



Hewlett Packard
Enterprise

HPE向けインテルOptane Persistent Memory 200シリーズユーザーガイド

部品番号: 30-B41F6FB9-003-ja-JP
発行: 2022年5月
版数: 3

HPE向けインテルOptane Persistent Memory 200シリーズユーザーガイド

摘要

このガイドでは、HPE向けインテルOptane Persistent Memory 200シリーズの取り付け、メンテナンス、および構成に関する情報について説明します。このガイドは、HPE ProLiant Gen10 PlusおよびHPE Synergyシステムの取り付け、管理、トラブルシューティングを行う担当者を対象としています。コンピューター機器の保守の資格があり、高電圧製品の危険性について理解していることを前提としています。

部品番号: 30-B41F6FB9-003-ja-JP

発行: 2022年5月

版数: 3

© Copyright 2022 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

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

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

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

SUSE[®]は、SUSE LLCの米国およびその他の国における登録商標です。

Windows Server[®]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。

VMware vSphere[®]は、VMware, Inc.の米国および各国での登録商標です。

目次

1 はじめに

1.1 HPE向けインテルOptane Persistent Memory 200シリーズ

1.1.1 不揮発性メモリモード

1.1.2 メモリキャッシュ比率

2 セキュリティ機能

2.1 パスワード

2.2 暗号化

2.3 サニタイズ

2.4 署名されたファームウェア

2.5 ファームウェアロールバック保護

3 コンポーネントの識別

3.1 HPE向けインテルOptane Persistent Memory 200シリーズのラベルの識別

4 取り付け

4.1 システム要件

4.2 メモリ取り付け情報

4.3 Persistent Memoryモジュールの取り扱いのガイドライン

4.4 DIMMまたは不揮発性モジュールの取り付け

5 システムの構成

5.1 構成の概要

5.1.1 構成ツール

5.2 目標構成の設定

5.2.1 UEFIシステムユーティリティを使用した目標構成の設定

5.2.2 ipmctlを使用した目標構成の設定

5.2.3 HPE iLO RESTful APIを使用した目標構成の設定

5.3 ネームスペースの作成

5.3.1 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

5.3.2 ipmctlを使用したネームスペースの作成

5.3.3 ndctlを使用したネームスペースの作成 (Linux)

5.4 キー管理の有効化

5.4.1 ローカルキー管理を使用したpersistent memory modulesの暗号化

5.4.2 リモートキー管理を使用したpersistent memory modulesの暗号化

5.4.2.1 キー管理サーバーの使用

5.4.2.1.1 サポートされているキーマネージャー

5.4.2.1.2 キーマネージャーサーバーの構成

5.4.2.1.2.1 キーマネージャーサーバーのオプション

5.4.2.1.3 キーマネージャー構成の詳細の追加

5.4.2.1.3.1 キーマネージャー構成の詳細

5.4.2.1.4 キーマネージャー構成のテスト

5.4.2.1.5 キーマネージャーイベントの表示

5.4.2.1.6 キーマネージャーログのクリア

5.5 他のBIOS/プラットフォーム構成 (RBSU) オプション

6 管理ツール

6.1 HPE向けインテルOptane Persistent Memoryの管理

6.2 UEFIシステムユーティリティ

6.2.1 UEFIシステムユーティリティを使用した目標構成の変更

6.2.2 UEFIシステムユーティリティを使用した目標構成の削除

6.2.3 persistent memory modulesパスワードの変更

- 6.2.4 persistent memory modulesステータスの表示
- 6.2.5 キー管理モードの変更
- 6.2.6 キー管理の無効化
- 6.2.7 persistent memory modulesの暗号化の無効化
- 6.2.8 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
- 6.3 HPE iLO RESTful API
 - 6.3.1 HPE iLO RESTful APIの概要
 - 6.3.1.1 データモデルの概要
 - 6.3.1.1.1 例：メモリリソースの取得
 - 6.3.2 HPE iLO RESTful APIを使用したHPE向けインテルOptane Persistent Memoryの管理
 - 6.3.3 HPE iLO RESTful APIを使用したPersistent Memoryモジュールのプロビジョニング
 - 6.3.4 例：persistent memory modulesのプロビジョニング
 - 6.3.4.1 RESTfulインターフェイスツールrawpostを使用した100% AppDirectインターリーブの構成
 - 6.3.4.2 pythonを使用した100% AppDirectインターリーブの構成
 - 6.3.4.3 Postmanを使用した100% AppDirectインターリーブの構成
 - 6.3.5 例：curlを使用したHPE向けインテルOptane Persistent Memoryの管理
- 6.4 RESTfulインターフェイスツール
 - 6.4.1 RESTfulインターフェイスツールの起動
 - 6.4.2 検出コマンド
 - 6.4.2.1 デバイスの検出
 - 6.4.2.2 デバイス構成の検出
 - 6.4.2.3 不揮発性インターリーブ領域の検出
 - 6.4.2.4 不揮発性メモリのサマリー
 - 6.4.3 構成コマンド
 - 6.4.3.1 保留中の構成を表示する
 - 6.4.3.2 事前定義された構成を適用する
 - 6.4.3.3 ユーザー定義構成を適用する
 - 6.4.3.4 保留中の構成をクリアする
 - 6.4.3.5 推奨構成を表示する
- 6.5 ipmctlツール
 - 6.5.1 ipmctlのインストール (Linux)
 - 6.5.2 ipmctlを使用したpersistent memory modules構成の表示
 - 6.5.3 ipmctlを使用した目標構成の削除
 - 6.5.4 ipmctlを使用したネームスペースの削除
 - 6.5.5 ipmctlによるメモリモードの判断

7 メンテナンス

- 7.1 Persistent Memoryモジュールの再配置のガイドライン
- 7.2 persistent memory modulesデータの手動でのバックアップ
- 7.3 DIMMまたはpersistent memory modulesの取り外し
- 7.4 システムボードの交換
- 7.5 persistent memory modulesの移行
 - 7.5.1 ローカルキー管理で暗号化されたpersistent memory modulesの移行
 - 7.5.2 リモートキー管理で暗号化されたpersistent memory modulesの移行
- 7.6 persistent memory modulesのサニタイズ
 - 7.6.1 サニタイズポリシー
 - 7.6.2 サニタイズガイドライン
 - 7.6.3 UEFIシステムユーティリティを使用したサニタイズ
 - 7.6.4 HPE iLO RESTful APIを使用したサニタイズ
 - 7.6.5 ipmctlを使用したサニタイズ

- 7.7 パスワードを紛失したpersistent memory modulesの撤去
- 7.8 persistent memory modulesファームウェアのアップデート
- 8 HPE向けインテルOptane Persistent Memory 200シリーズのLinuxのサポート
 - 8.1 nmemデバイス
 - 8.1.1 nmemデバイスのプロパティ
 - 8.1.2 nmemデバイスの一覧表示
 - 8.2 領域
 - 8.2.1 領域のプロパティ
 - 8.2.2 領域の一覧表示
 - 8.3 ネームスペース
 - 8.3.1 ネームスペースのプロパティ
 - 8.3.2 ネームスペースの作成
 - 8.3.3 すべてのネームスペースを一覧表示する
 - 8.3.4 ネームスペースモードの変更
 - 8.3.5 ネームスペースの削除
 - 8.4 pmemデバイスの初期化
 - 8.5 システムのメモリ容量の表示
 - 8.6 ファイルシステム
 - 8.7 I/Oの統計情報
- 9 HPE向けインテルOptane Persistent Memory 200シリーズのVMwareのサポート
- 10 HPE向けインテルOptane Persistent Memory 200シリーズのWindows Serverのサポート
- 11 トラブルシューティング
 - 11.1 既知の問題
 - 11.1.1 不揮発性メモリファイルシステムが原因でシステムブートが失敗する
 - 11.2 トラブルシューティングの資料
- 12 Webサイト
- 13 サポートと他のリソース
 - 13.1 Hewlett Packard Enterpriseサポートへのアクセス
 - 13.2 アップデートへのアクセス
 - 13.3 リモートサポート (HPE通報サービス)
 - 13.4 カスタマーセルフリペア (CSR)
 - 13.5 保証情報
 - 13.6 規定に関する情報
 - 13.7 ドキュメントに関するご意見、ご指摘

HPE向けインテルOptane Persistent Memory 200シリーズ

HPE向けインテルOptane Persistent Memory 200シリーズは、メモリを高密度メモリ（メモリモード）または高速ストレージ（App Directモード）として展開する柔軟性を提供し、最大6 TB（4 TB物理メモリ + 2 TB DIMM）のソケット単位のメモリ容量を可能にします。Persistent Memoryモジュールと従来の揮発性DRAM DIMMsの併用により、高速で大容量の、費用対効果の高いメモリとストレージを提供し、データの迅速な保存、移動、処理を可能にすることで、ビッグデータのワークロードと分析を実現します。

Persistent Memoryモジュールは、標準のDIMMフォームファクターを使用し、サーバーメモリスロット内で DIMMsの横に取り付けられます。HPE向けインテルOptane Persistent Memory 200シリーズは、第3世代インテルXeonスケーラブルプロセッサでのみ使用するように設計されており、次の容量が用意されています。

- 128 GB
- 256 GB
- 512 GB

不揮発性メモリモード

HPE向けインテルOptane Persistent Memory 200シリーズは、2つのモードで動作するように構成できます。

App Directモード

App Directモードに設定されている場合、persistent memory modulesは不揮発性メモリとして機能します。

メモリモード

メモリモードに設定されている場合、persistent memory modulesは揮発性システムメモリとして機能する一方で、DRAM容量はキャッシュとして動作します。詳細は、「メモリのキャッシュ比率」を参照してください。

メモリキャッシュ比率

Persistent Memoryモジュールは、揮発性領域と不揮発性領域に振り分けることができます。

揮発性領域の場合、DRAM容量に対する揮発性メモリ容量の比率がパフォーマンスに影響を及ぼします。DRAM容量に対して推奨される揮発性メモリ容量は4:1~16:1です。

- 4:1 - 最大キャッシュ。キャッシュヒットする可能性が最も高くなります。
- 8:1
- 16:1 - 最小キャッシュ。キャッシュヒットする可能性は最も低くなります。

パフォーマンスへの影響がより深刻なため、比率が1:1以下の場合は、メモリモードを構成しないことを強くお勧めします。

推奨されていないキャッシュ比率を使用した場合、メッセージがインテグレートドマネジメントログ (IML) に記録されます。

次の表は構成例を示したものです。persistent memory modulesの容量の100%が揮発性メモリに割り当てられています。メモリの一部が不揮発性メモリに振り分けられると、キャッシュ比率が向上します。

Persistent Memoryモジュールの容量 ¹	Persistent Memoryモジュール構成	DIMM容量 ¹	DIMMの構成	比率
1024 GB	8 x 128 GB	128 GiB	8 x 16 GiB	8:1
		256GiB	8 x 32 GiB	4:1
		512GiB	8 x 64 GiB	2:1 ²
		1024GiB	8 x 128 GiB	1:1 ²
2.0TB	8 x 256 GB	128 GiB	8 x 16 GiB	16:1
		256GiB	8 x 32 GiB	8:1
		512GiB	8 x 64 GiB	4:1
		1024GiB	8 x 128 GiB	2:1 ²
		2048GiB	8 x 256 GiB	1:1 ²
4.0 TB	8 x 512 GB	128 GiB	8 x 16 GiB	32:1 ³
		256GiB	8 x 32 GiB	16:1
		512GiB	8 x 64 GiB	8:1
		1024GiB	8 x 128 GiB	4:1
		2048GiB	8 x 256 GiB	2:1 ²

¹ 1プロセッサあたりの容量。

² 非推奨。キャッシュによるメリットはありません。

³ 非推奨。

セキュリティ機能

HPE向けインテルOptane Persistent Memoryには、データを安全に保護するための機能が多数用意されています。

- パスワード
- 暗号化
- サニタイズ
- 署名されたファームウェア
- ファームウェアロールバック保護

パスワード

Persistent Memoryモジュールでは、32バイトのバイナリパスワードを使用したパスワードベースのロックをサポートします。ロックされている場合は、ロックが解除されるまで、persistent memory modules上のデータにはアクセスできません。persistent memory modulesがロックされた状態で、パスワードが失われた場合、persistent memory modulesをサンタイズしてハードウェアへの領域アクセス権を取り戻すことはできますが、データにアクセスすることはできません。

HPE ProLiantおよびHPE Synergy Gen10 Plusサーバー製品は、persistent memory modulesパスワードを管理するための2つの方法を提供します。

- ローカルキー管理
- リモートキー管理

パスワードを管理するために一度に選択できるキー管理方法は、1つだけです。

ローカルキー管理

ローカルキー管理は、HPE Trusted Platform Module (TPM) 2.0がインストールされているサーバーで利用できます。有効にされると、サーバーは各persistent memory modulesのパスワードとして使用する32バイトの乱数を生成します。

Persistent Memoryモジュールのパスワードは、HPE iLOおよびシステムファームウェアによって共有されるフラッシュメモリに保存されます。パスワードデータベース内の各パスワードは、HPE TPM 2.0の改ざん防止機能を使用して暗号化されています。

POST中に、サーバーはデータベースからパスワードを抽出し、すべてのpersistent memory modulesのロックを解除します。パスワードをUSBキーにエクスポートして、別のサーバーに移行させることができます。この移行ファイルは、ユーザーが提供する必要がある一時パスワード (ASCII文字列) から生成されたキーで暗号化されます。このファイルを別のサーバーにインポートするには、ユーザーは同じ一時パスワードを入力する必要があります。

また、このファイルは、サーバーのシステムボードが故障した場合にパスワードを復元するためのバックアップとしても機能します。

リモートキー管理

リモートキー管理は、HPE iLOがキー管理サーバーに登録され、接続されているサーバーで利用できます。Persistent Memoryモジュールのパスワードは自動的に生成、管理され、キー管理サーバーに保存されます。リモートキー管理機能には、HPE iLO Advancedのライセンスが必要です。

