



Hewlett Packard
Enterprise

HPE ProLiant Gen10、ProLiant Gen10 Plusサーバー、およびHPE Synergy用UEFIシステムユーティリティユーザーガイド

部品番号: 30-293E3364-105-ja-JP
発行: 2021年11月
版数: 1

HPE ProLiant Gen10、ProLiant Gen10 Plusサーバー、およびHPE Synergy用UEFIシステムユーティリティユーザーガイド

摘要

このガイドでは、すべてのHPE ProLiant Gen10サーバー、ProLiant Gen10 Plusサーバー、およびHPE SynergyコンピュータモジュールのシステムROMに内蔵されているUnified Extensible Firmware Interface (UEFI) にアクセスして使用する方法について詳しく説明します。このガイドでは、BIOSプラットフォーム構成メニューのUEFIとレガシーBIOS両方のオプションを使用する方法について説明します。このメニューは以前、ROMベースセットアップユーティリティ (RBSU) として知られていたものです。すべてのオプションとあり得る応答が定義されています。このガイドは、サーバーおよびストレージシステムのインストール、管理、トラブルシューティングの担当者を対象としています。

部品番号: 30-293E3364-105-ja-JP

発行: 2021年11月

版数: 1

© Copyright 2017, 2021 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。Intel[®]、インテル、Itanium[®]、Pentium[®]、Intel Inside[®]、およびIntel Insideロゴは、インテルコーポレーションまたはその子会社のアメリカ合衆国およびその他の国における商標または登録商標です。

UEFI[®]はUEFI Forum, Inc. の登録商標です。

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。

目次

- はじめに
 - UEFIシステムユーティリティ
 - UEFIの概要
 - UEFIシステムユーティリティの概要
 - システムユーティリティの起動
 - システムユーティリティ内での移動
 - GUIモードでのシステムユーティリティ内での移動
 - UEFIシステムユーティリティGUI
 - システムユーティリティのキーの機能
 - 再起動が必要な場合
 - システムユーティリティメニューの概要
 - 共通のセットアップおよび構成に関するFAQ
 - ファームウェアまたはシステムROMのアップデート
- システムユーティリティメインメニューのオプション
 - システム構成
 - システム構成メニューオプション
 - BIOS/プラットフォーム構成 (RBSU)
 - iLO 5構成ユーティリティの使用
 - iLO 5構成ユーティリティオプション
 - ネットワークオプション
 - ネットワークオプションの構成
 - アドバンスドネットワークオプション
 - アドバンスドネットワークオプションの構成
 - ユーザー管理
 - ユーザーの追加
 - 新しいユーザーアカウントの追加
 - ユーザーの編集/削除
 - ユーザーアカウントの編集または削除
 - 設定オプション
 - アクセス設定の構成
 - 工場出荷時のデフォルトにセット
 - iLOの工場出荷時デフォルト設定へのリセット
 - iLOのリセット
 - iLOのアクティブな接続のリセット
 - バージョン情報
 - iLOに関する情報の表示
 - 内蔵デバイス情報の表示と構成
 - コントローラー情報の表示
 - コントローラー設定の構成
 - コントローラー設定の変更
 - 高度なコントローラー設定の変更
 - コントローラー構成の消去
 - バックアップ電源ステータスの表示
 - 電源設定の管理
 - アレイの構成
 - UEFIシステムユーティリティを使用したアレイの作成
 - 論理ドライブプロパティの表示

- 論理ドライブの作成
 - スペアドライブの割り当て
 - スペアドライブの削除
 - デバイスの確認
 - アレイの削除
 - 論理ドライブの編集
 - 論理ドライブの削除
- ディスクユーティリティ
 - ディスクデバイス情報の表示
 - ディスクデバイスの確認
- レガシーブートモード用のブート可能デバイスの設定
 - プライマリおよびセカンダリブート可能デバイスの設定（レガシーブートモード）
 - OSブート可能ドライブの数の設定（レガシーブートモード）
- NICおよびFCoE設定の表示と構成
- ワンタイムブートメニュー
 - ワンタイムブートメニューオプション
 - ワンタイムブートのオプションの選択
- 内蔵アプリケーション
 - 内蔵UEFIシェルの起動
 - インテグレートッドマネジメントログの表示および消去
 - Active Health Systemデータのダウンロード
 - Active Health Systemログのダウンロード
 - アクティブヘルスシステムビューアにログインする
 - AHSVへのAHSログのアップロード
 - 内蔵Diagnostics
 - 内蔵Diagnosticsの起動
 - Intelligent Provisioningの起動
 - 内蔵iPXEの起動
- システム情報およびシステムヘルス
 - システム情報
 - システム情報の表示
 - システムヘルスの表示
- システムの再起動、言語の選択、およびブラウザーモードの設定
 - システムの再起動
 - システムを終了して再起動
 - システムの再起動
 - 言語とブラウザーモードの選択
 - システム言語の選択
 - ブラウザーモードの選択
- BIOS/プラットフォーム構成オプション
 - このバージョンの新機能
 - ワークロードプロファイルとパフォーマンスオプション
 - Workload Matching
 - ワークロードプロファイルの依存関係の概要
 - インテル(R) Xeon(R) スケーラブルプロセッサのワークロードプロファイルの依存関係
 - 第1世代および第2世代AMD EPYC(TM) プロセッサのワークロードプロファイルの依存関係
 - ワークロードプロファイルの適用
 - プロファイルの適用後の依存オプションの変更
- システムオプションの変更

- ブート時間最適化の構成
 - 動的消費電力上限機能の設定
 - 拡張メモリテストの有効化または無効化
 - メモリファーストトレーニングの有効化または無効化
 - UEFI POST検出モードの設定
 - ウォームリセット時のメモリ消去の有効化または無効化
- シリアルポートオプションの構成
 - 内蔵シリアルポートの割り当て
 - 仮想シリアルポートの割り当て
 - USBポートへのシリアルコンソールのミラーリング
- USBオプションの構成
 - USB制御の設定
 - USBブートサポートの有効化または無効化
 - 取り外し可能フラッシュメディアブート順序の選択
 - 内部SDカードスロットの有効化または無効化
- IOSシリアルコンソールとEMSの構成
 - BIOSシリアルコンソールポートの有効化または無効化
 - BIOSシリアルコンソールエミュレーションモードの選択
 - BIOSシリアルコンソールボーレートの設定
 - EMSコンソールポート設定の構成
- サーバー可用性の構成
 - ASRの有効化または無効化
 - ASRタイムアウトの設定
 - ウェイクオンLANの有効化または無効化
 - POST F1プロンプトの遅延の設定
 - 電源ボタンを一瞬押す機能の有効化または無効化
 - 自動電源オン時の状態の設定
 - 電源投入遅延の設定
 - POST ASRの設定
 - POST ASRタイマーの設定
 - IPMIウォッチドッグタイマーの有効化または無効化
 - IPMIウォッチドッグタイマーのタイムアウトの設定
 - IPMIウォッチドッグタイマーのポリシーの設定
- サーバー資産情報の表示および入力
 - サーバー情報の入力
 - 管理者情報の入力
 - サービスコンタクト情報の入力
 - カスタムPOSTメッセージの入力
- プロセッサオプションの変更
 - インテルハイパースレッディングの有効化または無効化
 - インテルSGX制御オプションの構成
 - 有効にするプロセッサコアの数の設定
 - プロセッサx2APICサポートの有効化または無効化
 - AMD同時マルチスレッド (SMT) の有効化
 - Performance Determinismオプションの構成
 - AMDページテーブルエントリーの投機的ロックスケジューリングオプションの選択
- メモリオプションの変更
 - メモリの再マップの構成
 - アドバンスドメモリプロテクションの構成

- メモリリフレッシュレートの構成
- DRAMバーストリフレッシュモードの構成
- チャネルインターリーブの有効化または無効化
- IMCインターリーブの構成
- AMDインターリーブの構成
- Memory Interleave Sizeの設定
- Memory PStatesの有効化または無効化
- AMD 1TB再マップの構成
- AMD定期的ディレクトリリンスの構成
- 最大メモリバス周波数の設定
- メモリ巡回スクラビングの有効化または無効化
- ノードインターリーブの有効化または無効化
- AMDセキュアメモリ暗号化の構成
- 透過的セキュアメモリ暗号化の有効化または無効化
- メモリミラーリングモードの構成
- 便宜的セルフリフレッシュの構成
- 不揮発性メモリの構成
 - UEFIシステムユーティリティを使用したネームスペースの作成
 - HPE Persistent Memoryモジュールパスワードの変更
 - HPE Persistent Memoryモジュールステータスの表示
 - UEFIシステムユーティリティを使用したパフォーマンスオプションの変更
 - UEFIシステムユーティリティを使用したサニタイズ
 - キー管理モードの変更
 - キー管理の無効化
 - HPE Persistent Memoryモジュールの暗号化の無効化
- NVDIMM-Nオプションの構成
 - NVDIMM-Nサポート
 - 次回の再起動時のポリシーにNVDIMM-Nサニタイズ/消去
 - NVDIMM-Nインターリーブング
- メモリ構成違反レポートの有効化または無効化
- トータルメモリ暗号化（TME）の有効化または無効化
- 仮想化オプションの変更
 - 仮想化テクノロジーの有効化または無効化
 - インテルVT-dの有効化または無効化
 - アクセス制御サービスの有効化または無効化
 - SR-IOVの有効化または無効化
 - 最小のSEV ASIDの設定
 - 最大のSEV ASIDの設定
 - AMD仮想化オプションの有効化
 - AMD仮想化テクノロジーの有効化
 - AMD DMA再マッピングの有効化または無効化
- ブートオプションの変更
 - ブートモードの選択
 - UEFI最適化ブートの有効化または無効化
 - ブート順序ポリシーの設定
 - UEFIブート順序リストの変更
 - UEFIブート順序の制御
 - UEFIブート順序リストへのブートオプションの追加
 - UEFIブート順序リストからのブートオプションの削除

- レガシーBIOSブート順序リストの変更
- ネットワークオプションの変更
 - ネットワークブートオプション
 - プリブートネットワーク環境の設定
 - IPv6 DHCPユニーク識別子の方式の設定
 - ネットワークブートリトライサポートの有効化または無効化
 - NICのネットワークブートの有効化または無効化
 - PCIeスロットネットワークブートの有効化または無効化
 - HTTPサポートの設定
 - iSCSIポリシー（Gen10）またはソフトウェアイニシエーター（Gen10 Plus）の有効化
 - プリブートネットワーク設定の構成
 - プリブートネットワーク設定
 - URLからのブートの前提条件
 - iSCSIブート構成
 - iSCSIイニシエーター名の追加
 - iSCSIブート試行の追加
 - iSCSIブート試行の削除
 - iSCSIブート試行の詳細の表示および変更
 - VLANの構成
 - 内蔵iPXEオプションの変更
 - 内蔵iPXEの有効化または無効化
 - UEFIブート順序リストへの内蔵iPXEの追加
 - 内蔵iPXE起動スクリプトの自動実行の有効化または無効化
 - 内蔵iPXEスクリプト検証の有効化または無効化
 - 内蔵iPXE起動スクリプトロケーションの設定
 - 内蔵iPXE自動起動スクリプトのネットワーク上の場所の設定
- ストレージオプションの変更
 - 内蔵チップセットSATAコントローラーサポートの有効化
 - SATAセキュア消去の有効化
 - SATAサニタイズの有効化
 - 内蔵ストレージブートポリシーの設定
 - PCIeストレージブートポリシーの設定
 - デフォルトのファイバーチャネル/FCoEスキャンポリシーの変更
 - 内蔵NVM ExpressオプションROMの有効化または無効化
 - インテル(R) CPU VMDサポートの構成
 - インテル(R) PCH VMDサポートの構成
 - インテル(R) VROCサポートの構成
 - NVM Expressドライブの撤去
 - ローカルおよびリモートキー管理のためのSEDドライブの構成
- 電力およびパフォーマンスオプションの変更
 - AMDパフォーマンスワークロードプロファイルの有効化または無効化
 - パワーレギュレーターモードの設定
 - PCIピアツーピア直列化の構成
 - I/Oダイレクトキャッシュの構成
 - 最小プロセッサアイドル電力コアC状態の設定
 - 最小プロセッサアイドル電力パッケージC状態の設定
 - AMDデータファブリックC状態の有効化または無効化
 - インテルターボブーストテクノロジーの有効化または無効化
 - AMDコアパフォーマンスブーストの構成

- AMD Fmaxブースト制限制御の有効化または無効化
- AMD Cステート効率モードの変更
- エネルギー/パフォーマンスバイアスの設定
- AMD Infinity Fabricのパフォーマンス状態の設定
- 協調電力制御の有効化または無効化
- AMD XGMI強制リンク幅の構成
- AMD XGMI最大リンク幅の構成
- インテルDMIリンク周波数の設定
- AMD優先IOバス番号の構成
- AMD NBIO LCLK DPMレベルの構成
- NUMAグループサイズ最適化の設定
- インテルPerformance Counter Monitorの有効化または無効化
- アンコア周波数のスケーリングの構成
- UPIバンド幅の最適化 (RTID) の設定
- Sub-NUMAクラスタリングの有効化または無効化
- エネルギー効率ターボオプションの有効化または無効化
- ローカル/リモートしきい値の設定
- LLCデッドラインの割り当ての設定
- 古くなったAからSへの設定
- プロセッサプリフェッチャーオプションの無効化
- I/Oオプションの有効化または無効化
 - ACPI SLITオプションの有効化
 - インテルNIC DMAチャネルの有効化
 - Topic name not available
- I/O非ポストプリフェッチの有効化または無効化
- アドバンストパフォーマンスチューニングオプションの構成
 - UPIへの送信オプションの設定
 - メモリチャネルモードの設定
 - 独立チャネルモード (非ロックステップ) の設定
 - パフォーマンス管理
 - パフォーマンス管理機能の要件
 - Jitter Smoothing
 - 自動プロセッサジッター制御モード
 - コアブースト
- アドバンスト電力オプションの構成
 - 冗長電源装置モードの設定
 - Infinity Fabricの電力管理の有効化または無効化
 - パッケージ電力制限制御モードの構成
- 内蔵UEFIシェルオプションの変更
 - 内蔵UEFIシェルの有効化または無効化
 - UEFIブート順序リストへの内蔵UEFIシェルの追加
 - 内蔵UEFIシェル起動スクリプトの自動実行の有効化または無効化
 - シェルスクリプト検証の有効化または無効化
 - 内蔵UEFIシェル起動スクリプトロケーションの設定
 - DHCPを使用した、シェル自動起動スクリプトの検出の有効化または無効化
 - シェル自動起動スクリプトのネットワーク上の場所の設定
- サーバーセキュリティ設定の変更
 - サーバーセキュリティのオプション
 - 電源投入時パスワード設定

- iLOアカウントでのログイン許可
- 管理者パスワードの設定
- セキュアブート
- セキュアブートの有効化または無効化
- サーバーロック設定の構成
 - サーバー構成ロックのセットアップ
- アドバンスドセキュアブートオプション
 - アドバンスドセキュアブートオプションの設定の表示
 - セキュアブート証明書キーまたはデータベース署名の登録
 - セキュアブート証明書キーまたはデータベース署名の削除
 - すべてのキーを削除
 - セキュアブート証明書キーまたはデータベース署名のエクスポート
 - すべてのセキュアブート証明書キーのエクスポート
 - セキュアブート認証キーまたはデータベース署名をプラットフォームのデフォルトにリセット
 - すべてのセキュアブート認証キーをプラットフォームのデフォルトにリセット
- TLS (HTTPS) オプション
 - TLS証明書の詳細の表示
 - TLS証明書の登録
 - TLS証明書の削除
 - すべてのTLS証明書の削除
 - TLS証明書のエクスポート
 - すべてのTLS証明書のエクスポート
 - すべてTLS設定をプラットフォームのデフォルトにリセット
 - 高度なTLSセキュリティ設定の構成
- Trusted Platform Moduleオプションの構成
 - TPM FIPSモード切替操作の設定
- アドバンスドセキュリティオプションの変更
 - プラットフォーム証明書サポートの有効化または無効化
 - iLOアカウントによるログインの有効化または無効化
 - バックアップROMイメージ認証の有効化または無効化
 - ワンタイムブートメニュー (F11プロンプト) の有効化または無効化
 - Intelligent Provisioning (F10プロンプト) の有効化または無効化
- Microsoft (R) Secured-coreサポートの有効化または無効化
- アドバンスドオプションの変更
 - ROMイメージの選択
 - 内蔵ビデオ接続の構成
 - 電源装置要件のオーバーライドの構成
 - 一貫性のあるデバイスの名前付けの有効化または無効化
 - 電源装置混在レポートの有効化または無効化
 - POSTビデオサポート設定の変更
 - プラットフォームのRASポリシーの構成
 - SCI RASのサポートの構成
 - 高精度イベントタイマー (HPET) ACPIサポートの有効化または無効化
 - UEFI電源装置要件の変更
 - 温度構成の設定
 - 高温シャットダウンの有効化または無効化
 - ファン設置要件のメッセージングの設定
 - ファン故障ポリシーの設定
 - 上昇した周囲温度のサポートの有効化または無効化

- シリアル番号の再入力
- 製品IDの再入力
- アドバンスドデバッグオプションの構成
- UEFIシステムユーティリティによるUEFIシリアル出力ログデータの取得
- インテルTXTサポートの有効化または無効化
- インテル(R)ソフトウェアガードエクステンションズ (SGX) の有効化または無効化
- SGXパッケージ情報のインバンドアクセスの有効化または無効化
- ワンタイムブートメニュー (F11プロンプト) の有効化または無効化
- Intelligent Provisioning (F10プロンプト) の有効化または無効化
- プロセッサAES-NIサポートの有効化または無効化
- バックアップROMイメージ認証の有効化または無効化
- PCIeデバイス構成オプションの変更
 - 高度なPCIeデバイス設定の選択
 - PCIe分岐オプションの構成
 - PCIe MCTPオプションの構成
 - NVMe PCIeリソースパディングの構成
 - 最大PCI Express速度の設定
 - GPU構成の設定
 - PCIeスロットからプロセッサへのマッピングの構成
 - PCIeデバイスの分離サポートの有効化または無効化
 - PCIeエラー制御の構成
 - 特定のPCIeデバイスの構成
- 日付と時刻の設定
- バックアップおよびリストア設定の変更
- システムデフォルトのリセット
 - システムデフォルト設定のリストア
 - 工場デフォルト設定のリストア
 - デフォルトのUEFIデバイス優先順位の変更
 - ユーザーデフォルトオプションの保存または消去
- スクリプトによる構成手順の使用
 - スクリプトによる構成手順
 - UEFI用のiLO RESTful APIサポート
 - Configuration Replicationユーティリティ (CONREP)
 - HPE Smart Storage Administrator (HPE SSA)
- トラブルシューティング
 - デバイスをブートできない
 - システムデフォルトを復元できない
 - ネットワークブートURLのファイルをダウンロードできない
 - ダウンロードしたイメージファイルを使用してネットワークブートを行うことができない
 - UEFIシェルスクリプトから展開できない
 - 1つ以上のデバイスのオプションROMを実行できない
 - ブート順序リストに新しいネットワークまたはストレージデバイスが見つからない
 - インテルTXTが正常に動作していない
 - 無効なサーバーシリアル番号と製品ID
 - 無効な日付/時刻
 - ネットワークデバイスが正しく機能しない
 - システムが応答しなくなる
 - 単一デバイスで障害が発生した
 - サーバーが起動しない

- Smartアレイコントローラーが正しく機能しない
- VMwareはUEFIモードで起動しない
- Topic name not available
 - Webサイト
 - サポートと他のリソース
 - Hewlett Packard Enterpriseサポートへのアクセス
 - アップデートへのアクセス
 - リモートサポート（HPE通報サービス）
 - 保証情報
 - 規定に関する情報
 - ドキュメントに関するご意見、ご指摘

はじめに

UEFIシステムユーティリティ

UEFIシステムユーティリティは、システムROMに内蔵されています。これを使用すると、次のような広範な構成作業を実行できます。

- システムデバイスとインストールされたオプションの構成。
- システム機能の有効化と無効化。
- システム情報の表示。
- プライマリブートコントローラーまたはパーティションの選択。
- メモリオプションの構成。
- その他のプリブート環境の起動。

UEFIを搭載するHPEサーバーでは、以下を提供できます。

- サイズが2.2 TB以上のブートパーティションのサポート。このような構成は、以前まで、RAIDソリューションを使用している場合に、ブートドライブでしか使用できませんでした。
- セキュアブート。システムファームウェア、オプションカードファームウェア、オペレーティングシステム、ソフトウェアを連携して、プラットフォームのセキュリティを強化することができます。
- UEFIグラフィカルユーザーインターフェイス (GUI)
- 内蔵UEFIシェル。スクリプトやツールを実行するための起動前環境を提供します。
- UEFIオプションROMのみをサポートするオプションカード向けブートサポート。

UEFIの概要

UEFI (Unified Extensible Firmware Interface) は、起動中またはスタートアップ中のオペレーティングシステムとプラットフォームファームウェア間のインターフェイスを定義しています。UEFIは、BIOSよりも高度な起動前ユーザーインターフェイスをサポートします。UEFIネットワークスタックは、従来のPXE展開を引き続き支えながら、より豊富なネットワークベースのOS展開の環境での実装を可能にします。UEFIは、IPv4およびIPv6両方のネットワークをサポートします。さらに、セキュアブートなどの機能を使用することにより、プラットフォームのベンダーは、OSによらず起動前の環境でシステムを保護するアプローチを実装することができます。

BIOS/プラットフォーム構成 (RBSU) とその他の構成オプションは、UEFIインターフェイスから利用できます。

UEFIシステムユーティリティの概要

システムユーティリティの起動

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。
 - a. ブラウザーを開き、`https://<iLO host name or IP address>` と入力して、iLO Webインターフェイスにログオンします。
 - b. ログインページで、ディレクトリまたはローカルユーザーアカウント名とパスワードを入力して、ログインをク

リックします。

- c. iLOナビゲーションツリーでリモートコンソール&メディアを選択します。

起動タブが表示されます。

- d. ご利用のシステムが、使用するリモートコンソールアプリケーションの使用要件を満たしていることを確認します。
- e. 選択したアプリケーションの起動ボタンをクリックします。

以下を選択することによって、iLOリモートコンソールセッションを起動することもできます。

- 情報 - iLOの概要ページの統合リモートコンソールリンク。
- iLO Webインターフェイスの左下隅にあるコンソールサムネイル、および起動するアプリケーションタイプの選択。

2. サーバーを再起動するかまたは電源を入れます。

サーバーが再起動し、POST画面が表示されます。

3. F9キーを押します。

システムユーティリティ画面が表示されます。

注記:

システムユーティリティの使用には、BIOS管理者の許可が必要です。BIOS管理者がパスワードを必要とする場合、サーバーからシステムユーティリティを起動する前にパスワードを入力するように求められます。管理者パスワードの設定については、[サーバーセキュリティのオプション](#)を参照してください。

システムユーティリティ内での移動

手順

1. システムユーティリティを起動し、次のいずれかの操作を行います。

- 画面を移動して設定を変更するには、ポインティングデバイスを使用するか、またはいずれかのナビゲーションキーを押します。各システムユーティリティ画面の下部にキーの機能が表示されます。

ヒント:

セットアップブラウザの選択が自動（デフォルト設定）またはGUIの場合、ポインティングデバイスを使用してシステムユーティリティ画面をナビゲートすることができます。セットアップブラウザの選択がテキストに設定されているとき、ナビゲーションキーを使用する必要があります。

- モバイルオンラインヘルプにアクセスするには、ご使用のモバイルデバイスでシステムユーティリティ画面の左下部にあるQRコードをスキャンします。
2. システムユーティリティ画面を終了してサーバーを再起動するには、メインメニューが表示されるまでEscキーを押してから、次のオプションのいずれかを選択します。
- 終了し起動を再開 - システムを終了して、通常のブートプロセスを続行します。ブート順序のリストに従ってブートが続行され、システム内の最初のブート可能なオプションが起動されます。
 - システムを再起動 - システムを終了して、通常のブートプロセスを続行せずに、システムを再起動します。

GUIモードでのシステムユーティリティ内での移動

システムユーティリティのGUIでは、ポインティングデバイスまたはナビゲーションのキーを使用して移動することが

できます。GUIモードでは、選択したメニュー項目は緑色に変わります。

注記:

シリアルコンソールを使用してシステムユーティリティにアクセスした場合、GUIモードはサポートされません。

ブラウザーモードGUIに設定するには：

前提条件

- システムユーティリティには物理端末または統合リモートコンソールを通じてアクセスします。
- セットアップブラウザーの選択は自動またはGUIに設定されます。

手順

1. システムユーティリティ画面で、セットアップブラウザーの選択を選択します。
2. 自動またはGUIを選択します。
3. 設定を保存します。
4. システムを再起動します。

UEFIシステムユーティリティGUI

HPE ProLiant Gen10およびHPE Synergyコンピュートモジュールは、GUI UEFIシステムユーティリティをサポートしています。UEFIシステムユーティリティのGUIではマウスとキーボードの両方のデバイスがサポートされます。

領域

システムユーティリティのGUIには次の領域があります。

1. キャプションバー - この領域は、UEFIフォームのタイトルとシステムのボタンを示します。フォームのタイトルは、現在操作しているフォームの名前を示しています。
2. ナビゲーション履歴 - この領域には、以前ナビゲートしたフォームが表示されます。新しいシステムユーティリティのフォームにアクセスするたびに、ナビゲーション履歴にナビゲーション履歴ノードが追加されます。
3. サーバー情報 - この領域には、サーバー情報とファンクションキー情報が表示されます。
4. システムユーティリティフォーム - この領域には、現在のフォームのメニューオプションが表示されます。
5. アクティビティバー - この領域には、ファンクションキーやシステムステータスインジケーターなどのシステム全体の機能が表示されます。

GUIでのキーボードサポート

GUIではシステムユーティリティフォームをナビゲートするための基本的なキーがサポートされています。Tabキーを使用して、フォームのさまざまな領域にフォーカスを変更できます。サポートされるキーは、次のとおりです。

- 上下矢印キー
- Enter
- ファンクションキー
- Escキー

ナビゲーション履歴領域とキーボードサポート

ナビゲーション履歴は、ユーザーが以前ナビゲートしたシステムユーティリティフォームを表示します。新しいフォームにアクセスするたびに、ナビゲーション履歴にナビゲーション履歴ノードが追加されます。ナビゲーション履歴ノードをクリックして、以前アクセスしたユーティリティフォームに戻ることができます。

ナビゲーション履歴ノードが多すぎてナビゲーション履歴バーに収まらない場合、ホームノードが折り畳まれます。ホームノードを選択すると、アクセスしたナビゲーション履歴ノードのポップアップリストを表示できます。リストからナビゲーション履歴ノードをクリックして、以前アクセスしたフォームに戻ることができます。

ナビゲーション履歴領域を移動するには、次の機能を使用します。

- Tabキーを使用すると、ナビゲーション履歴領域内のフォーカスを変更できます。
- Enterキーを使用すると、ナビゲーション履歴ノード選択モードが開始してノードを選択できます。
- 矢印キーを使用すると、選択するノードに移動できます。
- Escキーを使用すると、ナビゲーション履歴ノード選択モードを終了します。

Gen10 Plusの機能

- 言語の選択 - キャプションバーにあります。
- 保留中の変更 - 保存されていない変更をリストします。
- 強制書き込み設定 - オプションの変更により強制的に変更されるオプションを表示します。
- 検索 - RBSUオプションを検索します。
- 依存関係ビューア - キャプションバーにある疑問符ボタンを押します。オプションがグレー表示されている理由に関する情報は、赤で表示されます。

システムユーティリティのキーの機能

- 上下矢印 - メニューオプションを選択します。選択すると、メニューオプションの色がテキストブラウザモードでは白色から黄色に変更され、GUIモードでは緑色に変更されます。
- Enter - エントリーを選択します。選択されたオプションによって、テキストブラウザモードでは白色から黄色に変更され、GUIモードでは緑色に変更されます。サブメニューが使用可能な場合は、サブメニューが表示されません。
- Esc - 前の画面に戻ります。
- F1 - テキストモードでの選択に関するオンラインヘルプを表示します。

注記:

GUIモードでオンラインヘルプを表示するには、システムユーティリティのメイン画面の右上隅にある?アイコンをクリックします。

- F7 - デフォルトのUEFI BIOS構成設定をロードします。

注記:

F7キーを押すとBIOS構成のみがリセットされます。オプションカードやiLOなどの他のエンティティはリセットされません。

- F10 - 変更した設定を保存するためのプロンプトが表示されます。
- F12 - 設定の変更を保存するプロンプトが表示され、システムユーティリティを終了します。
- 再起動が必要 (ラジオボタン) - 変更によってサーバーを再起動する必要がある場合、選択されて赤色に変化します。
- 変更保留中 (ラジオボタン) - 有効にするためには保存する必要がある変更が保留中の場合、選択されて赤色に変化します。

再起動が必要な場合

特定の構成変更を反映するには、再起動が必要になる場合があります。このような場合、動作の実行を求めるセットアップブラウザの選択に応じて、次のいずれかが発生します。

- GUIモードで、再起動が必要（ラジオボタン） - 変更によってサーバーを再起動する必要がある場合、選択されて赤色に変化します。
- テキストモードでは、該当するシステムユーティリティ画面でプロンプトが表示されます。

システムユーティリティメニューの概要

注記:

UEFIシステム構成オプションは、サーバープラットフォームごとに異なります。したがって、ここに記載されているオプションの中には、ご使用のシステムでは表示されないものがある可能性があります。

システムユーティリティ画面は、UEFIのメニュー方式インターフェイスのメイン画面です。この画面には、次の構成タスクのメニューオプションが表示されます。

- システム構成 - 表示および構成のオプションを表示します。
 - BIOS/プラットフォーム構成 (RBSU)
 - iLO 5構成ユーティリティ
 - その他のシステム固有のデバイス。取り付けられているSmartアレイデバイス、PCIeカード、NICなど。たとえば、内蔵FlexibleLOM Port 1があります。

注記:

インターフェイスのメニューでは、取り付けられているPCIデバイスの正しい製品名が表示されるようになっていますが、デバイスを認識できない場合は、`non-HPPE name`などの汎用的なラベルが割り当てられます。この汎用的なラベルは、デバイスの機能や動作に影響するものではありません。デバイスは、ご使用のシステムによって異なります。

- ワンタイムブートメニュー - ブートオーバーライドオプションを選択し、ファイルシステムからUEFIアプリケーションを実行するためのオプションを表示します。
- 内蔵アプリケーション - 表示および構成のオプションを表示します。
 - 内蔵UEFIシェル
 - インテグレートドマネジメントログ (IML)
 - Active Health Systemログ
 - ファームウェアのアップデート
 - 内蔵Diagnostics
 - Intelligent Provisioning
 - 内蔵iPXE
- システム情報 - サーバーの名前と世代、シリアル番号、製品ID、BIOSのバージョンと日付、パワーマネージメントコントローラー、バックアップBIOSのバージョンと日付、システムメモリ、ストレージデバイス、プロセッサを表示するオプションを表示します。
- システムヘルス - システム内のすべてのデバイスの現在のヘルスステータスを表示するためのオプションが表示されます。
- システムを終了して再起動 - システムを終了して、通常のブートプロセスを続行します。
- システムを再起動する - システムを終了し、UEFIブート順序リストを参照してシステム内の最初のブート可能なオプションを起動することで、システムを再起動します。たとえば、UEFIシェルが有効で、リスト内で最初のブート可能なオプションとしてリストされている場合、UEFIシェルを起動できます。
- 言語の選択 - ユーザーインターフェイスで使用する言語を選択することができます。デフォルトの言語は、英語で

す。

- セットアップブラウザの選択 - ブラウザーを選択することができます。

共通のセットアップおよび構成に関するFAQ

1. UEFIシステムユーティリティにアクセスする方法を教えてください。

システムユーティリティの起動 を参照してください。

2. RBSU設定からUEFI設定に移行するには、どうすればいいですか？

ROMベースセットアップユーティリティ (RBSU) は、BIOS/プラットフォーム構成 (RBSU) メニューに置き換えられます。このメニューを使用すると、UEFIオプションにアクセスしたり使用したりできます。BIOS/プラットフォーム構成 (RBSU) を参照してください。

3. ファームウェアまたはシステムROMのアップデートするには、どうすればいいですか？

ファームウェアまたはシステムROMのアップデート を参照してください。

4. ブートデバイスの選択方法を教えてください。

システムユーティリティの起動 を参照してください。ワンタイムブートオーバーライドのオプションを選択できるワンタイムブートメニューにアクセスするには、次のいずれかを実行します。

- サーバーのPOST処理中にF11を押します。
- システムユーティリティ画面で、ワンタイムブートメニューを選択します。ワンタイムブートオプションを参照してください。

すべてのブートのブート順序を変更するには、UEFIブート順序の変更を参照してください。

5. インテルハイパースレッディングを有効、または無効にするにはどうすればいいですか？

デフォルトでは、インテルハイパースレッディングは有効です。この設定を無効にするか、再度有効にするには、インテルハイパースレッディングの有効化または無効化 を参照してください。

6. 最小プロセッサアイドル電力パッケージステートをパッケージステートなしに構成する方法を教えてください。

デフォルトでは、これはパッケージC6 (リテンション) ステート、つまりプロセッサが最低アイドル電力の状態に設定されます。この設定を変更するには、最小プロセッサアイドル電力パッケージCステートを参照してください。

7. タイムゾーンを構成するにはどうすればいいですか？

日付と時刻の設定 を参照してください。

8. 構成変更を保存し、システムを再起動するにはどうすればいいですか？

- a. 変更が完了したとき、変更が保留中です。変更を保存して終了しますか？ というプロンプトが表示されない場合は、F10キーを押すと表示されます。

- b. Yキーを押して、変更内容を保存します。

変更の保存を確認するプロンプトが表示されます。

- c. リポートオプションを選択してEnterキーを押します。

- システムを終了して再起動 - システムを終了して、通常のブートプロセスを続行します。ブート順序のリストに従ってブートが続行され、システム内の最初のブート可能なオプションが起動されます。

- システムを再起動 - システムを終了して、通常のブートプロセスを続行せずに、システムを再起動します。

9. 内蔵UEFIシェルに移動する方法を教えてください。

内蔵UEFIシェルの起動 を参照してください。

10. 取り付けられているすべてのオプションおよびデバイスのヘルスステータスを表示する方法を教えてください。
システムヘルスの表示 を参照してください。
11. CONREPを使用してUEFIの設定を複製する方法を教えてください。
Configuration Replicationユーティリティ (CONREP) を参照してください。
12. ジッター制御を設定する方法を教えてください。
アドバンストパフォーマンスチューニングオプションの構成を参照してください。
13. ワークロードプロファイルを使用してパフォーマンスをチューニングする方法を教えてください。
ワークロードプロファイルとパフォーマンスオプションを参照してください。
14. RESTfulインターフェイスツールまたはAPIを使用してUEFI設定を複製する方法を教えてください。
Hewlett Packard EnterpriseのWebサイト (<https://www.hpe.com/info/redfish>) にあるRESTfulインターフェイスツールのドキュメントを参照してください。
15. セキュアブート、TPMなど、サーバー上のセキュリティ設定を変更する方法を教えてください。
サーバーセキュリティのオプションを参照してください。<https://www.hpe.com/support/gen10-intelligent-system-tuning-en>にあるHPE Gen10サーバーのIntelligent System Tuningも参照してください。
16. HPE Intelligent System Tuningはどんなツールですか。また、使用法を教えてください。
HPE Intelligent System Tuning (IST) には、Jitter Smoothing、Workload Matching、およびコアブーストが含まれています。アドバンストパフォーマンスチューニングオプションの構成およびワークロードプロファイルとパフォーマンスオプションを参照してください。

ファームウェアまたはシステムROMのアップデート

ファームウェアまたはシステムROMをアップデートするには、以下のいずれかの方法を使用します。

- システムユーティリティのファームウェアのアップデートオプション。
- 内蔵UEFIシェルの `fwupadte` コマンド。
- Service Pack for ProLiant (SPP)
- HPEオンラインフラッシュコンポーネント
- Moonshot Component Pack

システムユーティリティメインメニューのオプション

システムユーティリティメインメニューは、以下のオプションの開始点です。

- システム構成
- ワンタイムブートメニュー
- 内蔵アプリケーション
- システム情報
- システムヘルス
- システムを終了して再起動
- システムを再起動する
- 言語の選択

- セットアップブラウザの選択

システム構成

システム構成メニューオプション

- BIOS/プラットフォーム構成 (RBSU)
- iLO 5構成ユーティリティ
- その他のシステム固有のデバイス。取り付けられているPCIeカード、NIC、Smartアレイなど。たとえば、内蔵FlexibleLOM Port 1があります。

BIOS/プラットフォーム構成 (RBSU)

BIOS/プラットフォーム構成 (RBSU) メニューには、以下を含め、UEFIのオプションにアクセスするための多くのネストされたオプションが含まれます。

- ワークロードプロファイル
- システムオプション
- プロセッサオプション
- メモリオプション
- 仮想化オプション
- ブートオプション
- ネットワークオプション
- ストレージオプション
- 電力およびパフォーマンスオプション
- 内蔵UEFIシェルオプション
- サーバーセキュリティのオプション
- PCIデバイス構成のオプション
- アドバンストオプション
- 日付と時刻
- システムデフォルトオプション

iLO 5構成ユーティリティの使用

iLO 5構成ユーティリティオプション

iLO 5構成ユーティリティには、物理システムコンソールまたはiLO 5リモートコンソールセッションを使用してアクセスできます。このユーティリティは、次のオプションを備えています。

- [ネットワークオプション](#)
- [アドバンスドネットワークオプション](#)
- [ユーザー管理](#)
- [設定オプション](#)
- [工場出荷時のデフォルトにセット](#)
- [iLOのリセット](#)
- [バージョン情報](#)

ネットワークオプション

- MACアドレス（読み取り専用） - 選択しているiLOネットワークインターフェイスのMACアドレスを指定します。
- ネットワークインターフェイスアダプター - 使用するiLOネットワークインターフェイスアダプターを指定します。
 - オン - iLO専用ネットワークポートを使用します。
 - 共有ネットワークポート - 共有ネットワークポートを使用します。このオプションは、サポートされているサーバーでのみ使用できます。
 - オフ - iLOへのすべてのネットワークインターフェイスが無効になります。
- 送信速度自動選択（iLO専用ネットワークポートのみ） - ネットワークに接続しているときに、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iLOがネゴシエートできるようにします。このオプションは、ネットワークインターフェイスアダプターがオンに設定されている場合にのみ使用できます。
- 送信速度手動設定（iLO専用ネットワークポートのみ） - iLOネットワークインターフェイスのリンク速度を設定します。このオプションは、ネットワークインターフェイスアダプターがオンに設定され、送信速度自動選択がオフに設定されている場合にのみ使用できます。
- 送信デュプレックス設定（iLO専用ネットワークポートのみ） - iLOネットワークインターフェイスのリンクデュプレックス設定を設定します。このオプションは、ネットワークインターフェイスアダプターがオンに設定され、送信速度自動選択がオフに設定されている場合にのみ使用できます。
- VLAN有効（共有ネットワークポートのみ） - VLAN機能を有効にします。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。このオプションは、ネットワークインターフェイスアダプターが共有ネットワークポートに設定されている場合にのみ使用できます。
- VLAN ID（共有ネットワークポートのみ） - VLANが有効な場合は、VLANタグを指定します。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。このオプションは、ネットワークインターフェイスアダプターが共有ネットワークポートに設定されている場合にのみ使用できます。
- DHCP有効 - iLOがDHCPサーバーからIPアドレス（およびその他の多くの設定）を取得するよう構成します。
- DNS名 - iLOサブシステムのDNS名を設定します。この名前は、IPアドレスではなくiLOサブシステム名に接続するようDHCPとDNSを構成している場合にのみ使用できます。
- IPアドレス - iLOのIPアドレスを指定します。DHCPを使用している場合、iLO IPアドレスが自動的に提供します。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を指定します。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IPアドレス - iLOのゲートウェイIPアドレスを指定します。
DHCPを使用している場合、iLOゲートウェイのIPアドレスが自動的に提供されます。DHCPを使用しない場合は、iLOのゲートウェイIPアドレスを入力します。

