **test**、パスワードは **flash** です。ファームウェアイメージを iLO に送信するには、FTP クライアントの `PUT` コマンドを使用します。イメージを受信すると、iLO は、イメージを検証します。イメージが、署名された完全で有効なファームウェアイメージであれば、カーネルは、フラッシュパーティションのプログラミングを開始します

フラッシュパーティションにイメージがプログラミングされたら、iLO は自動的にリセットされます。

例：

```
F:\ilo>ftp 192.168.1.2
Connected to 192.168.1.2.
220 FTP Recovery server ready.
User (192.168.1.2:(none)): ftp
331 Password required.
Password:
231 Logged in.
ftp> put iLO.bin
200 Ok.
150 ready for file
226-Checking file
226-File acceptable
226-Flashing   3% complete
226-Flashing   4% complete
226-Flashing   6% complete
.
.
.
226-Flashing  97% complete
226-Flashing  99% complete
226-Flashing 100% complete
226-Flashing completed
226 Closing file
ftp: 8388608 bytes sent in 1.38Seconds 6100.81 Kbytes/sec.
ftp> quit
```

詳しくは

サーバーの電源オン(161 ページ)

iLO によるシステム ROM（BIOS）失敗のレポート

症状

システム ROM（BIOS）のステータスが失敗です。

このステータスがレポートされると、次のようになります。

- **iLO 概要**ページの**システムヘルス**ステータスは**クリティカル**です。
- **ヘルスサマリー**ページの **BIOS/ハードウェアヘルス**ステータスは**失敗**です。
- **ファームウェア検証**ページで、**システム ROM** の**ヘルス**は**クリティカル**で、**ステータス**が**障害/オフライン**です。
- イベントが IML に記録されます。

解決方法 1

アクション

1. ファームウェア検証機能が自動修復向けに構成されている場合は、システムの修復が完了するまで待機します。

   構成によっては、修復アクションによって、アクティブ ROM が冗長 ROM と置き換えられるか、リカバリセット（利用可能な場合）からシステム ROM ファームウェアが再インストールされる場合があります。

2. 修復が正常に完了したことを確認するには、**ファームウェア検証**ページを確認します。

解決方法 2

アクション

1. ファームウェア検証機能が自動修復向けに構成されていない場合は、手動で**アクティブなシステム ROM を冗長なシステム ROM と置き換えます**。
2. 修復が正常に完了したことを確認するには、**ファームウェア検証**ページを確認します。

解決方法 3

アクション

1. ファームウェア検証機能が自動修復向けに構成されていない場合は、手動で**システム ROM ファームウェアを再インストールします**。
2. 修復が正常に完了したことを確認するには、**ファームウェア検証**ページを確認します。

iLO による無効なファームウェアコンポーネントの検出

症状

インストールされたファームウェアコンポーネントで、失敗ステータスが報告されている。

注記:

このトピックは、システム ROM 以外のファームウェアタイプ用です。障害が発生したシステム ROM コンポーネントについては、**iLO によるシステム ROM（BIOS）失敗のレポート**(441 ページ)を参照してください。

このステータスが発生すると、以下のようになります。

- **iLO 概要**ページの**システムヘルス**ステータスは**クリティカル**です。
- **ヘルスサマリー**ページの **BIOS/ハードウェアヘルス**ステータスは**失敗**です。
- **ファームウェア検証**ページで、ファームウェアコンポーネントの**ヘルス**は**クリティカル**で、**ステータス**が**障害/オフライン**です。
- イベントが IML に記録されます。

解決方法 1

アクション

1. ファームウェア検証機能が自動修復向けに構成されている場合は、システムの修復が完了するまで待機します。
2. 修復が正常に完了したことを確認するには、**ファームウェア検証**ページを確認します。

解決方法 2

アクション

1. ファームウェア検証機能が自動修復向けに構成されていない場合は、手動で**影響を受けるファームウェアを再インストールします**。
2. 修復が正常に完了したことを確認するには、**ファームウェア検証**ページを確認します。

ライセンス問題

ライセンスキーインストールエラー

症状

ライセンスキーエラーまたはライセンスのインストールに失敗しましたメッセージが表示されます。

解決方法 1

原因

キーが iLO ライセンスキーではありません。

アクション

iLO ライセンスキーを入手し、もう一度やり直してください。

解決方法 2

原因

正規のライセンスがすでにインストールされた状態で、評価キーが送信されました。

アクション

なし。iLO は、正規のキーがすでにインストールされている場合、評価キーのインストールをサポートしません。

解決方法 3

原因

iLO の日時設定が不適切です。

アクション

iLO の日時設定を確認し、もう一度やり直してください。

解決方法 4

原因

入力したライセンスキーが間違っています。

アクション

ライセンスキーのエラーをチェックし、もう一度やり直してください。

仮想メディアまたはグラフィックリモートコンソールにアクセスできない

症状

仮想メディアおよびグラフィックリモートコンソール機能が使用できません。

原因

iLO の仮想メディアおよびグラフィックリモートコンソール機能は、オプションの iLO ライセンスをインストールすることによって有効にします。ライセンスがインストールされていない場合は、ライセンスがないとこれらの機能を使用できないことを示すメッセージが表示されます。