暗号化

Persistent Memoryモジュールは、メディアに書き込まれたすべてのデータを256ビットのXTS-AESアルゴリズムを使用して、暗号化します。

揮発性メモリ領域の場合、persistent memory modulesは電源投入時に新しい暗号化キーを生成し、そのキーを揮発性レジスタに保持します。揮発性レジスタは電源が失われると、失われます。メディアは当然不揮発性ですが、揮発性メモリ領域を効果的に揮発性にします。

不揮発性メモリ領域の場合、persistent memory modulesは電源を入れ直しても暗号化キーを記憶し続けるので、データは引き続きアクセス可能です。

- persistent memory modulesのパスワードが有効になっている場合、暗号化キー自体が、パスワードから派生した別のキーによって暗号化されます。この「キーラッピング」により、未認可ユーザーがメディアコンテンツを読み取ることが防止されます。

暗号化キーを利用できるのは、適切なパスワードがpersistent memory modulesに提示され、かつpersistent memory modulesが暗号化キーを揮発性レジスタに保持している場合のみです。

- persistent memory modulesのパスワードが有効になっていない場合、暗号化キーはメディアに保存されます。ユーザーデータは暗号化されていますが、未認可ユーザーでもそれを復号化できてしまう可能性があります。

どちらの場合も、「インスタント完全消去」サニタイズ機能が容易になります。暗号化キーを変更すると、すべてのデータが解読不能になります。

persistent memory modulesのパスワードがあれば、暗号化キーは決して公開されません。パスワードがなくても、暗号化キーがシステムに公開されることは決してありませんが、メディアに物理的にアクセスできる未認可ユーザーが、消去前に暗号化キーを取得していて、後で使用した可能性は否定できません。その改ざんは物理的に明らかです。

サニタイズ

メディアサニタイズは、「通常的手段および異常な手段の両方でメディアに書き込まれたデータを復旧不能にするために取られる措置を示す一般的な用語」として、NIST SP800-88 Guidelines for Media Sanitization (Rev 1: 2014年12月) によって定義されています。

仕様では、以下のレベルを定義しています。

- クリア：ユーザーがアドレス指定可能なストレージ領域を標準の書き込みコマンドを使用して上書きします。現在ユーザーがアドレス指定できない領域（不良ブロックやオーバプロビジョニングされている領域など）のデータをサニタイズしない場合があります。
- パージ：専用デバイスのサニタイズコマンドを使用してデータの保存に使用されたすべてのストレージ領域を上書きまたは消去します。データの検索は「最先端の技術を使用しても実行不能」になります。
- 破棄：データの検索は「最先端の技術を使用しても実行不能」であり、かつメディアにデータを格納できない（分解、粉碎、熔解、焼却、細断などと同様に）ことを保証します。

HPE向けインテルOptane Persistent Memoryは、暗号による消去技法および上書き技法を使用したパージレベルをサポートします。

HPE ProLiantおよびHPE Synergy Gen10 Plusサーバー製品は、POST中のpersistent memory modulesのサニタイズをサポートしています。次回の起動時にサニタイズをスケジュールするには、RESTfulインターフェイスツールまたはUEFIシステムユーティリティを使用してください。

暗号による消去技法

この技法では「インスタントセキュアイレース」が可能であり、容量に関係なく、1秒もかからずにpersistent memory modulesのすべての不揮発性の内容をすぐに処理できます。不揮発性メディアは、ランダムに見えるデータ（今は失われたキーで暗号化されたデータ）を読み取ります。

また、たとえこれらの領域にアクセスできたとしても、メディアの不良部分や消耗した部分のデータを判読できないようにします。この技法は、上書き技法よりも強力です。上書きではそのような領域を上書きできない可能性があるためです。

サニタイズは、persistent memory modulesがパスワードでロックされていても、この技法の下で実行できます。これにより、ユーザーがパスワードを忘れても、persistent memory modulesのハードウェアを確実に使用することができます。

上書き技法

Persistent Memoryモジュールは上書き技法もサポートします。デフォルトではクリアレベルに準拠していますが、メディアの不良部分や消耗した部分の上書きに成功した場合は、パージレベルにも準拠しています。

暗号化が有効になっている場合（パスワードがpersistent memory modules上で設定されている）、この操作によりメディアが暗号化されたゼロで上書きされます。暗号化が有効になっていないか、またはCryptoEraseOverwriteコマンドが使用された場合は、この操作によりメディアはゼロで上書きされます。

NIST SP800-88 Guidelines for Media Sanitization (Rev 1: 2014年12月) は、NISTのWebサイト (<https://www.ipa.go.jp/files/000094547.pdf>) からダウンロードできます。

署名されたファームウェア

Persistent Memoryモジュールのファームウェアイメージは、暗号的に署名されています。このイメージには、RSA公開秘密キー暗号化を使用して暗号化された暗号化ハッシュ値（たとえば、SHA-256）が含まれています。

ハッシュ値は秘密キーを使用して暗号化されます。persistent memory modulesは公開キーを使用してハッシュ値を復号化します。

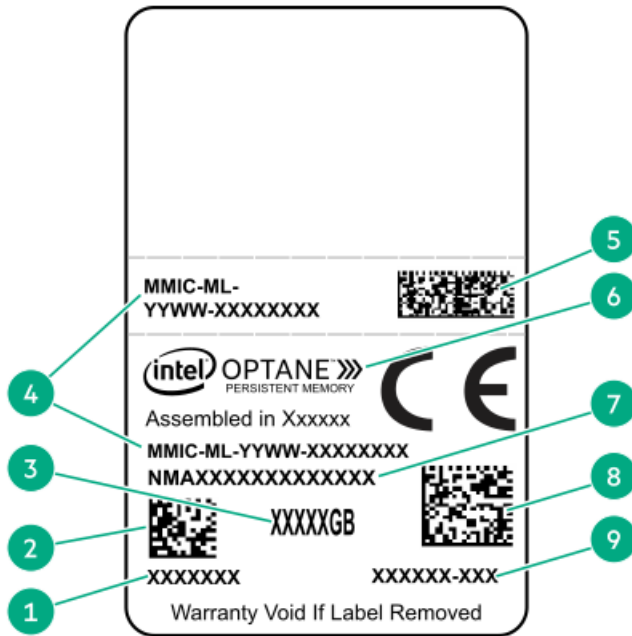
秘密キーは、FIPS 140-2レベル3またはレベル4（改ざん防止）のコード署名アプライアンスに保管されます。このアプライアンスは、認証された署名付きイメージのみを受け入れるようにアクセス制御を実施します。persistent memory modulesは正しく復号化されていないイメージは拒否します。

ファームウェアロールバック保護

ファームウェアイメージは、01.02.03.0405のようなバージョン番号で識別されます。

2番目のフィールド（たとえば、02）は、セキュリティバージョン番号を表します。この番号は、セキュリティが改善されてリリースされるたびに上がっていきます。Persistent Memoryモジュールは、現在実行中のものより古いセキュリティバージョン番号のファームウェアイメージを受け入れることはできません。この保護の仕組みにより、悪用可能な機能を含む可能性がある以前のイメージにファームウェアがロールバックすることが防止されます。ファームウェアロールバックは、BIOS内蔵FWアップデートアプリケーションを介して個々のバイナリファイルでのみ実行できます。

HPE向けインテルOptane Persistent Memory 200シリーズのラベルの識別



項目	説明	例
1	作業指示番号	XXXXXXX
2	作業指示番号のバーコード	XXXXXXX
3	容量	128 GB 256 GB 512 GB
4	固有のID番号	8089-A2-1802-1234567A
5	シリアル番号および部品番号のバーコード	S8089A218040000168APNMAXXXXXXXXXXXXX
6	製品名	インテル®Optane™ Persistent Memory
7	部品番号	1234567A
8	シリアル番号のバーコード	8089-A2-1802-1234567A
9	PBA番号	XXXXXX-XXX

製品の特長、仕様、オプション、構成、および互換性について詳しくは、Hewlett Packard EnterpriseのWebサイト (<https://www.hpe.com/support/persistentmemoryQS>) にある製品のQuickSpecsを参照してください。



システム要件

(i) 重要:

Hewlett Packard Enterpriseでは、高可用性 (HA) のためにクラスター構成などのベストプラクティス構成を実装することをお勧めします。

次のハードウェアコンポーネントが必要です。

- HPE DDR4標準メモリRDIMMまたはLRDIMM
- HPE向けインテルOptane Persistent Memory 200シリーズ
- 第3世代Intel Xeonスケーラブルプロセッサ

サポートされるファームウェアバージョン:

- システムROMバージョン1.40以降
- サーバプラットフォームサービス (SPS) ファームウェアバージョン04.04.04.053
- HPE iLO 5ファームウェアバージョン2.44
- HPE Innovation Engineファームウェアバージョン1.0.0.20以降

必要なファームウェアとドライバーをHewlett Packard EnterpriseのWebサイト (<https://www.hpe.com/support/hpesc>) からダウンロードします。

サポートされているオペレーティングシステム:

- Windows Server 2016 (Hewlett Packard Enterprise persistent memoryドライバー搭載)
- Windows Server 2019
- Red Hat Enterprise Linux 7.9以降
- Red Hat Enterprise Linux 8.2以降
- SUSE Linux Enterprise Server 12 SP5以降
- SUSE Linux Enterprise Server 15 SP2以降
- VMware vSphere 7.0 U2以降
- VMware vSphere 6.7 U3 (P03)

persistent memory modulesのオプションの暗号化のためのハードウェア要件とライセンス要件:

- HPE TPM 2.0 (ローカルキーの暗号化)
- HPE iLO Advancedライセンス (リモートキーの暗号化)
- キー管理サーバー (リモートキーの暗号化)

メモリ取り付け情報

DIMMとpersistent memory modulesは、サーバーのワークロード要件に基づいて、特定の構成で取り付けられます。サポートされている構成は、不揮発性メモリ容量、揮発性メモリ容量、およびパフォーマンスに合わせて最適化されています。

- 不揮発性メモリ容量 - 利用可能な容量は、persistent memory modulesの容量と同じです。
- 揮発性メモリ容量：
 - App Directモード - 揮発性容量はDRAM容量（取り付けられたすべての非persistent memory modulesの容量）と同じです。
- メモリ層容量 - メモリ層容量は、取り付けられているすべてのメモリ（DRAMとpersistent memory modules）の容量の合計です。

(i) 重要:

取り付けられているメモリがプロセッサの容量を超過した場合、システムは1つのDIMMチャンネルを除くすべてのDIMMチャンネルをマップアウトし、App Directモードで動作します。容量を超過すると、メッセージがIMLに記録されます。問題を解決するには、プロセッサの容量を超えるメモリを取り外します。

- パフォーマンス：
 - すべてのチャンネルを使用して、プロセッサリソースを効率的に利用します。
 - メモリモード - 通常のDIMMの数が多いほど、キャッシュ比率が向上します。

取り付けを開始する前に、[Hewlett Packard EnterpriseのWebサイト](#)でメモリ取り付けのガイドラインを確認してください。

Persistent Memoryモジュールの取り扱いのガイドライン

△ 注意:

persistent memory modulesを正しく取り扱わない場合、コンポーネントとシステムボードのコネクタに損傷が発生する原因となります。

persistent memory modulesを取り扱うときは、次のガイドラインに従ってください。

- 静電気対策を行ってください。
- persistent memory modulesは必ず側面の端部のみでつかみます。
- persistent memory modulesの下部にあるコネクタに触れないようにしてください。
- persistent memory modulesを握るようにして持たないでください。
- persistent memory modulesの両側のコンポーネントに触れないようにしてください。
- persistent memory modulesを曲げたり折ったりしないでください。

persistent memory modulesを取り付ける際は、次のガイドラインに従ってください。

- persistent memory modulesを固定する前に、persistent memory modulesスロットを開いて、persistent memory modulesの位置をスロットに合わせてください。
- persistent memory modulesの位置合わせをして取り付けるには、側面の端部にそって2本の指でpersistent memory modulesを押したままにします。
- persistent memory modulesを固定する際は、2本の指でpersistent memory modulesの上部をゆっくりと押ししてください。

詳しくは、Hewlett Packard EnterpriseのWebサイト (<https://www.hpe.com/support/DIMM-20070214-CN>) を参照してください。

DIMMまたは不揮発性モジュールの取り付け

この サーバー専用の手順については、Hewlett Packard EnterpriseのWebサイトにある [サーバーユーザーガイド](#)を参照してください。

- HPE ProLiant Gen10 Plusサーバー (<https://www.hpe.com/info/proliantgen10plus-docs>)
- HPE Synergy Gen10 Plusコンピュートモジュール (<https://www.hpe.com/info/synergy-docs>)

(i) 重要:

Hewlett Packard Enterpriseでは、高可用性 (HA) のためにクラスター構成などのベストプラクティス構成を実装することをお勧めします。

前提条件

取り付けを開始する前に、[Hewlett Packard EnterpriseのWebサイト](#)でメモリ取り付けのガイドラインを確認してください。

手順

1. 次のアラートに注意してください。

△ 注意:

DIMMおよびpersistent memory modulesは適切な配置のために重要です。コンポーネントを取り付ける前に、DIMMまたはpersistent memory modulesのノッチを対応するスロットのノッチに合わせます。DIMMまたはpersistent memory modulesをスロットに押し込まないでください。正しく取り付けられた場合、必ずしもすべてのDIMMまたはpersistent memory modulesが同じ方向に向く訳ではありません。