ネットワークオプションの構成

手順

1. 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 > ネットワークオプションを選択します。
2. ネットワークオプションのいずれかを選択し、そのオプションの設定を選択するかまたは値を入力します。
3. 設定を保存します。

アドバンスドネットワークオプション

- DHCPからのゲートウェイ - iLOがDHCPサーバー提供のゲートウェイを使用するかどうかを指定します。
- ゲートウェイ#1、ゲートウェイ#2、およびゲートウェイ#3 - DHCPからのゲートウェイが無効の場合は、最大3つのiLOゲートウェイのIPアドレスを指定します。
- DHCP経路 - iLOがDHCPサーバー提供の静的経路を使用するかどうかを指定します。
- 経路1、経路2、および経路3 - DHCP経路が無効の場合は、iLOの静的ルート先、マスク、およびゲートウェイアドレスを指定します。
- DHCPからのDNS - iLOがDHCPサーバー提供のDNSサーバーリストを使用するかどうかを指定します。
- DNSサーバー1、DNSサーバー2、DNSサーバー3 - DHCPからのDNSが無効の場合は、プライマリ、セカンダリ、およびターシャリDNSサーバーを指定します。
- DHCPからのWINS - iLOがDHCPサーバー提供のWINSサーバーリストを使用するかどうかを指定します。
- WINSサーバーに登録 - iLOがWINSサーバーに名前を登録するかどうかを指定します。
- WINSサーバー#1およびWINSサーバー#2 - DHCPからのWINSが無効の場合は、プライマリおよびセカンダリWINSサーバーを指定します。
- ドメイン名 - iLOのドメイン名。DHCPを使用していない場合は、ドメイン名を指定します。

アドバンスドネットワークオプションの構成

手順

1. 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 > アドバンスドネットワークオプションを選択します。
2. アドバンスドネットワークオプションのいずれかを選択し、そのオプションの設定を選択するかまたは値を入力します。
3. 設定を保存します。

ユーザー管理

- ユーザーの追加
- ユーザーの編集/削除

ユーザーの追加

このオプションを使用して、次の権限と情報を持つ新しいローカルiLOユーザーアカウントを追加します。

iLO 5ユーザー権限

- **ユーザーアカウントの管理** - 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。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。
- **リモートコンソールアクセス** - 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リモートでアクセスできます。
- **仮想電源およびリセット** - ホストシステムの電源再投入やリセットを実行できます。
これらの操作はシステムの可用性を中断します。この権限を持つユーザーは、システムにNMIを生成ボタンを使用してシステムを診断できます。
- **仮想メディア** - ホストシステム上の仮想メディア機能を使用できます。
- **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ファームウェアをリモートアップデート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、Webインターフェイス、HPQLCFG、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。iLO RBSU、iLO 5構成ユーティリティ、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することができます。
- **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。
- **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。

注記:

デフォルトでは、リカバリセット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iLO Webインターフェイスにログインします。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。

新しいユーザーの情報

- **新しいユーザー名** - ユーザー管理ページのユーザーリストに表示する名前を指定します。ユーザー名は、ログイン名と同じである必要はありません。ユーザー名は最長で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簡単に識別でき便利です。
- **ログイン名** - iLOにログインするときに使用する必要がある名前を指定します。ユーザー管理ページ、iLO概要ページ、およびiLOログのユーザーリストに表示されます。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** - iLOにログインするために使用するパスワードの設定と確認を行います。パスワードは、最長39文字です。パスワードは、確認のために2度入力します。

新しいユーザーアカウントの追加

手順

1. 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 > ユーザー管理 > ユーザーの追加を選択します。
2. いずれかのiLO 5ユーザー権限を選択します。
3. 各オプションで、次のいずれかの設定を選択します。
 - はい - このユーザーの権限を有効にします。
 - いいえ - このユーザーの権限を無効にします。
4. 新しいユーザー情報エントリーを選択します。
5. 新しいユーザーの各エントリーを入力します。
6. 必要な数のユーザーアカウントを作成し、設定を保存します。

ユーザーの編集/削除

このオプションを使用して、iLOのユーザーアカウントの設定を編集するか、ユーザーアカウントを削除します。

ユーザーアカウントの編集または削除

手順

1. 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 > ユーザー管理 > ユーザーの編集/削除を選択します。
2. 編集または削除するユーザーアカウントのアクションメニューを選択します。
3. 次のいずれかを選択します。
 - 削除 - ユーザーアカウントを削除します。
 - 編集 - ユーザーのログイン名、パスワード、またはユーザー権限を編集できます。
4. 必要な数のユーザーアカウントをアップデートし、設定を保存します。

設定オプション

このメニューを使用して、iLOアクセス設定の表示と構成を行います。

- iLO 5機能 - iLOの機能が利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の機能が無効になっている場合、iLOネットワークおよびオペレーティングシステムドライバーとの通信は切断されます。

注記:

ProLiantブレードサーバーの場合、iLO機能はブレードサーバーで無効にできません。

- iLO 5構成ユーティリティ - iLO 5構成ユーティリティを有効または無効にします。このオプションが無効に設定されている場合、UEFIシステムユーティリティにアクセスしても、iLO 5構成ユーティリティのメニュー項目は使用できません。

- iLO 5構成のためのログインが必要 - ユーザーがiLO機能に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指定します。
この設定が有効の場合は、SUMおよびRESTfulインターフェイスツールのアップデートなどを含む機能に対してユーザー認証情報を入力します。
- POST中にiLO 5のIPアドレスを表示 - 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。
- ローカルユーザー - ローカル ユーザー アカウントアクセスを有効または無効にします。
- シリアルCLI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指定します。設定は次のとおりです。
 - 有効 - 認証は必要 - ホストシリアルポートに接続された端末からiLO CLPI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iLO CLPI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iLO 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CLI速度(ビット/秒) - CLI機能のためのシリアルポートの速度を指定します。設定(ビット/秒)は、次のとおりです。
 - 9600
 - 19200
 - 57600
 - 115200

正常に動作するためには、シリアルポート構成がパリティなし、データビット8、ストップビット1 (N/8/1) に設定されている必要があります。

注記:

速度38400は、iLO Webインターフェイスでサポートされていますが、iLO 5構成ユーティリティでは現在サポートされていません。

- 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。

アクセス設定の構成

手順

1. 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 > 設定オプションを選択します。
2. ユーザーアクセスの設定オプションをアップデートします。
3. 設定を保存します。

工場出荷時のデフォルトにセット

注意:

この操作を行うと、すべてのユーザーおよびライセンスデータが消去されます。

このオプションを使用して、iLOを工場出荷時のデフォルト設定にリセットします。リセットした場合、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アクセスできません。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。

サーバーに工場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。

iLOの工場出荷時デフォルト設定へのリセット

手順

1. 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 > 工場出荷時のデフォルトにセットを選択します。
iLO 5構成ユーティリティに、はいまたはいいえを選択する画面が表示されます。
2. はい を選択します。
3. リセットの確認を求めるプロンプトが表示されたら、Enterキーを押します。
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。
4. 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. メインメニューで、終了して再起動を選択し、Enterキーを押します。
 - d. 要求の確認を求めるメッセージが表示されたら、Enterキーを押して画面を終了し、ブートプロセスを再開します。

iLOのリセット

iLOの応答が遅い場合は、このオプションを使用してリセットを実行することができます。

この方法でiLOをリセットしても構成が変更されることはありませんが、iLOへのアクティブな接続がすべて終了します。iLOをリセットすると、次の再起動までiLO 5構成ユーティリティを使用できなくなります。

iLOのアクティブな接続のリセット

前提条件

iLO設定権限の構成

手順

1. 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 > iLOをリセットを選択します。
iLO 5構成ユーティリティに、はいまたはいいえを選択する画面が表示されます。
2. はい を選択します。
3. リセットの確認を求めるプロンプトが表示されたら、Enterキーを押します。
アクティブなiLO接続がリセットされます。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。
4. 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. メインメニューで、終了して再起動を選択し、Enterキーを押します。
- d. 要求の確認を求めるメッセージが表示されたら、Enterキーを押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。

バージョン情報

このメニューを使用して、次のiLOコンポーネントに関する情報を表示します。

- ファームウェア日付 - iLOファームウェアのリビジョン日付。
- ファームウェアバージョン - iLOファームウェアバージョン。
- iLO CPLDバージョン - iLO CPLD (Complex Programmable Logic Device) のバージョン。
- ホストCPLDバージョン - サーバーのCPLDのバージョン。
- シリアル番号 - iLOのシリアル番号。
- PCI BUS - iLOプロセッサが接続されているPCIバス。
- デバイス - PCIバス内のiLOに割り当てられているデバイス番号。

iLOに関する情報の表示

手順

1. 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 > バージョン情報を選択します。
2. iLOコンポーネントのバージョン情報を表示します。

内蔵デバイス情報の表示と構成

コントローラー情報の表示

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > コントローラー情報を選択します。
2. コントローラー情報の画面で、情報を表示します。

コントローラー設定の構成

コントローラー設定の変更

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > コントローラー設定の構成 > コントローラー設定の変更を選択します。
2. コントローラー設定の変更画面で、次のいずれかの設定を変更します。

設定	説明
キャッシュ比率（読み取り）	書き込みキャッシュに対し、先読みキャッシュのメモリ量を調整します。 範囲は0～100です。値は5単位で増減できます。
構成された物理ドライブのライトキャッシュ状態	構成済みのすべての物理ドライブ上の書き込みキャッシュの設定を有効または無効にします。 オプションは、有効、無効、またはデフォルトです。
現在の並列表面のスキャン数	並行して動作できるコントローラーの表面スキャンの数を制御します。 <ul style="list-style-type: none">• 1：無効• 16：最大
バッテリーなしの書き込みキャッシュ	Energy Packが存在しない場合や充電されていない場合、書き込みキャッシュは有効または無効です。 オプションは、有効または無効です。
再構築の優先順位	コントローラーが内部コマンドを処理して、障害が発生した論理ドライブを再構築する優先度が決まります。 <ul style="list-style-type: none">• 低：再構築よりも通常のシステム動作が優先されます。• 中：再構築の時間は半分になり、残りの時間に通常のシステム動作が行われます。• やや高い：通常のシステム動作よりも再構築が優先されます。• 高：他のすべてのシステム動作よりも再構築が優先されます。
スペアのアクティベーションモード	予測スペアアクティベーションモードは、アレイ内のメンバードライブが障害予測を報告するたびにスペアドライブをアクティブ化します。 障害スペアのアクティベーションモードは、アレイ内のメンバードライブが故障した場合に、フォールトトレランス方式でデータを再生成することにより、スペアドライブをアクティブにします。
表面スキャン分析の優先順位	表面スキャン分析を再開する前に、コントローラーの遅延/アイドル時間の長さを修正します。 <ul style="list-style-type: none">• 0：無効• 1-30：アイドル状態（遅延あり）• 31：高
変換の優先順位	（NVM Express SmartRAID SW RAIDサポートには適用されません）。オペレーティングシステムからの要求が処理される速度： <ul style="list-style-type: none">• 高：通常のI/Oとひきかえにできるだけ早く完了します。• 中：通常のI/Oにいくらか影響を及ぼして完了します。• 低：通常のI/Oが発生していないときに実行します。

設定	説明
構成されていない物理ドライブのライトキャッシュ状態	構成されていないすべての物理ドライブ上の書き込みキャッシュを有効または無効にします。オプションは、有効、無効、またはデフォルトです。

3. 変更の送信をクリックします。

高度なコントローラー設定の変更

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > コントローラー設定の構成 > コントローラーの詳細設定を選択します。
2. コントローラーの詳細設定画面で、次のいずれかの設定を変更します。

設定	説明
代替不整合修復ポリシー	(NVM Express SmartRAID SW RAIDサポートには適用されません)。コントローラーの不整合修正ポリシーの動作を制御します。このオプションは、ビデオアプリケーションのコントローラー性能を調整するために使用され、有効なライセンスキーのインストールが必要です。オプションは、有効または無効です。
劣化モードパフォーマンス最適化	ビデオアプリケーションのコントローラー性能を調整するために使用され、有効なライセンスキーのインストールが必要です。オプションは、有効または無効です。
HDDフレキシブル遅延最適化	ホスト要求からの最大測定遅延時間を減らします。
最大ドライブ要求キュー深度	ファームウェアが任意の時点でドライブに送信する物理ドライブ要求の最大数を制御します。このオプションは、ビデオアプリケーション用コントローラーのパフォーマンスのチューニングに使用されます。オプションは、2、4、8、16、32、または自動です。
モニターおよびパフォーマンス解析遅延	コントローラーのモニターおよびパフォーマンス解析遅延の動作を制御し、0から60までの範囲の値で表します。このオプションは、主にビデオアプリケーションのコントローラー性能を調整するために使用され、有効なライセンスキーのインストールが必要です。
物理ドライブの要求エレベーターソート	コントローラーのキャッシュ書き込みエレベーターソートアルゴリズムの動作を制御します。 このオプションは、ビデオアプリケーションのコントローラー性能を調整するために使用され、有効なライセンスキーのインストールが必要です。オプションは、有効または無効です。
RAID 6/60代替不整合修復ポリシー	コントローラーの不整合修復ポリシーを設定します。オプションは、有効および無効です。

3. 変更の送信をクリックします。

コントローラー構成の消去

コントローラー構成を消去すると、アレイ構成およびパーティション情報を含むコントローラーメタデータが破棄されます。

△ 注意:

コントローラー構成を消去すると、接続されているメディアのすべてのデータにアクセスできなくなり、復旧できません。

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > コントローラー設定の構成 > 構成のクリアを選択します。
2. 構成のクリア画面で、次のいずれかまたは両方を選択します。
 - すべてのアレイ構成の削除 - コントローラーのすべてのアレイを削除します。アレイのすべてのデータも削除されます。
 - すべての物理ドライブの構成メタデータを削除する - アレイの一部ではないドライブ上のRAIDメタデータを削除します。

バックアップ電源ステータスの表示

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > コントローラー設定の構成を選択します。
2. バックアップ電源画面で、バックアップ電源のステータスを表示します。

ステータスオプションは、次のとおりです。

- 障害発生
- 未装着
- 充電中
- 充電完了

電源設定の管理

電源管理機能は、NVM Express SmartRAID SW RAIDサポートには適用されません。

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > コントローラー設定の構成 > 電源設定の管理を選択します。
2. 電源設定の管理画面で、次のいずれかの設定をアップデートします。

設定	説明
----	----

設定 説明

電力 オプションは次のとおりです。

- モード
- 最大パフォーマンス（デフォルト） - パフォーマンスに影響する電力節約オプションは無効です。
 - バランス - パフォーマンスへの影響を最小限に抑えて電力を節約するにはこの設定を使用します。
 - 最小電力 - システムパフォーマンスにこだわらずにこの設定を選択すれば、最大の電力の節約が実現されます。

注記:

Hewlett Packard Enterpriseは一部のアプリケーションには最小電力の設定をお勧めしていますが、ほとんどのお客様に適切な設定ではありません。ほとんどのアプリケーションにおいて大幅なパフォーマンスの低下が生じます。

サバイバルモード 温度がしきい値を超えたときにダイナミックパワー設定を最小値にまで低下させます。この最小の設定により、サーバーはほとんどの状況で動作することができますが、パフォーマンスは低下する可能性があります。

3. 変更の送信をクリックします。

アレイの構成

UEFIシステムユーティリティを使用したアレイの作成

アレイを作成するときは、ドライブを選択し、RAIDレベルを指定し、ストリップサイズや論理ドライブサイズなどのアレイ設定を構成することができます。

手順

1. UEFIシステムユーティリティ画面で、システム構成 > <コントローラー名> > アレイ構成 > アレイの作成を選択します。
2. アレイの作成画面で、アレイに含める各ドライブを選択して、次のフォームに進むをクリックします。

注記:

SASドライブは、NVM Express SmartRAID SW RAIDサポートではサポートされていません。

3. RAIDレベルの設定画面で、ドロップダウンメニューからRAIDレベルを選択し、次のフォームに進むをクリックします。
4. 論理ドライブ構成の設定画面で、構成設定を指定するか、デフォルトの選択を使用します。

設定 説明

論理ドライブのラベル ドライブラベルのデフォルト選択を使用するか、新しいラベルを入力します。ラベルの文字は英数字またはスペースを指定できます。

設定	説明
ストリップサイズ/フルストリップサイズ	ストリップサイズは、アレイの各物理ドライブに保存されるデータの量です。フルストリップサイズは、アレイ内のすべてのドライブ上でコントローラーが同時に読み取りまたは書き込みできるデータの量です。パリティを通じたフォールトトレランスをサポートするRAIDレベルでは、一度に1つのフルストリップサイズに対してパリティ情報が計算されます。 ハードウェアRAIDの場合、ディスクの数とRAIDレベルに応じて、16KiBから1024KiBまで指定できます。デフォルト値は利用可能なすべての領域です。 SmartRAID NVM Express SmartRAID SW RAIDサポートの場合、最小サイズは16KiBで、最大サイズは最大256KiBまで、RAIDレベルとデバイスタイプによって異なります。
サイズ	値は10進数で、最小のRAIDサイズは16MiBです。
ユニットサイズ	論理ドライブのユニットサイズ (MiB/GiB/TiB)。
高速化の方法	論理ドライブの高速化の方法 (コントローラーキャッシュまたはなし)。

5. 変更の送信をクリックします。
6. メインメニューに戻ります。
7. 変更内容の保存を行うための確認を求められたらOKをクリックします。
8. サーバーを再起動します。

論理ドライブプロパティの表示

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > アレイ構成 > アレイの管理 > アレイ > 論理ドライブのリスト > 論理ドライブ > 論理ドライブの詳細を選択します。
2. 論理ドライブの詳細画面で詳細を表示します。

論理ドライブの作成

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > アレイ構成 > アレイの管理 > アレイ > 論理ドライブの作成を選択します。
2. 論理ドライブの作成画面で、RAIDレベルを選択して次のフォームに進むをクリックします。
3. 論理ドライブ構成の設定画面で、構成のデフォルト値を使用するか異なる値を指定します。

設定	説明
論理ドライブのラベル	ドライブラベルのデフォルト選択を使用するか、新しいラベルを入力します。ラベルの文字は英数字またはスペースを指定できます。
ストリップサイズ/フルストリップサイズ	ストリップサイズは、アレイの各物理ドライブに保存されるデータの量です。フルストリップサイズは、アレイ内のすべてのドライブ上でコントローラーが同時に読み取りまたは書き込みできるデータの量です。パリティを通じたフォールトトレランスをサポートするRAIDレベルでは、一度に1つのフルストリップサイズに対してパリティ情報が計算されます。 ディスクの数とRAIDレベルに応じて、8KiBから1024KiBを指定できます。デフォルト値は利用可能なすべての領域です。 SmartRAID S100i SW RAIDを使用する場合、最小サイズは16KiB、最大サイズは256KiBです。

設定	説明
サイズ	値は10進数で、最小のRAIDサイズは16MiBです。
ユニットサイズ	論理ドライブのユニットサイズ (MiB/GiB/TiB)。
高速化の方法	論理ドライブの高速化の方法 (コントローラーキャッシュまたはなし)。

4. 変更の送信をクリックします。

スペアドライブの割り当て

スペアは論理ドライブ内で障害が発生したドライブに自動的に代わるドライブです。

前提条件

スペアドライブは、次の条件を満たす必要があります。

- 割り当てられていないドライブ、または別のアレイのスペアドライブである必要があります。
- アレイに含まれる既存のドライブと同じタイプ (SATA、SASなど) である必要があります。
- ドライブの容量は、アレイ内の最小ドライブ以上でなければなりません。

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > アレイ構成 > アレイの管理 > アレイ > スペアドライブの管理を選択します。
2. スペアドライブの管理画面で、スペアアクティブ化タイプを選択します。
 - 専用スペアの割当
 - 自動交換スペアの割当
3. スペアとして割り当てるドライブを選択します。

注記:

前提条件に記載されている条件を満たすドライブのみが表示されます。

スペアドライブの削除

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > アレイ構成 > アレイの管理 > アレイ > スペアドライブの管理 > スペアドライブの削除を選択します。
2. スペアドライブの削除画面で、削除するスペアを選択し、スペアドライブの削除をクリックします。

デバイスの確認

UEFIシステムユーティリティを使用して、そのデバイスの識別LEDをオンにして、ドライブを識別します。

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > アレイ構成 > アレイの管理 > アレイ > デバ

イスの確認を選択します。

2. デバイスの確認画面で、LEDを点灯させる時間を指定し（秒単位）、ドライブ構成タイプを選択し、開始をクリックします。

LEDをオフにするには、終了をクリックします。

アレイの削除

この手順では次のものを削除します。

- アレイ上のすべての論理ドライブ。
- アレイに組み込まれていた論理ドライブのすべてのデータ。

削除されたアレイがコントローラーで唯一のアレイである場合は、コントローラーの設定が削除され、デフォルト構成が復元されます。

個々の論理ドライブを削除するには、「論理ドライブの削除」を参照してください。

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > アレイ構成 > アレイの管理 > アレイ > アレイの削除を選択します。
2. アレイの削除画面で、変更の送信をクリックします。

論理ドライブの編集

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > アレイ構成 > アレイの管理 > アレイ > 論理ドライブのリスト > 論理ドライブ > 論理ドライブの編集を選択します。
2. 論理ドライブの編集画面で、次の設定を編集します。

設定	説明
高速化の方法	高速化の方法によって、直接論理ドライブにデータを書き込む代わりに、キャッシュメモリに書き込むことによって、データベースの性能が向上します。オプションは次のとおりです。 <ul style="list-style-type: none">• コントローラーキャッシュ - データをキャッシュメモリに書き込みます。• なし - アレイの他の論理ドライブ用にキャッシュモジュールを予約するために、キャッシュ機能を無効にします。
論理ドライブのラベル	このラベルの値は論理ドライブの詳細画面に表示されます。ラベルは英数字およびスペースのみを含めることができます。

3. 変更の送信をクリックします。

論理ドライブの削除

個々の論理ドライブを削除するには、この手順を使用します。アレイ内のすべての論理ドライブを削除するには、「アレイの削除」を参照してください。



重要:

論理ドライブを削除すると、論理ドライブ上のすべてのデータも削除されます。削除する論理ドライブがアレイ内の唯一の論理ドライブである場合、アレイも削除されます。

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > アレイ構成 > アレイの管理 > アレイ > 論理ドライブのリスト > 論理ドライブ > 論理ドライブの削除を選択します。
2. 論理ドライブの削除画面で、変更の送信をクリックします。

ディスクユーティリティ

ディスクデバイス情報の表示

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > ディスクユーティリティ > ディスク > デバイス情報を選択します。
2. デバイス情報の画面で、情報を表示します。

ディスクデバイスの確認

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > ディスクユーティリティ > ディスク > デバイスの確認を選択します。
2. デバイスの確認画面で、LEDを点灯させる時間を指定し（秒単位）、ドライブ構成タイプを選択し、開始をクリックします。

LEDの点滅を停止するには終了をクリックします。

レガシーブートモード用のブート可能デバイスの設定

プライマリおよびセカンダリブート可能デバイスの設定（レガシーブートモード）

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > レガシーブートモードにブート可能なデバイスを設定します > ブート可能な論理ドライブの選択 > 論理ドライブを選択します。
2. 論理ドライブ画面で、次のいずれかを選択します。
 - プライマリブートデバイスとして設定
 - セカンダリブートデバイスとして設定

OSブート可能ドライブの数の設定（レガシーブートモード）

手順

1. システムユーティリティ画面で、システム構成 > コントローラー > レガシーブートモードにブート可能なデバイスを設定します > OSブート可能ドライブの数を選択します。
2. OSのブート可能なドライブ数の画面で、OSブート可能ドライブの数を指定します。
3. 変更の送信をクリックします。

NICおよびFCoE設定の表示と構成

システム構成画面を使用して、内蔵のNICやFCoEなど、取り付けられているシステムデバイスに関する情報の表示や構成を行えます。一覧表示されるデバイスおよび使用できる構成オプションは、システムごとに異なります。

手順

1. システムユーティリティ画面からシステム構成を選択します。
2. デバイスを選択します。
システム構成画面に、内蔵デバイスの情報が表示されます。
3. 設定を表示、選択、または入力します。
4. 設定を保存します。

ワンタイムブートメニュー

ワンタイムブートメニューオプション

ワンタイムブートメニューを使用して、ワンタイムブートオーバーライドにUEFIブートオプションを選択できます。このオプションを選択しても、事前定義済みのブート順序の設定は選択したオプションにより変更されません。iLOリモートコンソールでUSBキーまたは仮想メディアを使用する場合、システムユーティリティを終了し、システムユーティリティに入りなおしてこのメニューを更新する必要があります。これにより、デバイスが表示されます。

以下のブートオプションがあります。

- Windows Boot ManagerなどのOSブートマネージャー - インストールされているOSのブートマネージャーをリストします。
- Generic USB Boot - UEFIで起動可能なUSBデバイスのプレースホルダーを提供します。このオプションのブート優先順位を設定し、今後取り付ける可能性があるUSBデバイスと使用する際にこの優先度を保持できます。この優先順位を設定しても、UEFIブート順序リスト内の個々のUSBデバイスの優先順位設定には影響しません。

注記:

このオプションは、UEFIモードでのみ使用できます。取り付けられた個々のUSBデバイスのブート順序が低く構成されている場合でも、システムはGeneric USB Bootエントリーで指定された順序ですべてのUEFIでブート可能なUSBデバイスのブートを試みます。

- 内部SDカード
- 内蔵フレキシブルLOM
- 内蔵UEFIシェル
- 内蔵SATAポート

- ファイルシステムからUEFIアプリケーションを実行 - ファイルシステムから実行するUEFIアプリケーションを選択できます。システムで使用できるすべてのFATファイルシステムを表示できます。x64 UEFIアプリケーション（拡張子.EFI）を選択して実行することもできます（OSブートローダー、その他のUEFIアプリケーションなど）。
- レガシーBIOSワнтаイムブートメニュー - レガシーBIOSワнтаイムブートメニューを起動、終了します。このメニューでは、このブートのみの特定の書き換えオプションを選択できます。このオプションでは、ご使用のブート順序やモードの設定は変更されません。
- 内蔵iPXE

ワнтаイムブートのオプションの選択

手順

1. システムユーティリティ画面で、ワнтаイムブートメニューを選択します。
2. ワнтаイムブートメニューオプションを選択します。
レガシーBIOSワнтаイムブートオプションを選択すると、システムが再起動します。

内蔵アプリケーション

内蔵UEFIシェルの起動

内蔵UEFIシェルオプションを使用して、内蔵UEFIシェルを起動します。内蔵UEFIシェルは、UEFIブートローダーを含むUEFIアプリケーションのスクリプトを作成し、実行するための起動前のコマンドライン環境です。このシェルには、システム情報を取得し、システムBIOSを構成およびアップデートするために使用できるCLIベースのコマンドも用意されています。

前提条件

- 内蔵UEFIシェルが有効に設定されていること。

手順

1. システムユーティリティ画面で、内蔵アプリケーション > 内蔵UEFIシェルを選択します。
内蔵UEFIシェル画面が表示されます。
2. 任意のキーを押して、その場にいることを知らせます。
この手順により、セキュアブートの無効化や他社製のUEFIツールを使用したセキュアブート証明書の管理など、特定の機能が制限されなくなります。
3. 管理者パスワードが設定されている場合はプロンプトで入力し、Enterキーを押します。
`Shell>` プロンプトが表示されます。
4. タスクの完了に必要なコマンドを入力します。
5. `Exit` コマンドを入力して、シェルを終了します。

インテグレートドマネジメントログの表示および消去

インテグレートドマネジメントログ（IML）オプションは、サーバーで発生した履歴イベントの記録を表示または消去できます。IMLのエントリ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。IMLは、各イベントに1分単位のタイムスタンプを設定します。

手順

1. システムユーティリティ画面で、内蔵アプリケーション > インテグレートドマネジメントログを選択します。
2. オプションを選択します。
 - IMLを表示 - インテグレートドマネジメントログレコードを表示します。
 - IMLをクリア - インテグレートドマネジメントログのすべてのエントリーをクリアします。

Active Health Systemデータのダウンロード

HPEサポートは、Active Health System (AHS) ログファイルを問題解決のために使用していました。ケースを送信するための高度な手順は次のとおりです。

手順

1. サポートの問題が発生しているサーバーからAHSログをダウンロードします。
2. Active Health System ViewerにAHSログをアップロードします (<https://www.hpe.com/servers/AHSV>) 。
3. 自己修復アクションの推奨については、障害検出解析を確認します。詳しくは、ASHVユーザーガイドを参照してください。
4. AHSVナビゲーションメニューを使用して、サポートケースを作成します。詳しくは、ASHVユーザーガイドを参照してください。

詳しくは

[Active Health Systemログのダウンロード](#)
[ASHVへのAHSログのアップロード](#)

Active Health Systemログのダウンロード

デフォルトでは、異なる期間を指定するための 範囲の開始日と 範囲の終了日フィールドを使用していない場合、システムは、前の7日間からのActive Health Systemログをダウンロードします。Hewlett Packard Enterpriseサポートから要求された場合は、保存されている .ahs ファイルをコピーし、カスタマーサポートの担当者に電子メールで送信することができます。

手順

1. システムユーティリティ画面で、内蔵アプリケーション > Active Health Systemログを選択します。
2. Active Health Systemログのダウンロードを選択します。
3. 次の情報を、選択または入力します。
 - ログ全体をダウンロード - サーバーの使用期間のAHSレコードをダウンロードするようにサポート担当者からアドバイスを受けない限り、この設定を無効のままにしておきます（選択しない）。デフォルト設定は、無効です。
 - 範囲の開始日 - ログの収集の開始日を入力します。
 - 範囲の終了日 - ログの収集の終了日を入力します。
 - ファイルの位置を選択 - このオプションを選択してFile Explorer画面を開き、AHSログをダウンロードするローカルまたは仮想の書き込み可能メディア上でFAT32/FAT16パーティションを選択します。

注記:

AHSログをUSBまたはHDDメディアに保存することをお勧めします。SDカードへのログの保存はサポートされていません。

- オプション：サポートケース番号や連絡先情報などのお客様の情報を追加します。
4. ダウンロードを開始を選択します。

UEFIファームウェアはiLOと通信をして、要求されたAHSログファイルをダウンロードし、そのファイルを1つ

の .ahs ファイルにまとめます。

5. Hewlett Packard Enterpriseサポートから要求された場合は、保存されている .ahs ファイルをコピーし、カスタマーサポートの担当者に電子メールで送信するか、またはAHSVへのAHSログのアップロードタスクを使用してください。

注記:

システムユーティリティ > システムヘルス > Active Health Systemログを選択しても、AHSログファイルをダウンロードできます。

詳しくは

[AHSVへのAHSログのアップロード](#)

アクティブヘルスシステムビューアにログインする

手順

1. AHSVのWebページにアクセスするには、サポートされているブラウザで<http://www.hpe.com/servers/ahsv>にアクセスします。以下では、サポートされているブラウザを示します。
 - Internet Explorer 11
 - Chrome v51以降
 - Firefox v46以降
2. ユーザーID（メールアドレス）と、パスワードを入力してサインインをクリックします。

注記:

HPEパスポートアカウントを使用してログインする場合やHPEパスポートアカウントを作成する場合は、<https://www.hpe.com/info/insightonline>にアクセスします。ほとんどの場合、HPEパスポートアカウントはHPEパスポートアカウン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。

注記:


ログイン認証情報をシステムに記憶させるには、ログイン情報を記憶を選択してからサインインをクリックしてください。

AHSVへのAHSログのアップロード

最大ファイルサイズ制限は250 MBです。250 MBよりも大きいログについては、HPEサポート センターまでお問い合わせください。

このタスクをAHSVで実行します。

前提条件

-
-  **重要:** AHSログを作成したサーバーには、有効な保証が必要です。サーバーが保証対象外場合、次のエラーメッセージが表示されます。 `Server is not Entitled. Check these options for renewing your license.` オプションは次のとおりです。

- ライセンスをさらに購入する
 - ライセンス購入のための認定パートナーを探す
 - HPEサポートに問い合わせる。
-

手順

1. AHSログをアップロードを選択します。
2. ログファイルに移動して、開くをクリックします。

解析とログ ロード動作状態を示すウィンドウが表示されます。AHSログをロードしているとき、画面に予想される完了時間が表示されます。

□ ヒント:

また、このウィンドウには、さまざまなプラットフォームのビデオが表示されます。ログファイルがロードされるのを待っている間に、さまざまなビデオを検索して再生できます。

ロード処理をキャンセルするには、キャンセルをクリックします。

内蔵Diagnostics

このオプションを使用して、ハードウェア診断メニューを起動します。そこから、ヘルス概要ステータスの表示、システムテストおよびコンポーネントテストの実行、テストログの表示を行うことができます。

内蔵Diagnosticsの起動

内蔵Diagnosticsオプションを使用して、ハードウェア診断メニューを起動します。そこから、ヘルス概要ステータスの表示、システムテストおよびコンポーネントテストの実行、テストログの表示を行うことができます。

手順

1. システムユーティリティ画面で、内蔵アプリケーション > 内蔵Diagnosticsの順に選択します。
Hardware Diagnostics画面が表示されます。
2. オプションを選択します。
 - システムヘルス - ヘルスの概要 (BIOSハードウェア、ファン、温度、バッテリー、メモリ、ネットワーク、およびストレージのステータス)、ファン (ゾーン、ラベル、ステータス、および速度)、温度 (ラベル、位置、ステータス、現在の測定値、および警告)、電源装置 (電源装置の概要およびSmart Storageバッテリー)、プロセッサ、メモリ、NIC情報、ストレージ、およびファームウェア情報をリスト表示します。
 - システムテスト - 情報をリスト表示し、ハードウェアサブシステムのチェック用のオプションを用意して、正しく動作していることを確認します。クイックテストオプションでは、10分間のハードウェアチェックを実行します。詳細テストオプションでは、ハードウェアの完全チェックが実行されます。このチェックは、完了まで2時間以上かかる可能性があります。
 - コンポーネントテスト - 情報をリスト表示し、プロセッサ、メモリ、ハードドライブ、キーボード、マウス、ネットワーク、オプティカルドライブ、システムボード、USBポート、およびビデオのテストを確認するためのオプションを用意しています。
 - テストログ - テストの種類と結果 (障害を含む) に関する情報が含まれるテストログを表示します。
 - IMLログ - すべてのIMLログファイルを表示します。IMLログファイルには、深刻度、クラス、開始時刻、およびアップデート時刻に関する情報が含まれます。
 - 言語 - 内蔵Diagnosticsで使用する言語を選択します。
 - 終了 - 内蔵Diagnosticsメニューを終了して、システムユーティリティ画面に戻ります。

Intelligent Provisioningの起動

Intelligent Provisioningは、組み込み型の単一サーバー用展開ツールで、サーバーのセットアップを簡素化し、信頼性と一貫性のあるサーバー構成の展開を実現します。 Intelligent Provisioningオプションでは、この起動に限り Intelligent Provisioningホストオーバーライドオプションを選択できます。このオプションでは、通常のブート順序も、ブートモードの設定も変更されません。詳しくは、Hewlett Packard EnterpriseのWebサイト (<https://www.hpe.com/info/intelligentprovisioning/docs>) の Intelligent Provisioningユーザーガイドを参照してください。

手順

1. システムユーティリティ画面で、内蔵アプリケーション > Intelligent Provisioningを選択します。
2. システムユーティリティメニューに戻るには、サーバーを再起動します。

内蔵iPXEの起動

内蔵iPXEオプションを使用して、内蔵iPXEを起動します。内蔵iPXEは、追加機能によって拡張された完全なPXE実装を提供します。

前提条件

内蔵iPXEが有効になっている。

手順

システムユーティリティ画面で、内蔵アプリケーション > 内蔵iPXEを選択します。

内蔵iPXEが起動し、ネットワークオプション > 内蔵iPXEで指定された操作が実行されます。

システム情報およびシステムヘルス

システム情報

このオプションを使用して、以下の情報を表示します。

- 概要 - 以下の項目を含むシステム設定の概要を示します。
 - システム名
 - シリアル番号
 - 製品ID
 - BIOS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/ユーザーデフォルト
 - ブートモード
 - システムメモリ
 - プロセッサタイプ
 - iLOファームウェアバージョン
 - 内蔵ネットワークデバイス
- プロセッサ情報 - 以下の項目を含む詳細なプロセッサ情報を表示します。
 - CPU数、ソケット番号、およびソケットロケータラベル
 - CPUソケットにCPUパッケージが装着されているかどうか
 - CPUの簡単な製造者の説明と、CPUがサポートする特性のリスト
 - コア数、有効なコア数、およびCPUパッケージ内のスレッド数（論理コア数）
 - CPUの定格速度と外部クロック

- CPUパッケージの電圧
- BIOSによってインストールされているマイクロコードパッチのリスト
- L1、L2、およびL2キャッシュのサイズと速度
- メモリ情報 - 以下の項目を含むメモリの詳細情報を表示します。
 - システムメモリの合計
 - メモリスロットの総数
 - 動作周波数と電圧
 - CPUに接続されたスロットの数
 - CPUに直接接続されているインストールされたモジュールの数
- ストレージ情報
- PCIデバイス情報 - 各PCIデバイスに関する詳細な情報を表示します。
- ファームウェア情報 - 以下の項目を含むファームウェアの詳細情報を表示します。
システム情報をファイルにエクスポート - 次のことを実行できる画面を開きます。
 1. ファイルの位置を選択 - エクスポートされる情報のための新規ファイルを選択または指定します。
 2. エクスポートするシステム情報の種類を選択します。
 - 概要
 - プロセッサ
 - メモリ
 - PCIデバイス
 - ファームウェア
 3. 情報をエクスポートするには、選択内容を保存し、システムユーティリティを終了します。

システム情報の表示

手順

1. システムユーティリティ画面で、システム情報を選択します。
2. 関連情報を表示するためのオプションを選択します。

注記:

RESTfulインターフェイスツールを使用して、ファームウェア情報を表示することもできます。次のRESTfulインターフェイスツールのドキュメントを参照してください：
<https://www.hpe.com/info/restfulinterface/docs>。

システムヘルスの表示

システムヘルスオプションを使用して、システム内のすべてのデバイスのヘルスステータスを確認できます。たとえば、この画面には、ブートプロセス中に検出されたサポートされていないデバイスが表示されず（存在する場合）。

手順

1. システムユーティリティ画面で、システムヘルスを選択します。
2. システムヘルスの表示を選択します。
3. オプション：AHSログをダウンロードします。詳しくは、[Active Health Systemログのダウンロード](#)を参照してください。

ださい。

システムの再起動、言語の選択、およびブラウザーモードの設定

システムの再起動

システムを終了して再起動

終了してシステムの起動を再開 オプションを使用して、システムを終了し、通常のブートプロセスを続行します。ブート順序のリストに従ってブートが続行され、システム内の最初のブート可能なオプションが起動されます。たとえば、UEFI内蔵シェルが有効で、UEFIブート順序リスト内で最初のブート可能なオプションとして選択されている場合、UEFI内蔵シェルを起動できます。

手順

1. システムユーティリティ画面で、終了してシステムの起動を再開を選択します。
確認メッセージが表示されます。
2. OKをクリックするか、Enterを押します。

システムの再起動

システムを再起動オプションを使用して、通常のブートプロセスを続行せずに、システムを終了して再起動します。

手順

1. システムユーティリティ画面で、システムを再起動を選択します。
確認メッセージが表示されます。
2. はい、再起動しますをクリックするか、またはEnterキーを押します。

言語とブラウザーモードの選択

システム言語の選択

手順

1. システムユーティリティ画面で、言語を選択を選択します。
2. 言語を選択します。
 - 英語
 - 日本語
 - 中文（簡体）

3. 設定を保存します。

ブラウザーモードの選択

手順

1. システムユーティリティ画面で、セットアップブラウザーの選択を選択します。
2. 設定を選択します。
 - GUI - 統合リモートコンソールまたは物理端末を使用してシステムユーティリティにアクセスするときにGUIベースのブラウザーを開きます。
 - テキスト - シリアルコンソールを使用してシステムユーティリティにアクセスするときにテキストベースのブラウザーを開きます。
 - 自動 - システムユーティリティへのアクセス方法に応じて、テキストベースのブラウザーまたはGUIベースのブラウザーを開きます。
3. 設定を保存します。

詳しくは

[GUIモードでのシステムユーティリティ内での移動](#)

BIOS/プラットフォーム構成オプション

このバージョンの新機能

このバージョンに特定のBIOS/プラットフォーム構成（RBSU）オプションが追加されました。

- 仮想化オプションの変更：
[AMD DMA再マッピングの有効化または無効化](#)
- サーバーセキュリティ設定の変更：
[Microsoft \(R\) Secured-coreサポートの有効化または無効化](#)
- PCIeデバイス構成設定の変更 > 高度なPCIe構成設定の選択
[PCIe MCTPオプションの構成](#)

ワークロードプロファイルとパフォーマンスオプション

ワークロードプロファイルは、HPE Intelligent System Tuning (IST) 機能の1つで、事前構成されたワークロードプロファイルを選択することにより、HPE ProLiantサーバーのリソースを調整することができます。サーバーは、選択したワークロードに一致するようにBIOS設定を自動的に構成します。

システムで提供されたワークロードプロファイル

システムは、これらのワークロードプロファイルを提供します。

一般的な電力効率のコンピューティング

このプロファイルは、ほとんどのProLiantサーバーとHPE Synergyコンピュートモジュールのデフォルトのプロ

ファイルです。

このプロファイルは、ほとんどのアプリケーションのワークロードに役立ち、しかも全体のパフォーマンスに及ぼす影響が最小限になる電力管理設定を有効にする、最も一般的なパフォーマンス設定を適用します。適用される設定は、一般的なアプリケーションパフォーマンスと電力効率の間のバランスのとれたアプローチに対して非常に有利に働きます。

このプロファイルは、通常BIOSをワークロード用に調整しないお客様にお勧めします。

一般的なピーク周波数のコンピューティング

このプロファイルは、任意の時点において個々のコアで可能な最大周波数を実現する必要があるプロセッサやメモリにとって一般的に有利になるワークロードを対象としています。電力管理設定は、任意のコンポーネントの上方周波数が容易に得られることが確実なときに適用されます。発生する可能性がある遅延時間よりも処理速度が優先されます。このプロファイルは汎用プロファイルであるため、プロセッサコアとメモリの速度を向上させるための全般的な最適化が行われます。

このプロファイルは、計算時間が短いことが通常有利になるワークロードに有利です。

一般的なスループットのコンピューティング

このプロファイルは、合計最大継続ワークロードスループットが必要な場合にワークロードに対して使用するためのものです。個々のコアが最大の速度でプロセッサが実行されても、スループットの向上が必ずしも実現されるわけではありません。スループットの向上は、プロセッサが最大使用率のときに使用可能なすべてのコアで持続的な処理を実行できるときに実現されます。到達可能な最大帯域幅に影響することが認識されている場合、電力管理設定は無効化されます。

最高のスループットが達成されるのは、ワークロードがNUMA (Nonuniformed Memory Access) を認識して最適化されているため、NUMAの認識が有利に働く設定が適用される場合です。

仮想化 - 電力効率

このプロファイルは、仮想化環境で使用するためのものです。このプロファイルにより、利用可能なすべての仮想化オプションが有効になります。特定の仮想化テクノロジーは、非仮想化環境にパフォーマンス上の影響を及ぼすことがあり、他のプロファイルで無効にすることができます。電力管理設定は、仮想化オペレーティングシステムを実行している場合にパフォーマンスに影響を及ぼすことがあり、このプロファイルは仮想化に配慮した電力管理設定を適用します。

仮想化 - 最大パフォーマンス

このプロファイルは、仮想化環境で使用するためのものです。このプロファイルにより、利用可能なすべての仮想化オプションが有効になります。最大のパフォーマンスを提供するため、電力管理設定は無効になります。

低レイテンシ

このプロファイルは、ワークロードの計算待機時間が最小になることを希望する顧客が使用するためのものです。このプロファイルは、HPE低レイテンシのホワイトペーパーに記載されている最も一般的なベストプラクティスに従っています。全体的な計算待機時間を減少させるために、最大速度およびスループットが犠牲になります。計算待機時間を導入する電力管理およびその他の管理機能も無効化されます。

このプロファイルは、リアルタイムのオペレーティングシステム (RTOS) またはトランザクション待ち時間の影響を受けやすい他のワークロードを実行している顧客に有利に働きます。

ミッションクリティカル

このプロファイルは、基本的なサーバーのデフォルト値を上回るサーバー信頼性とパフォーマンスの妥協点を探る顧客によって使用されるためのものです。プロファイルには、計算パフォーマンスに対して測定可能な影響を及ぼす、高度なメモリの信頼性、可用性、および保守性 (RAS) の機能があります。このプロファイルを有効にすると、最大メモリ帯域幅に影響を与え、メモリの遅延が大きくなります。

トランザクションアプリケーション処理

このプロファイルは、データベースバックエンドを必要とするオンライントランザクション処理 (OLTP) アプリケーションなどのビジネス処理環境で使用するためのものです。たとえば、ワークロードは通常、共同でホストされるデータベースコンポーネントを持つ単一サーバー上で実行されるユーザーベースの多数のトランザクションアプリケーションで構成されています。このプロファイルは、ピーク周波数とスループットの両方の管理要件のバランスを調整します。

ハイパフォーマンスコンピューティング (HPC)

このプロファイルは、従来のHPC環境で実行しているお客様向けです。通常これらの環境は、大規模な科学的および工学的なワークロードを処理するために、各ノードが長期間にわたって最大の使用率で実行できるクラスター環境です。Apolloシリーズサーバーのデフォルトの場合、継続的に利用可能な帯域幅およびプロセッサコンピュート容量を優先させるために、電力管理は通常無効化されます。このプロファイルは、最大スループットを達成するためにいくらかの遅延時間が受け入れられたことを除けば、低レイテンシプロファイルに似ています。

意思決定サポート

このプロファイルは、データマイニングやオンライン分析処理 (OLAP) などのデータウェアハウスでの操作およびアクセスに焦点を合わせたエンタープライズビジネスデータベース (Business Intelligence) ワークロードの

ためのものです。

グラフィック処理

このプロファイルは、Graphics Processing Unit (GPU) を使用するサーバー構成上で実行しているワークロードのためのものです。GPUは通常、I/Oとメモリ間の最大帯域幅によって異なります。I/Oとメモリ間のリンクに影響を与える電源管理機能は、無効化されています。ピア間トラフィックも重要であるため、仮想化も無効になります。

I/Oスループット

このプロファイルは、I/Oとメモリ間の最大スループットに依存している構成に使用されるものです。I/Oとメモリ間のリンクにパフォーマンス上の影響を与えるプロセッサ使用率に依存する電源管理機能は、無効化されています。

カスタム

ワークロードプロファイルメニューのこのオプションは、ワークロードプロファイルを無効にします。展開の特定のBIOSオプションを手動で設定する場合、このオプションを使用します。カスタムを選択すると、以前に選択したプロファイルの設定がすべて変換されます。すべてまたは一部のオプションを編集できます。

カスタムはプロファイルではなく、指定した設定はテンプレートとして保存されません。

サーバーのデフォルトプロファイル

ワークロードプロファイルのオプションは、さまざまな電力消費とパフォーマンス要件をサポートします。ほとんどのHPE ProLiant Gen10サーバーおよびHPE Synergyコンピュートモジュールでは、ワークロードプロファイルはデフォルトで一般的な電力効率のコンピューティングに設定されています。このワークロードプロファイルは、ほとんどのアプリケーションワークロードに適した一般的なパフォーマンスと消費電力の設定を提供します。HPE Apolloシステム内のProLiant XLサーバーの場合、ワークロードプロファイルはデフォルトでハイパフォーマンスコンピューティングに設定されています。

カスタムプロファイル以外のワークロードプロファイルを選択すると、他の設定オプションに影響します。たとえば、一般的なピーク周波数のコンピューティングプロファイルを選択すると、パワーレギュレーターモードがスタティックハイパフォーマンスになります。この設定は変更できず、グレー表示されます。

Workload Matching

Hewlett Packard EnterpriseサーバーのデフォルトのBIOS設定は、パフォーマンスと電力効率のバランスをとります。これらの設定は、特定のアプリケーションのワークロードに適するように調整できます。

HPE Gen10以降のサーバーには、お客様が既知のワークロードベースのチューニングプロファイルを使用して、BIOS設定を調整するUEFI構成オプションがあります。ワークロードのプロファイル設定と実際に展開されたワークロードを一致させると、すぐに使えるBIOSのデフォルトを使用するだけの場合と比べたパフォーマンスのゲインがわかります。

詳しくは、<https://www.hpe.com/support/Workload-UG-en>にあるHPE ProLiant Gen10、ProLiant Gen10 Plusサーバー、およびHPE Synergy用のUEFIワークロードベースのパフォーマンスおよびチューニングガイドを参照してください。

ワークロードプロファイルの依存関係の概要

依存関係

BIOS構成に使用できる複数のオプションがあります。すべてのプロファイルで、同じオプションが特定の設定に設定されるわけではありません。各プロファイルは、特定のパフォーマンス結果を得るために設計されており、それらの結果を満たすために異なるオプションを設定します。プロファイルが設定するオプションは、依存関係と呼ばれます。他のすべてのオプションは、ワークロードプロファイルの影響を受けないため、非依存設定と呼ばれます。

依存関係とプロファイルの切り替え

プロファイルを変更すると、そのプロファイルの依存関係の設定のみが変更されます。非依存設定は、プロファイルを

変更する前と変わりません。

以下に例を示します。

1. 一般的なパワー効率コンピューティングプロファイルを選択します。このプロファイルでは、エネルギーパフォーマンスバイアスがパフォーマンスをバランスに設定されています。
2. 一般的なピーク周波数のコンピューティングプロファイルを選択します。このプロファイルにはエネルギーパフォーマンスバイアスに対する依存関係はありません。エネルギーパフォーマンスオプションはパフォーマンスをバランスに設定されています。これは、その設定が一般的なパワー効率コンピューティングプロファイルから変換されるためです。
3. 一般的なスループットコンピューティングプロファイルを選択します。このプロファイルでは、エネルギーパフォーマンスバイアスが最大パフォーマンスに設定されています。
4. 一般的なピーク周波数のコンピューティングプロファイルを選択します。このプロファイルにはエネルギーパフォーマンスバイアスに対する依存関係はありません。エネルギーパフォーマンスバイアスは最大パフォーマンスに設定されています。これは、その設定が一般的なスループットコンピューティングプロファイルから変換されるためです。

以前のプロファイルと依存関係に戻すことはできません。新しいプロファイルに変更すると、新しい依存関係が適用されます。古いプロファイルに戻す唯一の方法は、変更を保存せずに終了することです。保存せずに終了すると、RBSUを入力したときの状態に戻ります。プロファイルを保存すると、そのプロファイルから中間の依存関係に戻すことはできません。

依存関係とオプションのマトリックス

この表は、ワークロードプロファイルとその依存関係を示しています。ワークロードプロファイルは、ユーザーインターフェイスにリストされている順序でリストされます。テーブル内の「X」は、オプションの設定にプロファイルの要件が存在せず、編集可能であることを示しています。依存関係は編集できません。

注記:

この表のオプションの一部は、サーバーによっては調整できません。ただし、これらの設定を調整するオプションがない場合でも、デフォルトはここに示す値です。

インテル(R) Xeon(R) スケーラブルプロセッサのワークロードプロファイルの依存関係

注記:

オプションは、サーバーに取り付けられているハードウェアによって異なります。

表13: ワークロードプロファイル：一般的な電力効率のコンピューティング - 低レイテンシ

	一般的な電力効率のコンピューティング	一般的なピーク周波数のコンピューティング	一般的なスループットのコンピューティング	仮想化 - 電力効率	仮想化 - 最大パフォーマンス	低レイテンシ
SR-I0V	x	x	x	有効	有効	無効
VT-D	x	x	x	有効	有効	無効
VT-x	x	x	x	有効	有効	無効
パワーレギュレーター	ダイナミックパワーセービング	スタティックハイパフォーマンス	スタティックハイパフォーマンス	OSコントロール	スタティックハイパフォーマンス	スタティックハイパフォーマンス
最小プロセッサアイドル電力コアCステート	C6	x	x	C6	Cステートなし	Cステートなし

	一般的な電力効 率のコンピュ ーティング	一般的なピーク 周波数のコン ピューティング	一般的なスルー プットのコン ピューティング	仮想化 - 電力 効率	仮想化 - 最大 パフォーマンス	低レイテンシ
最小プロセッ サーアイドル電 力パッケージC スタート	パッケージC6リ テンション	パッケージC6リ テンション	パッケージC6リ テンション	パッケージC6リ テンション	Cスタートなし	Cスタートなし
エネルギーパ フォーマンスバ イアス	パフォーマンス をバランス	x	最大パフォーマ ンス	パフォーマンス をバランス	最大パフォーマ ンス	最大パフォーマ ンス
協調電力制御	有効	無効	無効	有効	無効	無効
インテルDMIリ ンク周波数	自動	自動	自動	自動	自動	自動
インテルターボ ブーストテクノ ロジー	有効	有効	有効	x	有効	無効
インテルNIC DMAチャンネル (IOAT)	有効	x	x	x	x	x
HWプリフェッ チャー	有効	有効	有効	x	x	有効
隣のセクターの プリフェッチ	有効	有効	有効	x	x	有効
DCUストリーム プリフェッ チャー	有効	有効	有効	x	x	有効
DCU IPプリ フェッチャー	有効	有効	有効	x	x	有効
NUMAグループサ イズ最適化	フラット	クラスター構成	クラスター構成	クラスター構成	クラスター構成	クラスター構成
メモリ巡回スク ラビング	x	x	x	x	x	無効
メモリリフレッ シュレート	x	1x	1x	x	x	1x
UPIリンク電力 管理	有効	無効	無効	有効	無効	無効
Sub-NUMAクラス タリング	無効	x	有効	無効	有効	x
エネルギー効率 ターボ	有効	無効	無効	有効	無効	無効
アンコア周波数 のシフト	自動	最大	x	自動	最大	最大
x2APIC	x	x	x	x	x	無効
チャンネルイン ターリーブ	有効	有効	有効	有効	有効	有効
メモリバス周波 数	x	x	x	x	x	x
アドバンスドメモ リプロテク ション	x (ROMバージョ ン1.50以前) ADDDC (ROMバー ジョン1.50以 降)	x (ROMバージョ ン1.50以前) ADDDC (ROMバー ジョン1.50以 降)	x (ROMバージョ ン1.50以前) ADDDC (ROMバー ジョン1.50以 降)	x (ROMバージョ ン1.50以前) ADDDC (ROMバー ジョン1.50以 降)	x (ROMバージョ ン1.50以前) ADDDC (ROMバー ジョン1.50以 降)	ECC

表24: ワークロードプロファイル: ミッションクリティカル - I/Oスループット

ミッション クリティカル	トランザクショ ンアプリケーション 処理	ハイパフォーマ ンスコンピュー ティング (HPC)	意思決定サポー ト	グラフィック処 理	I/Oスループッ ト
-----------------	----------------------------	-------------------------------------	--------------	--------------	---------------

	ミッションクリティカル	トランザクションアプリケーション処理	ハイパフォーマンスコンピューティング (HPC)	意思決定サポート	グラフィック処理	I/Oスループット
SR-IOV	x	x	無効	x	無効	x
VT-D	x	x	無効	x	無効	x
VT-x	x	x	無効	x	無効	x
パワーレギュレーター	x	スタティックハイパフォーマンス	スタティックハイパフォーマンス	x	x	x
最小プロセッサアイドル電力 コアCステート	x	Cステートなし	Cステートなし	x	x	x
最小プロセッサアイドル電力 パッケージCステート	x	Cステートなし	Cステートなし	x	x	x
エネルギーパフォーマンス バイアス	x	最大パフォーマンス	最大パフォーマンス	x	最大パフォーマンス	最大パフォーマンス
協調電力制御	x	x	無効	x	x	x
インテルDMIリンク周波数	自動	自動	自動	自動	自動	自動
インテルターボブーストテクノロジー	x	有効	有効	x	x	x
インテルNIC DMAチャネル (IOAT)	x	有効	有効	x	x	有効
HWプリフェッチャー	有効	有効	有効	有効	有効	有効
隣のセクターのプリフェッチ	有効	有効	有効	有効	有効	有効
DCUストリームプリフェッチャー	有効	有効	有効	有効	有効	有効
DCU IPプリフェッチャー	有効	有効	有効	有効	有効	有効
NUMAグループサイズ最適化	x	クラスター構成	クラスター構成	クラスター構成	クラスター構成	クラスター構成
メモリ巡回スクラビング	x	x	x	x	x	x
メモリリフレッシュレート	2x	x	1x	x	x	x
UPIリンク電力管理	x	無効	無効	x	x	x
Sub-NUMAクラスタリング	x	x	x	x	x	x
エネルギー効率ターボ	x	x	無効	x	x	x
アンコア周波数のシフト	x	x	最大	x	最大	最大
x2APIC	x	x	無効	x	無効	x
チャンネルインターリーブ	有効	有効	有効	有効	有効	有効
メモリバス周波数	x	x	x	x	x	x

ミッションクリティカル	トランザクションアプリケーション処理	ハイパフォーマンスコンピューティング (HPC)	意思決定サポート	グラフィック処理	I/Oスループット
アドバンスドメモリープロテクション	ADDCC (ROMバージョン1.50以前) ADDCC (ROMバージョン1.50以降)	ECC (ROMバージョン1.50以前) ADDCC (ROMバージョン1.50以降)	x (ROMバージョン1.50以前) ADDCC (ROMバージョン1.50以降)	x (ROMバージョン1.50以前) ADDCC (ROMバージョン1.50以降)	x (ROMバージョン1.50以前) ADDCC (ROMバージョン1.50以降)

第1世代および第2世代AMD EPYC (TM) プロセッサのワークロードプロファイルの依存関係

注記:

オプションは、サーバーに取り付けられているハードウェアによって異なります。

表13: ワークロードプロファイル: 一般的な電力効率のコンピューティング - 低レイテンシ

	一般的な電力効率のコンピューティング	一般的なピーク周波数のコンピューティング	一般的なスループットのコンピューティング	仮想化 - 電力効率	仮想化 - 最大パフォーマンス	低レイテンシ	ミッションクリティカル
パワーレギュレーター	OSコントロール	スタティックハイパフォーマンス	スタティックハイパフォーマンス	OSコントロール	スタティックハイパフォーマンス	スタティックハイパフォーマンス	x
SR-IOV	x	x	x	有効	有効	無効	x
AMD IOMMU	x	x	x	有効	有効	x	x
AMDバーチャライゼーションテクノロジー	x	x	x	有効	有効	無効	x
最小プロセスサーアイドル電力コアステート	C6	x	x	C6	Cステートなし	Cステートなし	x
AMDターボコア	有効	有効	有効	x	有効	無効	x
L1ストリームHWプリフェッチャー	有効	有効	有効	x	x	有効	有効
L2ストリームHWプリフェッチャー	有効	有効	有効	x	x	有効	有効
NUMAグループサイズ最適化	フラット	クラスター構成	クラスター構成	クラスター構成	クラスター構成	クラスター構成	x
メモリ巡回スクラビング	x	x	x	x	x	無効	x
メモリアリフレッシュレート	x	1x	1x	x	x	1x	2x
x2APIC	x	x	x	x	x	自動	x

表24: ワークロードプロファイル: ミッションクリティカル - I/Oスループット

	トランザク ションアプリ ケーション処 理	ハイパフォー マンスコン ピューティン グ (HPC)	意思決定サ ポート	グラフィック 処理	I/Oスルー プット	カスタム	EV名
パワーレギュ レーター	スタティック ハイパフォー マンス	スタティック ハイパフォー マンス	x	x	x	x	CQHPER
SR-IOV	x	無効	x	無効	x	x	CQHSRIOV
AMD IOMMU	x	x	x	x	x	x	CQHSKTPROC
AMDバーチャ ライゼーショ ンテクノロ ジー	x	無効	x	無効	x	x	CQHAMD
最小プロセッ サーアイドル 電力コアCス テート	Cステートな し	Cステートな し	x	x	x	x	CQHSKTPOWER
AMDターボコ ア	有効	有効	x	x	x	x	CQHSKTPOWER
L1ストリーム HWプリフェッ チャー	有効	有効	有効	有効	有効	x	CQHSKTPROC
L2ストリーム HWプリフェッ チャー	有効	有効	有効	有効	有効	x	CQHSKTPROC
NUMAグループ サイズ最適化	クラスター構 成	クラスター構 成	クラスター構 成	クラスター構 成	クラスター構 成	x	CQHNUMA
メモリ巡回ス クラビング	x	x	x	x	x	x	CQHMEM
メモリリフ レッシュレー ト	x	1x	x	x	x	x	CQHMEM
x2APIC	x	自動	x	自動	x	x	CQHSKTPROC

ワークロードプロファイルの適用

システムで提供される定義済みの設定に応じて、システムでワークロードを管理するためのワークロードプロファイルを適用します。依存オプションは変更できず、グレー表示されます。非依存オプションはどれもプロファイル内で変更できません。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ワークロードプロファイルを選択します。
2. ワークロードプロファイルを選択します。
3. オプション:
変更したい非依存オプションをすべて変更します。
4. ワークロードプロファイルを保存し、再起動して適用します。

詳しくは

[ワークロードプロファイルとパフォーマンスオプション](#)

プロファイルの適用後の依存オプションの変更

ワークロードプロファイルで変更する依存オプションが1つまたは複数存在する場合があります。定義済みのプロファイルでは依存オプションを変更することはできません。カスタムモードでは、依存オプションを変更できます。カスタムモードでは、展開はプロファイルモードになっていないため、オプションの設定を手動で調整することができます。カスタムモードに入ると、以前に適用されたプロファイルのすべての設定が表示されます。

依存設定を変更する最も簡単な方法は、適用されているプロファイルを変更することです。まず、使用する設定の大部分が含まれるワークロードプロファイルを適用してから、カスタムモードに変更します。次に、新しい値を持つ設定だけを変更します。

前提条件

このタスクを実行する前に、ワークロードプロファイルを適用します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ワークロードプロファイルを選択します。
2. カスタムプロファイルオプションを選択します。
以前に適用されたワークロードプロファイルのすべての設定が表示されます。すべてのオプションは編集できます。
3. 新しい値を指定するオプションを変更します。
4. 変更を適用するには、保存して再起動します。

システムオプションの変更

手順

システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプションを選択します。

ブート時間最適化の構成

動的消費電力上限機能の設定


動的消費電力上限機能の構成オプションを使用して、ブート処理中にシステムROMが電力較正を実行するかどうかを制御します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > ブート時間最適化 > 動的消費電力上限機能を選択します。
2. 設定を選択します。
 - 自動 - 電力較正は、最初にサーバーが起動されたときに実行し、サーバーのハードウェア構成の設定が変更されたときにのみ、再度実行されます。
 - 有効 - システムブートのたびに、電力較正が実行されます。
 - 無効 - 電力較正は実行されず、動的消費電力上限はサポートされていません。
3. 設定を保存します。

拡張メモリテストの有効化または無効化

拡張メモリテストオプションを使用すると、メモリの初期化プロセスでシステムがメモリを検証するかどうかを構成できます。有効にすると、訂正不能メモリエラーが検出された場合に、そのメモリが特定され、故障したDIMMがIMLに記録されます。

 注記:

このオプションを有効にすると、ブート時間が大幅に伸びる可能性があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > ブート時間最適化 > 拡張メモリテストを選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

メモリファーストトレーニングの有効化または無効化

メモリファーストトレーニングオプションを使用して、サーバーの再起動時のメモリトレーニングを構成します。有効にすると、プラットフォームは、サーバーの前のコールドブートで決定された、保存済みのメモリトレーニングパラメーターを使用します。これによりサーバーのブート時間が改善されます。ご使用のサーバーにインストールされ、かつこの設定が有効になっていると、ウォームリセットの間、NVDIMM-Nメモリの内容は残ったままです。メモリファーストトレーニングが無効であると、ウォームリセットのたびにcold resetにアップグレードされ、その結果、NVDIMM-Nのバックアップと復元が行われることとなります。メモリファーストトレーニングを有効なままにしておくことをお勧めします。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > ブート時間最適化 > メモリファーストトレーニングを選択します。
2. 設定を選択します。
 - 有効 - 以前保存されたメモリトレーニングのパラメーターをサーバーが使用できるようにします。
 - 無効 - プラットフォームは、サーバーが再起動するたびに、完全なメモリトレーニングを実行します。
3. 設定を保存します。

UEFI POST検出モードの設定

UEFI POST検出モード オプションを使用して、システムがUEFIデバイスドライバーをロードする方法を制御します。


手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > ブート時間最適化 > UEFI POST検出モードを選択します。
2. 次のいずれかを選択します。
 - 自動 - システムは、UEFIブート順序リスト内のデバイスを起動するために必要なUEFIデバイスドライバーのみをロードします。
 - 完全検出の強制 - システムは、すべてのデバイスのUEFIドライバーをロードし、すべてのブートターゲットを使用可能にします。

 注記:

この設定により、ブート時間が大幅に増加する可能性があります。

- 高速検出の強制 - システムは、ブート時間を長くするためにできるだけ少ない数のデバイスを起動します。

 注記:

高速検出をサポートしていない一部のデバイスでは、正しく動作しない場合があります。

3. 設定を保存します。

ウォームリセット時のメモリ消去の有効化または無効化

ウォームリセット時のメモリ消去オプションを使用して、ウォームリセット時にメモリが消去される時期を構成します。このオプションを無効にすると、ウォームリセット時のメモリ消去がスキップされ、起動時間を短縮できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > ブート時間最適化 > ウォームリセット時のメモリ消去キーを押します。
2. 設定を選択します。
 - 有効-メモリはすべての再起動時に消去されます。
 - 無効-ウォームリセット時にオペレーティングシステムから要求された場合にのみメモリが消去されます。
3. 設定を保存します。

シリアルポートオプションの構成

内蔵シリアルポートの割り当て

内蔵シリアルポートオプションを使用して、論理COMポートアドレスと関連のデフォルトリソースを、選択した物理シリアルポートに割り当てます。

前提条件

適切な画面解像度を得るために、端末ソフトウェアのコンソール解像度を100x31に設定してください。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > シリアルポートオプション > 内蔵シリアルポートを選択します。
2. 設定を選択します。
 - COM 1: IRQ4: I/O: 3F8h-3FFh
 - COM 2: IRQ3: I/O: 2F8h-2FFh
 - 無効
3. 設定を保存します。

仮想シリアルポートの割り当て

仮想シリアルポートオプションを使用して、仮想シリアルポート (VSP) で使用する論理COMポートアドレスと関連のデフォルトリソースを割り当てます。VSPを使用すると、BIOSシリアルコンソールおよびオペレーティングシステムシリアルコンソールをサポートするために、iLO管理コントローラーを物理シリアルポートとして表示することができます。

前提条件

適切な画面解像度を得るために、端末ソフトウェアのコンソール解像度を100x31に設定してください。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > シリアルポートオプション > 仮想シリアルポートを選択します。
2. 設定を選択します。
 - COM 1
 - COM 2
 - 無効
3. 設定を保存します。

USBポートへのシリアルコンソールのミラーリング

このオプションを有効にすると、シリアルコンソールをUSBポートにミラーリングできます。ミラーリングにはHPEコンソールケーブルキットが必要です。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > シリアルポートオプション > USBコンソールリダイレクションを選択します。
2. オプションを選択します。
 - 有効
 - 無効
3. 設定を保存します。

USBオプションの構成

USB制御の設定

USBオプションのオプションを使用して、起動時のUSBポートと内蔵デバイスの動作を構成できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > USBオプション > USB制御を選択します。
2. 設定を選択します。
 - すべてのUSBポート有効 - すべてのUSBポートと内蔵デバイスを有効にします。
 - すべてのUSBポート無効 - すべてのUSBポートと内蔵デバイスを無効にします。
 - 外部USBポート無効 - 外部USBポートを無効にします。
 - 内部USBポート無効 - 内部USBポートを無効にします。
3. 設定を保存します。

USBブートサポートの有効化または無効化

USBブートサポートオプションを使用して、（サポートされている場合に）システムが仮想メディアデバイスなどの接続されているUSBデバイスや内蔵SDカードスロットからブートできるかどうかを制御します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > USBオプション > USBブートサポートを選択します。
2. 設定を選択します。
 - 有効 - システムは、サーバーに接続されているUSBデバイスから起動できます。
 - 無効 - システムは、サーバーに接続されているUSBデバイスから起動できません。
3. 設定を保存します。

取り外し可能フラッシュメディアブート順序の選択

取り外し可能フラッシュメディアブート順序オプションを使用すると、ブートデバイスが列挙されている場合に、最初に検索するUSBデバイスまたはSDカードデバイスを選択できます。

前提条件

ブートモードがレガシーBIOSモードに設定されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > USBオプション > 取り外し可能フラッシュメディアブート順序を選択します。
2. 設定を選択します。
 - 内部SDカードを最初 - 内蔵SDカードスロットを使用して起動します。
 - 内部ドライブキーを最初 - 内蔵USBドライブキーを使用して起動します。
 - 外部ドライブキーを最初 - 外部USBドライブキーを使用して起動します。
3. 設定を保存します。

内部SDカードスロットの有効化または無効化

内部SDカードスロットオプションを使用して、システムボードに内蔵されている、SD (Secure Digital) 不揮発性フラッシュメモリカードにサーバーがアクセスできるかどうかを制御します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > USB オプション > 内部SDカードスロットを選択します。
2. 設定を選択します。
 - 有効 - サーバーは内部SDカードスロットにアクセスできます。
 - 無効 - サーバーは内部SDカードスロットにアクセスできません。
3. 設定を保存します。

IOSシリアルコンソールとEMSの構成

BIOSシリアルコンソールポートの有効化または無効化

BIOSシリアルコンソールポートオプションを使用して、ビデオとキーストロークをシリアルポート経由でオペレーティングシステムブートにリダイレクトします。

注記:

このオプションは、シリアルポートに接続されている非端末デバイスに干渉する場合があります。その場合、このオプションを無効に設定します。

注記:

このオプションは、UEFI プリブートのシステムユーティリティを実行中は、英語モードのみサポートされます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > BIOSシリアルコンソール/EMSオプション > BIOSシリアルコンソールポートを選択します。
2. 設定を選択します。
 - 自動
 - 物理シリアルポート
 - 仮想シリアルポート
3. 設定を保存します。

BIOSシリアルコンソールエミュレーションモードの選択

BIOSシリアルコンソールエミュレーションモードオプションを使用して、エミュレーションモードタイプを選択します。シリアルターミナルプログラム (ハイパーターミナルまたはPuTTYなど) で使用するエミュレーションと一致させるには、このオプションを選択します。BIOSエミュレーションモードは、ターミナルプログラムで選択したモードと一致する必要があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > BIOSシリアルコンソール/EMS > BIOSシリアルコンソールエミュレーションモードを選択します。
2. 設定を選択します。
 - VT100
 - ANSI
 - VT100+
 - VT-UTF8
3. 設定を保存します。

BIOSシリアルコンソールボーレートの設定

BIOSシリアルコンソールボーレートオプションを使用します。これは、シリアルポートを介して通信されるデータの通信レートです。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > BIOSシリアルコンソール/EMS > BIOSシリアルコンソールボーレートを選択します。
2. 設定を選択します。
 - 9600
 - 19200
 - 57600
 - 115200
 - 38400
3. 設定を保存します。

EMSコンソールポート設定の構成

EMSコンソールポート設定オプションを使用して、物理または仮想シリアルポートを介したWindows Server Emergency Management console (EMS) のリダイレクト機能を含む、ACPIシリアルポートの設定を構成します。

EMSの構成オプションは変更されています。詳細については製品のドキュメントを参照してください。

注記:

すべてのBAUDレートがオペレーティングシステムによるシリアルポートリダイレクション (EMS) によって、サポートされていません。サポートされるモードについては、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。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > BIOSシリアルコンソール/EMS > EMSコンソールを選択します。
2. 物理または仮想ポート設定を選択します。
3. 設定を保存します。

サーバー可用性の構成

ASRの有効化または無効化

前提条件

システムマネジメントドライバーがロードされている。

ASRステータスオプションを使用して、自動サーバー復旧を有効または無効にします。ASRは、サーバーがロックアップした場合にサーバーを自動的に再起動します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > サーバー可用性 > ASRステータスを選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

注記:

ASRステータスオプションは、ProLiant Gen10サーバーでのみサポートされています。

ASRタイムアウトの設定

前提条件

ASRステータスが有効である。ASRタイムアウトオプションを使用して、オペレーティングシステムのクラッシュ時またはサーバーのロックアップ時のサーバーの再起動までの待ち時間を設定できます。選択した時間内にサーバーが応答しないと、サーバーは自動的に再起動します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > サーバー可用性 > ASRタイムアウトを選択します。
2. 待機時間を選択します。
 - 5分
 - 10分
 - 15分
 - 20分
 - 30分
3. 設定を保存します。

注記:

ASRタイムアウトオプションは、ProLiant Gen10サーバーでのみサポートされています。

ウェイクオンLANの有効化または無効化

ウェイクオンLANオプションを使用して、WOL対応NICを使用してサーバーの電源をリモートでオンにする機能を有効または無効にします。

前提条件

WOL対応のNIC、NICドライバー、およびオペレーティングシステム。

注記:

このオプションを有効にする場合、アダプターを挿入したり取り外したりする前に、すべての電源コードを外してください。アダプターによっては、サーバーに追加されたときにサーバーの電源をONにするものがあります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > サーバー可用性 > ウェイクオンLANを選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

POST F1プロンプトの遅延の設定

POST F1プロンプトオプションを使用して、サーバーのPOST画面での F1キーの表示方法を構成します。オプションが有効になっていてエラーが発生した場合、F1キーを押すと、サーバーの電源投入シーケンスを続行できます。POST処理中に、一連のシステムテストが実行され、次の処理を行います。

- システムが動作継続可能な状態で障害が発生した場合、システムは起動を続行した後、メッセージを出力します。
- 重要なコンポーネントに障害が発生したり欠落した場合、システムは起動を試みます。起動に成功した場合、メッセージとF1プロンプト（有効にしている場合）が表示されます。
- 欠落または障害が発生したコンポーネントがあり、システムが動作できない場合、そのコンポーネントが交換されるまでシステムは停止します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > サーバー可用性 > POST F1プロンプトを選択します。
2. 設定を選択します。
 - 20秒の遅延 - エラーが発生した場合、システムはF1プロンプトで20秒間動作を停止してから、OSの起動を続行します。
 - 2秒の遅延 - エラーが発生した場合、システムはF1プロンプトで2秒間動作を停止してから、OSの起動を続行します。
 - 無効 - エラーが発生した場合、システムはF1プロンプトを回避して起動を続行します。
3. 設定を保存します。

電源ボタンを一瞬押す機能の有効化または無効化

電源ボタンモードオプションを使用すると、電源ボタンの機能が一瞬有効または無効になります。このモードは4秒間の電源ボタンのオーバーライド、あるいはリモートの電源管理機能に影響がありません。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > サーバー可用性 > 電源ボタンモードを選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

自動電源オン時の状態の設定

自動電源オンオプションを使用して、AC電源が接続されたときにサーバーの電源を自動的にオンにする方法を構成します。デフォルトでは、AC電源の喪失後にAC電源が復旧したとき、システムは以前の電源状態に戻ります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > サーバー可用性 > 自動電源オンを選択します。
2. 設定を選択します。
 - 常に電源オン - AC電源が喪失した時点でシステムが「オフ」であった場合でも、システムは自動的に「オン」の状態に戻ります。
 - 常に電源オフ - システムは自動的に電源オフ状態に戻ります。

- 最後の電源状態を復元 - システムは自動的に以前の電源状態に戻ります。

3. 設定を保存します。

電源投入遅延の設定

電源投入遅延オプションを使用して、指定した時間にサーバーの電源をオンにすることを遅らせるかどうかを設定します。このオプションにより、電源喪失後のサーバーの電源オンを遅らせ、電力使用量の急激な増加を防ぐことができます。

注記:

次のイベントは電源投入遅延設定を上書きし、サーバーの電源をただちに投入します。

- iLO仮想電源ボタンを使用して電源ボタンを押す
- ウェイクオンLANイベント
- RTC (リアルタイムクロック) ウェイクアップイベント

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > サーバー可用性 > 電源投入遅延を選択します。
2. 設定を選択します。
 - 遅延なし
 - ランダムに遅延
 - 15秒遅延
 - 30秒遅延
 - 45秒遅延
 - 60秒遅延
3. 設定を保存します。

POST ASRの設定

POST ASRオプションを使用すると、POST ASR (自動サーバー復旧) を構成できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > サーバー可用性 > POST ASRを選択します。
2. 設定を選択します。
 - POST ASRがオン
 - POST ASRがオフ
3. 設定を保存します。