アクション

これら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。

iLO ライセンスキーのリカバリ

症状

以前にライセンスが適用されていた iLO システムにライセンスが付与されておらず、ライセンスキーのリカバリと再インストールが必要です。

解決方法 1

原因

iLO は工場出荷時のデフォルト設定に設定されていましたが、システムボードが交換されたか、ライセンスキーが誤って置き換わりました。

アクション

バックアップファイルからライセンスキーと他の構成情報を復元します。

1. ナビゲーションツリーで**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。

解決方法 2

アクション

交換キーを取得します。

詳しくは、Web サイト（**http://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。

Agentless Management、AMS、および SNMP の問題

AMS がインストールされているのに、iLO で使用できない

症状

AMS がサーバーにインストールされているのに、iLO の Web インターフェイスで**利用不可**と表示されます。

アクション

1. AMS がインストールされていることを確認します。
2. AMS を再起動します。
3. iLO をリセットします。

HPE SIM から SNMP 情報を取得できない

症状

HPE SIM が iLO から転送された SNMP 情報を受信しません。

原因

iLO と管理 PC が同じサブネット上に存在しません。

アクション

1. 管理 PC から iLO に Ping を送信して、iLO と管理 PC が同じサブネット上に存在することを確認します。
2. Ping が正常に送信されない場合は、ネットワーク構成を修正してください。

iLO から HPE SIM のアラーム（SNMP トラップ）を受信できない

症状

HPE SIM が iLO から SNMP トラップを受信しません。

アクション

1. iLO 設定権限を持つユーザーアカウントを使用して iLO にログインします。
2. **マネジメント - SNMP 設定**ページで、アラートタイプと SNMP トラップのパラメーターを構成します。

Web サイト

全般的な Web サイト

Hewlett Packard Enterprise Information Library

http://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

http://www.hpe.com/jp/servers/ilo

iLO 5 Information Library

http://www.hpe.com/support/ilo-docs

iLO サポート

http://www.hpe.com/support/ilo5

iLO Advanced

http://www.hpe.com/servers/iloadvanced

iLO Advanced Premium Security Edition

http://www.hpe.com/servers/ilopremium

iLO Mobile アプリケーション

http://www.hpe.com/info/ilo/mobileapp

アクティブヘルスシステムビューア

http://www.hpe.com/servers/ahsv

Intelligent System Tuning

http://www.hpe.com/info/ist

HPE ProLiant Gen10 サーバー

http://www.hpe.com/info/proliantgen10-docs

HPE ProLiant Gen 10 および HPE Synergy コンピュートモジュールのトラブルシューティング

http://www.hpe.com/info/Gen10-troubleshooting

UEFI システムユーティリティ

http://www.hpe.com/info/ProLiantUEFI/docs

SUM

http://www.hpe.com/info/sum-docs

SPP

http://www.hpe.com/info/spp/documentation

Intelligent Provisioning

http://www.hpe.com/info/intelligentprovisioning/docs

iLO RESTful API および RESTful インターフェイスツール

http://www.hpe.com/info/redfish

リモートサポート

http://www.hpe.com/info/insightremotesupport/docs

HPE OneView

http://www.hpe.com/info/oneview/docs

OA

http://www.hpe.com/support/oa/docs

HPE SIM

http://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。

  http://www.hpe.com/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。

  http://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

  http://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

  http://www.hpe.com/support/downloads

  Software Depot

  http://www.hpe.com/support/softwaredepot

- 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。

http://www.hpe.com/support/e-updates-ja

- お客様の資格を表示したりアップデートしたり、契約や保証をお客様のプロファイルにリンクしたりするには、Hewlett Packard Enterprise サポートセンターの **More Information on Access to Support Materials** ページにアクセスします。

  http://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。

カスタマーセルフリペア（CSR）

Hewlett Packard Enterprise カスタマーセルフリペア（CSR）プログラムでは、ご使用の製品をお客様ご自身で修理することができます。CSR 部品を交換する必要がある場合、お客様のご都合のよいときに交換できるよう直接配送されます。一部の部品は CSR の対象になりません。Hewlett Packard Enterprise もしくはその正規保守代理店が、CSR によって修理可能かどうかを判断します。

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 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

http://www.hpe.com/services/proactivecareadvancedsupportedproducts

保証情報

ご使用の製品の保証または*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*に関するドキュメントを確認するには、「エンタープライズの安全性、規制への適合」の Web サイトを参照してください。

http://www.hpe.com/support/Safety-Compliance-EnterpriseProducts

追加保証情報

HPE ProLiant と x86 サーバーおよびオプション

http://www.hpe.com/support/ProLiantServers-Warranties

HPE エンタープライズサーバー

http://www.hpe.com/support/EnterpriseServers-Warranties

HPE ストレージ製品

http://www.hpe.com/support/Storage-Warranties

HPE ネットワーク製品

http://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。

http://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。

http://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。

http://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。

http://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。この電子メールには、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。