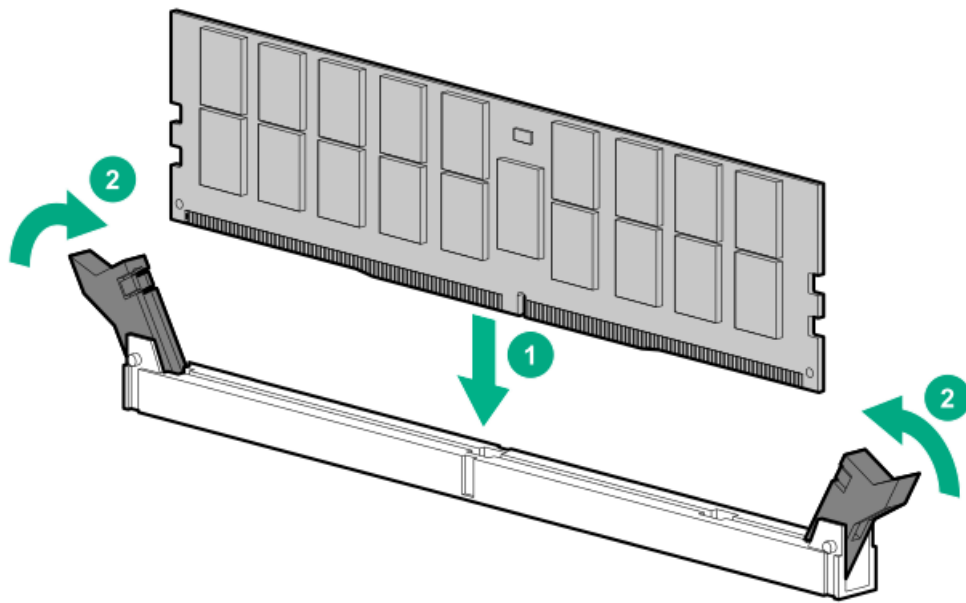
△ 注意:

静電気放電によって、電気回路などのコンポーネントが損傷することがあります。必ず、正しくアースを行ってからこの手順を開始してください。

△ 注意:

persistent memory modulesを正しく取り扱わない場合、コンポーネントとシステムボードのコネクタに損傷が発生する原因となります。

2. サーバーの電源を切ります。
 - a. OSのドキュメントの指示に従って、OSをシャットダウンします。
 - b. サーバーをスタンバイモードにするには、電源ボタンを押します。サーバーがスタンバイ電源モードに入ると、システム電源LEDがオレンジ色になります。
 - c. 電源コードを抜き取ります（ラックマウント型およびタワー型サーバー）。
3. 次のいずれかを実行します。
 - サーバーをラックから引き出します。
 - 必要に応じて、ラックからサーバーを取り外します。
 - サーバーまたはサーバーブレードをエンクロージャーから取り外します。
4. サーバーを平らで水平な面に置きます。
5. アクセスパネルを取り外します。
6. DIMMスロットにアクセスするために取り外す必要があるコンポーネントをすべて取り外します。
7. DIMMまたはpersistent memory modulesを取り付けます。



8. DIMMスロットにアクセスするために取り外したコンポーネントをすべて取り付けます。
9. アクセスパネルを取り付けます。
10. サーバーをラック内部へスライドさせるか、または取り付けます。
11. すべての電源ケーブルを取り外した場合は、接続し直します。
12. サーバーの電源を入れます。

構成の概要

HPE向けインテルOptane Persistent Memoryを次のようにして構成します。

1. 「目標構成」を設定します。これは、persistent memory modules上の揮発性メモリと不揮発性メモリの領域を定義します。
2. 結果として得られる不揮発性領域の上にネームスペースを作成します。
3. (オプション) ローカルまたはリモートのキー管理を有効にします。
4. (オプション) persistent memory modulesを暗号化します。

(i) 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。

構成ツール

HPE向けインテルOptane Persistent Memoryの構成および保守に使用できるツールは数多くあります。

内蔵ツール

- UEFIシステムユーティリティ
- ipmctlツール (UEFIシェル下)

REST/iLOベースのツール

- HPE iLO RESTful API
- RESTfulインターフェイスツール

OSベースのツール

- Windows PowerShellコマンドレット
- ipmctlツール (LinuxおよびWindows)
- ndctlツール (Linux)

目標構成の設定

揮発性メモリと不揮発性メモリの領域を定義する目標構成は、persistent memory modulesのメタデータに格納されません。persistent memory modulesはシステムメモリバス上にあるため、目標構成を変更するにはシステムの再起動が必要です。次の起動時に、システムファームウェアが目標構成要求を検出し、persistent memory modulesを再構成します。

目標構成は、推奨されるメモリのキャッシュ比率に準拠している必要があります。推奨されていない比率を選択すると、IMLにメッセージが生成されます。

(i) 重要:

データを保存しておく必要がある場合、Hewlett Packard Enterpriseでは、persistent memory modules上にあるすべてのユーザーデータについて手動でバックアップを取ってから、目標構成の変更または再配置の手順を実行することを強くお勧めします。

(i) 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。

UEFIシステムユーティリティを使用した目標構成の設定

(i) 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) > メモリオプション**を選択します。
2. 以下のデフォルト設定を確認します。
 - **最大メモリバス周波数** - 自動
 - **メモリ巡回スクラビング** - 有効
 - **メモリの再マップ** - 操作なし
3. **不揮発性メモリオプション**を選択し、次の選択項目を確認します。

不揮発性メモリアドレス範囲スクラブ - 有効。
4. **PMMオプション > 目標構成オプション**を選択します。

目標構成オプションは、最新の構成の各種設定を表示しますが、必ずしもアクティブな構成とは限りません。この画面で定義された構成設定は、次のサーバー再起動時にのみ適用されます。
5. 次のオプションを選択します。
 - **揮発性メモリ容量** - 揮発性メモリを提供するpersistent memory modules容量の%数。
 - **メモリモード** - 100%を選択します。
 - **App Directモード** - 0%を選択します。
 - **不揮発性メモリインターリーブ** - 有効または無効です。
6. **目標構成の適用**を選択します。

目標構成設定は、次の再起動時に適用されます。
7. **PMMオプション > セキュリティオプション > Security Freeze Lock** - 無効。
8. 選択内容を確認します。
9. 変更を保存するには、F12キーを押します。
10. 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。

ipmctlを使用した目標構成の設定

ipmctlツールは、UEFIコマンドライン、Windows OS、またはLinuxで実行できます。

```
create
[-dimm [(DimmIDs)]]
-goal
[-socket (SocketIDs)]
[MemoryMode=(0|%)]
[PersistentMemoryType=(AppDirect|AppDirectNotInterleaved)]
```

目標構成例

コマンド	説明
<code>ipmctl create -goal</code>	デフォルトで100%インターリーブ不揮発性メモリになります。
<code>ipmctl create -goal MemoryMode=0 Reserved=100</code>	100%未構成
<code>ipmctl create -goal MemoryMode=100</code>	100%揮発性メモリ
<code>ipmctl create -goal MemoryMode=0 PersistentMemoryType=AppDirect</code>	100%インターリーブ不揮発性メモリ
<code>ipmctl create -goal MemoryMode=0 PersistentMemoryType=AppDirectNotInterleaved</code>	100%非インターリーブ不揮発性メモリ
<code>ipmctl create -goal MemoryMode=80 PersistentMemoryType=AppDirect</code>	<ul style="list-style-type: none">80%揮発性メモリ20%インターリーブ不揮発性メモリ

これらの値は、メモリの推奨キャッシュ比率に準拠している必要があります。推奨されていない比率を選択すると、システム性能に影響を及ぼす可能性があり、IMLにメッセージが生成されます。

HPE iLO RESTful APIを使用した目標構成の設定

HPE iLO RESTful APIには、さまざまなツールを使用してアクセスできます。Hewlett Packard Enterpriseでは、RESTfulインターフェイスツールの使用をお勧めします。

`rawpost` コマンドは、JSONファイルを取り込みます。次の例は、RESTfulインターフェイスツールを使用して、インターリーブを有効にして100% AppDirect用にサーバーを構成するためのJSONファイルとバッチスクリプトを示しています。

Memorychunk-rawpost.txt

```
{
  "path": "/redfish/v1/Systems/1/MemoryDomains/PROClMemoryDomain/MemoryChunks",
  "body": {
    "AddressRangeType": "PMEM",
    "Oem": {
      "Hpe": {
        "MemoryChunkSizePercentage": 100
      }
    },
    "InterleaveSets": [{
      "Memory": {
        "@odata.id": "/redfish/v1/Systems/1/Memory/proclimm6/"
      }
    }, {
      "Memory": {
        "@odata.id": "/redfish/v1/Systems/1/Memory/proclimm7/"
      }
    }
  ]
}
```

Windowsバッチスクリプト

```
@echo off

set argC=0
for %%x in (*) do Set /A argC+=1
if %argC% LSS 3 goto :failCondition
goto :main

:failCondition
@echo Usage:
@echo ilorest-script-memory-remote.bat [URL] [ユーザー名] [パスワード]
goto :EOF

:main
@echo Logging in...
ilorest.exe --nologo login %1 -u %2 -p %3
@echo rawpost to Memory Chunk collection...
ilorest.exe --nologo rawpost memorychunk-rawpost.txt
@echo Note: Status of 202 is success.
```


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

(i) 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向けインテルOptane 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、persistent memory modules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 > アドバンスト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。

ipmctlを使用したネームスペースの作成

デフォルトのネームスペースは、UEFIコマンドラインで `ipmctl` ツールを使用して作成できます。

```
Shell> ipmctl create -namespace -region id
```

ndctlを使用したネームスペースの作成 (Linux)

Linuxでは、複数のネームスペースモードをサポートしています。これはLinuxで `ndctl` コマンドを使用して作成できます。

```
ndctl create-namespace [<options>]
```

`ndctl` コマンドを使用してネームスペースを作成または変更する方法については、以下を参照してください。

- [ネームスペース](#)
- <https://docs.pmem.io/ndctl-user-guide/>にあるndctl関連ドキュメント

キー管理の有効化

注記:

ipmctl OSツールは、キー管理機能をサポートしません。persistent memory modulesのキー管理を有効にしたり、暗号化の有効と無効を切り替えたりするには、UEFIシステムユーティリティで次の手順に従ってください。

前提条件

ローカルまたはリモートのキー管理を有効にする前に、次の点を確認してください。

- 目標構成が設定され、かつサーバーのワークロード要件に基づいてHPE向けインテルOptane Persistent Memoryが構成されています。
- ローカルキー管理の場合：
 - サーバーにHPE TPM 2.0がインストールされています。
 - HPE TPM 2.0がアクティブであり、非表示になっていません。
 - サーバーがUEFIブートモード向けに設定されています（レガシーブートモードでは、ローカルキー管理はサポートされていません）。
- リモートキー管理の場合：
 - HPE iLOがキー管理サーバーに登録され、接続されています。
 - サーバーにHPE iLO Advancedライセンスがあります。

詳しくは、[キー管理サーバーの使用](#)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) > 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ます。
 - **無効** - デフォルト設定です。キー管理は無効化されています。
 - **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。
5. 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。
6. 次のいずれかを実行します。
 - [ローカルキー管理を使用したpersistent memory modulesの暗号化](#)
 - [リモートキー管理を使用したpersistent memory modulesの暗号化](#)

ローカルキー管理を使用したpersistent memory modulesの暗号化

前提条件

ローカルキー管理を有効にしておく必要があります。詳しくは、[キー管理の有効化](#)を参照してください。

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 > デバイス暗号化設定 > 非暗号化デバイスを選択します。
3. 次のオプションを選択します。
 - **デバイスの選択** - 暗号化する特定のpersistent memory modulesを選択します。
 - **操作を選択** - 暗号化を有効にするを選択します。
4. パスフレーズのタイプを選択します。
 - **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。
 - **手動** - 32バイトのパスワードを手動で入力します。
5. 操作を開始を選択します。

これで、persistent memory modulesが暗号化されました。
6. 別のpersistent memory modulesを暗号化するには、デバイスの選択メニューから選択してください。
7. 個別のpersistent memory modulesごとに暗号化を有効にするには、この手順を繰り返します。
8. 暗号化されたpersistent memory modulesのステータスを表示します。

詳しくは、[persistent memory modulesステータスの表示](#)を参照してください。
9. 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 > デバイス暗号化エクスポートオプションを選択します。
 - b. パスワードを一時パスフレーズ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persistent memory modulesを復元するときに、入力する必要があります。
 - c. ファイルを選択を選択し、USBキーの場所を参照します。
 - d. 暗号化設定のエクスポートを選択して、ファイルを作成しエクスポートします。

リモートキー管理を使用したpersistent memory modulesの暗号化

リモートキー管理が有効な場合、persistent memory modules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。

前提条件

- HPE iLOが、キー管理サーバーに登録され接続され、かつHPE iLO Advancedのライセンスを持っている必要があります。詳しくは、[キー管理サーバーの使用](#)を参照してください。
- リモートキー管理を有効にしておく必要があります。詳しくは、[キー管理の有効化](#)を参照してください。

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 > デバイス暗号化設定 > 非暗号化デバイスを選択します。
3. 次のオプションを選択します。
 - **デバイスの選択** - 暗号化する特定のpersistent memory modulesを選択します。
 - **操作を選択** - 暗号化を有効にするを選択します。
4. 操作を開始を選択します。

これで、persistent memory modulesが暗号化されました。
5. 別のpersistent memory modulesを暗号化するには、デバイスの選択メニューから選択してください。
6. 個別のpersistent memory modulesごとに暗号化を有効にするには、この手順を繰り返します。

キー管理サーバーの使用

iLO 5はキーマネージャをサポートします。これは、HPE向けインテルOptane Persistent Memoryと組み合わせて使用できます。UEFI管理暗号化により、256ビットのXTS-AESアルゴリズムを使用して、persistent memory modulesの蓄積データの暗号化が可能になります。

キーマネージャは、データ暗号化キーの生成、保存、操作、制御、アクセスの監査を行います。これを使用して、ビジネスクリティカルで機密性のある保存済みデータの暗号化キーへのアクセスを保護し維持することができます。

iLOが、キーマネージャと他の製品との間のキー交換を管理します。iLOは、キーマネージャとの通信に、自身のMACアドレスに基づいた一意のユーザーアカウントを使用します。このアカウントを最初に作成するために、iLOは、管理者権限を持つ、キーマネージャに以前から存在する展開ユーザーアカウントを使用します。展開ユーザーアカウントについて詳しくは、キーマネージャのドキュメントを参照してください。

サポートされているキーマネージャー

iLOは以下のキーマネージャーをサポートしています。

- Utimaco Enterprise Secure Key Manager (ESKM) 4.0以降

FIPSセキュリティ状態が有効になっている場合は、ESKM 5.0以降が必要です。

△ 注意:

ESKMを使用する場合は、アップデートされたコード署名証明書が含まれているソフトウェアアップデートを必ずインストールしてください。必要なアップデートをインストールしないと、ESKMは2019年1月1日後に再起動するとエラー状態になります。詳しくは、[ESKMのドキュメント](#)を参照してください。