注記:

POST ASRオプションは、ProLiant Gen10 Plusサーバーでのみサポートされています。

POST ASRタイマーの設定

POST ASRタイマーを使用して、サーバーのロックアップ時のサーバーの再起動までの待ち時間を設定できます。

手順


1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > サーバー可用性 > POST ASRタイマーを選択します。
2. 設定を選択します。
 - 10分
 - 15分
 - 20分
 - 30分
3. 設定を保存します。

IPMIウォッチドッグタイマーの有効化または無効化

IPMIウォッチドッグタイマーオプションを使用すると、IPMIに準拠した起動時 (POST) のウォッチドッグタイマー (WDT) を有効にできます。このタイマーは、ユーザーがシステムに対してIPMIコマンドを発行すると無効になります。このタイマーは自動的に無効になりません。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > サーバー可用性 > IPMIウォッチドッグタイマーを選択します。
2. 設定を選択します。
 - 無効
 - 有効

 注記: IPMIウォッチドッグタイマーを有効にした後、ユーザーがシステムをRBSUまたはUEFIシェルに再起動した場合、タイマーは停止しません。WDTは選択された待機時間の後にタイムアウトし、システムは選択されたタイムアウトリセット動作を続行します。

3. 設定を保存します。

IPMIウォッチドッグタイマーのタイムアウトの設定

IPMIウォッチドッグタイマーのタイムアウトを使用すると、サーバーのロックアップが発生した場合にサーバーに対して必要なタイムアウト動作を実行するまでの待機時間を設定できます。

前提条件

IPMIウォッチドッグタイマーが有効になっている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > サーバー可用性 > IPMIウォッチドッグタイマーのタイムアウトを選択します。
2. 待機時間を選択します。
 - 10分
 - 15分
 - 20分
 - 30分
3. 設定を保存します。

IPMIウォッチドッグタイマーのポリシーの設定

IPMIウォッチドッグタイマーポリシーを使用して、サーバーのロックアップによってウォッチドッグタイマーが時間切れになったときのタイムアウト動作を構成します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > サーバー可用性 > IPMIウォッチドッグタイマーポリシーを選択します。
2. 設定を選択します。
 - 電源再投入
 - 電源切断
 - ウォームブート
3. 設定を保存します。

サーバー資産情報の表示および入力

サーバー情報の入力

サーバー情報オプションを使用して、サーバー管理者の参照情報を入力します。テキストの設定については、最大14文字を入力します。デフォルトでは、すべての値が空白です。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > サーバー資産情報 > サーバー情報を選択します。
2. エントリーを選択して入力します。
 - サーバー名 - サーバーの名前を入力します。
 - サーバー資産タグ - サーバー資産番号を入力します。
 - 資産タグ保護 - 次の設定を選択します。
 - 非固定
 - ロック - 資産タグ情報をロックします。デフォルトのシステム設定が復元されても、資産タグは消去されません。
 - サーバープライマリOS - サーバーのプライマリOSに関する説明を入力します。
 - サーバーのその他の情報 - サーバーについて説明する追加テキストを入力します。
3. 設定を保存します。

管理者情報の入力

管理者情報のオプションを使用して、サーバー管理者の連絡先情報を入力できます。各エントリーに入力できる文字数は、サーバーモデルによって異なります。デフォルトでは、すべての値が空白です。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > サーバー資産情報 > 管理者情報を選択します。

2. エントリーを選択して入力します。
 - 管理者名 - サーバーの管理者名を入力します。
 - 管理者電話番号 - サーバー管理者の電話番号を入力します。
 - 管理者メールアドレス - サーバー管理者の電子メールアドレスを入力します。
 - 管理者その他の情報 - サーバー管理者に関する追加テキストを入力します。
3. 設定を保存します。

サービスコンタクト情報の入力

サービスコンタクト情報オプションを使用して、サーバー管理者用にサービスコンタクト情報を入力します。各エントリーに入力できる文字数は、サーバーモデルによって異なります。デフォルトでは、すべての値が空白です。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > サーバー資産情報 > サービスコンタクト情報を選択します。
2. エントリーを選択して入力します。
 - サービスコンタクト名 - サービスコンタクトの名前を入力します。
 - サービスコンタクト電話番号 - サービスコンタクトの電話番号を入力します。
 - サービス連絡先E-mailアドレス - サービスコンタクトの電子メールアドレスを入力します。
 - サービスコンタクトその他情報 - サービスコンタクトに関する追加テキストを入力します。
3. 設定を保存します。

カスタムPOSTメッセージの入力

カスタムPOSTメッセージオプションを使用して、サーバーのPOST画面にカスタムメッセージを表示します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムオプション > サーバー資産情報 > カスタムPOSTメッセージを選択します。
2. 最大62文字のメッセージを入力します。
3. 設定を保存します。

プロセッサオプションの変更

手順

システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > プロセッサオプションを選択します。

インテルハイパースレッディングの有効化または無効化

Intel (R) ハイパースレッディングオプションを使用して、インテルのハイパースレッディングテクノロジーをサ

ポートするプロセッサ上で論理プロセッサコアを有効または無効にすることができます。インテルのハイパースレディングテクノロジーでは、プロセッサコア数が多いことにより恩恵を受けるアプリケーションで全体的なパフォーマンスを改善できます。

注記:

ハイパースレディングはすべてのプロセッサでサポートされているわけではありません。詳しくは、ご使用のプロセッサモデルのドキュメントを参照してください。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > プロセッサオプション > Intel (R)ハイパースレディングオプションを選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

インテルSGX制御オプションの構成

インテルSGX制御オプションを構成するには、この画面を使用します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > プロセッサオプション > インテルSGX制御を選択します。
2. 以下のオプションを構成します。
 - インテル(R) ソフトウェア ガード エクステンションズ (SGX) : ソフトウェア ガード エクステンションズ (SGX) を有効または無効 にします。
 - Intel (R) Speed Select : Speed Selectプロセッサには、より少ない有効コア数でより高い基本周波数をサポートする構成オプションがあります。この設定を変更すると、CPUの基本周波数が増加するとともに、使用可能なコアの数が減少します。これらのオプションの構成について詳しくは、プロセッサモデルのドキュメントを参照してください。
 - 基本
 - 構成1
 - 構成2
 - ソフトウェア制御
 - PRMRRサイズ : PRMRRのサイズを選択します。
 - オーナーエポック入力タイプの選択 : 次の3つのオーナーエポックモードがあります。オーナーエポックの変更なし、新しいランダムなオーナーエポックへの変更、新しいオーナーエポックの手動入力。オーナーエポックを変更すると、インテル(R) ソフトウェア ガード エクステンションズで保護されているすべての永続データが失われます。

注意:

オーナーエポック値が変更されると、インテル(R) ソフトウェア ガード エクステンションズテクノロジーで保護されているすべての永続データが失われます。

- ソフトウェア ガード エクステンションズエポック : ソフトウェア ガード エクステンションズ128ビットエポックの16進数値。
- SGXローンチコントロールポリシー : ソフトウェア ガード エクステンションズ (SGX) ローンチコントロールポリシー。オプションは次のとおりです。
 - インテルロック済み : インテルのローンチエンクレーブを選択します。

- 解除：ローンチエンクレーブのOS/VMM構成を有効にします
 - ロック済み：ローンチエンクレーブの構成を所有者に許可します。
 - SGX LE公開キーハッシュ0：ソフトウェア ガード エクステンションズ (SGX) ローンチエンクレーブ公開キーハッシュのバイト0から7
 - SGX LE公開キーハッシュ1：ソフトウェア ガード エクステンションズ (SGX) ローンチエンクレーブ公開キーハッシュのバイト8から15
 - SGX LE公開キーハッシュ2：ソフトウェア ガード エクステンションズ (SGX) ローンチエンクレーブ公開キーハッシュのバイト16から23
 - SGX LE公開キーハッシュ3：ソフトウェア ガード エクステンションズ (SGX) ローンチエンクレーブ公開キーハッシュのバイト24から31
3. オプションを保存します。

有効にするプロセッサコアの数の設定

このオプションを使用すると、物理プロセッサごとの有効なプロセッサコアの数を制限できます。有効なコアの数は、物理プロセッサでサポートされる値に設定できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > プロセッサオプション > プロセッサごとの有効なコアを選択します。
2. 有効にするコアの数を入力してください。
0またはプロセッサでサポートされていない値を入力した場合、すべてのコアが有効になります。
3. 設定を保存します。

プロセッサx2APICサポートの有効化または無効化

プロセッサx2APICサポートを有効にすると、高コア数構成でオペレーティングシステムをより効率的に実行できるようになります。また、仮想化された環境での割り込み配布が最適化されます。有効化モードは、x2APICハードウェアを有効にしますが、オペレーティングシステムに必要なサポートを提供します。古いハイパーバイザーまたはx2APICサポートと互換性がないオペレーティングシステムを使用していない限り、このオプションは有効のままにします。一部のハイパーバイザーおよびオペレーティングシステムは、起動前に プロセッサx2APICサポートを 強制的に有効に設定しなければ、X2APICを使用できません。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > プロセッサオプション > プロセッサx2APICサポートを選択します。
2. 設定を選択します。
 - 有効 - ACPI x2APIC制御構造が生成され、オペレーティングシステムがロードされるときにx2APICサポートを有効にするオプションが追加されます。
 - 強制的に有効 - 特定のプロセッサで、オペレーティングシステムがロードされるときに、オペレーティングシステムに対してx2APICサポートを有効にします。
 - 無効 - x2APICサポートが無効になります。
3. 設定を保存します。

AMD同時マルチスレッド (SMT) の有効化

AMD SMTオプションを使用して、AMD SMT機能を有効または無効にします。


 注記:

このオプションは、AMDプロセッサを搭載するサーバーで使用できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > プロセッサオプション > AMD SMTオプションを選択します。
2. 次のいずれかを選択します。
 - 有効 - 各物理プロセッサコアは2個の論理プロセッサコアとして動作します。このオプションを有効にすると、プロセッサコアの数が多いことによりメリットを受けるアプリケーションの全体パフォーマンスが向上します。
 - 無効 - 各物理プロセッサコアは1個の論理プロセッサコアとして動作します。
3. 設定を保存します。

Performance Determinismオプションの構成

 注記:

このオプションは、AMDプロセッサを搭載するサーバーで使用できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > プロセッサオプション > Performance Determinismを選択します。
2. 次のいずれかを選択します。

このオプションを使用してAMD決定論制御を構成します。

 - 自動: プロセッサ融合値が使用されます。
 - 手動
3. 次のいずれかを選択します。

これを使用して、ワークロード要件に合わせて、電力またはパフォーマンスを最大限に高めるようプロセッサを構成します。

 - Power Deterministic
 - Performance Deterministic
4. 設定を保存します。

AMDページテーブルエントリーの投機的ロックスケジューリングオプションの選択

AMDページテーブルエントリーの投機的ロックスケジューリングオプションを構成するには、この機能を使用します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > プロセッサオプション > AMDページテーブルエントリーの投機的ロックスケジューリングを選択します。
2. 有効または無効を選択します。

無効にすると、ページテーブルエントリーのロックを非投機的にのみスケジューリングします。この機能を無効にすると、パフォーマンスに影響します。

メモリオプションの変更

手順

システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプションを選択します。

メモリの再マップの構成

メモリの再マップオプションを使用して、障害イベント（訂正不能なメモリエラーなど）のために無効にされた可能性があるシステムメモリを再マップします。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > メモリの再マップを選択します。
2. 設定を選択します。
 - すべてのメモリの再マップ - 次回の起動時にシステム内のすべてのメモリを再度利用可能にします。
 - アクションなし - 影響を受けるすべてのメモリをシステムは依然として利用できません。
3. 設定を保存します。

アドバンスドメモリプロテクションの構成

アドバンスドメモリプロテクションオプションを使用すると、エラー検出および訂正 (ECC) による高度なメモリ保護を構成できます。アドバンスドECCサポートは、オペレーティングシステムに最も多くのメモリ容量を提供しており、NVDIMMがサーバーに取り付けられている場合は、必須の設定です。NVDIMMが取り付けられている場合は、他のオプションはサポートされません。NVDIMMが取り付けられている場合に未サポートのいずれかのオプションを選択すると、IMLに表示されるメッセージが作成されます。また、構成がアドバンスドECCサポートに設定されるまでNVDIMMは無効化されます。アドバンスドメモリプロテクションがアドバンスドECCサポートに設定されていると、メニュー上のアドバンスドメモリプロテクションは、非表示 (グレーアウト) になります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > アドバンスドメモリプロテクションを選択します。
2. 設定を選択します。
 - HPEファーストフォルトトレラント (ADDDC) - メモリエラーを訂正しDIMM上の複数のDRAMデバイスに障害が発生した場合でも引き続き、システムを動作させることを可能にします。アドバンスドECCで利用できる以上の、訂正不能メモリエラーに対する保護が提供されます。
 - アドバンスドECCサポート - すべてのシングルビットエラーと一部のマルチビットエラーに対してシステムを保護するとともに、オペレーティングシステムが最大のメモリ容量を使用できるようにします。
 - オンラインペア付きアドバンスドECCサポート - 訂正可能なメモリエラーが過度に発生しているメモリグループを自動的に特定します。このメモリはメモリのスペアグループと交換されます。
 - アドバンスドECCサポート付きミラーメモリ - 対処しないとシステム障害につながる可能性のある訂正されていないメモリエラーに対して最大限の保護を行います。ミラーメモリをオペレーティングシステムに提供するには、追加のメモリを取り付ける必要があります。
3. 設定を保存します。

メモリアリフレッシュレートの構成

メモリアリフレッシュレートオプションでは、メモリアリフレッシュレートの調整できますが、サーバーのメモリアリフレッシュレートのパフォーマンスと耐障害性に影響する場合があります。このサーバーの他のドキュメントに設定の指示がある場合を除き、この設定をデフォルトの状態にしておくことを推奨します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリアリフレッシュレートを選択します。
2. 設定を選択します。
 - 1xリフレッシュ
 - 2xリフレッシュ
3. 設定を保存します。

DRAMバーストリフレッシュモードの構成

DRAM Burst Refresh Modeオプションは、TRRpassおよび対象となる行のリフレッシュの悪用を緩和します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリアリフレッシュモード > DRAM Burst Refresh Modeを選択します。
2. 設定を選択します。
 - 有効 - 設定はデフォルトで有効になっています。
 - 無効 - 設定は、TRRpassを軽減するために無効になっています。
3. 設定を保存します。

チャンネルインターリーブの有効化または無効化

チャンネルインターリーブオプションを使用すると、メモリアリフレッシュレートのより高いレベルを有効または無効にすることができます。通常、メモリアリフレッシュレートのレベルを上げるとパフォーマンスは向上します。一方、レベルを下げると消費電力を節約できます。

NVDIMM-Nメモリアリフレッシュレートを有効にしている場合、チャンネルインターリーブも有効にする必要があります。

前提条件

ワークロードプロファイルがカスタムに設定されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリアリフレッシュモード > チャンネルインターリーブを選択します。
2. 設定を選択します。
 - 有効 - 最高レベルのインターリーブを有効にして、システムメモリをこのレベルに対して構成します。
 - 無効 - メモリアリフレッシュレートを有効にしません。
3. 設定を保存します。

IMCインターリーブの構成

このオプションを使用してメモリコントローラーインターリーブオプションを制御します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > メモリコントローラーインターリーブを選択します。
2. 設定を選択します。
 - 自動- (推奨) システム構成に基づいて、メモリコントローラーインターリーブ を自動的に有効または無効にします。
 - 無効-メモリコントローラーインターリーブを強制的に無効にすることができます。状況によっては、無効を選択すると、すべてのシステムメモリでパフォーマンスが向上する場合があります。
3. 設定を保存します。

AMD インターリーブの構成

このオプションを使用してメモリインターリーブモードのオプションを制御します。メモリシステムを構成するインターリーブのレベルを変更できます。通常、メモリインターリーブを自動化するとパフォーマンスが最大になります。

前提条件

このオプションは、ワークロードプロファイルがカスタムに設定されている場合のみ構成できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > AMD メモリインターリーブを選択します。
2. 次のいずれかを選択します。
 - チャンネルインターリーブ
 - ダイインターリーブ
 - ソケットインターリーブ
3. 設定を選択します。
 - 有効
 - 無効
4. 設定を保存します。

注記:

AMD メモリインターリーブオプションは、ProLiant Gen10サーバーでのみサポートされています。

Memory Interleave Sizeの設定

Memory Interleave Sizeオプションを使用して、メモリインターリーブのサイズを変更します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > Memory Interleave Sizeを選択します。
2. 設定を選択します。

- 256バイト
 - 512バイト
 - 1024バイト
 - 2048バイト
3. 設定を保存します。

Memory PStatesの有効化または無効化

Memory PStatesオプションを使用して、Memory PStatesを有効または無効にします。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > Memory PStatesを選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

AMD 1TB再マップの構成

AMD 1TB再マップオプションを有効にすると、少なくとも1TBのRAMを備えたシステムでIOMMUが有効になっている場合に、予約済みとマークされている12GBのRAMが回収されます。このオプションを有効にすると、アクセス可能なメモリマップに大きなギャップが発生するため、一部のオペレーティングシステムで問題が生じる場合があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > AMD 1TB再マップを選択します。
2. 次のいずれかを選択します。
 - 有効
 - 無効
3. 設定を保存します。

AMD定期的ディレクトリリンスの構成

ディレクトリ容量をより効率的に管理するために役立つ定期的ディレクトリリンスを有効にします。データベースやHPCアプリケーションのように、システム全体での共有度の高いワークロードでは、ディレクトリリンス操作の周期を短くすることでパフォーマンスが向上する場合があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > AMD 定期的ディレクトリリンスを選択します。
2. 次のいずれかを選択します。
 - 有効

- 無効

3. 設定を保存します。

最大メモリバス周波数の設定

最大メモリバス周波数オプションを使用すると、取り付けられているプロセッサ/DIMMの構成でサポートされているよりも低い最高速度でメモリが動作するように構成することができます。

前提条件

ワークロードプロファイルがカスタムに設定されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > 最大メモリバス周波数を選択します。
2. 設定を選択します。
 - 自動では、システム構成でサポートされている最大速度でメモリが動作します。
 - 2933 MHz
 - 2667 MHz
 - 2400 MHz
 - 2133 MHz
 - 1867 MHz

注記:

AMDサーバーは1867および2133 MHzのシステム構成をサポートしていません。

3. 設定を保存します。

メモリ巡回スクラビングの有効化または無効化

有効にした場合、メモリ巡回スクラビングは、メモリのソフトエラーを修正するので一定のシステム実行時間が経過すると、マルチビットエラーおよび訂正不能なエラーの発生が減少します。

前提条件

ワークロードプロファイルがカスタムに設定されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > メモリ巡回スクラビングを選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

ノードインターリーブの有効化または無効化

ノードインターリーブオプションを使用して、NUMAノードインターリーブを有効化または無効化します。通常、

NUMAノードでは、このオプションを無効のままにしておくことで、最適なパフォーマンスを得ることができます。このオプションを有効にすると、メモリアドレスが各プロセッサ用に取り付けられているメモリ全体でインターリーブされ、一部のワークロードでパフォーマンスが改善される可能性があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > ノードインターリーブを選択します。
2. 設定を選択します。
 - 有効 - 各プロセッサに取り付けられているメモリ全体でメモリアドレスがインターリーブされます。すべてのノードのメモリサイズが同じである必要があります。システムのパフォーマンスが影響を受ける可能性があります。
 - 無効 (デフォルト) - ノードインターリーブを無効にして、ほとんどの環境で最適なパフォーマンスを提供します。
3. 設定を保存します。

AMDセキュアメモリ暗号化の構成

この機能を有効にすると、AMDセキュアメモリの暗号化機能を使用することができます。

注記:

このオプションは、AMDプロセッサを搭載するサーバーで使用できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > AMDセキュアメモリ暗号化を選択します。
2. オプションを選択します。
 - 有効
 - 無効
3. 設定を保存します。

透過的セキュアメモリ暗号化の有効化または無効化

透過的セキュアメモリ暗号化オプションを使用して、透過的セキュアメモリ暗号化 (TSME) を有効または無効にします。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > 透過的セキュアメモリ暗号化を選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

メモリミラーリングモードの構成

メモリミラーリングオプションを使用して、ミラーリング用に予約する使用可能なシステムメモリの合計を構成します。

前提条件

この機能をアクティブ化するには、アドバンスドメモリプロテクションの構成メニューでアドバンスドECCサポート付きミラーメモリオプションを有効にします。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > メモリミラーリングモードを選択します。
2. 設定を選択します。
 - フルミラー - 使用可能なメモリの合計の50%をミラーリング用として予約します。
 - パーシャルミラー (4GB超の20%) - 4GBを超える使用可能なメモリの合計の20%をミラーリング用として予約します。
 - パーシャルミラー (4GB超の10%) - 4GBを超える使用可能なメモリの合計の10%をミラーリング用として予約します。
 - パーシャルミラー (4GB未満のメモリ) - メモリ構成に応じて、4GB未満の2GBまたは3GBのメモリをミラーリング用としてセットアップします。
 - パーシャルミラー (OSによる構成) - オペレーティングシステムがパーシャルメモリミラーリングを構成できるようにします。
3. 設定を保存します。

便宜的セルフリフレッシュの構成

便宜的セルフリフレッシュを使用すると、メモリ使用率が低い期間に、メモリコントローラーがセルフリフレッシュモードに入れるようになります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > 便宜的セルフリフレッシュを選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

不揮発性メモリの構成

システムユーティリティは、不揮発性メモリをインストール済みの場合に、このメニューを表示します。

注記:

このメニューはF9ブート画面からは使用できません。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > 不揮発性メモリオプションを選択します。
2. オプションを構成します。

- 不揮発性メモリバックアップ電源ポリシー - システムの起動時に、取り付けられた不揮発性メモリのバッテリーバックアップ電源が十分でない場合にバッテリーが充電されるまでシステムが待機するかどうかを制御します。
 - 起動時のバックアップ電源として待機 - バッテリーが充電されるまでシステムが起動中に待機します。
 - バックアップ電源なしで起動を続行 - バッテリーバックアップ電源が不十分で利用できない場合でも、システムは起動します。十分なバッテリーバックアップ電源を使用できない場合、構成されたメモリは永続的なストレージまたはシステムメモリとしてオペレーティングシステムによって使用されません。
- 不揮発性メモリの整合性チェック
 - 有効 - システムの起動時に不揮発性メモリをチェックし、データの整合性を確認します。データ整合性チェック中にエラーが検出されると、不揮発性メモリアドレス範囲スクラブの設定に応じて、検出されたエラーがオペレーティングシステムにリカバリ目的で提供されるか、不揮発性メモリがマップから除外されてオペレーティングシステムで使用できなくなります。
 - 無効 - データの整合性チェックを無効にします。データを読み取ることができない、またはデータが不良な不揮発性メモリは、システムがクラッシュする訂正不能エラーを引き起こす可能性があります。
- 不揮発性メモリアドレス範囲スクラブ
 - 有効 - サポートされるOSはNVDIMMメモリで検出された訂正不能なメモリエラーからのリカバリを試みることができます。
 - 無効 - NVDIMMメモリで訂正不能なメモリエラーが検出された後、次の起動時にNVDIMMメモリが無効になります。NVDIMMメモリのメモリアドレス範囲スクラブオプションが有効になっている場合、無効になったNVDIMMにセット内のすべてのモジュールとリージョンが含まれます。

3. 設定を保存します。

UEFIシステムユーティリティを使用したネームスペースの作成

① 重要:

UEFIシステムユーティリティに表示される、不揮発性メモリに関連するすべてのポップアップメッセージを確認してください。これらのメッセージの指示に従わないと、不揮発性メモリのデータが消失する可能性があります。

📄 注記:

HPE Persistent MemoryをVMware vSphereとともに使用している場合、ネームスペースを作成する必要はありません。再起動時にVMware vSphereが自動的にネームスペースを作成します。

ネームスペースは、HPE Persistent Memoryモジュール上の不揮発性メモリ領域を定義します。

手順

1. システムユーティリティ画面で、**システム構成** > **BIOS/プラットフォーム構成 (RBSU)** > **メモリオプション** > **不揮発性メモリオプション**を選択します。
2. **PMMオプション** > **アドバンスドオプション**を選択し、次のように選択します。
 - **デフォルトネームスペースの適用** - 有効または無効です。
 これを選択すると、まだネームスペースメタデータを持っていないインターリーブセットについて、次回起動時にネームスペースメタデータが作成されます。Linuxシステムの場合、Hewlett Packard Enterpriseではこの目的にはndctlなどのOSツールを使用することをお勧めします。
 - **ネームスペースの削除** - アクティブなネームスペースがあれば、ただちに削除します。
3. 変更を保存するには、F12キーを押します。
4. 目標構成と不揮発性メモリオプションを確定するには、サーバーを再起動します。

HPE Persistent Memoryモジュールパスワードの変更

① 重要:

UEFIシステムユーティリティに表示される、不揮発性メモリに関連するすべてのポップアップメッセージを確認してください。これらのメッセージの指示に従わないと、不揮発性メモリのデータが消失する可能性があります。

手順

1. POST中にF9キーを押してシステムユーティリティを起動します。
2. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > デバイス暗号化オプション > Device Encryption Settings > Encrypted Devicesを選択します。
3. Select DeviceからHPE Persistent Memoryモジュールを選択します。
4. Select OperationからModify Passphraseを選択します。
5. Passphrase Typeを選択します。

この選択肢は、ローカルキー管理が有効な場合にのみ使用できます。リモートキー管理が有効な場合、HPE Persistent Memoryモジュールのパスワードはキー管理サーバーで自動で生成、保存、および管理されます。

- 自動 - システムにより32バイトのランダムなパスワードが自動で生成されます。Hewlett Packard Enterpriseでは、ベストプラクティスとして、システム生成のパスワードを使用することをお勧めします。
 - Manual - 32バイトのパスワードを手動で入力します。
6. Start Operationを選択します。
これで、HPE Persistent Memoryモジュールパスワードが変更されます。
 7. 各個人のHPE Persistent Memoryモジュールパスワードを変更するには、この手順を繰り返します。
 8. Hewlett Packard Enterpriseでは、バックアップ目的でパスワードデータベースをUSBデバイスにエクスポートすることをお勧めします。
 - a. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > デバイス暗号化オプション > デバイス暗号化移行オプション > Device Encryption Export Optionsを選択します。
 - b. パスワードをTransient Passphraseフィールドに入力します。
このパスワードは、エクスポートされたファイルを保護します。移転後に暗号化されたHPE Persistent Memoryモジュールを復元するときに、入力する必要があります。
 - c. Select Fileを選択し、USBキーの場所を参照します。
 - d. Export Encryption Settingsを選択して、ファイルを作成しエクスポートします。

HPE Persistent Memoryモジュールステータスの表示

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > デバイス暗号化オプション > Device Encryption Statusを選択します。
Device Encryption Status画面には、サーバーに取り付けられた各HPE Persistent Memoryモジュールの名前、暗号化ステータス、およびパスワードが表示されます。
2. 各HPE Persistent Memoryモジュールのステータスを確認します。
 - Not encrypted - HPE Persistent Memoryモジュールは暗号化されていません。
 - Local/TPM - HPE Persistent Memoryモジュールはローカルキー管理で暗号化され、パスワードが表示されません。

このパスワードをメモして安全に保管してください。Hewlett Packard Enterpriseでは、バックアップ用にパスワードファイルをUSBドライブにダウンロードすることをお勧めします。

- Unknown key :
 - 別のサーバーから取り外された暗号化されたHPE Persistent Memoryモジュールが取り付けられ、まだ移行されていません。
 - UEFIシステムユーティリティでRestore Manufacturing Defaultオプションが選択されました。
 - HPE TPMに障害が発生しました。

UEFIシステムユーティリティを使用したパフォーマンスオプションの変更

① 重要:

UEFIシステムユーティリティに表示される、不揮発性メモリに関連するすべてのポップアップメッセージを確認してください。これらのメッセージの指示に従わないと、不揮発性メモリのデータが消失する可能性があります。

① 重要:

最大限のアップタイムとデータ保護を確保するには、高可用性のベストプラクティスに関するソフトウェアアプリケーションプロバイダの推奨事項に常に従ってください。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > 不揮発性メモリオプション > PMMオプション > パフォーマンスオプションを選択します。
2. サーバーのワークロードおよびパフォーマンス要件に基づいて、以下のオプションをアップデートしてください。
 - パフォーマンス設定 - ワークロードのビヘイビアーに応じて基本的なパフォーマンス設定を制御します。
 - 帯域幅に最適化 - デフォルト
 - レイテンシに最適化
 - バランスの取れたパフォーマンスモード
 - サービス品質 - サービス品質プロファイルを制御します。
 - 無効 - デフォルト
 - プロファイル1 - ソケットごとに4つ以上のHPE Persistent Memoryモジュールに推奨されます。
 - プロファイル2 - ソケットごとに2つのHPE Persistent Memoryモジュールに推奨されます。
 - プロファイル3 - ソケットごとに1つのHPE Persistent Memoryモジュールに推奨されます。
 - FastGo構成 - プロセッサ内のトラフィックの最適化を制御します。
 - 自動 - デフォルト
 - 有効
 - 無効
 - AppDirect用Snoopyモード - 非NUMA (不均一メモリアクセス) に最適化されたワークロードについて、HPE Persistent Memoryモジュールへのディレクトリアップデートを回避するには、このオプションを有効にします。
 - 無効 - デフォルト
 - 有効
 - メモリモード用Snoopyモード - 非NUMAに最適化されたワークロードについて、HPE Persistent Memoryモジュールへのディレクトリアップデートを回避するには、このオプションを有効にします。
 - 無効 - デフォルト

- 有効

3. 変更を保存するには、F12キーを押します。

UEFIシステムユーティリティを使用したサニタイズ

HPE Persistent Memoryモジュールをサニタイズする前に、このガイドのサニタイズポリシーとガイドラインを確認してください。

手順

1. システムユーティリティ画面で、**システム構成** > **BIOS/プラットフォーム構成 (RBSU)** > **メモリオプション** > **不揮発性メモリオプション** > **PMMオプション** > **サニタイズオプション**を選択し、以下を選択します。
 - **再起動時のサニタイズ/消去操作**：
 - 操作なし
 - 暗号による消去
 - メディアの上書き
 - 暗号化による消去およびメディアの上書き
 - **再起動時のサニタイズ/消去操作後のポリシー**：
 - サニタイズ/消去およびシステムの再起動
 - サニタイズ/消去およびシステムの電源オフ
 - サニタイズ/消去およびシステムユーティリティの再起動
 - 工場出荷時設定へのサニタイズ/消去およびシステムの電源オフ
2. **サニタイズ/消去操作の対象メモリ選択肢を有効にします。**
3. サニタイズするHPE Persistent Memoryモジュールを選択します。
 - システム内のすべてのPMM - サーバーに取り付けられたすべてのHPE Persistent Memoryモジュールをサニタイズします。
 - プロセッサXのすべてのPMM - 指定されたプロセッサのすべてのHPE Persistent Memoryモジュールをサニタイズします。
 - プロセッサX DIMM Y - プロセッサの指定されたHPE Persistent Memoryモジュールのみをサニタイズします。
4. 変更を保存して終了するには、F12キーを押します。
5. 必要に応じて、サーバーを再起動してください。

キー管理モードの変更

キー管理モードは、ローカルキー管理とリモートキー管理を切り替えることができます。暗号化された HPE Persistent Memoryモジュールは、暗号化されたままですが、パスワードとそれらのパスワードの保存場所は、選択されたキー管理モードに基づいて変わります。

① 重要:

UEFIシステムユーティリティに表示される、不揮発性メモリに関連するすべてのポップアップメッセージを確認してください。これらのメッセージの指示に従わないと、不揮発性メモリのデータが消失する可能性があります。

手順

1. システムユーティリティ画面で、**システム構成** > **BIOS/プラットフォーム構成 (RBSU)** > **サーバーセキュリティ** >

デバイス暗号化オプションを選択します。

2. キー管理設定を次のいずれかに変更します。

- ローカル - ローカルキー管理を有効にします。暗号化に使用されるパスワードは、サーバーにローカルに保存されます。

この設定を表示および選択するには、HPE TPM 2.0がインストールされている必要があります。

- リモート - リモートキー管理を有効にします。暗号化に使用されるパスワードは、リモートキーサーバーに保存されます。

この設定を表示および選択するには、HPE iLOがキーマネージャーに登録され接続されている必要があります。

3. F12キーを押して変更を保存し、終了します。

4. サーバーを再起動します。

キー管理の無効化

キー管理を無効にすると、サーバーで暗号化されたすべてのHPE Persistent Memoryモジュールについて、暗号化が無効になります。単一または特定のHPE Persistent Memoryモジュールのみ暗号化を無効にする方法については、[HPE Persistent Memoryモジュールの暗号化の無効化](#)を参照してください。

① 重要:

UEFIシステムユーティリティに表示される、不揮発性メモリに関連するすべてのポップアップメッセージを確認してください。これらのメッセージの指示に従わないと、不揮発性メモリのデータが消失する可能性があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > デバイス暗号化オプションを選択します。
2. キー管理設定を選択し、無効に変更します。
3. F12キーを押して変更を保存し、終了します。
4. サーバーを再起動します。

HPE Persistent Memoryモジュールの暗号化の無効化

この手順を使用して、単一または特定のHPE Persistent Memoryモジュールの暗号化を無効にします。

移行やサービス手順で必要とされる可能性があるような、サーバーにあるすべてのHPE Persistent Memoryモジュールについて暗号化を一度にまとめて無効にする方法については、[キー管理の無効化](#)を参照してください。

① 重要:

UEFIシステムユーティリティに表示される、不揮発性メモリに関連するすべてのポップアップメッセージを確認してください。これらのメッセージの指示に従わないと、不揮発性メモリのデータが消失する可能性があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > デバイス暗号化オプション > Device Encryption Settings > Encrypted Devicesを選択します。
2. 次のオプションを選択します。
 - a. Select Device - HPE Persistent Memoryモジュールを選択します。
 - b. Select Operation - Disable Encryption.

3. Start Operationを選択します。

ローカルキー管理が有効になっている場合は、HPE Persistent Memoryモジュールのパスフレーズを入力します。
これで、選択したHPE Persistent Memoryモジュールが非暗号化されました。

4. その他のHPE Persistent Memoryモジュールについて暗号化を無効にするには、この手順を繰り返します。

NVDIMM-Nオプションの構成

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > 不揮発性メモリオプション > NVDIMM-Nオプションを選択します。

2. 以下のオプションの有効または無効を選択します。

- NVDIMM-Nサポート
- NVDIMM-Nインターリーピング
- 次回の再起動時のポリシーにNVDIMM-Nサニタイズ/消去

① 重要:

NVDIMM-Nのサニタイズ/消去することは、NVDIMM-N内に保存されたすべてのユーザーデータの損失を招くこととなります。Hewlett Packard Enterpriseでは、NVDIMMのサニタイズ/消去を行う前に、NVDIMM-N内のすべてのユーザーデータのバックアップを手動で行うことを、強く推奨します。

- システム内のすべてのNVDIMM-Nのサニタイズ/消去
- プロセッサ上のすべてのNVDIMM-Nのサニタイズ/消去 - これらのメニュー項目は、サーバーの構成によって異なります。
- プロセッサ1 DIMM 2のサニタイズ/消去 - これらのメニュー項目は、サーバーの構成によって異なります。

3. 変更を保存します。

NVDIMM-Nサポート

このオプションを使用すると、NVDIMM-Nサポート（電源を切る、またはリセットするときにフラッシュするメモリの内容をバックアップする機能を含む）を有効または無効にできます。このオプションで無効が選択されていると、システム内のNVDIMM-Nは、パーシステントストレージとしてもシステムメモリとしてもオペレーティングシステムに提供されません。

次回の再起動時のポリシーにNVDIMM-Nサニタイズ/消去

この設定は、選択されたNVDIMM-Nに保存されたすべてのユーザーデータとエラーステータスデータをサニタイズまたは消去するプロセスの一部です。次回の再起動時のポリシーにNVDIMM-Nサニタイズ/消去を有効にすると、NVDIMMのサニタイズに関するさまざまなオプションが画面に表示されます。サーバーに取り付けられたNVDIMM-Nによって、以下を選択できます。

- システム内のすべてのNVDIMM-Nのサニタイズ/消去 - リブート時にサーバーに取り付けられているすべてのNVDIMM-Nをサニタイズします。
- プロセッサX上のすべてのNVDIMM-Nのサニタイズ/消去 - リブート時にプロセッサXのDIMMスロットに取り付けられているすべてのNVDIMM-Nをサニタイズします。

- プロセッサX DIMM Yのサンタイズ/消去 - リブート時にプロセッサXのDIMMスロットYに取り付けられているNVDIMM-Nをサンタイズします。NVDIMM-Nが格納されているプロセッサX DIMMスロットごとに選択できます。

選択されたNVDIMM-Nは、システムの次のリブート時にサンタイズされます。選択されたNVDIMM-Nの最大グループがサンタイズされます。たとえば、プロセッサ1上のすべてのNVDIMM-Nのサンタイズ/消去が有効で、かつサンタイズ/消去プロセッサ1 DIMM 8が無効になっている場合、プロセッサ1 DIMM 8を含むプロセッサ1上のすべてのNVDIMM-Nがサンタイズされます。

NVDIMM-Nがサンタイズ/消去された後のシステムの動作は、以下のポリシーで制御されます。

- NVDIMMのサンタイズ/消去後にシステムの電源を切断する
- NVDIMMのサンタイズ後にオペレーティングシステムを起動する
- NVDIMMのサンタイズ後にシステムユーティリティを起動する

NVDIMM-Nインターリーブング


このオプションは、メモリマップ内の他のNVDIMM-Nでインターリーブされる特定のプロセッサに取り付けられているNVDIMM-Nを有効にします。このオプションはHPE SmartMemory DIMMのインターリーブングに影響しません。インターリーブングは、NVDIMM-NとHPE SmartMemory DIMMの間は有効ではありません。異なるプロセッサ上に取り付けられたNVDIMM-Nは、一緒にインターリーブされることはありません。この設定が有効または無効に変更されると、取り付けられたすべてのNVDIMM-Nをサンタイズする必要があります。取り付けられたすべてのNVDIMM-Nがサンタイズされないと、次のブート時にエラー状態が報告され、NVDIMM-Nは使用できません。

メモリ構成違反レポートの有効化または無効化


メモリ構成違反レポートを使用して、システムがメモリ構成違反のメッセージを送信して、ログに記録する方法を構成します。

手順

- システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > メモリ構成違反レポートを選択します。
- 設定を選択します。
 - 有効: (デフォルト) この状態では、システムは、サポートされている検証済みのガイドラインに含まれていないメモリ構成を報告します。

 注記: 検証済みでサポートされている構成のリストについては、メモリ取り付けのガイドラインを参照してください。

 - 無効: この状態では、メモリ構成違反は報告されません。

 注記: デフォルト構成 (有効) を維持することをお勧めします。

- 設定を保存します。

トータルメモリ暗号化 (TME) の有効化または無効化

手順

- システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > メモリオプション > メモリ暗号化オプション > トータルメモリ暗号化 (TME) を選択します。
- 設定を選択します。
 - 有効
 - 無効

3. 設定を保存します。

仮想化オプションの変更

手順

システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 仮想化オプションを選択します。

仮想化テクノロジーの有効化または無効化

インテル(R)バーチャライゼーションテクノロジー(Intel VT)を使用して、UEFIインテルプロセッサによって提供されるハードウェア機能を、仮想化テクノロジーをサポートするVirtual Machine Manager (VMM) が使用できるようにするかどうかを制御します。

注記:

VMM、またはAMD-V仮想化をサポートしていないオペレーティングシステムを使用している場合、仮想化テクノロジーを無効にする必要はありません。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 仮想化オプション > インテル(R)バーチャライゼーションテクノロジー(Intel VT)を選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

インテルVT-dの有効化または無効化

インテル(R) VT-dオプションを使用して、Virtual Machine Manager (VMM) でダイレクトI/O (VT-d) 対応のインテル仮想化テクノロジーを有効または無効にします。

注記:

この機能をサポートするオペレーティングシステムまたはハイパーバイザーを使用していない場合は、インテル(R) VT-dオプションを無効に設定する必要はありません。有効のまま構いません。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 仮想化オプション > インテル(R) VT-dを選択します。
2. 設定を選択します。
 - 有効 - ハイパーバイザーまたはこのオプションをサポートするオペレーティングシステムで、ダイレクトI/Oのインテル仮想化テクノロジーが提供するハードウェア機能が使用できます。
 - 無効 - ハイパーバイザーまたはこのオプションをサポートするオペレーティングシステムで、ダイレクトI/Oのインテル仮想化テクノロジーが提供するハードウェア機能が使用できません。
3. 設定を保存します。

アクセス制御サードスの有効化または無効化

HP ProLiant Gen10、ProLiant Gen10 Plusサーバー、およびHPE Synergy用UEFIシステムユーティリティ
ユーザーガイド

アクセス制御サービスオプションを使用して、ビデオとキーストロークをシリアルポート経由でオペレーティングシステムブートにリダイレクトします。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 仮想化オプション > アクセス制御サービスを選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

SR-IOVの有効化または無効化

SR-IOV (Single Root I/O Virtualization) インターフェイスは、PCI express (PCIe) 仕様の拡張です。これにより、BIOSがPCIeデバイスに、より多くのPCIリソースを割り当てることができます。このオプションは、PCIeデバイスまたはSR-IOVをサポートするオペレーティングシステムで有効にします。ハイパーバイザーを使用する場合は、有効のままにしておきます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 仮想化オプション > SR-IOVを選択します。
2. 設定を選択します。
 - 有効 - ハイパーバイザーがPCIeデバイスの仮想インスタンスを作成できるため、パフォーマンスが向上する可能性があります。
 - 無効 - PCIeデバイスの仮想インスタンスを作成するためにハイパーバイザーを有効にしません。
3. 設定を保存します。

最小のSEV ASIDの設定

最小のSEV ASIDオプションを使用して、AMD Secure Encrypted Virtualization (SEV) を有効にしたゲストに使用できる最小のアドレス空間識別子 (ASID) を構成できます。この数値以下のASIDは、SEV-ES (暗号化状態) も有効にしているSEV有効ゲストのみが利用可能です。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 仮想化オプション > 最小のSEV ASIDを選択します。
2. 1~16の数を入力します。
3. 設定を保存します。

最大のSEV ASIDの設定

最大SEV ASIDオプションを使用して、SEV (Secure Encrypted Virtualization) に対応したゲストのために使用できるAMD SEVアドレス空間識別子 (ASID) の数を選択します。このオプションは、サーバーがサポートするシステムメモリの量に影響します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 仮想化オプション > 最大SEV ASIDを選択します。
2. 1~16の数を入力します。
3. 設定を保存します。

AMD仮想化オプションの有効化

有効にした場合、このオプションをサポートするハイパーバイザーまたはオペレーティングシステムは、AMDのI/O仮想化 (IOMMU) が提供するハードウェア機能を使用できます。ハイパーバイザーまたはこのオプションを使用するオペレーティングシステムを使用しない場合でも、この設定を有効にしておくことができます。

注記:

このオプションは、ROMバージョン1.38以前を実行しているすべてのAMD Gen10サーバーおよびAMD Gen10 Plusサーバーで使用できます。ただし、ROMバージョン2.40以降を搭載したAMD Gen10 Plusサーバーの場合、AMD IOMMUとAMD仮想化テクノロジーは、AMD I/O仮想化テクノロジーと呼ばれる単一の新しい設定に結合されました。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 仮想化オプション > AMD (R) IOMMUを選択します。
2. 次のいずれかを選択します。
 - 有効
 - 無効
3. 設定を保存します。

AMD仮想化テクノロジーの有効化

有効にした場合、このオプションをサポートするハイパーバイザーまたはオペレーティングシステムは、AMD VTが提供するハードウェア機能を使用できます。ハイパーバイザーまたはこのオプションを使用するオペレーティングシステムを使用しない場合でも、この設定を有効にしておくことができます。

注記:

このオプションは、ROMバージョン1.38以前を実行しているすべてのAMD Gen10サーバーおよびAMD Gen10 Plusサーバーで使用できます。ただし、ROMバージョン2.40以降を搭載したAMD Gen10 Plusサーバーの場合、AMD IOMMUとAMD仮想化テクノロジーは、AMD I/O仮想化テクノロジーと呼ばれる単一の新しい設定に結合されました。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 仮想化オプション > AMD 仮想化テクノロジーを選択します。
2. 次のいずれかを選択します。
 - 有効
 - 無効
3. 設定を保存します。

AMD DMA再マッピングの有効化または無効化

AMD DMA再マッピングは、DMA再マッピング設定を構成します。DMA再マッピングは、メモリの破損や悪意のあるDMA攻撃から保護します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 仮想化オプション > AMD DMA再マッピングを選択します。
2. 次のいずれかを選択します。
 - 有効
 - 無効
3. 設定を保存します。

ブートオプションの変更

手順

システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ブートオプションを選択します。

ブートモードの選択

このサーバーには、2つの ブートモード構成があります。UEFIモードおよびレガシーBIOSモードです。一部のブートオプションでは、特定のブートモードを選択することが必要です。デフォルトでは、ブートモードは UEFIモードに設定されています。次の特定のオプションを使用するには、システムを UEFIモードで起動する必要があります。

- セキュアブート、UEFI最適化ブート、汎用USBブート、IPv6 PXEブート、iSCSIブート、NVMeブート、およびURLからのブート
- ファイバーチャネル/FCoEスキャンポリシー

注記:

使用するブートモードはオペレーティングシステムのインストールと一致しなければなりません。そうでない場合、ブートモードを変更するとサーバーがインストール済みのオペレーティングシステムで起動する機能に影響を与える場合があります。

前提条件

UEFIモードで起動する場合は、UEFI最適化ブートを有効なままにしてください。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ブートオプション > ブートモードを選択します。
2. 設定を選択します。
 - UEFIモード (デフォルト) -UEFI互換性のあるオペレーティングシステムで起動するようにシステムを設定します。
 - レガシーBIOSモード -レガシーBIOS互換モードで従来のオペレーティングシステムに起動するようにシステムを構成します。
3. 設定を保存します。
4. サーバーを再起動します。

UEFI最適化ブートの有効化または無効化

UEFI最適化ブートを使用して、システムBIOSをネイティブのUEFIグラフィックドライバーを使用して起動するかどうかを制御します。UEFI最適化ブートは、デフォルトで有効になっています。Windows Server 2008、Windows Server 2008 R2またはWindows 7を使用している場合にのみ、UEFI最適化ブートを無効にします。

前提条件

- UEFI最適化ブートを有効化するときは、ブートモードをUEFIモードに設定する必要があります。UEFIモードは、デフォルトのブートモードです。
- 次の目的で、UEFI最適化ブートを有効にする必要があります。
 - セキュアブートを有効にして使用する。
 - VMware ESXiを動作させる。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ブートオプション > UEFI最適化ブートを選択します。
2. オプションを選択します。
 - 有効 - UEFIモードに設定されている場合、ネイティブのUEFIグラフィックドライバーを使用して起動するようにシステムBIOSを構成します。
 - 無効 - INT10レガシービデオ拡張ROMを使用して起動するようにシステムBIOSを構成します。ご使用のオペレーティングシステムとして、Windows Server 2008、Windows Server 2008 R2またはWindows 7を使用している場合、この設定が必要です。
3. 設定を保存します。
4. サーバーを再起動します。

ブート順序ポリシーの設定

UEFIブート順序リストに従ってデバイスのブートを試みたときにブート可能なデバイスが見つからない場合に、ブート順序ポリシーオプションを使用してシステムの動作を制御します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ブートオプション > ブート順序ポリシーを選択します。
2. 設定を選択します。
 - ブート順序を無限に再試行 - システムはブート可能なデバイスが検出されるまでブート順序の試行を繰り返します。
 - ブート順序を1回試行 - システムはブートメニュー内のすべての項目を1回ずつ試行してからシステムを停止します。
 - ブート試行の失敗後リセット - システムはすべての項目を1回ずつ試行した後でシステムを再起動します。
3. 設定を保存します。

UEFIブート順序リストの変更

UEFIブート順序オプションを使用して、UEFIブート順序リスト内のエントリーのブート順序を変更します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ブートオプション > UEFIブート設定 > UEFIブート設定 > UEFIブート順序を選択します。
2. ブート順序リスト内を移動するには、ポインティングデバイスまたは矢印キーを使用します。
3. エントリーを選択し、そのエントリーのリスト内での順序を変更します。
 - ブートリスト内でエントリーを上に移動するには、+キーを押すか、またはエントリーをドラッグアンドドロップします。
 - ブートリスト内でエントリーを下に移動するには、-キーを押すか、またはエントリーをドラッグアンドドロップします。
4. 変更を保存します。

UEFIブート順序の制御

個々のUEFIブートオプションを有効または無効にするには、UEFIブート順序制御オプションを使用します。有効になっている項目は選択 (チェック) されています。無効になっている項目は、UEFIブート順序リストの中に残りますが、ブートプロセス中に試行されません。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ブートオプション > UEFIブート設定 > UEFIブート設定 > UEFIブート順序制御を選択します。
2. 次の操作を実行します。
 - オプションを有効にするには、対応するチェックボックスを選択します。
 - オプションを無効にするには、対応するチェックボックスを選択します。
3. 変更を保存します。

UEFIブート順序リストへのブートオプションの追加

ブートオプションを追加を使用して、拡張子.EFIを持つx64 UEFIアプリケーション (OSブートローダーやその他のUEFIアプリケーションなど) を選択し、新しいUEFIブートオプションとして追加できます。

新しいブートオプションは、UEFIブート順序リストの最後に追加されます。ファイルを選択すると、ブートメニューに表示するブートオプションの説明と、.EFIアプリケーションに渡すデータ (オプション) を入力するよう求めるプロンプトが表示されます。

手順

1. FAT16/FAT32パーティションを持つメディアを接続します。
2. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ブートオプション > UEFIブート設定 > ブートオプションを追加を選択します。
3. リスト内の.EFIアプリケーションを選択してEnterキーを押します。
4. 必要に応じて、Enterキーを押してメニューオプションをドリルダウンします。
5. ブートオプションの説明とオプションのデータを入力し、Enterキーを押します。
UEFIブート順序リストに新しいブートオプションが表示されます。
6. 変更をコミットして終了しますを選択します。

UEFIブート順序リストからのブートオプションの削除



注記:

削除されたオプションがネットワークPXEブートやリムーバブルメディアデバイスなどの標準の起動場所を指している場合、システムBIOSは次の再起動時にオプションを追加します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ブートオプション > UEFIブート設定 > ブートオプションを削除を選択します。
2. リストからオプションを1つ以上選択します。
3. 変更をコミットして終了を選択します。

レガシーBIOSブート順序リストの変更

前提条件

ブートモードがレガシーBIOSモードに設定されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ブートオプション > レガシーBIOSブート順序を選択します。
2. ブート順序リスト内を移動するには、ポインティングデバイスまたは矢印キーを使用します。
3. エントリーを選択し、そのエントリーのリスト内での順序を変更します。
 - ブートリスト内でエントリーを上に移動するには、+キーを押すか、またはエントリーをドラッグアンドドロップします。
 - ブートリスト内でエントリーを下に移動するには、-キーを押すか、またはエントリーをドラッグアンドドロップします。
4. 変更を保存します。

ネットワークオプションの変更

手順

システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ネットワークオプションを選択します。

ネットワークブートオプション

- プリブートネットワーク環境ポリシー
- IPv6 DHCPユニーク識別子
- ネットワークブートリトライサポート
- ネットワークインターフェイスカード (NIC)
- PCIeスロットネットワークブート
- HTTPサポート
- iSCSIソフトウェアイニシエーター

プリブートネットワーク環境の設定

プリブートネットワーク環境オプションを使用して、ご使用のネットワークブートターゲットがUEFIブート順序リスト内で表示される方法を優先設定できます。このオプションは、内蔵UEFIシェルからプリブートネットワーク操作も制御できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ネットワークオプション > ネットワークブートオプション > プリブートネットワーク環境を選択します。
2. 設定を選択します。
 - 自動 - プリブート環境で開始したすべてのネットワーク操作がIPv4またはIPv6上で実行されます。UEFIブート順序リスト内の既存のネットワークブートターゲットの順序は変更されません。システムBIOSのデフォルトポリシーを使用して、新しいネットワークブートターゲットがリストの最後に追加されます。
 - IPv4 - プリブート環境で開始したすべてのネットワーク操作がIPv4上でのみ実行されます。UEFIブート順序リスト内にある既存のすべてのIPv6ネットワークブートターゲットを削除します。新しいIPv6ネットワークブートターゲットはリストに追加されません。
 - IPv6 - プリブート環境で開始したすべてのネットワーク操作がIPv6上でのみ実行されます。UEFIブート順序リスト内にある既存のすべてのIPv4ネットワークブートターゲットを削除します。新しいIPv4ネットワークブートターゲットはリストに追加されません。
3. 変更を保存します。

IPv6 DHCPユニーク識別子の方式の設定

IPv6 DHCPユニーク識別子オプションを使用して、IPv6 DHCPユニーク識別子 (DUID) の設定方法を制御します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ネットワークオプション > ネットワークブートオプション > IPv6 DHCPユニーク識別子を選択します。
2. 設定を選択します。
 - 自動 - サーバーのUUID (Universal Unique Identifier) を使用するか、サーバーを利用できない場合はリンク層アドレスと時刻値 (DUID-LLT) の方式を使用して、DUIDを設定します。
 - DUID-LLT - リンク層アドレスと時刻値 (DUID LLT) の方式を使用してDUIDを設定します。
3. 変更を保存します。

ネットワークブートリトライサポートの有効化または無効化

ネットワークブートリトライサポートのオプションを使用して、ネットワークブートリトライ機能を有効または無効にします。有効にした場合、システムBIOSはネットワークデバイスの起動を、最大でネットワークブートリトライ数オプションで設定された回数試行した後、次のネットワークデバイスの起動を試行します。この設定は、F12ファンクションキーとワンタイムブートオプションからネットワークデバイスのブートを試行したときにのみ有効です。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ネットワークオプション > ネットワークブートオプション > ネットワークブートリトライサポートを選択します。

2. 設定を選択します。
 - 有効 - ネットワークブートリトライを有効にします。
 - 無効 - ネットワークブートリトライを無効にします。
3. 変更を保存します。

NICのネットワークブートの有効化または無効化

ネットワークインターフェイスカード (NIC) オプションを使用してインストール済みNICのネットワークブートを有効または無効にします。リストされるデバイスはシステムによって異なりますが、次のようなものを含めることができません。

- 内蔵LOM 1ポート1
- 内蔵FlexibleLOM 1ポート1



注記:

ブートオプションの使用を開始するには、NICファームウェアの構成が必要になる場合があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ネットワークオプション > ネットワークブートオプションを選択します。
2. NICを選択します。
3. 設定を選択します。
 - ネットワークブート - ネットワークブートを有効にします。
 - 無効 - ネットワークブートを無効にします。
4. 変更を保存します。
5. ネットワークブートを選択した場合、ブート順序リストにNICブートオプションが表示されるようサーバーを再起動します。

PCIeスロットネットワークブートの有効化または無効化

PCIeスロットネットワークブートオプションを使用して、PCIeスロットのNICカードのUEFIネットワークブートを有効または無効にします。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ネットワークオプション > ネットワークブートオプション > PCIeスロットネットワークブートを選択します。
2. PCIeスロットエントリを選択します。
3. 設定を選択します。
 - 有効 - PCIeスロットのNICカードのUEFIネットワークブートを有効にします。
 - 無効 - PCIeスロットのNICカードのUEFIネットワークブートを無効にします。
4. 変更を保存します。

HTTPサポートの設定

前提条件

このオプションを使用して、UEFIモード時に、内蔵UEFIシェル > DHCPを使用したシェル自動起動スクリプトの検出設定を使用して、UEFI HTTP (s) ブートサポートを制御します。

自動またはHTTPSのみを選択してHTTPSブートを有効にするには、サーバーセキュリティ > TLS (HTTPS) オプションでHTTPSサーバーの各TLS証明書を登録する必要があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ネットワークオプション > ネットワークブートオプション > HTTPサポートを選択します。
2. 設定を選択します。
 - 自動 - ネットワークブートが有効になっている各ネットワークポートのUEFIブート順序リストにHTTP (S) ブートオプションを自動的に追加します。DHCPサーバーによって提供されたHTTPまたはHTTPSのURLからシステムを起動できます。DHCPサーバーによって提供されたその他のURLは無視されます。
 - HTTPのみ - ネットワークブートが有効になっている各ネットワークポートのUEFIブート順序リストにHTTPブートオプションを自動的に追加します。DHCPサーバーによって提供されたHTTP URLからシステムを起動でき、提供されたHTTPSまたはその他のURLは無視されます。
 - HTTPSのみ - ネットワークブートが有効になっている各ネットワークポートのUEFIブート順序リストにHTTPSブートオプションを自動的に追加します。DHCPサーバーによって提供されたHTTPS URLからシステムを起動でき、提供されたHTTPまたはその他のURLは無視されます。
 - 無効
3. 変更を保存します。

iSCSIポリシー (Gen10) またはソフトウェアイニシエーター (Gen10 Plus) の有効化

iSCSIソフトウェアイニシエーターを有効または無効にします。有効にすると、システムのiSCSIソフトウェアイニシエーターを使用して、構成済みのすべてのNICポート上のiSCSIターゲットへのアクセスが行われます。無効にすると、システムのiSCSIソフトウェアイニシエーターは構成済みのiSCSIターゲットへのアクセスを試行しません。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ネットワークオプション > ネットワークブートオプション > iSCSIポリシー (Gen10) またはiSCSIソフトウェアイニシエーター (Gen10 Plus) を選択します。
2. 設定を選択します。
 - 有効 - UEFI iSCSIソフトウェアイニシエーターを有効にします。
 - 無効 - UEFI iSCSIソフトウェアイニシエーターを無効にします。

注記:

このオプションは、iSCSIソフトウェアイニシエーターが有効か無効かのみを制御します。アダプターイニシエーターからのiSCSIブートを有効にするには、アダプターファームウェアでiSCSIを有効にして構成する必要があります。

3. 変更を保存します。

プリブートネットワーク設定の構成

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ネットワークオプション > プリブートネットワーク設定を選択します。
2. プリブートネットワーク設定オプションのいずれかを選択します。
3. 追加の設定を選択するか、そのオプションの追加の値を入力します。
4. 変更を保存します。

詳しくは

プリブートネットワーク設定

プリブートネットワーク設定

起動前のネットワークインターフェイスおよび関連設定を構成するには、このオプションを使用します。

① 重要:

同じインターフェイス上で `webclient` または `ftp` を実行する予定の場合、ネットワークインターフェイス上で内蔵UEFIシェル `ifconfig` コマンドを使用する必要はありません。システムユーティリティ内で構成されているプリブートネットワーク設定は、これらのインターフェイスを自動的に選択します。

`ftp` および `webclient` によって使用されるインターフェイスが `ifconfig` によって構成される場合、その設定は消去されます。代わりに、システムユーティリティプリブートネットワーク設定メニューは、コマンドが実行されるとインターフェイスに適用されます。

- プリブートネットワークインターフェイス—プリブートネットワーク接続に使用するネットワークインターフェイスを指定します。
 - 自動 (デフォルト) - システムは、ネットワーク接続されている最初の使用可能なポートを使用します。
 - 特定のポートの選択 - システムは選択されたNICポートを使用します。
- DHCPv4 - 内蔵UEFIシェルおよびURLから起動からのネットワーク操作のために、DHCPサーバーからのプリブートネットワークIPv4構成の取得を有効または無効にします。
 - 有効 - DHCPv4ネットワークアドレス構成を有効にします。個別の設定は使用できません。
 - 無効 - DHCPv4のアドレス構成を無効にします。したがって以下の静的IPアドレス設定を手動で構成する必要があります。
 - IPv4アドレス
 - IPv4サブネットマスク
 - IPv4ゲートウェイ
 - IPv4プライマリDNS
- プリブートネットワークプロキシ - プリブートネットワークプロキシを指定します。これが設定されている場合、プリブートネットワークインターフェイスのネットワーク操作は構成済みのプロキシ経由で試行されます。プロキシはHTTP URL形式である必要があり、`http://IPv4_address:port`, `http://[IPv6_address]:port` または `http://FQDN:port` として指定することができます。
- IPv6構成ポリシー
 - 自動 - 内蔵UEFIシェルからのネットワーク操作のために、プリブートネットワークIPv6構成を自動的に取得することができます。個別の設定は使用できません。
 - 手動 - 静的IPアドレス設定を個別に構成することができます。
- URL 1、2、3、または4から起動 - ブート可能なISOまたはEFIファイルのネットワークURLを指定します。HTTPまたはHTTPSのいずれかの形式で、IPv4またはIPv6のサーバーアドレスまたはホスト名を使用してURLを入力します。たとえば、URLを次のいずれかの形式にすることができます。 `http://192.168.0.1/file/image.iso`、`http://example.com/file/image.efi`、`https://example.com/file/image.efi`、`http://[1234::1000]/image.iso`。構成すると、このURLがUEFIブートメニューにブートオプションとして表示されます。その後、ブートメニューからこのオプションを選択し、指定されたファイルをシステムメモリにダウンロードして、そのファイルからシステムをブートできるようにすることができます。

📄 注記:

URLから起動では、プリブートネットワーク設定ページで構成されたIPアドレス設定が使用されます。ISOファイルからの起動には、予備のOS環境イメージ（WinPEやミニLinuxなど）または完全なOSインストールイメージの起動のみを含めることができます。ただし、OSがHTTPブート機能をサポートする場合（古いOSバージョンはISOファイルまたはOSインストールイメージからの起動をサポートしない可能性があります）。使用しているOSのドキュメントでHTTPブート機能がサポートされるかどうかを確認してください。

URLからのブートの前提条件

URLから起動を使用するときは、ブートモードはUEFIモードのままにしておきます。

iSCSI ブート構成

注記:

RESTfulインターフェイスツールを使用してiSCSIブート設定を構成することもできます。次のRESTfulインターフェイスツールのドキュメントを参照してください：<https://www.hpe.com/info/restfulinterface/docs>。

iSCSI イニシエーター名の追加

iSCSIイニシエーター名のオプションを使用して、IQN（iSCSI Qualified Name）形式で名前を設定します。EUIフォーマットはサポートされません。このオプションは、イニシエーターに設定されたデフォルト名に置き換わります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > ネットワークオプション > iSCSIの構成 > iSCSIイニシエーター名を選択します。
2. iSCSI修飾名（IQN）フォーマットを使用してiSCSIイニシエーターの一意の名前を入力します。たとえば、`iqn.2001-04.com.example:uefi-13021088` です。

この設定は自動的に保存されます。

iSCSI ブート試行の追加

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > ネットワークオプション > iSCSIの構成 > iSCSIブート試行を追加を選択します。

このブート試行が、次にサーバーが再起動されるまで有効にならないことを示すメッセージが表示されます。

2. Enterを押します。
3. iSCSI接続を試行するポートを選択します。
4. 構成設定を完了します。
 - iSCSI試行名 - 名前を入力します。
 - iSCSIブート制御 - 有効または MPI0を有効を選択します。

注記: デフォルト設定は、無効です。MPI0を有効を使用して、マルチパスI/O（MPI0）機能を有

HP ProLiant Gen10、ProLiant Gen10 Plusサーバー、およびHPE Synergy用UEFIシステムユーティリティ
ユーザーガイド

効にします。

- IPアドレスタイプ - アドレスタイプを選択します。
 - 接続再試行カウント - 0~16の値を入力します。デフォルトの再試行回数は3回です。
 - 接続タイムアウト - 100~20000の値（ミリ秒単位）を入力します。デフォルトは、20000（20秒）です。
 - イニシエーターDHCP - デフォルト設定です。イニシエーターについて静的IPアドレスを構成する必要がある場合は、このオプションをオフにします。イニシエーターについて静的アドレスを構成する場合は、ターゲット名、IPアドレス、ポート、およびブートLUNも手動で構成する必要があります（ターゲットDHCP構成を無効にします）。
 - ターゲットDHCP構成 - デフォルト設定です。ターゲット設定を手動で構成する必要がある場合は、このチェックボックスをオフにして、ターゲット名、IPアドレス、ポート、およびブートLUNを入力します。
 - オプション：認証タイプ - デフォルトはNONEです。必要な場合、CHAPを選択してCHAPエントリーを入力します。
5. 変更の保存を選択します。
 6. システムを再起動します。

iSCSI ブート試行の削除

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > ネットワークオプション > iSCSIブート構成 > iSCSIブート試行を削除を選択します。
2. 1つ以上のiSCSIブート試行エントリーを選択します。
3. 変更をコミットして終了を選択します。

iSCSI ブート試行の詳細の表示および変更

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > ネットワークオプション > iSCSIブート構成 > iSCSI試行を選択します。
2. リストからエントリーを選択します。
3. ブート試行の詳細を表示または変更します。

VLANの構成

VLAN構成オプションを使用して、すべての有効なネットワークインターフェイスにグローバルVLAN設定を構成します。構成には、PXEブート、iSCSIブート、およびHTTP/HTTPSブートで使用されるインターフェイス、および内蔵UEFIシェルからのすべてのプリブートネットワークアクセス用のインターフェイスが含まれます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > ネットワークオプション > VLAN構成を選択します。
2. 以下の操作を実行します。
 - a. VLANコントロール - 有効を選択すると、有効なすべてのネットワークインターフェイス上でVLANタギングを有効にできます。この設定は、デフォルトでは無効になっています。

- b. VLAN ID - VLANコントロールが有効な場合、1から4094の範囲でVLAN IDを入力します。
 - c. VLAN優先順位 - VLANコントロールが有効な場合、VLANタグ付きフレームに0~7の優先順位の値を入力します。
3. 変更を保存します。

内蔵iPXEオプションの変更

内蔵iPXEは、システムBIOSに組み込まれたオープンソースのネットワークブートアプリケーションであり、ネットワークブートの実行に使用できます。このオプションにより、UEFIシェルコマンド `ipxe` と内蔵アプリケーションリストのエントリーも有効になります。どちらも内蔵iPXEの起動に使用できます。

手順

システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ネットワークオプション > 内蔵iPXEを選択します。

内蔵iPXEの有効化または無効化

内蔵iPXEオプションを使用して、システムBIOSに組み込まれているiPXEオープンソースネットワークブートイメージを有効または無効にします。内蔵iPXEは、追加機能によって拡張された完全なPXE実装を提供します。有効にして、内蔵iPXEをブート順序に追加を有効にすると、内蔵iPXEがUEFIブート順序リストに追加されます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ネットワークオプション > 内蔵iPXE > 内蔵iPXEを選択します。
2. 設定を選択します。
 - 有効 - 起動前環境から内蔵iPXEを起動してUEFIブート順序リストに追加できます。
 - 無効 - 内蔵iPXEは起動前環境で使用できないため、UEFIブート順序リストに追加できません。
3. 設定を保存します。

UEFIブート順序リストへの内蔵iPXEの追加

前提条件

ブートモードがUEFIモードに設定されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ネットワークオプション > 内蔵iPXE > 内蔵iPXEをブート順序に追加を選択します。
2. 設定を選択します。
 - 有効 - 次の再起動時に内蔵iPXEをブート順序リストに追加します。
 - 無効 - 内蔵iPXEは、ブート順序リストに追加されません。
3. 設定を保存します。

内蔵iPXE起動スクリプトの自動実行の有効化または無効化

内蔵iPXE起動中の内蔵iPXE起動スクリプトの自動実行を有効または無効にするには、iPXEスクリプト自動起動オプションを使用します。

- 起動スクリプトを使用して、iPXEの起動時に一連のiPXEコマンドを自動化できます。
- スクリプトファイルはローカルメディアに保存したりネットワークの場所からアクセスできます。
- スクリプトファイルに `Startup.ipxe` という名前を付けて、ローカルメディアのルートディレクトリに配置します。サーバーからアクセス可能なネットワーク上の場所に起動スクリプトを配置することもできます。スクリプトファイル名は任意であり、ネットワークの場所を使用する場合はファイルのURLを指定する必要があります。
- 自動起動が有効な場合、iPXE自動起動スクリプトロケーションオプションが自動的に設定されていると、内蔵iPXEは、スクリプトファイルを、最初にネットワーク上、次にローカル接続のFAT16またはFAT32フォーマットのメディアで探します。
- 1つのファイルシステムに、`Startup.ipxe` ファイルを1つだけ配置することをお勧めします。

前提条件

- ブートモードがUEFIモードに設定されている。
- 内蔵iPXEが有効になっている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ネットワークオプション > 内蔵iPXE > iPXEスクリプト自動起動を選択します。
2. 設定を選択します。
 - 有効 - 内蔵iPXEの起動時に、内蔵iPXE起動スクリプトが実行されます。
 - 無効 - 内蔵iPXEの起動時に、内蔵iPXE起動スクリプトが実行されません。
3. 設定を保存します。

内蔵iPXEスクリプト検証の有効化または無効化

前提条件

- ブートモードがUEFIモードに設定されている。
- 内蔵iPXEが有効になっている。
- iPXEスクリプト自動起動が有効になっている。
- セキュアブートが有効になっている。
- 内蔵iPXEスクリプトがセキュアブートデータベースに登録されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ネットワークオプション > 内蔵iPXE > iPXEスクリプトの検証を選択します。
2. 設定を選択します。
 - 有効 - iPXEスクリプトの検証を有効にします。
 - 無効 - (デフォルト) iPXEスクリプトの検証を有効にしません。
3. 設定を保存します。

内蔵iPXE起動スクリプトロケーションの設定

iPXE自動起動スクリプトロケーションオプションを使用して、内蔵iPXE起動スクリプトの場所を選択します。iPXEスクリプト自動起動を有効にすると、この設定は内蔵iPXEが起動スクリプトファイルを検索する場所を指定します。

前提条件

- 内蔵iPXEが有効になっている。
- iPXEスクリプト自動起動が有効になっている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ネットワークオプション > 内蔵iPXE > iPXE自動起動スクリプトロケーションを選択します。
2. 設定を選択します。
 - 自動：内蔵iPXEは、起動スクリプトの取得を最初にネットワーク上の場所から試行し、続いてローカルに接続されたメディアから試行します。
 - 接続メディア上のファイルシステム 内蔵iPXEは、USBディスク上のFAT32パーティション、iL0仮想ドライブ、HDDなど、UEFIでアクセス可能なローカルファイルシステム上のStartup. ipxeスクリプトファイルを検索します。
 - ネットワークの場所 内蔵iPXEは、この設定で指定されたURLが指す. ipxeスクリプトを実行します。
3. 設定を保存します。

内蔵iPXE自動起動スクリプトのネットワーク上の場所の設定

前提条件

- 内蔵iPXEが有効になっている。
- 内蔵iPXE自動起動スクリプトロケーションがネットワーク上または自動に設定されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ネットワークオプション > 内蔵iPXE > iPXE自動起動スクリプトのためのネットワーク上の場所を選択します。
2. `.ipxe` ファイルのネットワーク上の場所を入力します。

有効な値は次のとおりです。

- IPv4またはIPv6サーバーアドレスかホスト名のHTTP/HTTPS形式のURL。
- IPv4サーバーアドレスかホスト名のFTP形式のURL。

例：

- `http://192.168.0.1/file/file.ipxe`
- `http://example.com/file/file.ipxe`
- `https://example.com/file/file.ipxe`
- `http://[1234::1000]/file.ipxe`

3. 設定を保存します。

ストレージオプションの変更

手順

システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ストレージオプションを選択します。

内蔵チップセットSATAコントローラーサポートの有効化

内蔵SATA構成オプションを使用して、内蔵チップセットSATA (Serial Advanced Technology Attachment) コントローラーサポートを有効にします。AHCIまたはHPE SmartアレイSW RAIDサポートを選択できます。選択したオプションに対応する正しいオペレーティングシステムドライバが使用されていることを確認してください。

△ 注意:

ブートモードがレガシーBIOSモードに構成されている場合は、Dynamic Smartアレイはサポートされません。Dynamic SmartRAID RAIDを有効にすると、データが損失するか、既存のSATAドライブ上のデータが破壊されます。このオプションを有効にする前にすべてのドライブのデータをバックアップしてください。

SATA AHCIサポートを有効にする前に、ご使用のオペレーティングシステムのドキュメントを参照して、ベースメディアのドライバがこの機能をサポートしていることを確認します。

前提条件

- 選択したオプションに対応する、正しいオペレーティングシステムのドライバであること。
- ブートモードがUEFIモードに設定されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ストレージオプション > SATAコントローラーオプション > 内蔵SATA構成を選択します。
2. ご使用のSATAオプションに対して、正しいAHCIまたはRAIDシステムドライバを使用していることを確認します。
3. 設定を選択します。
 - SATA AHCIサポート - AHCI用の内蔵チップセットSATAコントローラーを有効化します。
 - SmartRAID SW RAIDサポート - Dynamic SmartRAID RAID用の内蔵チップセットSATAコントローラーを有効にします。
 - Intel VROC SATAサポート
4. 設定を保存します。

SATAセキュア消去の有効化

SATAセキュア消去オプションを使用すると、SATAセキュア消去機能がサポートされているかどうかを制御できます。この機能により、セキュアフリーズロックコマンドがSATAハードディスクドライブへ送信されません。

前提条件

- ハードドライブ上のSATAコントローラーがACHIモードになっている。
- ハードドライブがセキュア消去コマンドをサポートしている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ストレージオプション > SATAコントローラーオプション > SATAセキュア消去を選択します。
2. 設定を選択します。
 - 有効 - Security Freeze LockコマンドはサポートされたSATAハードディスクドライブに送信されず、セキュア消去機能は有効になります。
 - 無効 - セキュア消去を無効にします。
3. 設定を保存します。

SATAサニタイズの有効化

SATAサニタイズオプションを使用して、サニタイズ機能をサポートするかどうかを制御します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ストレージオプション > SATAコントローラーオプション > SATAサニタイズを選択します。
2. 設定を選択します。
 - 有効 - Security Freeze LockコマンドはサポートされたSATAハードディスクドライブに送信されず、セキュア消去機能は有効になります。
 - 無効 - サニタイズを無効にします。
3. 設定を保存します。

内蔵ストレージブートポリシーの設定

内蔵ストレージブートポリシーオプションを使用して、内蔵ストレージコントローラーにUEFI BIOSブートターゲットを選択します。デフォルトでは、UEFIブート順序リストでは、ストレージコントローラーに接続されているすべての有効なブートターゲットを使用できます。

前提条件

ブートモードがUEFIモードに設定されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ストレージオプション > 内蔵ストレージブートポリシーを選択します。
2. ストレージコントローラーを選択します。
3. 設定を選択します。
 - すべてのターゲットを起動 - ストレージコントローラーに接続されているすべての有効なブートターゲットが、UEFIブート順序リストに使用できます。
 - 24のターゲットに起動を制限 - ストレージコントローラーに接続されている最大24のブートターゲットが、UEFIブート順序リストに使用できます。
 - ターゲットで起動なし - ストレージコントローラーに接続されているブートターゲットは、UEFIブート順序リストに使用できません。
4. 設定を保存します。

PCIeストレージブートポリシーの設定

前提条件

ブートモードがUEFIモードに設定されている。

PCIeストレージブートポリシーオプションを使用して、PCIeスロット内のストレージコントローラーにUEFI BIOSブートターゲットを選択します。



注記:

この設定は、PCIeスロット内のファイバーチャネルコントローラーに対するファイバーチャネル/FCoEスキャンポリシー設定よりも優先されます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ストレージオプション > PCIeストレージブートポリシーを選択します。
2. ストレージコントローラーを選択します。
3. ブートターゲットを選択します。

4. 設定を保存します。

デフォルトのファイバーチャネル/FCoEスキャンポリシーの変更

前提条件

ブートモードがUEFIモードに設定されている。

ファイバーチャネル/FCoEスキャンポリシーオプションを使用して、有効なFC/FCoE（または、SANからのブート）ブートターゲットのスキャンのためのデフォルトのポリシーを変更します。デフォルトでは、取り付けられている各FC/FCoEアダプターは、デバイス設定で事前構成されているターゲットのみをスキャンします。PCIeスロット内のファイバーチャネルコントローラーの場合、この設定はPCIeストレージブートポリシー設定によって上書きされます。

注記:

UEFIモードでのみサポートされます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ストレージオプション > ファイバーチャネル/FCoEスキャンポリシーを選択します。
2. 設定を選択します。
 - すべてのターゲットをスキャン - インストールされている各FC/FCoEアダプターは、すべての利用可能なターゲットをスキャンします。
 - 構成済みターゲットのみスキャン - インストールされている各FC/FCoEアダプターは、デバイスの設定で構成済みのターゲットだけをスキャンします。この設定は、デバイス固有のセットアップで構成された個々のデバイス設定を上書きします。
3. 設定を保存します。

内蔵NVM ExpressオプションROMの有効化または無効化

内蔵NVM ExpressオプションROMオプションを使用して、NVM ExpressオプションROMがロードされる方法を制御します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ストレージオプション > NVM Expressオプション > 内蔵NVM ExpressオプションROMを選択します。
2. 設定を選択します。
 - 有効 - システムは、システムBIOSによって提供されるNVM ExpressオプションROMをロードします。
 - 無効 - システムは、アダプターによって提供されるNVM ExpressオプションROMをロードします。
3. 設定を保存します。

インテル(R) CPU VMDサポートの構成

インテル(R) CPU VMDサポートオプションを使用して、NVMe用のインテルCPUボリューム管理デバイスサポートを有効/無効にします。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ストレージオプション > NVM Expressオプション > インテル(R) VMDおよびVROCのオプション > インテル(R) CPU VMDサポートを選択しま