-
- Thales TCT KeySecure for Government G350v (旧称SafeNet AT KeySecure G350v 8.6.0)
 - Thales KeySecure K150v (旧称SafeNet KeySecure 150v 8.12.0)
 - Thales CipherTrust Manager 2.2.0、K170v (仮想) およびK570 (物理) アプライアンス

☰ 注記:


CNSAセキュリティ状態を使用するようiLOが構成されている場合、キーマネージャーの使用はサポートされません。

キーマネージャーサーバーの構成

前提条件

- iLOの設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト (<https://www.hpe.com/support/ilo-docs>) にあるライセンス文書を参照してください。
- CNSAセキュリティ状態を使用するようiLOが構成されていない。

手順

1. ナビゲーションツリーで管理をクリックして、キーマネージャータブをクリックします。
2.  (キーマネージャーサーバーセクション内) をクリックします。
キーマネージャーサーバー設定を編集ページが開きます。
3. 次の情報を入力します。
 - プライマリーキーサーバーアドレス
 - プライマリーキーサーバーポート
 - セカンダリキーサーバーアドレス
 - セカンダリキーサーバーポート
4. (オプション) プライマリーおよびセカンダリキーサーバーを使用した構成でサーバーの冗長化を確認するには、冗長化が必要オプションを有効にします。
Hewlett Packard Enterpriseでは、このオプションを有効にすることをお勧めします。
5. OKをクリックします。

Thales CipherTrust Manager 2.2.0について詳しくは、[Remote Key Manager Support for Cipher Trust Manager](#)構成ガイドを参照してください。

キーマネージャーサーバーのオプション

プライマリーキーサーバーアドレス

プライマリーキーサーバーのホスト名、IPアドレス、またはFQDN。この文字列の最大長は79文字です。

プライマリーキーサーバーポート

プライマリーキーサーバーポート。

セカンダリキーサーバーアドレス

セカンダリキーサーバーのホスト名、IPアドレス、またはFQDN。この文字列の最大長は79文字です。

セカンダリキーサーバーポート

セカンダリキーサーバーポート。

冗長化が必要

このオプションが有効になっていると、iLOは、構成された両方のキーサーバーに暗号化キーがコピーされていることを確認します。

このオプションが無効になっていると、iLOは、構成された両方のキーサーバーに暗号化キーがコピーされていることを確認しません。

Hewlett Packard Enterpriseでは、このオプションを有効にすることをおすすめします。


キーマネージャー構成の詳細の追加

前提条件

- iLOの設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト (<https://www.hpe.com/support/ilo-docs>) にあるライセンス文書を参照してください。
- CNSAセキュリティ状態を使用するようiLOが構成されていない。
- 少なくとも1つのキーマネージャーサーバーが構成されている。

手順

1. ナビゲーションツリーで管理をクリックして、キーマネージャータブをクリックします。

2.  (キーマネージャー構成セクション内) をクリックします。

キーマネージャー構成設定を編集ページが開きます。

3. 次の情報をキーマネージャー上のiLOアカウントセクションに入力します。

- アカウントグループ
- (オプション) キーマネージャーローカルCA証明書名

アカウント名の値は読み取り専用です。

4. 次の情報をキーマネージャー管理者アカウントセクションに入力します。

- ログイン名
- パスワード

5. OKをクリックします。

iLOは情報要求をキーマネージャーサーバーに送信します。

- ilo-<iLOのMACアドレス>というアカウント名が存在しない場合：
 - キーマネージャー管理者アカウントセクションで入力したユーザーアカウントが、アカウント名を作成して、キーマネージャーのローカルユーザーとその生成済みパスワードに関連付けます。
 - アカウント名は、手順3で入力したアカウントグループに追加されます。
- ilo-<iLOのMACアドレス>というアカウント名が存在する場合：
 - キーマネージャー管理者アカウントセクションで入力したユーザーアカウントが、キーマネージャーのローカルユーザーにアカウント名を関連付けて、新しいパスワードが生成されます。
 - キーマネージャー管理者アカウントセクションで入力したユーザーアカウントが、ilo-<iLOのMACアドレス>アカウントに関連付けられたアカウントグループのメンバーでない場合、そのアカウントがアカウントグループに追加されます。
 - ilo-<iLOのMACアドレス>がすでに、キーマネージャーのローカルグループのメンバーである場合、手順3で入力したグループは無視されます。キーマネージャーでの既存のグループ割り当てが使用され、iLOのWebインターフェイスに表示されます。新しいグループの割り当てが必要な場合は、iLO設定をアップデートする前にキーマネージャーをアップデートする必要があります。

手順3でキーマネージャーローカルCA証明書名を入力した場合、キーマネージャーページのインポートされた証明書の詳細セクションに証明書情報が一覧表示されます。

キーマネージャー構成の詳細

アカウント名

キーマネージャー上のiLOアカウントに表示されているアカウント名はilo-<iLO MACアドレス>です。アカウント名は読み取り専用で、iLOがキーマネージャーと通信するときに使用されます。

アカウントグループ

iLOユーザーアカウントと、iLOがキーマネージャーにインポートしたキーで使用するために、キーマネージャー上に作成されたローカルグループ。キーはインポートされると、自動的に、同じグループに割り当てられたすべてのデバイスで使用可能になります。

グループと、キー管理でのグループの使用については、セキュア暗号化インストール/ユーザーガイドを参照してください。

キーマネージャーローカルCA証明書名

iLOが信頼済みのキーマネージャーサーバーと通信していることを確認するには、ローカル認証機関の証明書の名前をキーマネージャーに入力します。通常はLocal CAという名前で、キーマネージャーのローカルCAの下に表示されます。iLOは証明書を取得し、それを使用して、今後のすべてのトランザクションでキーマネージャーのサーバーを認証します。

セキュア暗号化では、信頼された第三者認証機関または中間CAの使用はサポートされません。

ログイン名

キーマネージャーで構成された管理者アクセス権を持つローカルユーザー名。このユーザー名はキーマネージャーデプロイメントユーザーです。

iLOでキーマネージャーの構成詳細を追加する前に、デプロイメントユーザーアカウントを作成する必要があります。

パスワード

キーマネージャーで構成された管理者アクセス権を持つローカルユーザー名に応じたパスワード。

キーマネージャー構成のテスト


構成設定を確認するには、キーマネージャー構成をテストします。以下のテストが試行されます。

- キーマネージャーソフトウェアのバージョンがiL0と互換性があることを確認します。
- TLSを使用してプライマリーキーマネージャーサーバー（および構成されている場合はセカンダリーキーマネージャーサーバー）に接続します。
- 構成済みの認証情報およびアカウントを使用して、キーマネージャーに認証します。

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト (<https://www.hpe.com/support/iLO-docs>) にあるライセンス文書を参照してください。
- キーマネージャーがセットアップされ、iL0でキーマネージャーの構成が完了している。

手順

1. ナビゲーションツリーで管理をクリックして、キーマネージャータブをクリックします。
2.  をクリックします。

テスト結果は、キーマネージャーイベントテーブルに表示されます。成功または失敗のメッセージがiL0のWebインターフェイスウィンドウの上部に表示されます。

キーマネージャーイベントの表示

前提条件

この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト (<https://www.hpe.com/support/ilo-docs>) にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで管理をクリックして、キーマネージャータブをクリックします。
2. キーマネージャーイベントセクションまでスクロールします。
各イベントがタイムスタンプと説明とともに一覧表示されます。

キーマネージャーログのクリア

前提条件

- iLOの設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト (<https://www.hpe.com/support/ilo-docs>) にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーで管理をクリックして、キーマネージャータブをクリックします。
2. キーマネージャーログをクリックします。
iLOが要求を確認するように求めます。
3. はい、クリアしますをクリックします。

他のBIOS/プラットフォーム構成 (RBSU) オプション

persistent memory modulesが取り付けられている場合、次のBIOS/プラットフォーム構成 (RBSU) 設定は、persistent memory modulesには適用されずサポートされないか、デフォルト値に設定されている場合にのみサポートされます。

- **アドバンスドメモリプロテクション** - Persistent Memoryモジュール構成がアドバンスドECCに設定されていない場合は無効になります。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になります。アドバンスドECCは、(BIOS 1.50より前のADでサポートされている) MMモードでサポートされています。HPE Fast Fault Tolerance (ADDDCとも呼ばれます) は、BIOS 1.50以降のADモードでサポートされています。
 - UEFIシステムユーティリティ：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
 - iLO RESTful APIのプロパティ名：
`AdvancedMemProtection`
- **最大メモリバス周波数** - このオプションは、persistent memory modulesが取り付けられている場合、デフォルトで有効になります。その場合、搭載されているプロセッサおよびDIMM構成でサポートされる速度よりも低い最高速度でメモリが動作するように、システムで構成できます。
 - UEFIシステムユーティリティ：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
 - iLO RESTful APIのプロパティ名：
`MaxMemBusFreqMHz`
- **メモリ巡回スクラビング** - このオプションは、persistent memory modulesが取り付けられている場合、デフォルトで有効になります。このオプションは、メモリのソフトウェアエラーを修正するため、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エラーの発生が減少します。
 - UEFIシステムユーティリティ：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
 - iLO RESTful APIのプロパティ名：
`MemPatrolScrubbing`
- **メモリミラーリングモード** - このオプションは、persistent memory modulesが取り付けられている場合、サポートされません。
 - UEFIシステムユーティリティ：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
 - iLO RESTful APIのプロパティ名：
`MemMirrorMode`
- **メモリリフレッシュレートオプション** - このオプションは、メモリコントローラーのリフレッシュレートを調整できますが、サーバーのメモリのパフォーマンスと耐障害性に影響する場合があります。Hewlett Packard Enterpriseでは、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。

最適な消費電力とパフォーマンスを得るため、Hewlett Packard Enterpriseでは1xリフレッシュを選択することをお勧めします。

 - UEFIシステムユーティリティ：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 > メモリリフレッシュレート
 - iLO RESTful APIのプロパティ名：
`MemRefreshRate`
- **Sub-NUMAクラスタリング** - このオプションはサポートされておらず、persistent memory modulesが取り付けられている場合に自動的に無効に設定されます。
 - UEFIシステムユーティリティ：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
 - iLO RESTful APIのプロパティ名：
`SubNumaClustering`

- **eADR (拡張非同期DRAMリフレッシュ)** - 不揮発性メモリモジュールが取り付けられている場合、このオプションはデフォルトで無効になっています。eADRは、第3世代インテルXeonスケーラブルプロセッサやインテルOptane PMem 200シリーズメモリモジュールなどのハードウェア要件を備えたプラットフォーム機能です。IIOキャッシュ+CPU キャッシュ+iMC WPQから不揮発性メモリモジュールにデータをフラッシュすることにより、電源障害が発生したときにデータの永続性を提供します。eADRは、CF9ウォームリセットやコールドリセットが発生した場合にのみ、RBSUで有効にする必要があります。

2.6.13以降のすべてのLinuxカーネルに存在するipmi_poweroffモジュールには、IPMIシャーシの電源オフコマンドを使用してACPI電源制御方式をオーバーライドする機能が備わっています。このIPMIメカニズムによって、eADRの操作が中断され、不要なダーティシャットダウンイベントが発生する可能性があります。インテルは、ipmi_poweroffモジュールを無効にするか、ipmi_poweroffを使用するとダーティシャットダウンイベントが発生する可能性があることを考慮することをお勧めします。

modprobe -r ipmi_poweroffコマンドを使用して、2.6.13以降のすべてのLinuxカーネルでipmi_poweroffモジュールを無効にします。モジュールを無効にする方法については、Linuxのmodprobe.dマニフェストページを参照してください。

- UEFIシステムユーティリティ：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 > PMEMオプション > パフォーマンスオプション > eADR

- iLO RESTful APIプロパティ名：

eADR

- **インテルPerformance Counter Monitorのサポート** - インテルプロセッサには、DRAMのパフォーマンス (persistent memory modules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、インテルプロセッサ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。

Hewlett Packard Enterpriseでは、persistent memory modulesパフォーマンスモニターツールを実行できるようになるため、**インテルPerformance Counter Monitor**を有効にすることをお勧めします。

- UEFIシステムユーティリティ：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

- iLO RESTful APIのプロパティ名：

IntelPerfMonitoring

- **ユーザーデフォルトオプション** - Hewlett Packard Enterpriseでは、サーバーに不揮発性メモリ設定を構成したら、その設定をユーザーのデフォルト設定として保存することをお勧めします。

- UEFIシステムユーティリティ：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

- iLO RESTful APIのプロパティ名：

SaveUserDefaults

HPE向けインテルOptane Persistent Memoryの管理

HPE向けインテルOptane Persistent Memoryの管理に使用できるツールは、次に示すようにたくさんあります。

- UEFIシステムユーティリティ
- RESTfulインターフェイスツール
- Ipmitl。これはコマンドラインまたはUEFIシェル下で実行できます



UEFIシステムユーティリティを使用した目標構成の変更

目標構成オプションは、最新の構成の各種設定を表示しますが、必ずしもアクティブな構成とは限りません。この画面で定義された構成設定は、次のサーバー再起動時にのみ適用されます。

(i) 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。

(i) 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。

(i) 重要:

データを保存しておく必要がある場合、Hewlett Packard Enterpriseでは、persistent memory modules上にあるすべてのユーザーデータについて手動でバックアップを取ってから、目標構成の変更または再配置の手順を実行することを強くお勧めします。

前提条件

1. persistent memory modulesが暗号化されている場合、目標構成を変更する前に、キー管理機能を無効にする必要があります。
2. メディアの上書き方法を使用して、サーバーのすべてのpersistent memory modulesをサニタイズします。詳しくは、[persistent memory modulesのサニタイズ](#)を参照してください。

手順

1. persistent memory modulesの暗号化が有効にされている場合、無効にしてください。
詳しくは、[キー管理の無効化](#)を参照してください。
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) > 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 > 目標構成オプションを選択します。
3. 次の選択項目をアップデートします。
 - 揮発性メモリ容量 - 揮発性メモリを提供するpersistent memory modules容量の%数。
 - メモリモード - 100%を選択します。
 - App Directモード - 0%を選択します。
 - 不揮発性メモリインターリーブ - 有効または無効です。
4. 目標構成の適用を選択します。
5. 変更を保存するには、F10キーを押します。
6. 新しい目標構成設定をすぐに確定するには、サーバーを再起動します。
7. 目標構成を変更するために暗号化が無効にされていた場合は、有効にします。
詳しくは、[キー管理の有効化](#)を参照してください。