す。

2. 設定を選択します。
 - 個々のCPU NVMeルートポートが有効
 - すべてのCPU NVMeルートポートが有効
 - 無効
3. 設定を保存します。

インテル(R) PCH VMDサポートの構成

インテル(R) PCH VMDサポートオプションを使用して、NVMe用のインテルPCHボリューム管理デバイスサポートを有効/無効にします。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ストレージオプション > NVMe Expressオプション > インテル(R) VMDおよびVROCのオプション > インテル(R) PCH VMDサポートを選択します。
2. 設定を選択します。
 - すべてのPCH NVMeルートポートが有効
 - 無効
3. 設定を保存します。

インテル(R) VROCサポートの構成


インテル(R) VROCサポートオプションを使用して、さまざまなタイプのVROCライセンスを選択します。

前提条件

インテル(R) PCH VMDサポートは すべてのPCH NVMeルートポートが有効に設定されています。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ストレージオプション > NVMe Expressオプション > インテル(R) VMDおよびVROCのオプション > インテル(R) VROCサポートを選択します。
2. 設定を選択します。
 - HPE VROC for Intel NVMe
 - HPE VROC for HPE NVMe

 **注記:** Intel VROCのサポートを有効にするには、HPEからライセンスを購入する必要があります。

3. 設定を保存します。

NVM Expressドライブの撤去

次のオプションを使用して、NVM Expressドライブを撤去します。選択したドライブは、次のブート時に安全に消去されます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > ストレージオプション > NVM Expressオプション > NVM Expressドライブ撤去オプションを選択します。
2. 撤去するドライブを選択します。
3. 設定を保存します。

ローカルおよびリモートキー管理のためのSEDドライブの構成

キー管理モードは、ローカルキー管理とリモートキー管理を切り替えることができます。暗号化された自己暗号化ドライブ (SED) は暗号化されたままですが、暗号化キーとそれらのキーのストレージは、選択されたキー管理モードに基づいて変更されます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > デバイス暗号化オプションを選択します。
2. キー管理設定を次のいずれかに変更します。
 - ローカル - ローカルキー管理を有効にします。暗号キーは、サーバーにローカルに保存されます。
この設定を表示および選択するには、HPE TPM 2.0がインストールされている必要があります。
 - リモート - リモートキー管理を有効にします。暗号キーは、リモートキーサーバーに保存されます。
この設定を表示および選択するには、HPE iLOがキーマネージャーに登録され接続されている必要があります。
3. F12キーを押して変更を保存し、終了します。
4. サーバーを再起動します。

電力およびパフォーマンスオプションの変更

手順

システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプションを選択します。

AMDパフォーマンスワークロードプロファイルの有効化または無効化

AMDパフォーマンスワークロードプロファイルは、特定のパフォーマンス要件に対応する機能セットを提供します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > AMDパフォーマンスワークロードプロファイルを選択します。
2. 設定を選択します。
 - 有効
 - 無効 (デフォルト)
3. 設定を保存します。

パワーレギュレーターモードの設定

パワーレギュレーターの設定を使用することで、サーバーの効率が向上し、消費電力を管理することができます。

注記:

特定のプロセッサは、1種類の電力状態のみをサポートし、どのパワーレギュレーターモードが選択されていても常に初期化された周波数で稼働します。

前提条件

ワークロードプロファイルがカスタムに設定されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > パワーレギュレーターを選択します。
2. 設定を選択します。
 - ダイナミックパワーセービングモード - プロセッサの利用率に基づいてプロセッサ速度と電力使用量を自動的に変化させます。このモードは、プロセッサの動作を監視するのに、ROMベースのアルゴリズムを使用します。このモードを使用すると、パフォーマンスにほとんど、またはまったく影響を与えずに全体的な電力消費を削減し、OSのサポートは必要ありません。
 - スタティックローパワーモード - プロセッサ速度を下げ、電力使用量を減らします。システムの最大電力使用量の低下が保証されます。このモードは、電力供給能力が制約されている場合に有益で、システムの最大電力使用を低減するのに必要です。
 - スタティックハイパフォーマンスモード - プロセッサは、電力と性能が最大の状態で動作します。OSの電源管理ポリシーは無視されます。このモードは、性能が重視され、電力消費はそれほど重要ではない環境で役立ちます。
 - 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限り、プロセッサは常に最大電力/パフォーマンス状態で稼働します。
3. 設定を保存します。

PCI ピアツーピア直列化の構成

PCI ピアツーピア直列化オプションを使用して、PCI ピアツーピア直列化を構成します。

この機能が有効になっていると、プロセッサソケット上に複数のGPUが搭載されているシステムなど、特定の構成では、パフォーマンスの向上が見られる場合があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > PCI ピアツーピア直列化を選択します。
2. 設定を選択します。
 - 有効 - 有効にすると、PCIe トランザクションがプロセッサのPCIe ルートポート全体でインターリーブされるため、ピアツーピア通信のパフォーマンスが向上する可能性があります。
 - 無効
3. 設定を保存します。

I0ダイレクトキャッシュの構成

I0ダイレクトキャッシュオプションを使用して、PCI ピアツーピア直列化を構成します。

この機能が有効になっていると、プロセッサソケット上に複数のGPUが搭載されているシステムなど、一部の構成では、パフォーマンスの向上が見られる場合があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > I0ダイレクトキャッシュを選択します。
2. 設定を選択します。
 - I0DC (I0ダイレクトキャッシュ) の有効化/無効化 - リモートInvItoM (IIO) またはWCiLF (コア) に対してメモリアルックアップの代わりにスヌープを生成します。
 - リモートInvItoMハイブリッドブッシュに対して有効
 - InvItoM AllocFlow
 - InvItoMハイブリッドAllocFlow
 - リモートInvItoMおよびリモートWViLFに対して有効
3. 設定を保存します。

最小プロセッサアイドル電力コアCステートの設定

最小プロセッサアイドル電力コアCステートオプションを使用して、オペレーティングシステムが使用するプロセッサの最小アイドル電力状態 (Cステート) を選択します。Cステートを高く設定すればするほど、そのアイドル状態の消費電力は少なくなります。

前提条件

ワークロードプロファイルがカスタムに設定されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > 最小プロセッサアイドル電力コアCステートを選択します。
2. 設定を選択します。
 - C6ステート (デフォルト - 最小)
 - C3ステート
 - C1Eステート
 - Cステートなし
3. 設定を保存します。

最小プロセッサアイドル電力パッケージCステートの設定

最小プロセッサアイドル電力パッケージCステートオプションを使用して、最小プロセッサアイドル電力状態 (Cステート) を選択します。プロセッサは、プロセッサのコアの移行先のCステートに基づいて、自動的にパッケージCステートに移行します。パッケージCステートを高く設定すればするほど、そのアイドルパッケージ状態の消費電力は少なくなります。

前提条件

ワークロードプロファイルがカスタムに設定されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > 最小プロセッサアイドル電力パッケージCステートを選択します。
2. 設定を選択します。
 - パッケージC6 (リテンション) ステート (デフォルト - 最小)
 - パッケージC6 (リテンションなし) ステート

- パッケージステートなし

3. 設定を保存します。

AMDデータファブリックCステートの有効化または無効化

データファブリックCステート有効オプションを使用して、データファブリックCステートを有効または無効にします。

注記:

このオプションは、AMDプロセッサを搭載するサーバーで使用できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > データファブリックCステート有効を選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

インテルターボブーストテクノロジーの有効化または無効化

インテルターボブーストテクノロジーは、プロセッサが使用できる電力に余裕があり、温度が仕様内である場合に、定格よりも高い周波数にプロセッサを移行するかどうかを制御します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > インテル(R)ターボブーストテクノロジーを選択します。
2. 設定を選択します。
 - 有効
 - 無効 - この機能を無効にすると電力使用は減りますが、ワークロードによってはシステムが実現できる最大のパフォーマンスも低くなります。
3. 設定を保存します。

AMDコアパフォーマンスブーストの構成

AMDコアパフォーマンスブーストは、プロセッサが使用できる電力に余裕があり、温度が仕様内である場合に、定格よりも高い周波数にプロセッサを移行するかどうかを制御します。

注記:

このオプションは、AMDプロセッサを搭載するサーバーで使用できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > AMDコアパフォーマンスブーストを選択します。
2. 設定を選択します。

- 有効
 - 無効
3. 設定を保存します。

AMD Fmaxブースト制限制御の有効化または無効化

AMD Fmaxブースト制限設定は、最大プロセッサースト周波数を設定します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > AMD Fmaxブースト制限制御を選択します。
2. 設定を選択します。
 - 自動 - プロセッサは可能な最高のブースト周波数で動作できます。
 - 手動 - 最大ブースト周波数を低く構成できます。
3. 設定を保存します。

AMD Cステート効率モードの変更

Cステートの変更時にコア周波数を少しずつ調整するようにシステムを構成します。このオプションを有効にすると、ワークロードが監視され、高いC0レジデンシを保つようにコア周波数が調整されます。これにより、コアが100%使用されていないときの電力とレイテンシに利点が得られます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > Cステート効率モードを選択します。
2. 次のいずれかを選択します。
 - 有効
 - 無効
3. 設定を保存します。

エネルギー/パフォーマンスバイアスの設定

エネルギー/パフォーマンスバイアスオプションを使用すると、複数のプロセッササブシステムを、プロセッサのパフォーマンスと消費電力が最適化されるように構成できます。

前提条件

ワークロードプロファイルがカスタムに設定されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > エネルギー/パフォーマンスバイアスを選択します。
2. 設定を選択します。
 - 最大パフォーマンス - パフォーマンスが最大になり、遅延が最小になります。この設定は、消費電力に関する制約が厳しくない環境で使用してください。
 - パフォーマンスに最適化 - 電力効率が最適化されるため、ほとんどの環境にお勧めします。

- 電力に最適化 - サーバーの使用率に基づいて電力効率が最適化されます。
 - 省電力モード - 消費電力に関する制約が厳しく、パフォーマンスの低下を容認できる環境で使用してください。
3. 設定を保存します。

AMD Infinity Fabricのパフォーマンス状態の設定

Infinity Fabricの出力パフォーマンスが無効になっているときにInfinity Fabricのパフォーマンス状態 (P-state) をカスタマイズするには、[Infinity Fabric Performance Stateオプション](#)を使用します。



注記:

このオプションは、Infinity Fabricの電力管理が無効になっている場合にのみ表示されます。
詳しくは、この章の関連トピックを参照してください。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > Infinity Fabricのパフォーマンス状態を選択します。
2. 設定を選択します。
 - 自動
 - P0
 - P1
 - P2
 - P3
3. 設定を保存します。

詳しくは

[Infinity Fabricの電力管理の有効化または無効化](#)

協調電力制御の有効化または無効化

プロセッサクロッキングコントロール (PCC) インターフェイスをサポートしているオペレーティングシステムで協調電力制御を有効にすると、サーバーで [パワーレギュレーターオプション](#)が [ダイナミックパワーセービングモード](#)に設定されている場合でも、プロセッサ周波数の変更を要求するようにオペレーティングシステムが構成されます。PCCインターフェイスをサポートしていないオペレーティングシステムの場合や [パワーレギュレーターモード](#)が [ダイナミックパワーセービングモード](#)に構成されていない場合、このオプションはシステムの動作に影響しません。

前提条件

ワークロードプロファイルがカスタムに設定されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > 協調電力制御を選択します。
2. 設定を選択します。
 - 有効 - オペレーティングシステムは、プロセッサの周波数の変更を要求します。
 - 無効 - オペレーティングシステムは、プロセッサの周波数の変更を要求しません。
3. 設定を保存します。



注記:

協調電力制御オプションは、ProLiant Gen10サーバーでのみサポートされています。

AMD XGMI強制リンク幅の構成

XGMI強制リンク幅設定は、XGMIリンク幅を強制的にユーザー設定値にします。

 注記: この設定は、CPUを2基搭載しているシステムにのみ存在します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > XGMI強制リンク幅を選択します。
2. 設定を選択します。
 - 自動 - システムが必要に応じてXGMIリンク幅を動的に変更できるようにします。
 - x2 - XGMIリンク幅を強制的にx2にします。
 - x8 - XGMIリンク幅を強制的にx8にします。
 - x16 - XGMIリンク幅を強制的にx16にします。
3. 設定を保存します。

AMD XGMI最大リンク幅の構成

XGMI最大リンク幅設定は、最大XGMIリンク幅をユーザー設定値に設定します。

 注記: この設定は、CPUを2基搭載しているシステムにのみ存在します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > XGMI最大リンク幅を選択します。
2. 設定を選択します。
 - 自動 - システムが必要に応じてXGMI最大リンク幅を動的に変更できるようにします。
 - x2 - XGMIリンク幅を最大x2に制限します。
 - x8 - XGMIリンク幅を最大x8に制限します。
 - x16 - XGMIリンク幅を最大x16に制限します。
3. 設定を保存します。

インテルDMIリンク周波数の設定

インテルDMIリンク周波数オプションを使用して、プロセッサとサウスブリッジのリンク速度を強制的に遅くできます。そうすることにより電力消費を削減できますが、システムパフォーマンスにも影響する可能性があります。

 注記:
このオプションは、2個以上のCPUを持つシステムで構成できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > インテルDMIリンク周波数を選択します。
2. 設定を選択します。
 - Gen 1速度
 - Gen 2速度

3. 設定を保存します。

AMD優先I/Oバス番号の構成

優先I/Oバス番号オプションを使用すると、PCIeパフォーマンスの向上に効果があります。

前提条件


優先I/OバスAMDオプションを有効にしていることを確認してください。
手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > I/Oオプション > 優先I/Oバス番号を選択します。
2. 優先I/Oを与えるデバイスのPCIバス番号 (0~255) を入力します。
同じAMD NBIO (NorthBridge I/O) 上のすべてのエンドポイントに対してパフォーマンスが同様に向上します。
3. 設定を保存します。

AMD NBIO LCLK DPMレベルの構成

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > I/Oオプション > NBIO LCLK DPMレベルを選択します。
2. 値を選択します。
 - 自動
 - 静的 (低)
 - 静的 (高)

 **注記:** NBIOを静的 (高) に構成すると、NBIO上のPCIeデバイスのパフォーマンスが向上する場合がありますが、プロセッサのその他の部分のパフォーマンスが低下します。この設定は、PCIeデバイス要件のレビュー後にのみ使用する必要があります。

3. 設定を保存します。

NUMAグループサイズ最適化の設定

NUMAグループサイズ最適化オプションを使用して、システムROMがNUMA (Non-Uniform Memory Access) ノード内の論理プロセッサ数をレポートする方法を構成します。結果の情報を使用すると、オペレーティングシステムがアプリケーションでの使用のためにプロセッサをグループ化するのに役立ちます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > NUMAグループサイズ最適化を選択します。
2. 設定を選択します。
 - クラスタ - NUMAの境界に沿ってグループを最適化し、より優れたパフォーマンスを提供します。
 - フラット - 複数グループにスパンニングするプロセッサを利用できるように最適化されていないアプリケーションが、より多くの論理プロセッサを使用することが可能になります。

3. 設定を保存します。

インテルPerformance Counter Monitorの有効化または無効化

インテルプロセッサには、DRAMのパフォーマンス（NVDIMM-Nのパフォーマンスを含む）を測定するためにソフトウェアで使用できるパフォーマンスカウンターが搭載されています。このオプションは監視ツールであり、パフォーマンスには影響を与えません。たとえば、インテルパフォーマンスカウンターモニター（PCM）ツールは、チャンネルごとの帯域幅をレポートできます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > 電力およびパフォーマンスオプション > インテルPerformance Counter Monitorを選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

アンコア周波数のスケーリングの構成

アンコア周波数のスケーリングオプションを使用して、プロセッサの内部バスの周波数のスケーリングを制御します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > 電力およびパフォーマンスオプション > アンコア周波数のスケーリングを選択します。
2. 設定を選択します。
 - 自動 - プロセッサはワークロードに基づいて周波数を動的に変更できます。
 - 最大または最小の周波数 - レイテンシまたは消費電力の調整ができます。
3. 設定を保存します。

UPIバンド幅の最適化（RTID）の設定

UPIバンド幅の最適化（RTID）オプションを使用して、ほとんどのアプリケーションに最高のパフォーマンスを提供する、プロセッサ間のUPIリンクを構成します。



注記:

このオプションは2つ以上のCPUがある場合にのみ構成できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > 電力およびパフォーマンスオプション > UPIバンド幅の最適化（RTID）を選択します。
2. 設定を選択します。
 - バランス - このオプションは、ほとんどのアプリケーションおよびベンチマークで最高のパフォーマンスを提供します。
 - I/Oに最適化（代替RTID） - このオプションは、システムメモリへの直接アクセスに依存するGPUなどのI/Oデバイスからの帯域幅を増やすことができます。
3. 設定を保存します。

Sub-NUMAクラスタリングの有効化または無効化

Sub-NUMAクラスタリングを使用して、プロセッサのコア、キャッシュ、およびメモリを複数のNUMAドメインに分割できます。NUMAに対応し、最適化されているワークロードでは、このオプションを有効にするとパフォーマンスが向上する可能性があります。

注記:

Sub-NUMAクラスタリングを有効にすると、最大1GBのシステムメモリを使用できなくなる可能性があります。

前提条件

このオプションを有効にするために、XPTプリフェッチャーを有効にする。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > Sub-NUMAクラスタリングを選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

エネルギー効率ターボオプションの有効化または無効化

エネルギー効率ターボオプションを使用して、プロセッサが、エネルギー効率ベースのポリシーを使用するかどうかを制御します。

前提条件

インテル(R)ターボブーストテクノロジーを有効にする。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > エネルギー効率ターボを選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

ローカル/リモートしきい値の設定

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > ローカル/リモートしきい値を選択します。
2. 設定を選択します。
 - 無効
 - 低

- 中
 - 高
3. 設定を保存します。

LLCデッドラインの割り当ての設定

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > LLCデッドラインの割り当てを選択します。
2. 次のいずれかを選択します。
 - 有効 - LLCのデッドラインを状況に応じて満たします。
 - 無効 - LLCのデッドラインを満たすことはありません。
3. 設定を保存します。

古くなったAからSへの設定

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > 古くなったAからSへを選択します。
2. 次のいずれかを選択します。
 - 有効 - 古くなったAからSへのディレクトリ最適化を有効にします。
 - 無効 - 古くなったAからSへのディレクトリ最適化を無効にします。
3. 設定を保存します。

プロセッサプリフェッチャーオプションの無効化

デフォルトでは、ほとんどの環境に最適なパフォーマンスを提供するために、プロセッサプリフェッチャーオプションが有効になっています。場合によっては、これらのオプションを無効にするとパフォーマンスが向上する可能性があります。


① 重要:

環境内のパフォーマンスを改善できることを確認するには、プロセッサプリフェッチャーオプションを無効にする前に、アプリケーションベンチマーク評価を実行します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > プロセッサプリフェッチャーオプションを選択します。
2. 設定を選択します。
 - HWプリフェッチャー
 - 隣接セクターのプリフェッチャー
 - DCUストリームプリフェッチャー
 - DCU IPプリフェッチャー

- XPTプリフェッチャー

 注記:

Sub-NUMAクラスタリングを有効にする場合、この設定を有効にする必要があります。

- LLCのプリフェッチ
3. 無効を選択します。
 4. 変更を保存します。

ACPI SLITオプションの有効化

Advanced Configuration and Power Interface System Locality Information Table (ACPI SLIT) を有効または無効にします。ACPI SLITは、プロセッサ、メモリサブシステム、およびI/Oサブシステム間の相対アクセス時間を定義します。SLITをサポートするオペレーティングシステムでは、この情報を使用してリソースやワークロードの割り当てを効率化し、パフォーマンスを改善できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > I/Oオプションを選択します。
2. オプションACPI SLITで、次のいずれかを選択します。
 - 有効
 - 無効
3. 変更を保存します。

インテルNIC DMAチャンネルの有効化

インテルNIC上でのDMAアクセラレーションを有効または無効にします。ご使用のサーバーにインテルNICが搭載されていない場合は、この設定を無効のままにしてください。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > I/Oオプションを選択します。
2. オプションインテルNIC DMAチャンネルで、次のいずれかを選択します。
 - 有効
 - 無効
3. 変更を保存します。


アドバンストパフォーマンスチューニングオプションの構成

ジッターの原因になり遅延を発生させる周波数の変動を抑制するために、高度なパフォーマンスチューニングを使用します。ジッター制御は、手動または自動で管理できます。プロセッサ周波数の変動があるかどうかに関わらず、使用する周波数を指定することもできます。ジッター制御について詳しくは、HPE Gen10 Servers Intelligent System Tuning (<https://www.hpe.com/support/gen10-intelligent-system-tuning-en>) を参照してください。


手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > アドバンスドパフォーマンスチューニングオプションを選択します。
2. 設定を構成します。

- プロセッサジッター制御 - 電力、温度、およびアクティブコア数に基づいて周波数を変化させる技術 (ターボなど) によるプロセッサ周波数の変化を管理します。ジッター制御により、プロセッサのジッターとレイテンシが低減または除去され、サーバーのパフォーマンスが向上します。オプションを選択します。
 - 自動調整 - 周波数の変化を監視し、長期的な変動を最小限に抑えるように周波数を自動的に調整します。
 - 手動調整 - プロセッサを固定した周波数で動作させ、ユーザーが低い周波数かまたは高い周波数を静的に選択できるようにします。
 - 無効 - プロセッサのジッター制御を無効にします。
- プロセッサジッター制御周波数 - 以下のいずれかを実行してください。
 - 自動調整を選択した場合は、開始周波数単位をMHzで入力します。
 - 手動調整を選択した場合は、周波数単位をMHzで入力します。

 **注記:** 指定した周波数がサポートされていない場合、システムファームウェアは、それよりも高くても近い、プロセッサがサポートする中間周波数に周波数を調整します。

- プロセッサジッター制御最適化 - このオプションは、自動調整機能がプロセッサ周波数の変動を検出したときに使用されるしきい値を最適化します。次のいずれかを選択します。
 - スループットに最適化では、計算スループット全体に影響を及ぼさない量の変動のみが発生します。
 - レイテンシに最適化では、プロセッサ周波数を低下させる前に非常に少量の変動がときおり発生します。
 - ゼロレイテンシでは、すべての周波数変動の除去を試行します。
- コアブースト - この機能を使用して、よりアクティブなプロセッサ間でより高いパフォーマンスを実現します。コアブースト機能を搭載したサーバーは、サーバーの余分な電源と温度のヘッドルームを使用して、共通の障害を減らし、プロセッサの処理能力を最大化します。

 **注記:**

厳選したHPE ProLiant Gen10サーバー、インテルプロセッサ、およびハードウェア構成で使用可能です。iLO Advanced Premium Security Editionライセンスが必要です。

- プロセッサパフォーマンス強化: この機能を有効または無効にするには、このオプションを使用します。有効にした場合、プロセッサの設定がより活動的な設定に調整され、パフォーマンスが向上する可能性があります。消費電力が高くなる可能性があります。
 - プロセッサ構成TDPレベル: このオプションは、SSE、AVX、およびAVX-512の確定的周波数に関するデフォルトのCPUポリシーを上書きします。これにより、確定的動作周波数が低下します。ターボモードを無効にすると、確定的動作が増強されますが、結果的に動作周波数が低下します。オプションは、正常、レベル1、レベル2です。
3. 変更を保存します。

UPIへの送信オプションの設定

手順

1. システムユーティリティ画面から、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > アドバンスドパフォーマンスチューニングオプション > UPIへの送信の順に選択します。
2. オプションを選択します。
 - 有効: このオプションを有効にすると、リモートメモリまたはI/OのアクセスをUPIバスに依存しているマルチプロセッサ構成のシステムで、パフォーマンス上の利点が得られます。
 - 無効

3. 変更を保存します。

メモリチャネルモードの設定

メモリチャネルモードオプションを使用して、通常のアドバンストECCモードでは不可能なインスタンスでマルチビットメモリエラーを訂正することで最大のデータ保護を提供します。結合チャネルモードのメモリ搭載ルールについては、製品のドキュメントを参照してください。

手順

1. システムユーティリティ画面から、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > アドバンストパフォーマンスチューニングオプション > メモリチャネルモードの順に選択します。
2. 設定を選択します。
 - 独立チャネルモード (非ロックステップ)
 - 結合チャネルモード (ロックステップ)
3. 設定を保存します。

独立チャネルモード (非ロックステップ) の設定

パフォーマンス管理

選択したHPE Gen10以降のサーバーでは、以下のサーバーのパフォーマンス管理およびチューニング機能がサポートされています。

- **Workload Matching** - 構成済みのサーバープロファイルを使用して、アプリケーションパフォーマンスを最大化します。
- **Jitter Smoothing** - プロセッサジッター制御モード設定を使用して、周波数変動 (ジッター) をならしてバランスさせ、低レイテンシを実現します。
- **パフォーマンス監視** - Innovation Engineのサポートによってサーバーでサポートされたセンサーから収集したパフォーマンスデータを表示します。収集したデータに基づいてアラートを構成できます。
- **ワークロードパフォーマンスアドバイザー** - 選択されたサーバーワークロード特性を表示します。監視対象データに基づき、推奨のパフォーマンスチューニング設定を表示したり、構成したりできます。
- **コアブースト** - アクティブなプロセッサコア間のパフォーマンスを高めるためにこの機能を有効にします。

この機能はGen10サーバーのみでサポートされています。Gen10 Plusサーバーではサポートされていません。

iLOを工場出荷時のデフォルト設定にリセットすると、パフォーマンス管理のすべての設定とデータが削除されます。

iLOのバックアップおよびリストア機能を使用するときは、パフォーマンス管理設定が保持されます。収集されたパフォーマンスデータはバックアップまたはリストアされません。

パフォーマンス管理機能の要件

要件	Workload Matching	Jitter Smoothing	コアブースト	パフォーマンス監視	ワークロードアダプタイザー
HPE Gen10 Plusサーバー	✓	✓		✓	✓
HPE Gen10サーバー	✓	✓	✓ ¹	✓	✓
Intel プロセッサー		✓	✓ ²	✓	✓
iLO 5	✓	✓	✓	✓	✓
iLO Advancedのライセンス		✓	✓	✓	✓
最小システムROM	1.00	1.00 静的 1.20 動的 1.40 最適化	1.20	2.00	2.00
最小iLOファームウェア	該当なし	1.15 iLO RESTful API 1.30 iLOのWebインターフェイス	1.15 iLO RESTful API 1.30 iLOのWebインターフェイス	1.40 iLO RESTful API 1.40 iLOのWebインターフェイス	1.40 iLO RESTful API 1.40 iLOのWebインターフェイス
最小のHPE Innovation Engineファームウェア ³	該当なし	1.2.4	1.2.4	2.0.11	2.0.11

¹ 特定のサーバーのみ。高性能ヒートシンクとファンが必要です。

² 特定のIntelプロセッサーのみ（サポート終了2019）

³ iLO

のWebインターフェイスの
パフォーマンス

ページは、Innovation Engineがサポートされていないサーバーでは使用できません。Innovation Engineがサポートされているかどうかを確認するには、インストールされたファームウェアページでInnovation Engineファームウェアを検索します。

Jitter Smoothing

過去数年間、サーバークラスの顧客は、プロセッサーベースのパフォーマンスが世代を重ねるたびに向上するのを見てきました。この向上は、ほとんどがコア数の増加と効率的な命令セットアーキテクチャーによるものです。前の10年とは異なり、CPUの基本周波数は、コア数の増加とアーキテクチャー強化に由来するパフォーマンスの改善と並行して安定しています。ただし、プロセッサーベンダーは、すべてのワークロードがコア数の増加による恩恵を受けるとは限らないことを理解し始めたため、電源ヘッドルームを利用できる高い周波数で一部のコアを便宜的に実行し、その他のコアの実行を抑制する機能を導入しました。

これらの便宜的な周波数ではパフォーマンスが向上する反面、望ましくない副作用もあります。周波数の変化自体が、コンピューティングジッター、不確定性、望ましくない遅延時間をもたらします。ジッターおよび関連する遅延は、いくつかの顧客セグメントで問題を生じています。たとえば、高頻度のトレーダーは、時間が重要となる取引に頼っています。周波数の変化によって引き起こされるマイクロ秒単位の遅延が取引に不確定的に追加されるのを容認できません。このような遅延が度重なると、トレーダーに数百万ドル以上のコストをもたらすことがあります。他の環境でも、RTOS（リアルタイムオペレーティングシステム）を実行して重要な機能を制御しているサーバーは、日和見的周波数機能が有効になっているときに発生するランダムな遅延は容認できません。

遅延に敏感な顧客の間では、関連するジッターを回避するために、通常はアプリケーションのパフォーマンスの向上につながる機能を無効にする傾向があります。プロセッサーが高速で実行されれば取引も高速で実行されますが、ランダムな遅延のコストが発生すると、パフォーマンスの向上のメリットが失われます。

Hewlett Packard Enterpriseでは、Gen10サーバーにプロセッサーのジッター制御を導入して、顧客が高周波数の利点と低ジッターの両方を実現できるようにしています。この機能は、Intel Xeon スケラブルプロセッサーを使用するGen10以降のサーバーで利用できます。この機能は、AMDプロセッサーを使用しているサーバーではサポートされていません。この機能により、日和見的周波数管理によって引き起こされるジッターを除去するか低減することが可能となり、遅延応答が改善されスループットのパフォーマンスが向上します。

プロセッサージッター制御機能を有効にすると、オペレーティングシステムの電力管理設定の変更が必要となる場合があります。

自動プロセッサジッター制御モード

プロセッサのジッター制御を自動モードで実行するように構成すると、HPEサーバーファームウェアは、電源管理の影響を無効にし、実行時にプロセッサを動的に調整して、ジッターを誘発する周波数変化を排除します。自動チューニングモードで実行すると、プロセッサは最終的に、周波数変更を中止して、温度、電源、およびコアの使用制限の範囲内で達成できる最も高い周波数で実行します。自動チューニングモードでは、次の理由で引き起こされる周波数変更が検出されると周波数を下げます。

- Cステート移行
- AVXに誘発された移行
- ターボ移行（電源、温度、およびコア使用状況による）
- サーマルスロットリング制御

ジッター制御は、プロセッサのすべてのコアに等しく影響を与えます。

コアブースト

コアブーストテクノロジーでは、プロセッサを特定の使用事例、構成、および環境に適合させる、ゆとりのある最適化されたターボプロファイルを使用します。コアブーストプロセッサは、革新的なHPE電圧レギュレーター設計と冷却技術によってもたらされる、余分なサーバー電力とサーマルヘッドルームを利用します。その結果、コアブーストプロセッサを搭載したシステムは、共通の失敗を緩和することができ、プロセッサの計算能力を最大限に引き出すことができます。

たとえば、プロセッサには、多数のコアとコアが動作する基本周波数を備えることができます。プロセッサをターボモードにして、基本周波数よりも高速の周波数でプロセッサコアを実行することもできます。ターボモードでは、熱および電力容量ヘッドルームを状況に応じて使用して、高い周波数でプロセッサコアを動作させることもできます。ターボモードでは、プロセッサのパフォーマンスを高めつつ、同じTDP（熱設計電力）を維持できます。

一部のプロセッサはTDPおよび最大電力レベルが設定済みです。これらのパラメーターを安全に維持するために、定義済み設定は、通常、プロセッサに組み込まれロックされています。これらの設定では、プロセッサを、標準的な電気、温度、および電源設計の仕様内で動作させます。プロセッサのターボプロファイルは、固定周波数レジスタとコア対周波数比レジスタを使用して、これらの制約が適用されます。消費電力上限は、TDPレベルに組み入れることができます。指定したTDPレベルを維持するために、CPUターボ周波数は、コア対周波数比レジスタに組み入れられたアクティブなコアの数によって決定されます。ターボ周波数プロファイルは、全コアアクティブから単一コアアクティブまでスケールされます。したがって、低いワークロード要求、またはコアパーキングテクノロジー、または無効化テクノロジーによって利用されているアクティブコアの数に応じて、ターボ周波数は増加します。

これらの周波数レジスタとコア対周波数比レジスタの融合によって、プロセッサの計算能力が特定のレベルに制限されます。ただし、汎用コンピューティングプロセッサでは、さまざまなワークロードまたは最悪の温度条件に対応できるように、ターボプロファイルを控え目に設定できます。つまり、ターボモードを、プロセッサが動作する構成または環境を考慮しないワンパターンプロファイルにすることもできます。したがって、プロセッサは、動作を最大限まで使用するようにチューニングできない可能性があります。

アドバンスト電力オプションの構成

チャネルインターリーブや協調電力制御のような高度な電力機能を有効にするには、アドバンスト電力オプションメニューを使用します。また、UPIリンク周波数を低速に設定したり、プロセッサのアイドル電力状態を設定したりできます。

手順

システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > アドバンスト電力オプションを選択します。

冗長電源装置モードの設定

冗長電源装置モードオプションを使用すると、システムによる冗長電源装置の構成の取り扱い方法を設定できます。冗長電源装置を使用している場合は、どの高効率モード設定を使用しても、電力の半分が電力使用レベルの低いスタンバイモードに維持されるため、電力効率の最も高い動作が実現します。 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。

前提条件

ワークロードプロファイルがカスタムに設定されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > アドバンスド電力オプション > 冗長電源装置モードを選択します。
2. 設定を選択します。
 - バランスモード - システムでは、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) - システムは、システムのグループ内のセミランダム分布に基づいて、奇数または偶数の電源装置から選択します。
 - 高効率モード (奇数電源スタンバイ) - システムは、奇数の電源装置をスタンバイ状態にします。
 - 高効率モード (偶数電源スタンバイ) - システムは、偶数の電源装置をスタンバイ状態にします。
3. 設定を保存します。

Infinity Fabricの電力管理の有効化または無効化

Infinity Fabricの電力管理を有効にすると、EPYCプロセッサはアクティビティレベルに基づいてInfinity Fabricのクロック周波数を動的に変更します。

NUMAに最適化されたワークロードの場合は、Infinity Fabricの実行速度を下げると、CPUブーストの増加によって全体的なパフォーマンスが向上する可能性があります。レイテンシの影響を受けやすいワークロードの場合は、この機能を無効にすることが必要になる場合があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプション > アドバンスド電力オプションを選択します。
2. Infinity Fabricの電力管理で、設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

パッケージ電力制限制御モードの構成

パッケージ電力制限制御モードは、システム内に取り付けられたすべてのプロセッサに適用されるプロセッサあたりのパッケージ電力制限値です。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 電力およびパフォーマンスオプションを選択します。
2. パッケージ電力制限制御モードで、設定を選択します。
 - 自動 - デフォルトのプロセッサ値が使用されます。
 - 手動 - パッケージ電力制限値をワット単位で変更できます。資格のある担当者の指示に従って行ってください。
3. 設定を保存します。

内蔵UEFIシェルオプションの変更

手順

システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 内蔵UEFIシェルオプションを選択します。

内蔵UEFIシェルの有効化または無効化

内蔵UEFIシェルオプションを使用すると、UEFIブートローダーを含むUEFIアプリケーションのスクリプトを作成し、実行するための起動前のコマンドライン環境を有効または無効にすることができます。内蔵UEFIシェルには、システム情報を取得し、システムBIOSを構成およびアップデートするために使用できるCLIベースのコマンドも用意されています。このオプションを有効にして、内蔵UEFIシェルをブート順序に追加を有効にすると、内蔵UEFIシェルがUEFIブート順序リストに追加されます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 内蔵UEFIシェル > 内蔵UEFIシェルを選択します。
2. 設定を選択します。
 - 有効 - 起動前環境から内蔵UEFIシェルを起動してUEFIブート順序リストに追加できます。
 - 無効 - 内蔵UEFIシェルは起動前環境で使用できないため、UEFIブート順序リストに追加できません。
3. 設定を保存します。

UEFIブート順序リストへの内蔵UEFIシェルの追加

前提条件

ブートモードがUEFIモードに設定されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 内蔵UEFIシェル > 内蔵UEFIシェルをブート順序に追加を選択します。
2. 設定を選択します。
 - 有効 - 次の再起動時に内蔵UEFIシェルをブート順序リストに追加します。
 - 無効 - 内蔵UEFIシェルは、ブート順序リストに追加されません。
3. 設定を保存します。

内蔵UEFIシェル起動スクリプトの自動実行の有効化または無効化

シェル起動中の内蔵UEFIシェル起動スクリプトの自動実行を有効または無効にするには、UEFIシェルスクリプト自動起動オプションを使用します。

- 起動スクリプトを使用して、RAMディスクの作成、ネットワークからのファイルをダウンロード、データの収集、結果のネットワークへの再アップロードを行い、システムを再起動せずにOSを再起動できます。
- ローカルメディア上にスクリプトファイルを保存したり、ネットワーク上の位置からスクリプトファイルにアクセスしたりできます。

- スクリプトファイルに `startup.nsh` という名前を付け、ローカルメディア上、またはサーバーがアクセスできるネットワーク上の位置に配置する必要があります。
- 自動起動が有効な場合、シェル自動起動スクリプトロケーションオプションが自動的に設定されていると、シェルは、スクリプトファイルを、最初にネットワーク上、次にローカル接続のFAT16またはFAT32フォーマットのメディアで探します。
- 1つのファイルシステムには、`startup.nsh` ファイルを1つだけ配置することをお勧めします。

前提条件

- ブートモードがUEFIモードに設定されている。
- 内蔵UEFIシェルが有効になっている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 内蔵UEFIシェル > UEFIシェルスクリプト自動起動を選択します。
2. 設定を選択します。
 - 有効 - シェルの起動中に、UEFIシェル起動スクリプトを実行します。
 - 無効 - シェルの起動中に、UEFIシェル起動スクリプトを実行しません。
3. 設定を保存します。

シェルスクリプト検証の有効化または無効化

前提条件

- ブートモードがUEFIモードに設定されている。
- 内蔵UEFIシェルが有効になっている。
- セキュアブートが有効になっている。
- シェルスクリプトがセキュアブートデータベースに登録されている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 内蔵UEFIシェル > シェルスクリプトの検証を選択します。
2. 設定を選択します。
 - 有効 - シェルスクリプトの検証を有効にします。
 - 無効 - (デフォルト) シェルスクリプトの検証を有効にはしません。
3. 設定を保存します。

内蔵UEFIシェル起動スクリプトロケーションの設定

シェル自動起動スクリプトロケーションオプションを使用して、内蔵UEFIシェル起動スクリプトの位置を選択します。UEFIシェルスクリプト自動起動を有効にする場合は、この設定でシェルが `startup.nsh` ファイルを検索する場所を指定します。

前提条件

- 内蔵UEFIシェルが有効になっている。
- UEFIシェルスクリプト自動起動が有効になっている。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 内蔵UEFIシェル > シェル自動起動スクリプトロケーションを選択します。
2. 設定を選択します。
 - 自動 - シェルは起動スクリプトの取得を最初にネットワーク上の場所から試行し、続いてローカルに接続されたメディアから試行します。
 - 接続メディア上のファイルシステム - シェルはUSBディスクまたはHDD上のFAT32パーティションのようなUEFIからアクセス可能なローカルファイルシステム上で `startup.nsh` スクリプトファイルを探します。
 - ネットワーク上 - シェルはシステムからアクセス可能なHTTPおよびHTTPSまたはFTPの場所から `.nsh` スクリプトを探します。
3. 設定を保存します。

DHCPを使用した、シェル自動起動スクリプトの検出の有効化または無効化

DHCPを使用したシェル自動起動スクリプトの検出オプションを使用して、シェルがDHCPを使用して、起動スクリプトのURLを検出できるようにします。有効に設定した場合、シェルは、DHCP `User Class` オプションを文字列 `UEFIShell` に設定してDHCP要求を送信します。

前提条件

- 内蔵UEFIシェルが有効になっている。
- UEFIシェルスクリプト自動起動が有効になっている。
- HTTPサポートポリシーが有効になっており、DHCPサーバーによって提供されたURLが、HTTPサポートポリシーの設定と一致する。
- シェル自動起動スクリプトロケーションがネットワーク上または自動的に設定されている。
- DHCPサーバーが、HTTP/HTTPSまたはFTPのURLを提供するように構成されている。
- `UEFIShell` に設定されている `User Class` オプションに応答するように、DHCPサーバーが構成されている。IPv4上のDHCPを使用する場合、`User Class` オプションはオプション77です。IPv6上のDHCPを使用する場合はオプション15です。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 内蔵UEFIシェル > DHCPを使用したシェル自動起動スクリプトの検出を選択します。
2. 設定を選択します。
 - 有効 - シェルは、起動スクリプトのURLを検出するのにDHCPを使用します。
 - 無効 - シェルは、起動スクリプトのURLを検出するためのDHCP要求を送信しません。
3. 設定を保存します。

シェル自動起動スクリプトのネットワーク上の場所の設定

前提条件

- 内蔵UEFIシェルが有効になっている。
- シェル自動起動スクリプトロケーションがネットワーク上または自動的に設定されている。
- DHCPを使用したシェル自動起動スクリプトの検出が無効に設定されている。
- HTTPS URLを指定するとき、サーバーセキュリティ > TLS (HTTPS) オプションを使用して、HTTPSサーバーのTLS証明書が構成されます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 内部UEFIシェル > シェル自動起動スクリプトのためのネットワーク上の場所を選択します。
2. `.nsh` ファイルのネットワーク上の位置を入力します。次の値が有効です。
 - IPv4またはIPv6サーバーアドレスかホスト名のHTTP/HTTPS形式のURL。
 - IPv4またはIPv6サーバーアドレスかホスト名のFTP形式のURL。

例:

 - `http://192.168.0.1/file/file.nsh`
 - `http://example.com/file/file.nsh`
 - `https://example.com/file/file.nsh`
 - `http://[1234::1000]/file.nsh`
3. 設定を保存します。

サーバーセキュリティ設定の変更

手順

システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティを選択します。

サーバーセキュリティのオプション

- 電源投入時パスワードの設定
- 管理者パスワードの設定
- セキュアブート設定
- TLS (HTTPS) オプション
- Trusted Platform Moduleオプション
- インテル (R) TXTサポート
- ワンタイムブートメニュー (F11プロンプト)
- バックアップROMイメージの認証

電源投入時パスワード設定

電源投入時パスワード設定オプションを使用して、ブートプロセス中にサーバーにアクセスするためのパスワードを設定できます。サーバーの電源を投入すると、プロンプトが表示されます。続行するには、ここにパスワードを入力する必要があります。パスワードを無効化または消去するには、パスワードの入力を求めるメッセージが表示されたときに、パスワードの後に/ (スラッシュ) を付けて入力します。



注記:

ASR (自動サーバー復旧) 再起動の場合、電源投入時パスワードはバイパスされ、サーバーは通常どおり起動します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > 電源投入時パスワード設定を選択します。

2. パスワードを入力します。
パスワードは次の条件を満たしている必要があります。
 - 最大31文字
 - 英数字および特殊文字の任意の組み合わせ
3. 確認のためもう一度パスワードを入力して、Enterを押します。
パスワードが設定されていることを確認するメッセージが表示されます。
4. 変更を保存します。
5. サーバーを再起動します。

iLOアカウントでのログイン許可

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > iLOアカウントでのログインを許可を選択します。
2. ユーザーがCONFIGURE_BIOS権限を持つiLOアカウントでログインできるようにするには、iLOアカウントでのログインを許可を選択します。
3. 変更を保存します。

管理者パスワードの設定

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > 管理者パスワードの設定を選択します。
2. パスワードを入力します。
パスワードは次の条件を満たしている必要があります。
 - 最大31文字
 - 英数字および特殊文字の任意の組み合わせ
3. 確認のためもう一度パスワードを入力して、Enterを押します。
パスワードが設定されていることを確認するメッセージが表示されます。
4. 変更を保存します。
5. サーバーを再起動します。

セキュアブート

セキュアブートはサーバーのセキュリティ機能で、完全にBIOSに組み込まれており、特殊なハードウェアは不要です。セキュアブートにより、ブートプロセス中に起動した各コンポーネントにデジタル記号が付けられ、この署名がUEFI BIOSに内蔵された一連の信頼済みの証明書と照合されて検証されます。セキュアブートは、ブートプロセス中に次のコンポーネントのソフトウェアIDを検証します。

- PCIeカードからロードされたUEFIドライバー

- 大容量ストレージデバイスからロードされたUEFIドライバー
- プリブートUEFIシェルアプリケーション
- OS UEFIブートローダー

セキュアブートが有効になっている場合には、以下が必要です。

- ブートプロセス中、ブートローダーを持つオペレーティングシステムとファームウェアコンポーネントは、実行するために適切なデジタル署名を持っている必要があります。
- オペレーティングシステムは、起動するためには、セキュアブートをサポートし、認証済みキーの1つで署名されたEFIブートローダーを持っている必要があります。サポートされるオペレーティングシステムについて詳しくは、<https://www.hpe.com/servers/ossupport>を参照してください。

独自の証明書を追加または削除することにより、UEFI BIOSに組み込まれている証明書をカスタマイズできます。カスタマイズは、サーバーに直接取り付けられた管理コンソールから行うことも、またはiLOリモートコンソールを使用してサーバーにリモート接続して行うこともできます。

セキュアブートは、次のように構成できます。

- 以下の各項で説明されているシステムユーティリティオプションを使用する。
- iLO RESTful APIを使用して、証明書をクリアし、復元する。詳しくは、Hewlett Packard EnterpriseのWebサイト (<https://www.hpe.com/info/redfish>) を参照してください。
- 内蔵UEFIシェルで `secboot` コマンドを使用し、セキュアブートデータベース、キー、およびセキュリティレポートを表示する。

セキュアブートの有効化または無効化

前提条件

このオプションを有効にするには、次の操作を行います。

- ブートモードをUEFIモードに設定します。
- UEFI最適化ブートを有効にします。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > セキュアブート設定 > セキュアブートの試行を選択します。
2. 設定を選択します。
 - 有効 - セキュアブートを有効にします。
 - 無効 - セキュアブートを無効にします。
3. 変更を保存します。
4. サーバーを再起動します。

サーバーロック設定の構成

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > サーバー構成ロックの設定を選択します。
画面に、サーバー構成ロックの状態が表示されます。
2. 以下のオプションを変更できます。
 - サーバー構成ロックのチャレンジが必要：有効または無効を選択します。

- システムのトランスポートの準備：有効または無効を選択します。
 - サーバー構成ロックの障害検出時に停止：有効または無効を選択します。
3. 設定を保存します。

サーバー構成ロックのセットアップ

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > サーバー構成ロックの設定 > サーバー構成ロックのセットアップを選択します。
2. 以下を選択します。
 - システムボードを除外。
 - DIMMを除外。
 - CPUを除外。
 - PCIeスロットを除外。
 - セキュリティ構成を除外。
 - システムのファームウェアリビジョンを除外。
3. デジタルフィンガープリントを作成するには、サーバー構成ロックのデジタルフィンガープリントの生成をクリックします。
4. 設定を保存します。

アドバンストセキュアブートオプション

- PK - プラットフォームキー - プラットフォームオーナーとプラットフォームファームウェア間の信頼関係を確立します。
- KEK - キー交換キー - 許可されていない変更から署名データベースを保護できます。このキーのプライベート部分がないと、署名データベースに変更を加えることはできません。
- DB - 許可済み署名データベース - プラットフォーム上での実行を許可された署名のセキュアブート許可済み署名データベースを保持します。
- DBX - 禁止された署名データベース - プラットフォーム上での実行を許可されていない署名のセキュアブートブラックリスト署名データベースを保持します。
- DBT - タイムスタンプ署名データベース - タイムスタンプ署名データベース内のコードの署名を保持します。
- すべてのキーを削除
- すべてのキーをエクスポート
- すべてのキーをプラットフォームのデフォルトにリセット

注記:

デフォルトのセキュリティ証明書を変更すると、一部のデバイスからシステムの起動に失敗することがあります。さらに、Intelligent Provisioningのようなシステムソフトウェアの起動に失敗することもあります。

アドバンストセキュアブートオプションの設定の表示

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > セキュアブート設定 > アドバンスドセキュアブートオプションを選択します。
2. 交換キーまたは署名データベースオプションを選択します。
3. 交換キーまたは署名データベースオプションに対してViewエントリーを選択します。
4. 表示するオプションのエントリーを選択します。

例：HPE UEFIセキュアブート2016 PKキーの詳細の表示

システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > セキュアブート設定 > アドバンスドセキュアブートオプション > PK - プラットフォームキー > PKエントリーを表示 > HPE UEFI Secure Boot 2016 PKキーを選択します。

セキュアブート証明書キーまたはデータベース署名の登録

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > セキュアブート設定 > アドバンスドセキュアブートオプションを選択します。
2. 交換キーまたは署名データベースオプションを選択します。
3. Enroll <option name> (<オプション名>を登録) を選択します。
4. Enroll <option name> using file (ファイル名を使用して<オプション名>を登録) を選択します。
ファイルエクスプローラー画面に、接続されているメディアデバイスが表示されます。
5. 証明書ファイルが配置されている接続されているメディアデバイスを選択し、Enterを押します。
6. 証明書ファイルのメニューのパスの選択を続行します。選択するごとに、Enterキーを押します。
7. オプション：署名所有者のGUIDを選択します。
8. オプション：署名所有者GUIDでその他を選択した場合、署名のGUIDを入力します。

次の形式を使用します (36文字) : 11111111-2222-3333-4444-1234567890ab

- Hewlett Packard Enterpriseの証明書の場合は、F5A96B31-DBA0-4faa-A42A-7A0C9832768Eを入力します。
 - Microsoftの証明書の場合は、77fa9abd-0359-4d32-bd60-28f4e78f784bを入力します。
 - SUSEの証明書の場合は、2879c886-57ee-45cc-b126-f92f24f906b9を入力します。
9. 変更をコミットして終了を選択します。

例：KEKエントリーを登録

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > セキュアブート設定 > アドバンスドセキュアブートオプション > KEK - キー交換キー > KEKエントリーを登録を選択します。
2. ファイルを使用してKEKを登録を選択します。
3. 接続されているメディアデバイスから証明書ファイルの場所を選択します。
4. オプション：署名所有者のGUIDを選択します。
5. オプション：署名所有者GUIDでその他を選択した場合、署名のGUIDを入力します。

- 変更をコミットして終了を選択します。

セキュアブート証明書キーまたはデータベース署名の削除

手順

- システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > セキュアブート設定 > アドバンスドセキュアブートオプションを選択します。
- 交換キーまたは署名データベースオプションを選択します。
- 次のいずれかを実行します。
 - 削除できるオプションが1つある場合は、次の手順に従います。
 - 削除 <オプション名> チェックボックスを選択します。
 - はいをクリックします。
 - 削除できるオプションが2つ以上ある場合は、次の手順に従います。
 - 削除 <オプション名> を選択します。
 - 削除するオプションのチェックボックスを選択します。
 - はいをクリックします。

例：KEKエントリーの削除

- システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > セキュアブート設定 > アドバンスドセキュアブートオプション > KEK - キー交換キー > KEKエントリーを削除を選択します。
- 削除するエントリーのチェックボックスを選択します。
- はいをクリックします。

すべてのキーを削除

すべてのキーを削除オプションを選択すると、プラットフォームキーを含む、システム内のすべてのキーが削除されます。

① 重要:

すべてのキーが削除されると、システムのセキュアブートはただちに強制的に無効になります。システムを再起動しても、セキュアブートは無効なままです。これは、有効なセキュアブートキーが復元されるまで続きます。

手順

- システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > セキュアブート設定 > アドバンスドセキュアブートオプション > すべてのキーを削除を選択します。
- Enterキーを押して、すべてのキーを削除します。
- 削除を確認します。

セキュアブート証明書キーまたはデータベース署名のエクスポート

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > セキュアブート設定 > アドバンスドセキュアブートオプションを選択します。
2. 交換キーまたは署名データベースオプションを選択します。
3. 選択エクスポート <オプション名>を選択します。
4. エクスポートするエントリーを選択します。
ファイルエクスプローラー画面に、接続されているメディアデバイスが表示されます。
5. 次のいずれかを実行します。
 - ファイルをエクスポートする接続されているメディアデバイスを選択し、証明書ファイルのメニューパスの選択を続けます。選択するごとに、Enterキーを押します。
 - 新しいファイルにエクスポートするには、+キーを押して、ファイル名を入力します。

例：許可済み署名データベース署名のエクスポート

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > セキュアブート設定 > アドバンスドセキュアブートオプション > DB - 許可済み署名データベース > 署名をエクスポート > HPE UEFI Secure Boot 2016 DB Keyを選択します。
2. エクスポートするエントリーを選択します。
ファイルエクスプローラー画面に、接続されているメディアデバイスが表示されます。
3. 次のいずれかを実行します。
 - ファイルをエクスポートする接続されているメディアデバイスを選択し、証明書ファイルのメニューパスの選択を続けます。選択するごとに、Enterキーを押します。
 - 新しいファイルにエクスポートするには、+キーを押して、ファイル名を入力します。

すべてのセキュアブート証明書キーのエクスポート

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > セキュアブート設定 > アドバンスドセキュアブートオプション > すべてのキーをエクスポートを選択します。
ファイルエクスプローラー画面に、接続されているメディアデバイスが表示されます。
2. 次のいずれかを実行します。
 - ファイルをエクスポートする接続されているメディアデバイスを選択し、証明書ファイルのメニューパスの選択を続けます。選択するごとに、Enterキーを押します。
 - 新しいファイルにエクスポートするには、+キーを押して、ファイル名を入力します。

セキュアブート認証キーまたはデータベース署名をプラットフォームのデフォルトにリセット

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > セキュアブート設定 > アドバンスドセキュアブートオプションを選択します。
2. 交換キーまたは署名データベースオプションを選択します。

3. プラットフォームのデフォルトにリセットを選択します。
4. はいをクリックします。

すべてのセキュアブート認証キーをプラットフォームのデフォルトにリセット

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > セキュアブート設定 > アドバンスドセキュアブートオプション > すべてのキーをプラットフォームのデフォルトにリセットを選択します。
2. はいをクリックします。

TLS (HTTPS) オプション

TLS証明書の詳細の表示

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > TLS (HTTPS) オプション > 証明書を表示を選択します。
2. 証明書を選択します。

TLS証明書の登録

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > TLS (HTTPS) オプション > 証明書を登録を選択します。
2. ファイルエクスプローラーを使用して証明書を登録を選択します。
ファイルエクスプローラー画面に、接続されているメディアデバイスが表示されます。
3. 証明書ファイルが配置されている接続されているメディアデバイスを選択し、Enterを押します。
4. 証明書ファイルのメニューのパスの選択を続行します。選択するごとに、Enterキーを押します。
5. 変更をコミットして終了を選択します。

TLS証明書の削除

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > TLS (HTTPS) オプション > 証明書を削除を選択します。
2. 証明書のリストで、削除する証明書を選択します。
3. 変更をコミットして終了を選択します。

すべてのTLS証明書の削除

証明書をすべて削除オプションを選択すると、システム内のすべての証明書を削除できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > TLS (HTTPS) オプション > 証明書をすべて削除を選択します。
2. Enterを押します。
3. 削除を確認します。

TLS証明書のエクスポート

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > TLS (HTTPS) オプション > 証明書をエクスポートを選択します。
2. エクスポートされる証明書のファイル形式を選択します。
ファイルエクスプローラー画面に、接続されているメディアデバイスが表示されます。
3. 次のいずれかを実行します。
 - ファイルをエクスポートする接続されているメディアデバイスを選択し、証明書ファイルのメニューパスの選択を続けます。選択するごとに、Enterキーを押します。
 - 新しいファイルにエクスポートするには、+キーを押して、ファイル名を入力します。

すべてのTLS証明書のエクスポート

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > TLS (HTTPS) オプション > すべての証明書をエクスポートを選択します。
ファイルエクスプローラー画面に、接続されているメディアデバイスが表示されます。
2. 次のいずれかを実行します。
 - ファイルをエクスポートする接続されているメディアデバイスを選択し、証明書ファイルのメニューパスの選択を続けます。選択するごとに、Enterキーを押します。
 - 新しいファイルにエクスポートするには、+キーを押して、ファイル名を入力します。

すべてTLS設定をプラットフォームのデフォルトにリセット

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > TLS (HTTPS) オプション > すべての設定をプラットフォームのデフォルトにリセットを選択します。
2. OKをクリックします。

高度なTLSセキュリティ設定の構成

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > TLS (HTTPS) オプション > 高度なセキュリティ設定を選択します。
2. オプションを構成します。
 - TLS接続でどの暗号スイートが許可されるのかについて構成を行うには、次の手順に従います。
 - a. TLS接続で許可する暗号スイートを選択します。
 - b. 次のいずれかを選択します。
 - 許可する暗号スイートに対応する個々のチェックボックス。
 - プラットフォームのデフォルトの暗号スイートを選択
 - c. 変更をコミットして終了を選択します。
 - TLS接続ごとに証明書検証プロセスを構成するには、次の手順に従います。
 - a. すべてのTLS接続の証明書の検証を選択します。
 - b. 設定を選択します。
 - PEER (推奨) - セキュアな通信を実現するために、ピアで提供される証明書を検証します。
 - なし - 証明書を検証しません。
 - 厳密なホスト名のチェックを有効または無効にするには、次の手順に従います。
 - a. ホスト名を厳密にチェックを選択します。
 - b. 設定を選択します。
 - ENABLE - 接続されているサーバーのホスト名がサーバーが提供する証明書のホスト名と照合されます。
 - DISABLE - 接続されているサーバーのホスト名の、サーバーが提供する証明書のホスト名との照合は行われません。
 - TLS接続に使用するプロトコルバージョンを指定するには、次の手順に従います。
 - a. TLSプロトコルバージョンをサポートを選択します。
 - b. 設定を選択します。
 - AUTO - TLSサーバーとクライアントの両方でサポートされる最新のプロトコルバージョンがネゴシエートされます。
 - 1.0 - TLSプロトコルバージョン1.0を使用します。(Gen10 Plusではサポートされません)
 - 1.1 - TLSプロトコルバージョン1.1を使用します。(Gen10 Plusではサポートされません)
 - 1.2 - TLSプロトコルバージョン1.2を使用します。
3. 変更を保存します。

Trusted Platform Moduleオプションの構成

Trusted Platform 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。Trusted Platform Moduleで構成されているサーバーでは、ファームウェアおよびオペレーティングシステムは、TPMを使用して、ブートプロセスのすべてのフェーズを測定できます。TPMモジュールオプションの取り付けおよび有効化については、ご使用のサーバーモデルの

ユーザードキュメントを参照してください。

Trusted Platform Moduleを有効にするには、次のガイドラインに従ってください。

- デフォルトでは、Trusted Platform Moduleを取り付けた後にサーバーの電源がオンになると、Trusted Platform ModuleはTPM 2.0として有効化されます。
- UEFIモードでは、Trusted Platform ModuleをTPM 2.0またはTPM 1.2として動作するように構成できます。
- レガシーブートモードでは、Trusted Platform Module構成をTPM 1.2とTPM 2.0に切り替えることができますが、サポートされている動作はTPM 1.2のみです。

△ 注意:

サーバーの変更や、適切な手順を使用してOSでのTPMのサスペンドまたは無効化を実行しないと、TPMを使用しているOSですべてのデータアクセスがロックされる場合があります。これには、システムまたはオプションファームウェアのアップデート、ハードウェア（システムボードやハードドライブなど）の交換、TPMのOS設定の変更が含まれます。OSのインストール後にTPMモードを変更すると、データ消失などの問題の原因となります。

手順

1. システムユーティリティ画面で、System Configuration > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > Trusted Platform Moduleオプションを選択します。
2. オプションを選択します。オプションのTPMを使用して構成されているサーバーでは、以下を設定できます。
 - TPM 2.0操作 - 再起動後に実行するTPM 2.0の動作を設定します。オプションは次のとおりです。
 - 操作なし - 構成されているTPMはありません。
 - クリア - 再起動中にTPMがクリアされます。また、TPM 2.0操作は、操作なしに設定されます。
 - TPMモードの切り替え - TPMモードを設定して、再起動後に実行されるようにします。オプションは次のとおりです。
 - 操作なし
 - TPM 1.2
 - TPM 2.0
 - TPM 2.0ビジビリティ - オペレーティングシステムがTPMを認識しないようにするかどうかを設定します。オプションは次のとおりです。
 - 隠さない
 - 隠す - オペレーティングシステムからTPMを隠します。この設定を使用して、実際のハードウェアを取り外さずにTPMオプションをシステムから削除します。
 - TPM UEFIオプションROM測定 - UEFI PCI操作ROMの計測を有効または無効（スキップ）にします。オプションは次のとおりです。
 - 有効
 - 無効
 - バックアップROMイメージの認証 - このオプションを使用して、起動時のバックアップROMイメージの暗号化認証を有効にします。このオプションを無効にした場合、起動ごとにプライマリイメージの認証のみが実行されます。このオプションを有効にすると、バックアップROMイメージの暗号化認証も実行されます。
3. 変更を保存します。
4. システムを再起動します。

システムが再起動したら、現在のTPMのタイプと現在のTPMの状態の設定を表示できます。
5. 新しい現在のTPMのタイプと現在のTPMの状態の設定が、画面の上部に表示されることを確認します。

TPM FIPSモード切替操作の設定

TPM 1.2モードをPOSTを介してFIPS対応にする場合は、TPM FIPSモード切替操作オプションを使用します。デフォルトでは、TPM 2.0モードは、POSTを介したFIPS対応です。

前提条件

- ご使用のオペレーティングシステムでは、TPM 1.2連邦情報処理規格（FIPS）モードをサポートしています。
- Trusted Platform ModuleのTPMモードの切り替えは、1.2, FIPSに設定されています。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > サーバーセキュリティ > Trusted Platform Moduleオプション > TPM FIPSモード切替操作を選択します。
2. 設定を選択します。
 - 操作なし - モードは設定されません。
 - 通常モード - TPMはFIPSモードで動作しません。
 - FIPSモード - TPMは連邦情報処理規格を使用して動作します。
3. 設定を保存します。

アドバンストセキュリティオプションの変更

手順

システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > アドバンストセキュリティオプションを選択します。

プラットフォーム証明書サポートの有効化または無効化

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > サーバーセキュリティ > アドバンストセキュリティオプション > プラットフォーム証明書サポートを選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

iLOアカウントによるログインの有効化または無効化

ユーザーがCONFIGURE BIOS 権限を持つiLOアカウントでログインできるようにするには、iLOアカウントでのログインを許可オプションを使用します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > サーバーセキュリティ > アドバンストセキュリティオプション > iLOアカウントでのログインを許可を選択します。
2. 設定を選択します。
 - 有効
 - 無効

3. 設定を保存します。

バックアップROMイメージ認証の有効化または無効化

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > アドバンスドセキュリティオプション > バックアップROMイメージの認証を選択します。
2. 設定を選択します。
 - 有効: 有効にした場合、起動時にバックアップROMイメージの暗号化認証が行われます。
 - 無効: 無効にした場合、起動のたびにプライマリROMイメージのみが認証されます。
3. 設定を保存します。

ワンタイムブートメニュー (F11プロンプト) の有効化または無効化

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > アドバンスドセキュリティオプション > ワンタイムブートメニュー (F11プロンプト) を選択します。
2. 設定を選択します。
 - 有効
 - 無効: これは、POSTワンタイムブートF11プロンプトを無効にします。無効の場合、`boot` シェルコマンドは使用できません。
3. 設定を保存します。

Intelligent Provisioning (F10プロンプト) の有効化または無効化

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > アドバンスドセキュリティオプション > Intelligent Provisioning (F10プロンプト) を選択します。
2. 設定を選択します。
 - 有効: 有効にすると、Intelligent Provisioning機能を使用できます。
 - 無効: 無効にすると、サーバーの起動時にF10を押している間に、Intelligent Provisioning環境に入れません。
3. 設定を保存します。

Microsoft (R) Secured-coreサポートの有効化または無効化

Microsoft (R) Secured-coreサポートオプションを使用して、Microsoft (R) Secured-coreサポート用にサーバーを構成します。有効にすると、さまざまな仮想化とセキュリティの設定が自動的に有効になります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > Microsoft (R) Secured-coreサポートを選択します。
2. 設定を選択します。

- 有効



注記:

Intelシステムでこの機能を有効にすると、次が有効になります。

- すべてのプロセッサコア
- インテルVT
- インテルVT-d
- インテルTXT
- セキュアブート
- UEFI最適化ブート
- ブートモードがUEFIモードに設定されている
- TPMモードがTPM 2.0に設定されている
- TPMの状態が装着済で有効に設定されている

AMDシステムでこの機能を有効にすると、次が有効になります。

- すべてのプロセッサコア
- AMD DMA再マッピング
- AMD I/Oバーチャライゼーションテクノロジー
- AMD仮想DRTMデバイス
- 透過的セキュアメモリ暗号化
- UEFI最適化ブート
- セキュアブート
- ブートモードがUEFIモードに設定されている。
- TPMモードがTPM 2.0に設定されている
- TPMの状態が装着済で有効に設定されている

- 無効

3. 設定を保存します。

アドバンストオプションの変更

手順

システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンストオプションを選択します。

ROMイメージの選択

冗長ROMを搭載するサーバーでは、ROMの選択オプションを使用して、サーバーを以前のBIOS ROMイメージに戻してください。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンストオプション > ROMの選択を選択します。
2. 設定を選択します。
 - 現在のROMを使用
 - バックアップROMへ切り替え - 最後のフラッシュイベントの前に使用されていたイメージに戻ります。
3. 設定を保存します。

内蔵ビデオ接続の構成

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンストオプション > 内蔵ビデオ接続を選択します。
2. 設定を選択します。
 - 自動 - モニターが接続されていないと、内蔵ビデオコントローラーへの外部ビデオ接続は消費電力を節約するため、自動的に無効になります。モニターが接続されると自動的に有効になります (サーバーが動作中の場合を含む)。
 - 常に無効 - 内蔵ビデオコントローラーへの外部ビデオ接続は無効であり、システムの起動中を除いて、このポートに接続されているモニターには表示されません。
 - 常に有効 - 内蔵ビデオコントローラーへの外部ビデオ接続は常に有効です。このオプションが必要なのは、動作しないモニター検出機器にモニターが接続されていて、自動モードが適切に動作しなくなる場合だけです。
3. 設定を保存します。

電源装置要件のオーバーライドの構成

電源装置要件のオーバーライドオプションを使用して、システムの通常の電源装置要件をオーバーライドします。サーバーは、要件に適合する電源装置が搭載されている状態で、幅広いワークロードと構成で動作できます。このオプションは、1台の電源装置で動作して冗長化するようにシステムの電源装置要件を変更します。また、2台の電源装置で動作して、3台の電源装置で冗長化できるように、システムの電源装置要件を変更することもできます。

注記:

デフォルトの電源装置要件をオーバーライドするオプションを有効にする前に、Power Advisorを使用してシステムの電源装置要件を確認してください。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンストオプション > 電源装置要件のオーバーライドを選択します。
2. 設定を選択します。
 - デフォルトの電源装置要件
 - 1台が最低要件、2台が冗長化の要件として構成
 - 2台が最低要件、3台が冗長化の要件として構成
 - 2台が最低要件、4台が冗長化の要件として構成
 - 3台が最低要件、4台が冗長化の要件として構成
 - 4台が最低要件、冗長化なしで構成
3. 変更を保存します。

一貫性のあるデバイスの名前付けの有効化または無効化

サポートされているオペレーティングシステムで、一貫性のあるデバイスの名前付けオプションを使用して、システム内のNICポートの位置に基づいてNICポートに名前を付ける方法を制御します。

注記:

既存のNIC接続は、OS環境で取り付けなおされるまではその名前を維持します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンスドオプション > 一貫性のあるデバイスの名前付けを選択します。
2. 設定を選択します。
 - LOMおよびスロットのCDNサポート - システムのすべてのNICポートに名前を付けます。
 - LOMのみのCDNサポート - 内蔵NICおよびFlexible LOMには名前を付けますが、その他のNICポートには付けません。
 - 無効 - 一貫性のあるデバイスの名前付けを無効にします。
3. 設定を保存します。

電源装置混在レポートの有効化または無効化

電源装置混在レポートオプションを使用すると、混合電源装置構成が存在する場合にサーバーがメッセージを記録するかどうかを設定できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンスドオプション > 電源装置混在レポートを選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

POSTビデオサポート設定の変更

このオプションを使用して、POSTビデオサポート設定を構成します。このオプションはUEFIブートモードでのみサポートされており、POST (プリブート) 環境中のビデオ出力にのみ適用されます。

手順


1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンスドオプション > ビデオオプションを選択します。
2. 設定を選択します。
 - すべて表示: システムは設置済みのすべてのビデオコントローラーにPOSTビデオを表示します。
 - 組み込み型のみ表示: システムは組み込み型ビデオコントローラーにのみPOSTビデオを表示します。
3. 設定を保存します。


プラットフォームのRASポリシーの構成

プラットフォームのRASポリシーは、プラットフォームの耐障害性および保守性（RAS）ポリシーを制御します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > アドバンスドオプション > プラットフォームのRASポリシーを選択します。
2. 設定を選択します。
 - ファームウェア優先（デフォルト） - このモードでは、BIOSは訂正済みエラーを監視し、ユーザーが訂正済みエラーに対処する必要がある場合はエラーをログに記録します。OSは、訂正済みエラーを監視またはログに記録しません。

 注記： このオプションは、推奨される構成です。
 - OS優先 - このモードでは、訂正済みエラーはOSに対してマスクされず、OSが訂正済みエラーのログ記録のためのポリシーを制御します。一部のオペレーティングシステムでは、OSはすべての訂正済みエラーをログに記録します。


 注記： 訂正済みエラーは予期される自然に発生するものであり、（BIOSでもイベントのログが記録されている場合を除き）訂正済みエラーのOSのログ機能に基づいたアクションは必要ありません。
3. 設定を保存します。

SCI RASのサポートの構成

SCI RASのサポートを使用して、動作のシステム制御割り込み（SCI）信号モードを選択します。この設定は、特定のエラー条件に対してシステムがOSに信号を送る方法を監視するために使用できます。ページ廃棄などの特定の耐障害性機能では、OSがエラーイベントに適切に対応できるように、この設定を適切に構成する必要があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > アドバンスドオプション > SCI RASのサポートを選択します。
2. 設定を選択します。
 - GHES v1サポート
 - GHES v2サポート

 注記： どのオペレーティングシステムがSCI操作のどのモードをサポートするかについては、ドキュメントを参照してください。インストールされているOSは、適切な動作を保証するために、適切なGHES信号モードをサポートする必要があります。
3. 設定を保存します。

高精度イベントタイマー（HPET）ACPIサポートの有効化または無効化

高精度イベントタイマー（HPET）ACPIサポートオプションを使用すると、ACPIの高精度イベントタイマー（HPET）テーブルとデバイスオブジェクトを有効または無効にすることができます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > アドバンスドオプション > 高精度イベントタイマー（HPET）ACPIサポートを選択します。
2. 設定を選択します。

- 有効 - 業界標準のACPI名前空間を使用してHPETをサポートするオペレーティングシステムはHPETを利用できません。
 - 無効 - 業界標準のACPI名前空間を使用してHPETをサポートするオペレーティングシステムはHPETを利用できません。
3. 設定を保存します。

UEFI電源装置要件の変更

このオプションを使用して、電源装置冗長論理を構成します。サーバーは、要件に適合する電源装置が搭載されている状態で、幅広いワークロードと構成で動作できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンスオプションを選択します。
2. 電源装置要件で、次のいずれかを選択します。
 - 1+1冗長に構成済み：1つの電源が必要で、冗長構成に追加の電源が必要です。
 - 2+2冗長に構成済み：2つの電源が必要で、冗長構成に2つの追加の電源が必要です。
 - 3+1冗長に構成済み：3つの電源が必要で、冗長構成に追加の電源装置が必要です。
 - 4+0冗長に構成済み：冗長性なしで4つの電源が必要です。
3. 設定を保存します。

温度構成の設定

温度構成オプションを使用すると、システムのファン冷却方法を選択できます。このオプションの変更をお勧めするのは、最適な冷却では適切に冷却できない、Hewlett Packard Enterpriseがサポートする通常の構成とは異なる構成を使用する場合に限られます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンスオプション > ファンと温度のオプション > 温度構成を選択します。
2. 設定を選択します。
 - 最適な冷却 - ファンが適切な冷却を行うために必要な最低限の速度に構成されるため、最も効率的な冷却が可能になります。
 - 増強した冷却 - ファンの回転速度を上げます。
 - 最大冷却 - システムで使用できる最大の冷却能力を提供します。
 - 強化されたCPU冷却 - プロセッサへの冷却を強化することにより、パフォーマンスが向上する可能性があります。
3. 設定を保存します。

高温シャットダウンの有効化または無効化

高温シャットダウンオプションを使用すると、非冗長ファンモードでファンに障害が発生した場合、システムをシャットダウンするように構成できます。非冗長ファンの障害、またはあらかじめ設定されたしきい値を超える温度の上昇が発生した場合に、シャットダウンを開始できます。無効にした場合、システムマネジメントドライバーは高温イ

イベントを無視します。データが破壊されるような状況になると、システムの電源はただちにオフになります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンスドオプション > ファンと温度のオプション > 高温シャットダウンを選択します。
2. 設定を選択します。
 - 有効 - サーバーの内部温度がクリティカルなレベルの5度以内に達すると、サーバーは自動的にシャットダウンされます。
 - 無効 - サーバーの内部温度がクリティカルなレベルの5度以内に達しても、サーバーは自動的にシャットダウンされません。温度がクリティカルなレベルに達するとシャットダウンされます。
3. 設定を保存します。

ファン設置要件のメッセージングの設定

ファン設置要件オプションを使用すると、すべての必要なファンが取り付けられていない場合のサーバーの対応方法を構成できます。必要なファンがない状態でサーバーを動作すると、ハードウェアコンポーネントが損傷を受ける可能性があります。必要なファンが取り付けられていない場合、デフォルトでは、サーバーは、メッセージを表示し、イベントをIMLに記録します。サーバーは引き続き、起動して動作することが可能です。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンスドオプション > ファンと温度のオプション > ファン設置要件を選択します。
2. 設定を選択します。
 - メッセージング有効 - 必要なファンが取り付けられていない場合、サーバーは、メッセージとログイベントをIMLに表示します。サーバーは引き続き、起動して動作することが可能です。この設定は推奨される設定です。
 - メッセージング無効 - 必要なファンが取り付けられていない場合、サーバーは、メッセージとログイベントを表示しません。必要なファンがない状態でサーバーが動作していることを示すものがすべてが削除されます。
3. 設定を保存します。

ファン故障ポリシーの設定

ファン故障ポリシーオプションを使用すると、ファンの障害によって、稼働に必要なファンがサーバーからなくなったときのサーバーの対応方法を構成できます。

注記:

必要なファンを取り付けずにサーバーを動作させるのはお勧めできません。システムがコンポーネントを正しく冷却する機能に影響を及ぼす可能性があります。ハードウェアコンポーネントに損傷を与える可能性もあります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンスドオプション > ファンと温度のオプション > ファン故障ポリシーを選択します。
2. 設定を選択します。
 - 重大なファン故障時にシャットダウン/停止 - 1つまたは複数のファンの障害によって必要なファンが動作していない場合、サーバーの起動または動作ができません。この設定は推奨される設定です。
 - 重大なファン故障時に稼働許可 - 1つまたは複数のファンの障害によって必要なファンが動作していない場合も、サーバーは起動して動作することが可能です。
3. 設定を保存します。

上昇した周囲温度のサポートの有効化または無効化

拡張周囲温度サポートオプションを使用すると、通常サポートされる温度よりも高い周囲温度でサーバーが動作するようになります。

注記:

このオプションは、特定のハードウェア構成によってのみサポートされます。周囲温度の拡張サポートを有効にする前に、HPEサーバーのドキュメントを参照してください。不適切なシステムの動作やハードウェアコンポーネントの損傷は、未サポートの構成でこれらの機能を有効にすることが原因である場合があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンストオプション > ファンと温度のオプション > 拡張周囲温度サポートを選択します。
2. 設定を選択します。
 - 無効
 - 周囲温度40cに対応 (ASHRAE 3) - 周囲温度が最大40度 (摂氏) の環境でサーバーの動作を許可します。
 - 周囲温度45cに対応 (ASHRAE 4) - 周囲温度が最大45度 (摂氏) の環境でサーバーの動作を許可します。

注記:

すべてのサーバーが周囲温度40c (ASHRAE 3) と45c (ASHRAE 4) の両方をサポートするとは限りません。

3. 設定を保存します。

シリアル番号の再入力

シリアル番号オプションは、システムボードの交換後、サーバーのシリアル番号を再入力するのに使用します。この値はシャーシの背面に貼付されているシリアル番号のステッカーと一致する必要があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンストオプション > アドバンストサービスオプション > シリアル番号を選択します。
2. シリアル番号を入力し、Enterを押します。
3. 設定を保存します。

製品IDの再入力

製品IDオプションは、システムボードの交換後、製品IDを再入力するのに使用します。この値は、シャーシの背面に貼付されている製品IDステッカーと一致する必要があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンストオプション > アドバンストサービスオプション > 製品IDを選択します。
2. 製品IDを入力して、Enterを押します。
3. 設定を保存します。

アドバンストデバッグオプションの構成

前提条件

ブートモードがUEFIモードに設定されている。

アドバンストデバッグオプションを使用して、デバッグおよびPOSTブートの進捗状況メッセージの出力レベルを制御している。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンストオプション > アドバンストデバッグオプションを選択します。
2. 設定を選択します。
 - UEFIシリアルデバッグメッセージレベル - シリアルコンソールへのデバッグメッセージ出力のレベルを設定します。
 - 無効
 - エラーのみ
 - 中
 - ネットワーク
 - 詳細

注記:

この設定により、ブート時間が大幅に増加する可能性があります。

- カスタム
 - ポスト冗長ブート処理 - 起動プロセス中にサーバーが応答しなくなった理由を判定するために役立つ可能性がある詳細なメッセージ出力を有効にします。
 - 無効
 - シリアルのみ - 詳細なメッセージをシリアルコンソールに出力します。
 - すべて - 詳細なメッセージをPOST画面とシリアルコンソールに出力します。
3. 設定を保存します。