UEFIシステムユーティリティを使用した目標構成の削除

目標構成オプションは、最新の構成の各種設定を表示しますが、必ずしもアクティブな構成とは限りません。この画面で定義された構成設定は、次回のサーバー再起動時にのみ適用されます。

(i) 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。

(i) 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。

前提条件

persistent memory modulesが暗号化されている場合、目標構成を削除する前に、キー管理機能を無効にする必要があります。

手順

1. persistent memory modulesの暗号化が有効にされている場合、無効にしてください。
詳しくは、[キー管理の無効化](#)を参照してください。
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) > 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 > 目標構成オプション**を選択します。
3. **目標構成の削除**を選択します。
4. 変更を保存するには、F10キーを押します。
5. 目標の構成設定をすぐに削除するには、サーバーを再起動します。
6. 目標構成を変更するために暗号化が無効にされていた場合は、有効にします。
詳しくは、[キー管理の有効化](#)を参照してください。

persistent memory modulesパスワードの変更

(i) 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persistent memory modules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、persistent memory modules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、persistent memory modulesパスワードが変更されます。
7. 各個人のpersistent memory modules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persistent memory modules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。

persistent memory modules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persistent memory modules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persistent memory modulesのステータスを確認します。

- Not encrypted – persistent memory modulesは暗号化されていません。
- Local/TPM – persistent memory modules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す。

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persistent memory modules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。

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 persistent memory modules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。

i 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persistent memory modulesについて、暗号化が無効になります。単一または特定のpersistent memory modulesのみ暗号化を無効にする方法については、[persistent memory modulesの暗号化の無効化](#)を参照してください。

(i) 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。

persistent memory modules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persistent memory modules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persistent memory modules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。

(i) 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 - persistent memory modules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、persistent memory modulesのパスフレーズを入力します。

これで、選択したpersistent memory modulesが非暗号化されました。
4. その他のpersistent memory modules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。

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

(i) 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。

(i) 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。App Direct (AD) のパフォーマンスを最適化します
 - バランス - メモリモードのパフォーマンスを最適化します
 - 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 - App Directモードでのシーケンシャル書き込みトラフィック負荷の帯域幅を改善するために推奨されます
 - AppDirect用Snoopyモード - 非NUMA (non-uniform memory access) に最適化されたワークロードについて、persistent memory modules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、persistent memory modules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。



HPE iLO RESTful APIの概要

サーバー管理用のHPE iLO RESTful APIは、インテリジェントなリモートコントロールを提供します。この単一インターフェイスを使用して、リモートサーバーのプロビジョニング、構成、インベントリ、および監視を実行します。HPE iLO RESTful APIは、DMTF Redfish API規格に準拠しています。HPE iLO RESTful APIについて詳しくは、Hewlett Packard EnterpriseのWebサイト (<https://www.hpe.com/us/en/servers/restful-api.html>) を参照してください。

HPE iLO RESTful APIには、さまざまなツールを使用してアクセスできます。Hewlett Packard Enterpriseでは、RESTfulインターフェイスツールの使用をお勧めします。Postman、curl、wgetなどのサードパーティツールも利用できます。

データモデルの概要

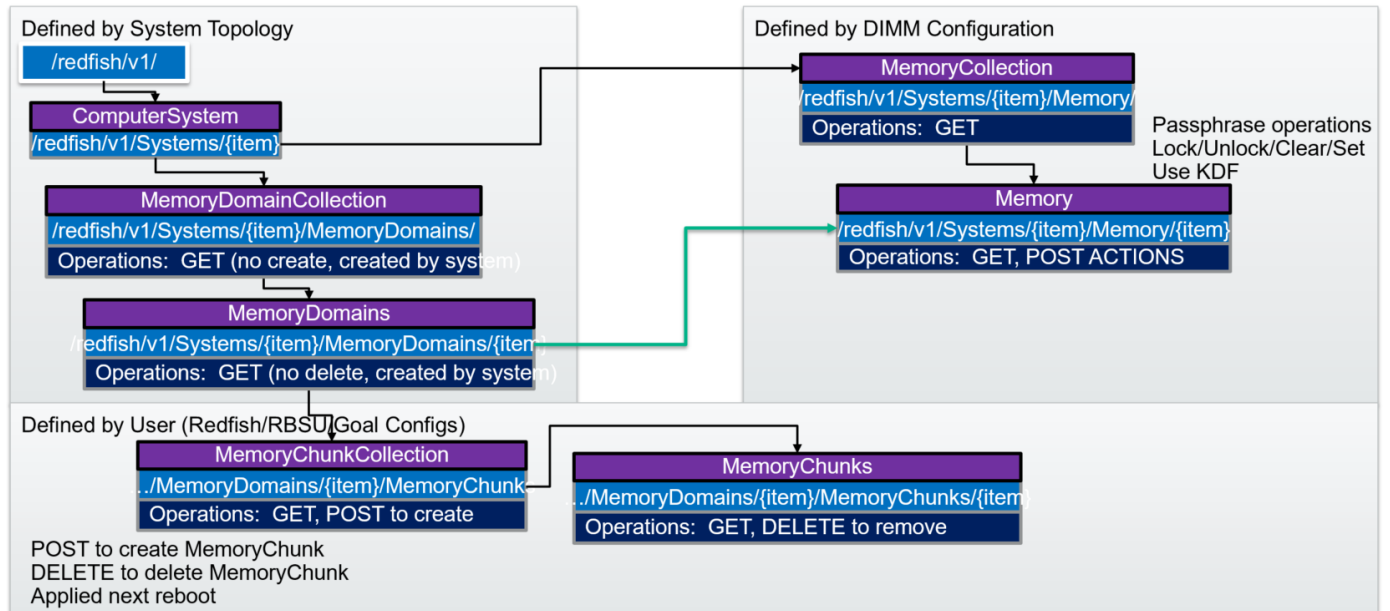
persistent memory modulesの物理的特性と構成は、特定のリソースによって詳細に説明されます。

- メモリ
- メモリチャンク
- メモリドメイン
- メモリ領域

用語	意味
メモリ	メモリとは、システムに取り付けられたDIMMのことです。
メモリチャンク	メモリチャンクとは、1つ以上の領域のグループのことです。メモリチャンクとは、インターリーブセットのことです。メモリドメインとメモリチャンクは、不揮発性領域についてのみ報告されます。揮発性領域は、そのようなデータが報告されないDIMMとまったく同様に扱われます。
メモリドメイン	メモリドメインは、どのメモリ (DIMM) をインターリーブセットを形成するためにメモリチャンクにまとめることができるのか、またはそれ以外の目的 (情報提供のみ。構成不可) でまとめることができるのかをクライアントに示すために使用されます。
メモリ領域	領域とは、特定のサイズおよびモードを持つpersistent memory modulesの一部のことです。1つのpersistent memory modulesは1つ以上の領域を持つことができます。1つのpersistent memory modules上で、領域は同じモードにすることもできれば、違うモードにすることもできます。たとえば、1つのpersistent memory modules上で、不揮発性領域と揮発性領域が同時に存在することが可能です。
インターリーブセット	まとめてインターリーブされる複数のメモリ領域を1つにまとめたグループ。Redfishでは「メモリチャンク」で表現されます。

データモデル図

次の図は、persistent memory modulesのデータモデルを示しています。この図は、各リソースの階層構造、URI、およびサポートされている操作を示しています。



例：メモリリソースの取得

RESTfulインターフェイスツールのselectとlistでメモリを取得

RESTfulインターフェイスツールを使用して、リソースを取得できます。利用可能なコマンドがいくつかあります。

- `select`
- `get`
- `list`
- `rawget`

以下は、システム内のすべてのメモリリソースを取得して、JSON形式で出力するためのWindowsバッチスクリプトの例です。

```
@echo off

set argC=0
for %%x in (*) do Set /A argC+=1
if %argC% LSS 3 goto :failCondition
goto :main

:failCondition
@echo Usage:
@echo ilorest-script-memory-remote.bat [URL] [ユーザー名] [パスワード]
goto :EOF

:main
@echo Logging in...
ilorest.exe --nologo login %1 -u %2 -p %3
@echo selecting Memory type...
ilorest.exe --nologo select Memory.
@echo list Memory data in JSON format...
ilorest.exe --nologo list -json
```

pythonを使用した拡張メモリコレクションの取得

次の例では、Pythonのリクエストライブラリを使用して、所定のサーバーのメモリコレクションを取得しています。展開クエリは、一度にすべてのメンバーを取得するために使用されます。

```

import requests
from requests.auth import HTTPBasicAuth
import sys
import json

# server info
if len(sys.argv) < 4:
    sys.stdout.write("\nPlease supply the URL, username and password:" \
        "\nUsage: python clear_all_tasks.py https://ilourl username password\n")
    exit(-1)

iLO_URL = sys.argv[1]
username = sys.argv[2]
password = sys.argv[3]

# REST info
MEMORY_URI = "/redfish/v1/systems/1/Memory?$expand=.#"

# Get the Memory
sys.stdout.write("Retrieving all Memory...")
with requests.Session() as s:
    get_response = s.get(iLO_URL + MEMORY_URI, \
        auth=HTTPBasicAuth(username, password))
    body = get_response.json()
s.close()
if get_response.status_code != 200:
    sys.stdout.write("error occurred: {}".format(get_response.status_code))
else:
    sys.stdout.write(json.dumps(body, indent=2, separators=(',', ': ')))

```

Postmanを使用した拡張メモリコレクションの取得

次の例では、Postmanを使用して、所定のサーバーのメモリコレクションを取得しています。展開クエリは、一度にすべてのメンバーを取得するために使用されます。

動作： GET

パス： /redfish/v1/systems/1/memory?\$expand=.#

The screenshot shows the Postman interface for a GET request to `https://ilo.fulldomain.com/redfish/v1/systems/1/memory?$expand=.#`. The request is configured with Basic Auth, using the username `user` and a masked password. The response status is `200 OK` with a response time of `220 ms`. The response body is displayed in JSON format, showing a list of memory members with detailed properties.

```

36 }
37 },
38 "Members": [
39 {
40   "@odata.context": "/redfish/v1/$metadata#Memory.Memory",
41   "@odata.id": "/redfish/v1/Systems/1/Memory/proc1dimm1",
42   "@odata.type": "#Memory.v1_7_0.Memory",
43   "Id": "proc1dimm1",
44   "BusWidthBits": 72,
45   "CacheSizeMiB": -1,
46   "CapacityMiB": 0,
47   "DataWidthBits": 64,
48   "DeviceLocator": "PROC 1 DIMM 1",
49   "ErrorCorrection": "MultiBitECC",
50   "LogicalSizeMiB": 0,
51   "MemoryLocation": {
52     "Channel": 6,
53     "MemoryController": 2,
54     "Slot": 1,
55     "Socket": 1
56   }
57 }
58 ]
59 }
60 }

```


HPE iLO RESTful APIを使用したHPE向けインテルOptane Persistent Memoryの管理

HPE iLO RESTful APIを使用してpersistent memory modulesを管理するには、関連するコマンドを使用します。

コマンド	システムユーティリティオプション
PmmPerformance	パフォーマンス設定
BandwidthOptimized	帯域幅に最適化 (デフォルト)
Balanced	バランス
PmmFastGo	FastGo構成
Enabled	有効
Disabled	無効
Auto	自動 (デフォルト)
PmmAppDirectSnoopyMode	AppDirect用Snoopyモード
Enabled	有効
Disabled	無効 (デフォルト)
PmmMemModeSnoopyMode	メモリモード用Snoopyモード
Enabled	有効
Disabled	無効 (デフォルト)
VolatileMemCapacityPercent	揮発性メモリ容量
PersistentMemoryInterleaving	不揮発性メモリインターリーブ
Enabled	有効
Disabled	無効
ApplyDefaultNamespaces	デフォルトネームスペースの適用
Enabled	有効
Disabled	無効
SecurityFreezeLock	Security Freeze Lock
Enabled	有効
Disabled	無効
PmmSanitizeOperation	再起動時のサニタイズ/消去操作
NoAction	アクションなし
CryptoErase	暗号による消去
Overwrite	メディアの上書き
CryptoEraseOverwrite	暗号による消去の後、メディアの上書き
PmmSanitizePolicy	再起動時のサニタイズ/消去後のポリシー
SanitizeAndRebootSystem	サニタイズ/消去およびシステムの再起動
SanitizeAndShutdownSystem	サニタイズ/消去およびシステムの電源オフ
SanitizeAndBootToFirmwareUI	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
SanitizeToFactoryDefaults	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
SanitizeAllPmm	サニタイズ/消去操作の対象メモリ: システム内のすべてのpersistent memory modules
SanitizeProcXPmm1	サニタイズ/消去操作の対象メモリ: プロセッサXのすべてのpersistent memory modules
SanitizeProcXPmmY1	サニタイズ/消去操作の対象メモリ: プロセッサX DIMM Y

¹ ここで、XとYはプロセッサとDIMMスロット番号を表します。例: `SanitizeProc1Pmm4`。

HPE iLO RESTful APIを使用したPersistent Memoryモジュールのプロビジョニング

HPE iLO RESTful APIは、persistent memory modulesを構成するための仕組みを提供します。この構成を修正するには、メモリチャンクを作成するか削除します。構成後には再起動する必要があるため、HPE iLO RESTful APIはRedfishタスクを使用して、保留中および完成した構成操作を表します。

persistent memory modulesのプロビジョニングに必要なRESTアクション

構成	RESTアクション
100% App Directインターリーブ (プロセッサごとに、メモリチャンクが1つ必要です)	構成するメモリドメインに1つのメモリチャンクをPOSTします。タイプをPMEMに設定し、サイズ/パーセンテージを100%に設定するか、またはサイズをメモリドメインのpersistent memory modules容量の合計量に設定します。 インターリーブするには、すべてのpersistent memory modulesをメモリチャンクインターリーブセットに含めます。
100% App Direct非インターリーブ (persistent memory modulesごとに、メモリチャンクが1つ必要です)	構成するメモリドメインに複数のメモリチャンクをPOSTします。タイプをPMEMに設定し、パーセンテージの場合は100に設定し、サイズの場合はpersistent memory modulesの容量に設定します。 インターリーブされていない場合については、persistent memory modulesごとにインターリーブセットがありません。
100%揮発性 (プロセッサごとに、メモリチャンクが1つ必要です)	構成するメモリドメインに1つのメモリチャンクをPOSTします。タイプをPMEMに、サイズ/パーセンテージをゼロに設定します。 インターリーブするには、すべてのpersistent memory modulesをメモリチャンクインターリーブセットに含めます。
既存の構成をクリアする	既存のメモリチャンクを削除します。
保留中の構成をクリアする	TaskStateがNewで、かつTargetUriがメモリチャンクコレクションのいずれか1つである場合には、タスクを削除します。

例 : persistent memory modulesのプロビジョニング

RESTfulインターフェイスツールrawpostを使用した100% AppDirectインターリーブの構成

rawpost コマンドは、JSONファイルを取り込みます。次の例は、サーバーを構成するためのJSONファイルとバッチスクリプトを示しています。

Memorychunk-rawpost.txt

```
{
  "path": "/redfish/v1/Systems/1/MemoryDomains/PROClMemoryDomain/MemoryChunks",
  "body": {
    "AddressRangeType": "PMEM",
    "Oem": {
    "Hpe": {
      "MemoryChunkSizePercentage": 100
    }
  },
  "InterleaveSets": [{
    "Memory": {
      "@odata.id": "/redfish/v1/Systems/1/Memory/proclimm6/"
    }
  }, {
    "Memory": {
      "@odata.id": "/redfish/v1/Systems/1/Memory/proclimm7/"
    }
  }
  ]
}
```

Windowsバッチスクリプト

```
@echo off

set argC=0
for %%x in (*) do Set /A argC+=1
if %argC% LSS 3 goto :failCondition
goto :main

:failCondition
@echo Usage:
@echo ilorest-script-memory-remote.bat [URL] [ユーザー名] [パスワード]
goto :EOF

:main
@echo Logging in...
ilorest.exe --nologo login %1 -u %2 -p %3
@echo rawpost to Memory Chunk collection...
ilorest.exe --nologo rawpost memorychunk-rawpost.txt
@echo Note: Status of 202 is success.
```

pythonを使用した100% AppDirectインターリーブの構成

次の例では、リクエストライブラリを使用して、メモリチャンクを作成するためのPOSTリクエストを行います。再起動が必要であるため、タスクが生成されます。

(i) 重要:

コマンドラインからパスワードを送信するのは、安全ではありません。Hewlett Packard Enterpriseでは、パスワードをファイルに保存するなど、コマンドラインの使用にベストプラクティスを適用することをお勧めします。

```
import requests
from requests.auth import HTTPBasicAuth
import sys
import json

# server info from command line
if len(sys.argv) < 4:
    sys.stdout.write("\nPlease supply the URL, username and password:" \
    "\nUsage: python post_test.py https://ilourl username password\n")
    exit(-1)

iLO_URL = sys.argv[1]
username = sys.argv[2]
password = sys.argv[3]

# REST info
CHUNKS_URI = "/redfish/v1/Systems/1/MemoryDomains/PROClMemoryDomain/MemoryChunks"
headers = {'Content-type': 'application/json', 'Accept': 'application/json'}

MemoryChunk = {
    "AddressRangeType": "PMEM",
    "Oem": {
        "Hpe": {
            "MemoryChunkSizePercentage": 100
        }
    },
    "InterleaveSets": [
        {
            "Memory" : { "@odata.id": "/redfish/v1/Systems/1/Memory/procl1dim6/" }
        },
        {
            "Memory" : { "@odata.id": "/redfish/v1/Systems/1/Memory/procl1dim7/" }
        }
    ]
}

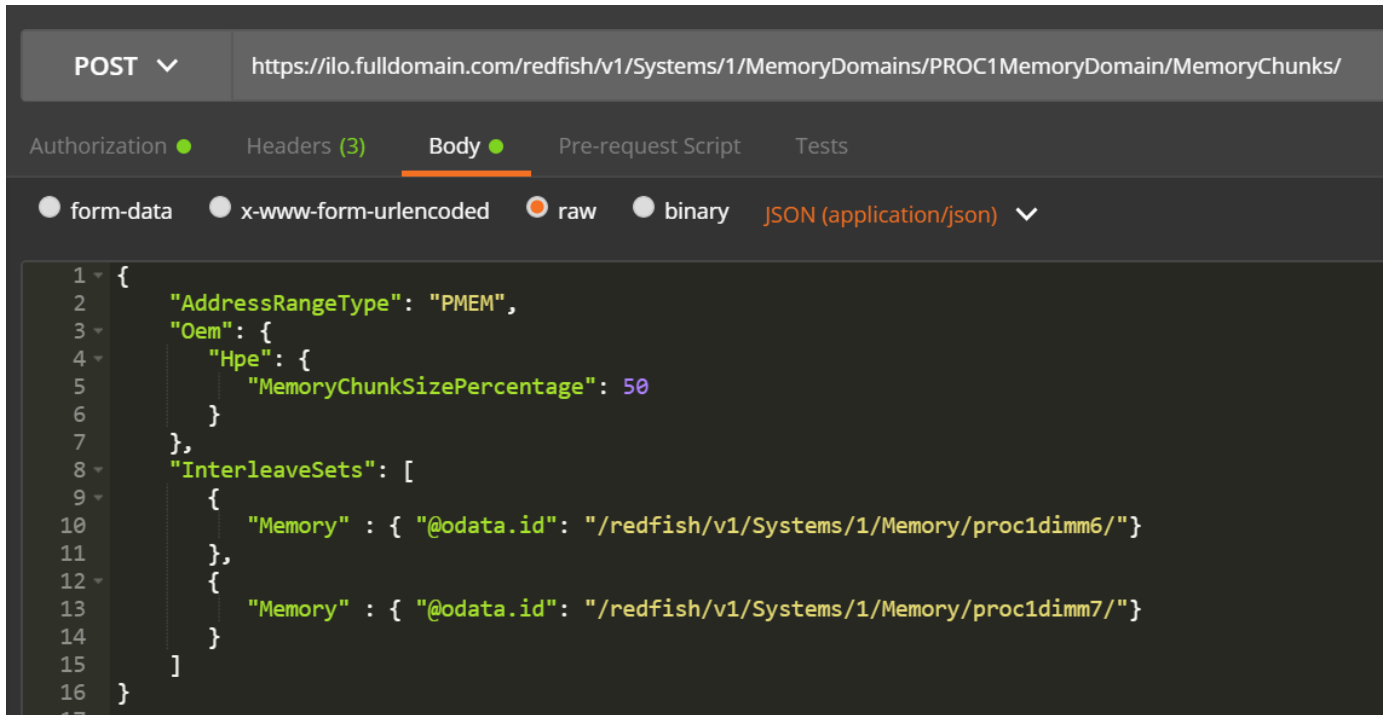
# POST to the URI until there is an error
sys.stdout.write("POST MemoryChunk...")
with requests.Session() as s:
    response = requests.post(iLO_URL + CHUNKS_URI, data=json.dumps(MemoryChunk),
    headers=headers, \
                                auth=HTTPBasicAuth(username, password), verify=False)
s.close()
if response.status_code != 202:
    sys.stdout.write('\n\nREST error; POST unsuccessful. Status={}'\
    '\n'.format(response.status_code))
else:
    output = json.loads(response.text)
    sys.stdout.write("\nPOST successful: {}".format(output.get("Name")))
```

Postmanを使用した100% AppDirectインターリーブの構成

動作: POST

PathとBody (生のJSON) は、[RESTfulインターフェイスツールrawpostを使用した100% AppDirectインターリーブの構成の例と同じです。](#)

ヘッダー: Accept: application/json, Content-Type: application/json



The screenshot shows a Postman interface for a POST request. The URL is `https://ilo.fulldomain.com/redfish/v1/Systems/1/MemoryDomains/PROC1MemoryDomain/MemoryChunks/`. The request body is a JSON object with the following structure:

```
1 {
2   "AddressRangeType": "PMEM",
3   "Oem": {
4     "Hpe": {
5       "MemoryChunkSizePercentage": 50
6     }
7   },
8   "InterleaveSets": [
9     {
10    "Memory" : { "@odata.id": "/redfish/v1/Systems/1/Memory/proc1dim6/" }
11    },
12    {
13    "Memory" : { "@odata.id": "/redfish/v1/Systems/1/Memory/proc1dim7/" }
14    }
15  ]
16 }
```

例：curlを使用したHPE向けインテルOptane Persistent Memoryの管理

各DIMMと persistent memory modulesは、プロセッサ番号とDIMMスロットで識別されるメモリオブジェクトで表されます。 persistent memory modulesの場合、属性は次の例のようになります。

```
curl --insecure --noproxy '*' --location --user 'user:password' --request GET --header 'Content-Type:application/json' --header 'Accept:application/json'
http://iloname.full.domain.name/redfish/v1/systems/1/Memory/procldimm11/
{
  "@odata.context": "/redfish/v1/$metadata#Memory.Memory",
  "@odata.etag": "W/\"EEEEAA879\"",
  "@odata.id": "/redfish/v1/Systems/1/Memory/procldimm11/",
  "@odata.type": "#Memory.v1_7_0.Memory",
  "AllocationAlignmentMiB": 1024,
  "AllocationIncrementMiB": 1024,
  "BaseModuleType": "PMM",
  "BusWidthBits": 72,
  "CacheSizeMiB": 0,
  "CapacityMiB": 514624,
  "DataWidthBits": 64,
  "DeviceID": "16721",
  "DeviceLocator": "PROC 1 DIMM 11",
  "ErrorCorrection": "MultiBitECC",
  "FirmwareApiVersion": "01.01.00.5253",
  "FirmwareRevision": "01.01.00.5253",
  "Id": "procldimm11",
  "LogicalSizeMiB": 0,
  "Manufacturer": "INTEL",
  "MemoryDeviceType": "DDR4",
  "MemoryLocation": {
    "Channel": 3,
    "MemoryController": 1,
    "Slot": 11,
    "Socket": 1
  },
  "MemoryMedia": [
    "Intel3DXPoint"
  ],
  "MemoryType": "IntelOptane",
  "Name": "procldimm11",
  "NonVolatileSizeMiB": 514048,
  "Oem": {
    "Hpe": {
      "@odata.context": "/redfish/v1/$metadata#HpeMemoryExt.HpeMemoryExt",
      "@odata.type": "#HpeMemoryExt.v2_1_0.HpeMemoryExt",
      "BaseModuleType": "PMM",
      "BlocksRead": 36366041872668,
      "BlocksWritten": 2603586169856,
      "DIMMStatus": "GoodInUse",
      "MinimumVoltageVoltsX10": 12,
      "PredictedMediaLifeLeftPercent": 100,
      "ProductName": "HPE Persistent Memory"
    }
  },
  "OperatingMemoryModes": [
    "Volatile",
    "PMEM"
  ],
  "OperatingSpeedMhz": 2666,
  "PartNumber": "835810-B21",
  "PersistentRegionNumberLimit": 48,
  "PersistentRegionSizeLimitMiB": 514048,
  "PersistentRegionSizeMaxMiB": 0,
```

```

"RankCount": 1,
"Regions": [
  {
    "MemoryClassification": "Volatile",
    "PassphraseEnabled": false,
    "RegionId": "15",
    "SizeMiB": 576
  },
  {
    "MemoryClassification": "ByteAccessiblePersistent",
    "PassphraseEnabled": false,
    "RegionId": "16",
    "SizeMiB": 514048
  }
],
"SecurityCapabilities": {
  "PassphraseCapable": true
},
"SerialNumber": "8089-A2-1834-000026B6",
"Status": {
  "Health": "OK",
  "State": "Enabled"
},
"SubsystemDeviceID": "2426",
"SubsystemVendorID": "35200",
"VendorID": "35200",
"VolatileRegionNumberLimit": 1,
"VolatileRegionSizeLimitMiB": 576,
"VolatileRegionSizeMaxMiB": 0,
"VolatileSizeMiB": 576
}

```

persistent memory modulesがインストールされた各プロセッサは、MemoryDomainsオブジェクトで表されます。

```

{
  "@odata.context": "/redfish/v1/$metadata#MemoryDomainCollection.MemoryDomainCollection",
  "@odata.etag": "W/\\"AA6D42B0\"",
  "@odata.id": "/redfish/v1/Systems/1/MemoryDomains/",
  "@odata.type": "#MemoryDomainCollection.MemoryDomainCollection",
  "Description": "Memory Domains Collection",
  "Name": "Memory Domains Collection",
  "Members": [
    {
      "@odata.id": "/redfish/v1/Systems/1/MemoryDomains/PROClMemoryDomain/"
    }
  ],
  "Members@odata.count": 1
}

```


RESTfulインターフェイスツール

RESTfulインターフェイスツールを使用して、HPE向けインテルOptane Persistent Memory 200シリーズを管理します。

RESTfulインターフェイスツールは、HPE iLOを通じてRESTful APIを使用してシステムを構成するCLIツールです。このツールは、サーバーでローカルに実行することも、サーバーを通じてHPE iLOでリモート接続することもできます。RESTfulインターフェイスツールは、対話型モードでもコマンドラインからでも実行できます。後者はスクリプト実行に便利です。

iLO RESTfulインターフェイスツールのコマンドの詳細については、<https://hewlettpackard.github.io/ilo-rest-api-docs/>にあるHPE iLO 5向けiLO RESTful APIドキュメントを参照してください。

RESTfulインターフェイスツールの起動

RESTfulインターフェイスツールでは、2つのモードをサポートします。

- 対話型モード
- スクリプトモード

このガイドに記載した例は、対話型モードで表示されています。スクリプトモードの使用も、同様に機能します。

手順

次のいずれかを実行します。

- ツールを対話型モードで起動するには、以下の操作を行います。

1. ilorest.exeビルドファイルを見つけて実行します。
2. サーバーにログインします。

```
iLOrest > login iLO_IP -u username -p password
```