UEFIシステムユーティリティによるUEFIシリアル出力ログデータの取得

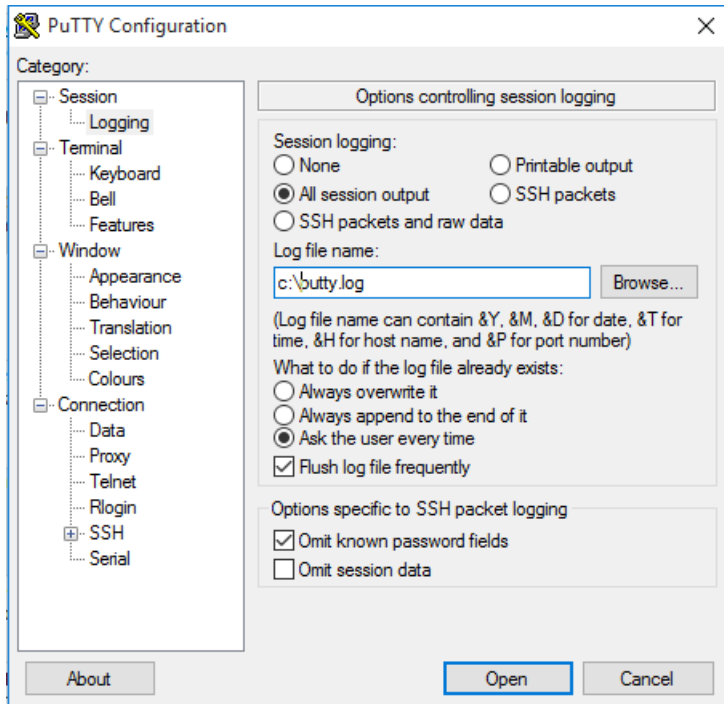
サーバーに物理的にアクセスできない場合、このタスクを使用して、シリアル出力ログデータを取得します。PCIe拡張カードを使用している場合、カードからのデバッグ収集を有効にできます。

手順

1. POST中にF9キーを押してシステムユーティリティを起動します。
2. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > アドバンストオプション > アドバンストデバッグオプションを選択します。
3. デバッグレベルを設定します。
 - a. UEFIシリアルデバッグレベルを選択します。
 - b. 詳細を選択します。
4. 拡張カードを使用している場合、拡張カードからのデバッグデータ収集を有効にします。
 - a. ポスト冗長ブート処理を選択します。
 - b. シリアルのみまたはすべてのいずれかを選択します。

5. 保存して、システムユーティリティを終了します。
6. iLO仮想シリアルポート（VSP）セッションを開始します。
7. PuTTYなどのユーティリティを使用して接続を確立し、ファイルへのログを有効にしてください（All session outputを選択します）。

次の例は、ログデータの収集のためのPuTTY設定の例を示します。



詳しくは
[システムユーティリティの起動](#)

インテルTXTサポートの有効化または無効化

インテルTXTサポートオプションを使用すると、この機能をサポートするインテルプロセッサ搭載のサーバーで、インテルTXT（Trusted Execution Technology）サポートを有効または無効にすることができます。

注記:

インテルTXTはTPM 2.0とTPM 1.2の両方のモードでサポートされます。

前提条件

インテルTXTサポートを有効にするには、次のものを有効にする必要があります。

- すべてのインテルプロセッサコア
- ハイパースレッディング
- VT-d
- TPM

TXTが有効な場合にこれらの機能のいずれかを無効にすると、TXTが正しく動作しなくなる可能性があります。

注記:

物理TPMは常に有効で、検出可能で、デフォルトで動作しています。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > サーバーセキュリティ > インテルセキュリティオプション > インテル(R) TXTサポートを選択します。
2. 設定を選択します。

- 有効 - TXTサポートを有効にします
- 無効 - TXTサポートを無効にします。

3. 変更を保存します。

インテル(R) ソフトウェアガードエクステンションズ (SGX) の有効化または無効化

前提条件

以下の事柄を確認します。


- トータルメモリ暗号化 (TME) を有効にしている。
- システム構成は1チャンネルメモリ構成でない。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > インテルセキュリティオプション > インテル(R) ソフトウェアガードエクステンション (SGX) を選択します。

2. 設定を選択します。

- 有効

 注記: サポートされないシステム構成ではSGXを有効化または構成できません。

- 無効

3. 変更を保存します。

SGXパッケージ情報のインバンドアクセスの有効化または無効化

前提条件

以下の事柄を確認します。


- トータルメモリ暗号化 (TME) を有効にしている。
- システム構成は1チャンネルメモリ構成でない。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > インテルセキュリティオプション > SGXパッケージ情報のインバンドアクセスを選択します。

2. 設定を選択します。

- 有効

 注記: サポートされないシステム構成ではSGXを有効化または構成できません。

- 無効

3. 変更を保存します。

ワンタイムブートメニュー (F11プロンプト) の有効化または無効化

このオプションを使用して、現在のブート時に、F11キーを押してワンタイムブートメニューに直接ブートできるかどうかを制御します。このオプションでは、通常のブート順序の設定は変更されません。このオプションを有効にすると、サーバーの再起動後にPOST画面でF11キーを押すことにより、システムユーティリティのワンタイムブートメニューを直接起動できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > ワンタイムブートメニュー (F11プロンプト) を選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 変更を保存します。

Intelligent Provisioning (F10プロンプト) の有効化または無効化

Intelligent Provisioning (F10プロンプト) オプションを使用して、POST画面からユーザーがF10キーを押してIntelligent Provisioningにアクセスできるようにするかどうかを制御します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > Intelligent Provisioning (F10プロンプト) を選択します。
2. 設定を選択します。
 - 有効
 - 無効
3. 設定を保存します。

プロセッサAES-NIサポートの有効化または無効化

プロセッサAES-NIオプションを使用して、プロセッサ内のAdvanced Encryption Standard Instruction Setを有効または無効にします。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > プロセッサAES-NIサポートを選択します。
2. 設定を選択します。
 - 有効 - AES-NIサポートを有効にします。
 - 無効 - AES-NIサポートを無効にします。
3. 変更を保存します。

バックアップROMイメージ認証の有効化または無効化

起動時にバックアップROMイメージの暗号認証を有効または無効にするには、バックアップROMイメージの認証オプションを使用します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > バックアップROMイメージの認証を選択します。
2. 設定を選択します。

- 有効 - 起動時に、バックアップROMイメージが認証されます。
- 無効 - バックアップROMイメージの起動時の認証は行われません。プライマリイメージのみが認証されます。

3. 変更を保存します。

PCIeデバイス構成オプションの変更

手順

システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > PCIeデバイス構成を選択します。

高度なPCIeデバイス設定の選択

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > PCIeデバイス構成 > アドバンスドPCIe構成を選択します。
2. 設定を選択します。
 - NVMe PCIeリソースパディング - NVMeドライブのPCIeホットアドをサポートするようにPCIeリソースを構成します。
 - 正常 - ブート時にインストールされたデバイスにのみPCIeリソースを割り当てます。PCIeホットアドはサポートされていません。
 - 中 - 追加のPCIeリソースがPCIeルートポートごとに割り振られます。これで、PCIeホットアドイベントはシステムを再起動せずにデバイスを列挙できるようになります。
 - 高 - PCIeリソースの最大量が割り振られ、PCIeホットアドイベントをサポートする最適な機会を活用できます。
 - 最大PCI Express速度 - ワークロードプロファイルがカスタムに設定されている場合、PCI Expressデバイスがサーバーで稼働できる最大速度を設定します。
 - ポートあたりの制御
 - PCIe Generation 1.0
3. 設定を保存します。

PCIe分岐オプションの構成

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > PCIeデバイス構成 > アドバンスドPCIe構成 > PCIe分岐オプションを選択します。
2. 各PCIeスロットの分岐オプションを選択します。
 - 自動
 - 分岐
 - デュアル分岐

注記:

- デュアル分岐は、ProLiant MicroServer Gen10 Plusではサポートされていません。
- デュアル分岐はMicroServer Gen10 Plusでサポートされておらず、またAMD Gen10 Plus製品

3. 設定を保存します。

PCIe MCTPオプションの構成

PCIe MCTPオプションを使用して、指定されたスロットのPCIe管理コンポーネント転送プロトコル (MCTP) を制御します。このオプションは、このプロトコルを適切にサポートしない可能性のある指定されたPCIeエンドポイントに対するMCTPのサポートを無効にするために使用できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > PCIeデバイス構成 > アドバンスドPCIe構成 > PCIe MCTPオプションを選択します。
2. 各PCIeスロットのMCTPブロードキャストサポートを選択します。
 - 有効 (システムの全機能を利用するために推奨)
 - 無効
3. 設定を保存します。

NVMe PCIeリソースパディングの構成

NVMe PCIeリソースパディングオプションを使用して、NVMeドライブのPCIeホットアドをサポートするようにPCIeリソースを構成します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > PCIeデバイス構成 > アドバンスドPCIe構成 > NVMe PCIeリソースパディングを選択します。
2. 設定を選択します。
 - 通常 - このオプションが選択されている場合、PCIeリソースは起動時にインストールされたデバイスにのみ割り振られ、PCIeホットアドはサポートされません。
 - 中 - このオプションが選択されている場合、追加のPCIeリソースがPCIeルートポートごとに割り振られます。これで、PCIeホットアドイベントはシステムを再起動せずにデバイスを列挙できるようになります。
 - 高 - このオプションが選択されている場合、PCIeリソースの最大量が確保され、PCIeホットアドイベントをサポートする最適な機会を活用できます。
3. 設定を保存します。

最大PCI Express速度の設定

最大PCI Express速度オプションを使用すると、PCI Expressデバイスがサーバーで稼働できる最大PCI Express速度を下げるすることができます。また、このオプションを使用して、問題のあるPCI Expressデバイスの問題に対処することもできます。この値を最大サポートに設定すると、プラットフォームまたはPCIeデバイスでサポートされる最大速度 (どちらか低い方) で動作するようにプラットフォームが構成されます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > PCIeデバイス構成 > アドバンスドPCIe構成 > 最大PCI Express速度を選択します。
2. 設定を選択します。
 - ポートあたりの制御

- PCIe Generation 1.0
- PCIe Generation 2.0
- PCIe Generation 3.0
- PCIe Generation 4.0

3. 設定を保存します。

GPU構成の設定

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > PCIeデバイス構成 > GPU CFG設定の順に選択します。
2. オプションを選択します。
 - 4:1-取り付けられている各プロセッサーに4つのPCIeスロットをマップします。
 - 8:1-1つのプロセッサーにすべてのスロットをマップします。
3. 設定を保存します。

PCIeスロットからプロセッサーへのマッピングの構成

PCIeスロットからプロセッサーへのマッピングオプションを使用して、PCIeからプロセッサーへのマッピング構成を変更します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > PCIeデバイス構成オプション > PCIeスロットからプロセッサーへのマッピングを選択します。
2. 設定を選択します。
 - 4:1 - このオプションが選択されている場合、4つのPCIeスロットが、取り付けられている各プロセッサーにマップされます。
 - 8:1 - このオプションが選択されている場合、すべてのスロットが1つのプロセッサーにマップされます。
3. 設定を保存します。

PCIeデバイスの分離サポートの有効化または無効化

PCIeスロットからプロセッサーへのマッピングオプションを使用して、PCIe分離サポートを構成します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > PCIeデバイス構成オプション > PCIeデバイスの分離サポートを選択します。
2. 設定を選択します。
 - 有効 - 有効にした場合、実行時にエラーが検出されると、PCIeデバイスが無効になります。
 - 無効 - 無効にした場合、実行時にエラーが検出されると、PCIeデバイスが有効になります。

このオプションを有効にする前に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。
3. 設定を保存します。

PCIeエラー制御の構成

PCIeスロットからプロセッサへのマッピングオプションを使用して、PCIeエラーをファームウェアで制御するかオペレーティングシステムで制御するかを選択します。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > PCIeデバイス構成オプション > PCIeエラー制御を選択します。
2. 設定を選択します。
 - ファームウェアコントロール
 - OSコントロール
3. 設定を保存します。

特定のPCIeデバイスの構成

PCIeデバイス構成オプションを使用して、内蔵PCIデバイスまたは増設したPCIデバイスの構成設定を、有効化、無効化、および選択します。デバイスを無効にすると、通常そのデバイスに割り当てられているリソース（メモリ、I/O、ROMスペース、電力など）が割り当て直されます。デフォルトでは、すべてのデバイスが有効です。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > PCIeデバイス構成を選択します。
2. リストからデバイスを選択します。
3. 設定を選択します。デバイスに応じて、以下のオプションがあります。
 - PCIeデバイスが無効
 - 自動 - デバイスは、サーバーの起動時に自動的に有効になります。
 - 無効 - デバイスは、自動では有効になりません。
 - PCIeリンク速度
 - 自動 - PCIeリンクのサポートされる最大速度にリンク速度を設定します。
 - PCIe Generation 1.0 - リンク速度をPCIe Generation 1.0の最大速度に設定します。
 - PCIe Generation 2.0 - リンク速度をPCIe Generation 2.0の最大速度に設定します。

注記:

この機能がサポートされていない場合、オプションは使用できません。

- PCIe電力管理 (ASPM)
 - 自動
 - 無効
 - L1有効 - デバイスのリンクは、長い終了レイテンシを犠牲にした低電力スタンバイ状態に入ります。
 - PCIeオプションROM
 - 有効 - プラットフォームはPCIeオプションROMのロードを最適化し、ブート時間を節約します。
 - 無効 - プラットフォームは、古いPCIeデバイスで必要になる可能性があるすべてのPCIeオプションROMの最適化を無効にします。
4. 設定を保存します。

日付と時刻の設定

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > 日付と時刻を選択します。
2. 設定を選択し、項目を入力します。
 - 日付 (mm-dd-yyyy) - 日付を月-日-年 (mm-dd-yyyy) 形式で入力します。
 - 時刻 (hh:mm:ss) - 時刻を24時間形式 (hh:mm:ss) で入力します。
 - 時刻形式 -12時間形式と24時間形式で時刻を入力します。
 - 時間形式
 - 協定世界時 (UTC) - ハードウェアのReal Time Clock (RTC) に格納された時刻を、関連したタイムゾーン設定から計算します。
 - 現地時間 - タイムゾーン設定の使用を解除します。
このオプションは、レガシーBIOSブートモードで設定されたWindowsオペレーティングシステム間で発生する通信問題に対処する場合に役立ちます。
 - タイムゾーン - システムの現在のタイムゾーンを選択します。
 - サマータイム
 - 有効 - 表示された現地時間を夏時間に合わせて1時間だけ調節します。
 - 無効 - 表示された現地時間を夏時間に調節しません。
3. 設定を保存します。

注記:

時間形式オプションは、ProLiant Gen10 Plusサーバーでのみサポートされています。

バックアップおよびリストア設定の変更

バックアップファイルには、シリアル番号と製品ID情報が含まれます。バックアップからリストアする場合、この情報をシステムに適用するかどうかを求められます。バックアップを使用して新しいシステムをセットアップする場合は、シリアル番号と製品IDのリストアを省略できます。

デバイス暗号化設定を変更するには、システム構成 > BIOS/プラットフォーム構成 (RBSU) > サーバーセキュリティ > デバイス暗号化オプション > デバイス暗号化移行オプションにアクセスします。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムデフォルトオプション > バックアップおよびリストア設定を選択します。
2. 次のいずれかを選択します。
 - a. バックアップ
 - b. リストア
3. 手順に従って、バックアップファイルがある場所に移動するか、バックアップファイルを作成する場所に移動します。

注記:

バックアップをリストアする場合、バックアップファイルは .json か .zip ファイルである必要があります。

4. 操作を開始をクリックします。

システムデフォルトのリセット

システムデフォルト設定のリストア

システムデフォルト設定のリストアオプションを使用すると、すべてのBIOS構成設定がデフォルト値にリセットされ、サーバーは自動的に直ちに再起動します。このオプションを選択すると、以下を除くすべてのプラットフォーム設定をリセットします。

- セキュアブートBIOS設定
- 日付と時刻の設定
- プライマリおよび冗長のROMの選択（サポートされる場合）

システムの復元時にカスタムのデフォルト構成を保存するには、ユーザーデフォルトオプションを使用します。そうすることにより、保存していないと失うおそれのある設定を保存できます。

- オプションカードやiLOなどの他のエンティティは、個別にリセットする必要があります。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > システムデフォルトオプション > システムデフォルト設定のリストアを選択します。
2. はい、デフォルト設定をリストアしますを選択します。
3. サーバーを再起動します。

工場デフォルト設定のリストア

工場デフォルト設定のリストアオプションを使用すると、すべてのBIOS構成設定を工場デフォルト値にリセットして、ブート構成、セキュアブートのセキュリティキー（セキュアブートが有効になっている場合）など、不揮発性のすべてのUEFI変数を削除できます。それまでの変更内容が失われる可能性があります。

この動作と、システムデフォルト設定のリストアオプションの違いは、工場デフォルト設定のリストアではUEFI変数がすべて消去されることです。OSは、ブート順序のエントリやセキュアブート用キーデータベース情報などを保存するUEFI変数を書き込むことができます。工場デフォルト設定のリストアを行うときは、この情報はクリアされるのに対し、システムデフォルト設定のリストアでは保持されます。

システムの復元時にカスタムのデフォルト構成を保存するには、ユーザーデフォルトオプションを使用します。そうすることにより、保存していないと失うおそれのある設定を保存できます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成（RBSU） > システムデフォルトオプション > 工場デフォルト設定のリストアを選択します。
2. はい、デフォルト設定をリストアしますを選択します。
3. サーバーを再起動します。

デフォルトのUEFIデバイス優先順位の変更

デフォルトのUEFIデバイス優先順位オプションを使用して、デフォルトのシステム設定が復元されるときに使用されるUEFIデバイスの優先順位を変更します。このオプションで定義された優先順位に基づいて、初期のUEFIブート順序リストが作成されます。デフォルトの構成設定がロードされる時、工場出荷時のデフォルト設定ではなく、保存された

デフォルトのUEFIデバイス優先順位が使用されます。

前提条件

ユーザーデフォルトオプションは、構成され、保存されています。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムデフォルトオプション > デフォルトのUEFIデバイス優先順位を選択します。
2. エントリーを選択します。
3. リスト内のエントリーを上に移動するには、+キーを使用します。リスト内のエントリーを下に移動するには、-キーを使用します。リスト内の移動には、ポインティングデバイスまたは矢印キーを使用します。
4. 設定を保存します。

ユーザーデフォルトオプションの保存または消去

ユーザーデフォルトオプションを使用すると、構成を、カスタムデフォルト構成として保存または消去できます。必要に応じてシステムを構成した後、このオプションを有効にして、構成をデフォルト構成として保存します。システムがデフォルト設定をロードするとき、工場デフォルト設定の代わりにカスタムデフォルト設定が使用されます。

手順

1. システムユーティリティ画面で、システム構成 > BIOS/プラットフォーム構成 (RBSU) > システムデフォルトオプション > ユーザーデフォルトオプションを選択します。
2. オプションを選択します。
 - ユーザーデフォルトの保存
 - はい、保存します。 - 現在の設定をシステムのデフォルト設定として保存します。
 - いいえ、キャンセルします。 - 現在の設定はシステムのデフォルト設定として保存されません。
 - ユーザーデフォルトの消去
 - はい、現在の設定を消去します。 - 現在のユーザー定義のデフォルト設定を消去 (削除) します。消去した設定は、手動でのみ復元できます。
 - いいえ、キャンセルします。 - 現在のユーザー定義のデフォルト設定を消去しません。
3. 設定を保存します。

スクリプトによる構成手順の使用

スクリプトによる構成手順

BIOS/プラットフォーム構成 (RBSU) をRESTful APIツールとともに使用して、標準的なサーバー構成スクリプトを作成することにより、サーバーの設定プロセスでの手動による手順の多くを自動化できます。

UEFI用のiLO RESTful APIサポート

ProLiantサーバーおよびHPE Synergyコンピュートモジュールには、RESTful APIを使用してUEFI BIOS設定を構成するためのサポートが含まれています。RESTful APIツールは、サーバー管理ツールから使用することでサーバーの構成、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。RESTクライアントは、HTTPS操作を使用して、iLO

5、UEFI BIOS設定など、サポートされているサーバー設定を構成します。RESTful APIおよびRESTfulインターフェイスツールについては、Hewlett Packard EnterpriseのWebサイト (<https://www.hpe.com/info/restfulinterface/docs>) を参照してください。

Configuration Replicationユーティリティ (CONREP)

CONREPは、STKに含まれます。このユーティリティは、BIOS/プラットフォーム構成 (RBSU) と連携して、ハードウェア構成を複製します。このユーティリティは、スクリプトによるサーバーの展開の際に、「State 0, Run Hardware Configuration Utility」で実行されます。CONREPユーティリティは、システム環境変数を読み出して構成を判定し、その結果を、編集可能なスクリプトファイルに書き出します。このファイルは、同様のハードウェアおよびソフトウェアコンポーネントを持つ複数のサーバーに展開できます。STKは、Hewlett Packard EnterpriseのWebサイト (<https://www.hpe.com/info/stk/docs>) にあります。詳しくは、Hewlett Packard EnterpriseのWebサイト <https://www.hpe.com/info/stk/docs>にある、ご使用のオペレーティングシステム環境用のScripting Toolkitユーザーガイドを参照してください。

HPE Smart Storage Administrator (HPE SSA)

HPE SSAスクリプティングは、HPE SSA CLIアプリケーションとともに配布されるスタンドアロンアプリケーションで、Smartアレイデバイス上にアレイを構成するために使用されます。

- Scripting Toolkit for Windowsユーザーガイド
https://www.hpe.com/support/STK_Windows_UG_en
- HPE SSAガイド
<https://www.hpe.com/info/smartstorage/docs>

トラブルシューティング

デバイスをブートできない

症状

起動するオプションまたはデバイスが見つからない、または不明なデバイスとしてシステム構成内にリストされている、というメッセージが表示されます。

解決方法 1

原因

UEFIオプションROMドライバーがないオプションを起動しようとしています。

アクション

1. ブート機能にx64またはEFIバイトコードのいずれかをサポートしているUEFIオプションドライバー (オプションROM) がご使用のオプションカードにあることを確認してください。

注記:

- UEFIドライバーは、システムユーティリティ画面にメッセージを表示したり、ファンクションキーのプロンプトを表示したりしません。
- マザーボードを交換すると、UEFI変数は失われます。
- ブートイメージでPXEサーバーを構成する必要があります。また、x64 EFIマシンの場合、x64 EFI DHCPのブート要求をサポートするようにDHCPサーバーを構成する必要があります。詳しくは、UEFI Information Library (<https://www.hpe.com/info/ProLiantUEFI/docs>) を参照してく

ださい。

2. ブート手順を再度試みます。

解決方法 2

原因

サポートされていないオプションまたは最新のファームウェアを実行していないオプションで起動しようとしています。

アクション

1. ご使用のサーバーのQuick SpecsまたはRead This Firstカードを参照して、ご使用のカードがサポートされていることを取り付ける前に確認します。他社製のオプションカードも動作する可能性がありますが、これらは、UEFIシステムユーティリティを実行しているサーバー用に最適化されていません。
2. オプションのシステムヘルス設定に正しい情報が一覧表示されることを確認します。
3. 必要に応じて、最新のSPPをオフラインモードで使用して、ファームウェアを最新バージョンにアップグレードします。

解決方法 3

原因

デフォルトブートモード設定がユーザー定義の設定と異なります。

アクション

1. ユーザーデフォルトオプションは、カスタムのデフォルト構成を保存して、システムの復元時に使用します。
2. ブート手順を再度試みます。

システムデフォルトを復元できない

症状

- Windowsで、あるサーバーから別のサーバーにドライブを移動した後、特定の設定が検出できないというエラーメッセージが表示されます。
- マザーボードを交換した後、セキュアブートなどの構成設定が失われます。

原因

ドライブを移動したり、システムのハードウェアを交換したりすると、以前に構成した設定へのポインターが破壊される可能性があります。

アクション

1. システムデフォルト設定のリストアオプションまたは工場デフォルト設定のリストアを使用して、設定を復元します。
2. この手順を再度試みます。

ネットワークブートURLのファイルをダウンロードできない

症状

ネットワークブート用として指定したURLのファイルをダウンロードしようすると、エラーメッセージが表示されます。

解決方法 1

原因

静的構成時に指定したネットワークURLが正しくありません。

アクション

1. 内蔵UEFIシェルのpingコマンドを使用してネットワーク接続をチェックします。UEFIシェルのユーザーガイドの「Ping」を参照してください。
2. 静的なネットワーク接続設定を変更し、URLにあるファイルをもう一度ダウンロードします。

解決方法 2

原因

DHCPサーバーが応答していません。

アクション

1. DHCPサーバーが使用可能で、動作していることを確認します。
2. URLのファイルをもう一度ダウンロードします。

解決方法 3

原因

選択したNICポートにケーブルが接続されていません。

アクション

1. ケーブルが接続されていることを確認します。
2. URLをもう一度ダウンロードします。

解決方法 4

原因

ファイルが正しくないかサーバーに存在しない、または必要な権限がないためダウンロードできません。ファイル名をチェックし、サーバーに存在していることを確認します。そのサーバーに対する管理者権限があることを確認します。

アクション

1. ファイルが存在し、正しいファイル名を使用していること、そのファイルをダウンロードする十分な権限を持っていることを確認します。
2. URLのファイルをもう一度ダウンロードします。

解決方法 5

原因

HTTPまたはFTPサーバーが停止、または応答しませんでした。

アクション

1. 指定したHTTPまたはFTPサーバーが利用可能で動作可能であるか確認します。
2. URLのファイルをもう一度ダウンロードします。

ダウンロードしたイメージファイルを使用してネットワークブートを行うことができない

症状

URLに指定されているイメージからの起動に失敗します。

解決方法 1

原因

イメージが署名されておらず、セキュアブートが有効になっています。

アクション

1. イメージが署名されており、そのセキュアブート設定が正しいことを確認します。
2. URLのファイルをもう一度ダウンロードします。

解決方法 2

原因

ダウンロードしたファイルが破損しています。

アクション

1. 新規ファイルを選択します。
2. URL構成を繰り返して新しいファイルを指定します。
3. URLにある新規ファイルのダウンロードを再度試行します。

UEFIシェルスクリプトから展開できない

症状

UEFIシェルスクリプトを使用してOSを展開しようとする、展開が失敗したことを示すエラーメッセージが表示されます。

原因

構成設定が正しくありません。

アクション

1. 以下を確認します。
 - a. 内蔵UEFIシェルインターフェイスがUEFIブート順序リストまたはワнтаイムブートメニューに追加されている。
 - b. UEFIブート順序リストに追加されると、内蔵UEFIシェルインターフェイスがUEFIブート順序リスト内の最初のブートオプションになり、ロードする他のブートオプションよりも優先される。
 - c. UEFIシェルスクリプト自動起動が有効になっている。
 - d. 接続されているメディアの `startup.nsh` スクリプトファイルの場所またはネットワーク上の場所が正しく指定されている。接続メディア内の場合は、`startup.nsh` スクリプトは `fsX:\` または `fsX:\efi\boot\` ディレクトリ内になければなりません。
 - e. `.nsh` スクリプトに、サポートされているコマンドのみが含まれている。
 - f. 使用しているシステムに、自動スクリプトの実行中にRAMディスクを作成するための十分なRAMメモリがある。
 - g. `.nsh script` を使用して起動されたOSブートローダーや診断アプリケーションのUEFI環境での実行がサポートされている。
 - h. シェルスクリプトの検証が有効になっている場合、スクリプトがセキュアブートデータベースに登録され、スクリプトが `#!NSH` 行で始まることを確認する。
2. 展開をやり直します。

1つ以上のデバイスのオプションROMを実行できない

症状

1つ以上のデバイスのオプションROMを実行できません。

原因

利用可能なオプションROMの総容量を超えました。

アクション

1. 不要なオプションROMがあれば（PXEなど）無効にします。
2. この手順を再度試みます。

ブート順序リストに新しいネットワークまたはストレージデバイスが見つからない

症状

ネットワークまたはストレージデバイスを接続しましたが、ブート順序リストに表示されません。

原因

新しく追加されたデバイスは、システムを再起動するまで、ブート順序リストには表示されません。

アクション

1. システムを再起動します。
2. ご使用のデバイスがブート順序リストに表示されることを確認します。

インテルTXTが正常に動作していない

原因

いずれかの前提条件が有効になっていない可能性があります。

アクション

前提条件が有効になっていることを確認します。

- すべてのインテルプロセッサコア
- ハイパースレッディング
- VT-d
- TPM

無効なサーバーシリアル番号と製品ID

症状

サーバーのシリアル番号と製品IDが無効化、破損、または喪失したことを示すエラーメッセージが表示されます。

原因

シリアル番号、製品ID、またはその両方が有効でない、壊れている、あるいは失われました。

アクション

1. これらのフィールドに正しい値を入力します。
2. エラーメッセージが再び表示されないことを確認します。

無効な日付/時刻

症状

日付と時刻が設定されていないことを示すメッセージが表示されます。

原因

構成メモリの時間または日付が無効です。

アクション

1. 日付と時刻オプションを使用して、設定を変更します。
2. メッセージが再び表示されないことを確認します。

ネットワークデバイスが正しく機能しない

原因

サポートされるサーバーオプションのリストにあるネットワークデバイスのみを使用する必要があります。

アクション

ネットワークデバイスをサーバーで使用する前に、ファームウェアを最新バージョンにアップデートすることをお勧めします。オペレーティングシステムをインストールする前に、最新のService Pack for ProLiantをオフラインモードで使用して、ファームウェアを最新バージョンにアップグレードしてください。

注記:

デフォルトのブートモード設定とユーザーが構成した設定が異なる場合は、デフォルト設定に復元すると、システムがOSインストールを起動しなくなる可能性があります。この問題を回避するには、UEFIシステムユーティリティのユーザーデフォルトオプション機能を使用して、工場出荷時のデフォルト設定をオーバーライドしてください。

システムが応答しなくなる

原因

PCIe拡張カードが誤って構成されているか誤動作を起こしています。

アクション

問題のカードを識別するためにPCIeデバッグ情報の収集を有効にします。

単一デバイスで障害が発生した

症状

POST中に起動が失敗しました。

アクション

サーバーが起動しない場合は、[HPE ProLiant Gen10およびGen10 Plusサーバートラブルシューティングガイド](#)に記載の「POST実行時の問題-起動時にビデオが表示されない場合のフローチャート」を参照してください。

サーバーが起動しない

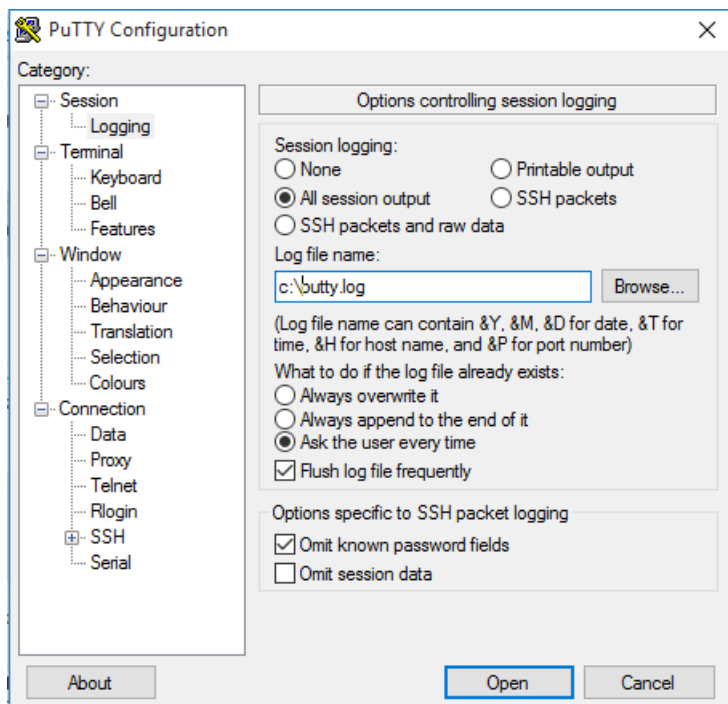
原因

メンテナンススイッチでシリアルデバッグを有効にします。

アクション

1. サーバーの電源を切断します。
2. サーバーメンテナンススイッチ（12ポジションスイッチ）を探して、DIP 4をオンの位置に設定します。スイッチの位置についてはシャーシのフードラベルを参照してください。
3. NULLモードケーブルをサーバーのシリアルポートに接続するか、iLO仮想シリアルポート（VSP）セッションを開きます。
4. PuTTYなどのユーティリティを使用して接続を確立し、ファイルへのログを有効にしてください（**All session output**を選択します）。

次の例は、ログデータの収集のためのPuTTY設定の例を示します。



Smartアレイコントローラーが正しく機能しない

原因

他のSmartアレイコントローラーはサポートされておらず、正しく機能しません。

サポートされるオプションについて詳しくは、Hewlett Packard EnterpriseのWebサイトにあるサーバーのQuickSpecs (<https://www.hpe.com/info/qs>) を参照してください。

ファームウェアとドライバーの最新バージョンについて詳しくは、Hewlett Packard EnterpriseのWebサイト (<https://www.hpe.com/support/hpesc>) を参照してください。

アクション

Smartアレイコントローラーをサーバーで使用する前に、ファームウェアを最新バージョンにアップデートすることをお勧めします。オペレーティングシステムをインストールする前に、最新のService Pack for ProLiantをオフラインモードで使用して、ファームウェアを最新バージョンにアップグレードしてください。

VMwareはUEFIモードで起動しない

原因

UEFI最適化ブートは有効ではありません。

アクション

UEFI最適化ブートを有効にします。

Webサイト

全般的なWebサイト

Single Point of Connectivity Knowledge (SPOCK) ストレージ互換性マトリックス

<http://www.hpe.com/storage/spock>

ストレージのホワイトペーパーおよび分析レポート

<http://www.hpe.com/storage/whitepapers>

UEFIの仕様

<http://www.uefi.org/specifications>

UEFIの学習資料

http://www.uefi.org/learning_center

RESTful APIツール

<https://www.hpe.com/info/redfish>

Hewlett Packard Enterprise Worldwideの連絡先

<https://www.hpe.com/assistance>

サブスクリプションサービス/サポートのアラート

<https://www.hpe.com/support/e-updates-ja>

Software Depot

<https://www.hpe.com/support/softwaredepot>

Customer Self Repair

<https://www.hpe.com/support/selfrepair>

Insight Remote Support

<https://www.hpe.com/info/insightremotesupport/docs>

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。

サポートと他のリソース

Hewlett Packard Enterpriseサポートへのアクセス

- ライブアシスタンスについては、Contact Hewlett Packard Enterprise WorldwideのWebサイトにアクセスします。

<https://www.hpe.com/info/assistance>

- ドキュメントとサポートサービスにアクセスするには、Hewlett Packard EnterpriseサポートセンターのWebサイトにアクセスします。

<https://www.hpe.com/support/hpesc>

ご用意いただく情報

- テクニカルサポートの登録番号（該当する場合）
- 製品名、モデルまたはバージョン、シリアル番号
- オペレーティングシステム名およびバージョン
- ファームウェアバージョン
- エラーメッセージ
- 製品固有のレポートおよびログ
- アドオン製品またはコンポーネント
- 他社製品またはコンポーネント

アップデートへのアクセス

- 一部のソフトウェア製品では、その製品のインターフェイスを介してソフトウェアアップデートにアクセスするためのメカニズムが提供されます。ご使用の製品のドキュメントで、ソフトウェアの推奨されるソフトウェアアップデート方法を確認してください。
- 製品のアップデートをダウンロードするには、以下のいずれかにアクセスします。

Hewlett Packard Enterpriseサポートセンター

<https://www.hpe.com/support/hpesc>

Hewlett Packard Enterpriseサポートセンター：ソフトウェアのダウンロード

<https://www.hpe.com/support/downloads>

マイHPEソフトウェアセンター

<https://www.hpe.com/software/hpesoftwarecenter>

- eNewslettersおよびアラートをサブスクライブするには、以下にアクセスします。

<https://www.hpe.com/support/e-updates-ja>

- お客様の資格を表示、アップデート、または契約や保証をお客様のプロファイルにリンクするには、Hewlett Packard EnterpriseサポートセンターのMore Information on Access to Support Materialsページに移動します。

<https://www.hpe.com/support/AccessToSupportMaterials>

① 重要:

一部のアップデートにアクセスするには、Hewlett Packard Enterpriseサポートセンターからアクセスするときに製品資格が必要になる場合があります。関連する資格を使ってHPEパスポートをセットアップしておく必要があります。

リモートサポート（HPE通報サービス）

リモートサポートは、お客様の保証またはサポート契約の一部として、サポートされているデバイスで使用できます。これは優れたイベント診断、Hewlett Packard Enterpriseへのハードウェアイベント通知の自動かつ安全な送信を提供します。また、お使いの製品のサービスレベルで高速かつ正確な解決方法を開始します。Hewlett Packard Enterpriseでは、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勧めします。

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。

HPE通報サービス

<http://www.hpe.com/jp/hpaalert>

HPE Pointnext Tech Care

<https://www.hpe.com/jp/ja/services/tech-care.html>

HPEデータセンターケア

<https://www.hpe.com/jp/ja/services/datacenter-hybrid-services.html>

保証情報

ご使用の製品の保証情報を確認するには、以下のリンクを参照してください。

HPE ProLiantとIA-32サーバーおよびオプション

<https://www.hpe.com/support/ProLiantServers-Warranties>

HPE EnterpriseおよびCloudlineサーバー

<https://www.hpe.com/support/EnterpriseServers-Warranties>

HPEストレージ製品

<https://www.hpe.com/support/Storage-Warranties>

HPEネットワーク製品

<https://www.hpe.com/support/Networking-Warranties>

規定に関する情報

安全、環境、および規定に関する情報については、Hewlett Packard Enterpriseサポートセンターからサーバー、ストレージ、電源、ネットワーク、およびラック製品の安全と準拠に関する情報を参照してください。

<https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts>

規定に関する追加情報

Hewlett Packard Enterpriseは、REACH（欧州議会と欧州理事会の規則EC No 1907/2006）のような法的な要求事項に準拠する必要に応じて、弊社製品の含有化学物質に関する情報をお客様に提供することに全力で取り組んでいます。この製品の含有化学物質情報レポートは、次を参照してください。

<https://www.hpe.com/info/reach>

RoHS、REACHを含むHewlett Packard Enterprise製品の環境と安全に関する情報と準拠のデータについては、次を参照してください。

<https://www.hpe.com/info/ecodata>

社内プログラム、製品のリサイクル、エネルギー効率などのHewlett Packard Enterpriseの環境に関する情報については、次を参照してください。

<https://www.hpe.com/info/environment>

ドキュメントに関するご意見、ご指摘

Hewlett Packard Enterpriseでは、お客様により良いドキュメントを提供するように努めています。ドキュメントの改善に役立てるために、Hewlett Packard Enterpriseサポートセンターポータル

(<https://www.hpe.com/support/hpesc>)にあるフィードバックボタンとアイコン（開いているドキュメントの下部にあります）から、エラー、提案、またはコメントを送信いただけます。すべてのドキュメント情報は、プロセスによ

てキャプチャーされます。