3. 次のコマンドを実行します

```
iLOrest > command [options]
```

- ツールをスクリプトモードで起動するには、以下の操作を行います。

1. ilorest.exeファイルがあるフォルダに移動します。
2. サーバーにログインします。

```
C:\ilorest>ilorest.exe login iLO_IP -u username -p password
```

3. 以下のコマンドを実行します。

```
C:\ilorest>ilorest.exe command [options]
```

検出コマンド

このコマンドは、指定されたフラグに基づいて、persistent memory modulesの物理ビューと構成、およびApp Directインターリーブセットに関する情報を表示します。

```
showpmm [flag] [options]
```

検出コマンドの各種フラグ

このコマンドでは、次のフラグを使用できます。

フラグ	説明
<code>-D, --device</code>	物理的不揮発性メモリモジュールに関する情報を表示します。
<code>-C, --config</code>	persistent memory modulesの構成を表示します。
<code>-L, --logical</code>	不揮発性インターリーブセットを表示します。
<code>-M, --summary</code>	メモリサマリーを表示します。

デバイスの検出

このコマンドは、persistent memory modulesの物理ビューに関する情報を表示します。 `showpmm` コマンドをオプションなしで実行した場合、 `--device` フラグがデフォルトビューになります。

```
showpmm -D|--device [-I|--dimm=(DimmIDs)] [-j|--json] [-h|--help]
```

オプション

このコマンドでは、次のオプションを使用できます。

オプション	説明
<code>-h, --help</code>	コマンドのヘルプを表示します。
<code>-I, --dimm</code>	特定のpersistent memory modulesに関する情報を表示するには、DIMM IDのコンマ区切りリストを指定します。形式は <code>P@S</code> です。ここで、P = プロセッサ、S = スロットです。 以下に例を示します。 <code>1@1,1@12</code> 。
<code>-j, --json</code>	データをJSON形式で出力します。jsonフラグが指定されていない場合、デフォルトの表示形式はテーブルです。

例

- すべての物理的persistent memory modulesに関する情報を表示するには、次のコマンドを実行します。

```
iLOrest > showpmm -D
```

- プロセッサ1のスロット12とプロセッサ2のスロット1に取り付けられたpersistent memory modulesに関する情報を表示するには、次のコマンドを実行します。

```
iLOrest > showpmm -D --dimm=1@12,2@1
```

戻りデータ

戻りデータは、各persistent memory modulesの以下の属性を表形式で表示します。

属性	説明
Location	persistent memory modulesの物理的な位置。
Capacity	persistent memory modulesの使用可能容量。
Status	persistent memory modulesの全体的なヘルス。
DIMM Status	メモリモジュールのステータスおよびモジュールが使用中かどうか。
Life	デバイスの推定残存寿命（%単位）。
FWVersion	アクティブなファームウェアのリビジョン。

デバイス構成の検出

このコマンドは、`--config` フラグを使用して個別のpersistent memory modulesの構成を表示します。

```
showpmm -C|--config [-I|--dimm=(DimmIDs)] [-j|--json] [-h|--help]
```

オプション

このコマンドでは、次のオプションを使用できます。

オプション	説明
<code>-h, --help</code>	コマンドのヘルプを表示します。
<code>-I, --dimm</code>	特定のpersistent memory modulesに関する情報を表示するには、DIMM IDのコンマ区切りリストを指定します。形式は <code>P@S</code> です。ここで、 <code>P</code> = プロセッサ、 <code>S</code> = スロットです。 以下に例を示します。 <code>1@1,1@12</code> 。
<code>-j, --json</code>	データをJSON形式で出力します。jsonフラグが指定されていない場合、デフォルトの表示形式はテーブルです。

例

- すべてのpersistent memory modulesについて構成の詳細を表示するには、次のコマンドを実行します。

```
iLOrest > showpmm -C
```

- プロセッサ1のスロット12とプロセッサ2のスロット1に取り付けられたpersistent memory modulesについて、構成の詳細を表示するには、次のコマンドを実行します。

```
iLOrest > showpmm -C --dimm=1@12,2@1
```

- プロセッサ2のスロット12に取り付けられたpersistent memory modulesについて、構成の詳細をJSON形式で表示するには、次のコマンドを実行します。

```
iLOrest > showpmm -C --dimm=2@12 --json
```

戻りデータ

戻りデータは、ホストサーバーに取り付けられた各persistent memory modulesについて、以下の属性を表形式で表示します。

属性	説明
Location	persistent memory modulesの物理的な位置。
VolatileSize	persistent memory modules上の揮発性領域の合計サイズ。
PmemSize	persistent memory modules上の不揮発性領域の合計サイズ。
PmemInterleaved	不揮発性領域がインターリーブされているかどうかを示します。

不揮発性インターリーブ領域の検出

このコマンドは、persistent memory modulesの論理ビューである不揮発性インターリーブ領域に関する情報を表示します。

```
showpmm -L|--logical [-j|--json] [-h|--help]
```

オプション

このコマンドでは、次のオプションを使用できます。

オプション	説明
<code>-h, --help</code>	コマンドのヘルプを表示します。
<code>-j, --json</code>	データをJSON形式で出力します。jsonフラグが指定されていない場合、デフォルトの表示形式はテーブルです。

例

- 不揮発性インターリーブ領域に関する情報を表示するには、次のコマンドを実行します。

```
iLOrest > showpmm --logical
```

- 不揮発性インターリーブ領域に関する情報をJSON形式で表示するには、次のコマンドを実行します。

```
iLOrest > showpmm --logical --json
```

戻りデータ

戻りデータは、各不揮発性インターリーブセットの以下の属性を表形式で表示します。

属性	説明
TotalPmemSize	インターリーブされた不揮発性領域の合計サイズ。
DIMMids	インターリーブされたDIMMの物理的な位置。形式は <code>P@S</code> です。ここで、P = プロセッサインデックス、S = スロットインデックスです。

不揮発性メモリのサマリー

このコマンドは、`--summary` フラグを使用して、persistent memory modulesの構成サマリーを表示します。

```
showpmm -M|--summary [-j|--json] [-h|--help]
```

オプション

このコマンドでは、次のオプションを使用できます。

オプション	説明
<code>-h, --help</code>	コマンドのヘルプを表示します。
<code>-j, --json</code>	データをJSON形式で出力します。jsonフラグが指定されていない場合、デフォルトの表示形式はテーブルです。

例

- メモリのサマリーを表示するには、次のコマンドを実行します。

```
iLOrest > showpmm --summary
```

- メモリのサマリーをJSON形式で表示するには、次のコマンドを実行します。

```
iLOrest > showpmm --summary --json
```

戻りデータ

戻りデータは、各不揮発性インターリーブセットの以下の属性を表形式で表示します。

属性	説明
TotalCapacity	すべてのpersistent memory modulesの使用可能容量の総和。
TotalVolatileSize	各モジュール上の揮発性領域の合計サイズの総和。
TotalPmemSize	各モジュール上の不揮発性領域の合計サイズの総和。

保留中の構成を表示する

このコマンドは、有効にするには再起動が必要なpersistent memory modulesに関連する保留中の構成タスクを表示します。

```
showpmpendingconfig [-j|--json] [-h|--help]
```

オプション

このコマンドでは、次のオプションを使用できます。

オプション	説明
<code>-h, --help</code>	コマンドのヘルプを表示します。
<code>-j, --json</code>	データをJSON形式で出力します。jsonフラグが指定されていない場合、戻りデータはデフォルトで表形式で表示されます。

例

- 保留中の構成の詳細を表示するには、次のコマンドを実行します。

```
iLOrest > showpmpendingconfig
```

- 保留中の構成の詳細をJSON形式で表示するには、次のコマンドを実行します。

```
iLOrest > showpmpendingconfig --json
```

戻りデータ

戻りデータは、以下の属性を表形式で表示します。

属性	説明
Operation	実行するアクション。
PmemSize	すべての不揮発性領域の合計サイズ。
VolatileSize	すべての揮発性領域の合計サイズ。
DIMMids	インターリーブされたDIMMの物理的な位置。形式はP@Sです。ここで、P = プロセッサインデックス、S = スロットインデックスです。

事前定義された構成を適用する

このコマンドは、事前定義された構成をすべてのpersistent memory modulesに適用したり、既存または保留中の構成を削除したりします。

このコマンドは、3つのモードをサポートします。

- 100%メモリモード
- 100%不揮発性でインターリーブあり
- 100%不揮発性でインターリーブなし

```
Applypmmconfig (-C|--config =(configID)| -L|--list) [-f|--force] [-h|--help]
```

構成変更を反映させるには、再起動する必要があります。

オプション

このコマンドでは、次のオプションを使用できます。

オプション	説明
<code>-h, --help</code>	コマンドのヘルプを表示します。
<code>-C, --config</code>	適用するconfigIDを指定します。
<code>--list</code>	使用可能なすべてのconfigIDとその説明をリストします。
<code>-f, --force</code>	あらゆるプロンプトを自動的に受け入れて、構成を強制的に適用します。このオプションは、既存の構成または保留中の構成に対する警告を無視します。

例

- 使用可能なすべてのconfigIDとその説明のリストを表示するには、次のコマンドを実行します。

```
iLOrest > applypmmconfig --list
```

- すべてのpersistent memory modulesについて、100%メモリモード向けに構成するには、次のコマンドを実行します。

```
iLOrest > applypmmconfig -C MemoryMode -f
```

- すべてのpersistent memory modulesについて、100%不揮発性でインターリーブあり向けに構成するには、次のコマンドを実行します。

```
iLOrest > applypmmconfig -C PmemInterleaved -f
```

- すべてのpersistent memory modulesについて、100%不揮発性でインターリーブなし向けに構成するには、次のコマンドを実行します。

```
iLOrest > applypmmconfig -C PmemNotInterleaved -f
```

戻りデータ

戻りデータは、以下の属性を表形式で表示します。

属性	説明
Operation	実行するアクション。
PmemSize	すべての不揮発性領域の合計サイズ。
VolatileSize	すべての揮発性領域の合計サイズ。
DIMMids	インターリーブされたDIMMの物理的な位置。形式はP@Sです。ここで、P = プロセッサインデックス、S = スロットインデックスです。

ユーザー定義構成を適用する

このコマンドは、ユーザー定義構成をすべてのpersistent memory modulesに適用したり、既存または保留中の構成を削除したりします。

構成は、推奨されるメモリのキャッシュ比率に準拠している必要があります。推奨されていない比率を定義すると、システム性能に影響を及ぼす可能性があります、IMLにメッセージが生成されます。

```
provisionpmm [-m|--memory-mode=(0|%) ] [-i|--pmem-interleave=(On|Off)] [-p|--proc=(processorID)]  
[-f|--force] [-h|--help]
```

構成変更を反映させるには、再起動する必要があります。

オプション

このコマンドでは、次のオプションを使用できます。

オプション	説明
<code>-h, --help</code>	コマンドのヘルプを表示します。
<code>-m, --memory-mode</code>	揮発性メモリとして設定する総容量のパーセンテージを指定します。デフォルトは0%の揮発性メモリで、残量は不揮発性メモリとして構成されます。
<code>-i --pmem-interleave</code>	不揮発性メモリ領域をインターリーブする必要があるかどうかを示します。指定できる値は <code>on</code> または <code>off</code> です。
<code>-p --proc</code>	選択された構成が適用されるプロセッサ（プロセッサ番号のカンマ区切りリスト）を指定します。デフォルトはすべてのプロセッサです。
<code>-f, --force</code>	あらゆるプロンプトを自動的に受け入れて、構成を強制的に適用します。このオプションは、既存の構成または保留中の構成に対する警告を無視します。

例

- プロセッサ1と3で、すべてのpersistent memory modulesについて50%の揮発性メモリ、不揮発性インターリーブ領域なし向けに構成するには、次のコマンドを実行します。

```
iLOrest > provisionpmm -m 50 -i off -p 1,3
```

- すべてのpersistent memory modulesについて25%の揮発性メモリ、不揮発性インターリーブ領域あり向けに構成するには、次のコマンドを実行します。

```
iLOrest > provisionpmm -m 25 -i on
```

戻りデータ

戻りデータは、以下の属性を表形式で表示します。

属性	説明
Operation	実行するアクション。
PmemSize	すべての不揮発性領域の合計サイズ。
VolatileSize	すべての揮発性領域の合計サイズ。
DIMMids	インターリーブされたDIMMの物理的な位置。形式は <code>P@S</code> です。ここで、P = プロセッサインデックス、S = スロットインデックスです。

保留中の構成をクリアする

このコマンドは、保留中のすべての構成タスクをクリアします。

```
clearpmpendingconfig [-h|--help]
```

オプション

このコマンドでは、次のオプションを使用できます。

オプション	説明
-------	----

<code>-h, --help</code>	コマンドのヘルプを表示します。
-------------------------	-----------------

例

保留中の不揮発性メモリ構成タスクをすべて削除するには、次のコマンドを実行します。

```
iLOrest > clearpmpendingconfig
```

戻りデータ

戻りデータは、削除されたすべてのタスクのリストを出力します。

```
Deleted Task #701  
Deleted Task #702  
Deleted Task #703  
Deleted Task #704
```

推奨構成を表示する

このコマンドは、推奨される不揮発性メモリ構成を表示します。

```
showrecommendedpmmconfig [-h|--help]
```

オプション

このコマンドでは、次のオプションを使用できます。

オプション	説明
-------	----

<code>-h, --help</code>	コマンドのヘルプを表示します。
-------------------------	-----------------

例

推奨構成を表示するには、次のコマンドを実行します。

```
iLOrest > showrecommendedpmmconfig
```

戻りデータ

戻りデータは、以下の属性を表形式で表示します。

属性	説明
MemoryModeTotalSize	揮発性領域の合計サイズ。
PmemTotalSize	すべての不揮発性メモリ領域の合計サイズ。
CacheRatio	キャッシュ比率。

注記:

オペレーティングシステムから実行される ipmctl ツールでは、キー管理機能はサポートされません。persistent memory modules のキー管理を有効にしたり、暗号化の有効と無効を切り替えたりするには、UEFI システムユーティリティを使用してください。

ipmctlのインストール (Linux)

SUSE Linux Enterprise Server 12 SP4

ipmctlを使用するため、Hewlett Packard Enterpriseでは最新のopenSUSE事前ビルドパッケージを以下からダウンロードすることをお勧めします。

- https://build.opensuse.org/package/binaries/home:jhli/ipmctl/SLE_12_SP4
- https://build.opensuse.org/package/binaries/home:jhli/safeclib/SLE_12_SP4

SUSE Linux Enterprise Server 15

ipmctlを使用するため、Hewlett Packard Enterpriseでは最新のopenSUSE事前ビルドパッケージを以下からダウンロードすることをお勧めします。

- https://build.opensuse.org/package/binaries/home:jhli/ipmctl/SLE_15
- https://build.opensuse.org/package/binaries/home:jhli/safeclib/SLE_15

SUSE Linux Enterprise Server 15 SP1

ipmctlを使用するため、Hewlett Packard Enterpriseでは最新のopenSUSE事前ビルドパッケージを以下からダウンロードすることをお勧めします。

- https://build.opensuse.org/package/binaries/home:jhli/ipmctl/SLE_15
- https://build.opensuse.org/package/binaries/home:jhli/safeclib/SLE_15

Red Hat Enterprise Linux 7.6

ipmctlを使用するため、Hewlett Packard EnterpriseではCentOS7事前ビルドパッケージを以下からダウンロードすることをお勧めします。

- <https://copr.fedorainfracloud.org/coprs/jhli/ipmctl/>
- <https://copr.fedorainfracloud.org/coprs/jhli/safeclib/>

Red Hat Enterprise Linux 8.0

ipmctlを使用するため、Hewlett Packard EnterpriseではCentOS7事前ビルドパッケージを以下からダウンロードすることをお勧めします。

- <https://copr.fedorainfracloud.org/coprs/jhli/ipmctl/>
- <https://copr.fedorainfracloud.org/coprs/jhli/safeclib/>

ipmctlを使用したpersistent memory modules構成の表示

ipmctlは、persistent memory modulesの現在の構成を表示できます。

```
ipmctl show -dimm
DimmID | Capacity | LockState | HealthState | FWVersion
=====
0x0001 | 502.5 GiB | Disabled | Healthy | 2.2.0.1553
0x0011 | 502.5 GiB | Disabled | Healthy | 2.2.0.1553
0x0021 | 502.5 GiB | Disabled | Healthy | 2.2.0.1553

ipmctl show -d Capacity,MemoryCapacity,AppDirectCapacity,UnconfiguredCapacity -dimm 0x1
---DimmID=0x0001---
Capacity=502.5 GiB
MemoryCapacity=0 B
AppDirectCapacity=502.0 GiB
UnconfiguredCapacity=0 B
```

目標構成がすでに保留中であるかどうかを判断するには、次のコマンドを実行します。

```
ipmctl show -goal
```


ipmctlを使用した目標構成の削除

```
ipmctl delete -goal
```

システムは以前の目標構成設定を保持します。

ipmctlを使用したネームスペースの削除

```
ipmctl delete -namespace
```

ipmctlによるメモリモードの判断

次のコマンドを実行して、サーバーがメモリモードになっているかどうかを判断します。

```
ipmctl show -memoryresources
```

```
Capacity=3015.5 GiB  
MemoryCapacity=0.0 GiB  
AppDirectCapacity=3012.0 GiB  
UnconfiguredCapacity=3.3 GiB  
InaccessibleCapacity=0.0 GiB  
ReservedCapacity=0.2 GiB
```

コマンドがゼロ以外のMemoryCapacity値を返した場合、サーバーはメモリーモードです。

Persistent Memoryモジュールの再配置のガイドライン

以下の手順を実行する場合は、再配置のガイドラインを確認してください。

- persistent memory modulesをサーバーの別のDIMMスロットに再配置する場合。
- persistent memory modulesを別のサーバーに再配置する場合。
- サーバーのシステムボードを交換してからpersistent memory modulesを再び取り付ける場合。

(i) 重要:

データを保存しておく必要がある場合、Hewlett Packard Enterpriseでは、persistent memory modules上にあるすべてのユーザーデータについて手動でバックアップを取ってから、目標構成の変更または再配置の手順を実行することを強くお勧めします。

データを保持する必要がある場合にpersistent memory modulesまたはpersistent memory modulesのセットを再配置するための要件

- 再配置先のサーバーハードウェアは、再配置元のサーバーハードウェア構成と一致する必要があります。
- 再配置先サーバーのシステムユーティリティのすべての設定は、再配置元サーバーの元のシステムユーティリティの設定と一致する必要があります。
- 再配置元のサーバーでpersistent memory modulesを不揮発性メモリーインターリーブが有効な状態で使用している場合は、以下の手順を実行します。
 - 再配置先サーバーの同一のDIMMスロットにpersistent memory modulesを取り付けます。
 - インターリーブするセット全体（プロセッサのすべてのDIMMとpersistent memory modules）を再配置先のサーバーに取り付けます。

再配置に関していずれかの要件を満たせない場合は、以下の手順を実行します。

- persistent memory modulesを別のサーバーに再配置する前に、手動で不揮発性メモリのデータのバックアップを取ります。
- persistent memory modulesを別のサーバーに再配置します。
- 新しいサーバー上のpersistent memory modulesを使用する前に、すべてサニタイズします。

データを保持する必要がある場合に暗号化persistent memory modulesまたはpersistent memory modulesのセットを再配置するための要件

- persistent memory modulesがローカルキー管理で暗号化されている場合は、persistent memory modulesのパスワードをサーバーから手動で取得するか（ユーザーが生成したパスワードのみ）、パスワードファイルをUSBキーにエクスポートします。

Hewlett Packard Enterpriseでは、パスワードファイルをUSBキーにエクスポートすることをお勧めします。

- データを保持する必要がある場合は、persistent memory modulesまたはpersistent memory modulesのセットを再配置するための要件に従います。
- 次のいずれかを実行します。
 - persistent memory modulesがローカルキー管理で暗号化されている場合は、システムユーティリティでpersistent memory modulesのパスワードを手動で入力するか、パスワードファイルをUSBキーからインポートします。
 - persistent memory modulesがリモートキー管理で暗号化されている場合は、HPE iLOをキー管理サーバーに登録してpersistent memory modules上のデータへのアクセス権を付与します。

データを保持する必要がない場合にpersistent memory modulesまたはpersistent memory modulesのセットを再配置するための要件

- persistent memory modulesを新しい場所に取り付けた後、persistent memory modulesをサニタイズします。
- DIMMとpersistent memory modulesの取り付けガイドラインを確認します。
- persistent memory modulesを取り外すためのプロセスを確認します。
- persistent memory modulesを取り付けるためのプロセスを確認します。

- HPE向けインテルOptane Persistent Memoryのシステム設定を確認して、構成します。

persistent memory modulesデータの手動でのバックアップ

Hewlett Packard Enterpriseでは、persistent memory modulesにデータのバックアップを取ってから、目標構成の変更またはサービスの手順を実行することをお勧めします。

△ 注意:

静電気放電によって、電気回路などのコンポーネントが損傷することがあります。必ず、正しくアースを行ってからこの手順を開始してください。

△ 注意:

DIMMを正しく処理できない場合、DIMMコンポーネントとシステムボードのコネクタに損傷が発生する可能性があります。

この サーバー専用の手順については、Hewlett Packard EnterpriseのWebサイトにあるお使いの製品向けの サーバーメンテナンス&サービスガイドを参照してください。

- HPE ProLiant Gen10 Plusサーバー (<https://www.hpe.com/info/proliantgen10plus-docs>)
- HPE Synergy Gen10 Plusコンピュータモジュール (<https://www.hpe.com/info/synergy-docs>)

前提条件

DIMMまたはpersistent memory modulesの取り扱いまたは取り外しの前に、Persistent Memoryモジュールの取り扱いのガイドラインを参照してください。

手順

1. persistent memory modulesから別のストレージデバイス（SSD、ハードディスクドライブなど）にデータをコピーします。
2. persistent memory modulesの暗号化が有効にされている場合、無効にしてください。
詳しくは、キー管理の無効化を参照してください。
3. サーバーの電源を切ります。
 - a. OSのドキュメントの指示に従って、OSをシャットダウンします。
 - b. 電源ボタンを押して、サーバーをスタンバイモードにします。
サーバーがスタンバイモードに入ると、システム電源LEDがオレンジ色になります。
 - c. 電源コードを抜き取ります（ラックマウント型およびタワー型サーバー）。
4. 次のいずれかを実行します。
 - サーバーをラックから引き出します。
 - 必要に応じて、ラックからサーバーを取り外します。
 - サーバーまたはサーバーブレードをエンクロージャーから取り外します。
5. サーバーを平らで水平な面に置きます。
6. アクセスパネルを取り外します。
7. DIMMスロットにアクセスします。
8. 再配置または交換の手順を実行します。
9. DIMMスロットにアクセスするために取り外したコンポーネントをすべて取り付けます。
10. アクセスパネルを取り付けます。
11. サーバーをラックに取り付けます。
12. サーバーの電源を入れます。
13. ストレージデバイスからpersistent memory modulesにデータをコピーします。

DIMMまたはpersistent memory modulesの取り外し

△ 注意:

静電気放電によって、電気回路などのコンポーネントが損傷することがあります。必ず、正しくアースを行ってからこの手順を開始してください。

△ 注意:

DIMMを正しく処理できない場合、DIMMコンポーネントとシステムボードのコネクタに損傷が発生する可能性があります。

この サーバー専用 の手順については、Hewlett Packard EnterpriseのWebサイトにあるお使いの製品向けの サーバーメンテナンス&サービスガイドを参照してください。

- HPE ProLiant Gen10 Plusサーバー (<https://www.hpe.com/info/proliantgen10plus-docs>)
- HPE Synergy Gen10 Plusコンピュートモジュール (<https://www.hpe.com/info/synergy-docs>)

前提条件

- DIMMまたはpersistent memory modulesの取り扱いまたは取り外しの前に、Persistent Memoryモジュールの取り扱いのガイドラインを参照してください。
- persistent memory modulesが暗号化されている場合は、故障したpersistent memory modulesを交換する前に、暗号化を無効にする必要があります。

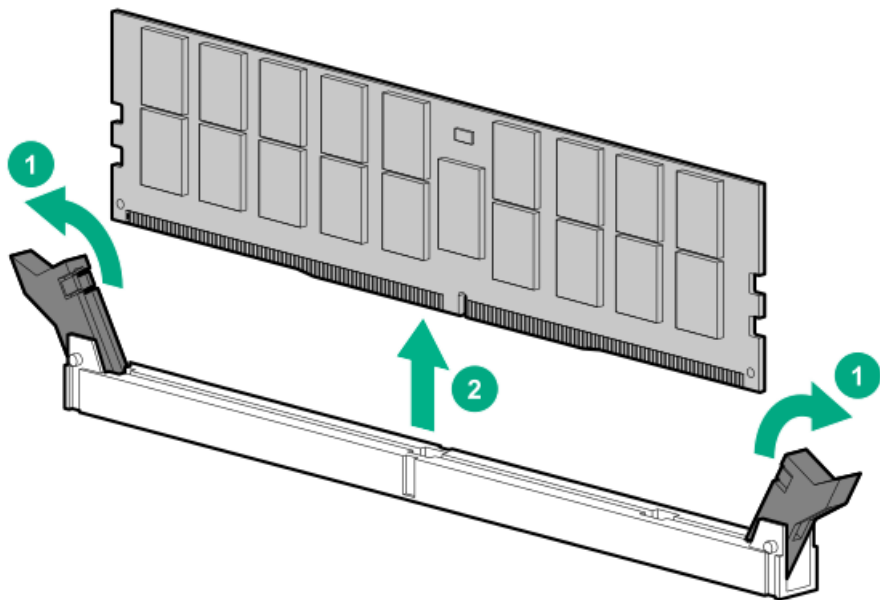
手順

1. persistent memory modulesの暗号化が有効にされている場合、無効にしてください。

詳しくは、キー管理の無効化を参照してください。

2. サーバーの電源を切ります。
 - a. OSのドキュメントの指示に従って、OSをシャットダウンします。
 - b. 電源ボタンを押して、サーバーをスタンバイモードにします。

サーバーがスタンバイモードに入ると、システム電源LEDがオレンジ色になります。
 - c. 電源コードを抜き取ります（ラックマウント型およびタワー型サーバー）。
3. 次のいずれかを実行します。
 - サーバーをラックから引き出します。
 - 必要に応じて、ラックからサーバーを取り外します。
 - サーバーまたはサーバーブレードをエンクロージャーから取り外します。
4. サーバーを平らで水平な面に置きます。
5. アクセスパネルを取り外します。
6. DIMMスロットにアクセスします。
7. DIMMまたはpersistent memory modulesを取り外します。



システムボードの交換

persistent memory modulesを暗号化せずに、サーバーのシステムボードを交換する方法の概要については、この手順を参照してください。

このサーバー専用の手順については、Hewlett Packard EnterpriseのWebサイトにあるお使いの製品向けのサーバーメンテナンス&サービスガイドを参照してください。

- HPE ProLiant Gen10 Plusサーバー (<https://www.hpe.com/info/proliantgen10plus-docs>)
- HPE Synergy Gen10 Plusコンピュートモジュール (<https://www.hpe.com/info/synergy-docs>)

前提条件

- Persistent Memoryモジュールの再配置のガイドラインに従います。
- persistent memory modulesが暗号化されている場合は、次のいずれかを参照してください。
 - ローカルキー管理で暗号化されたpersistent memory modulesの移行
 - リモートキー管理で暗号化されたpersistent memory modulesの移行

手順

1. サーバーの電源を切ります。
2. 次のいずれかを実行します。
 - サーバーをラックから引き出します。
 - 必要に応じて、ラックからサーバーを取り外します。
 - サーバーまたはサーバーブレードをエンクロージャーから取り外します。
3. サーバーを平らで水平な面に置きます。
4. DIMMスロットにアクセスします。
5. 各DIMMとpersistent memory modulesが取り付けられているスロットの位置をメモした後、サーバーからコンポーネントを取り外します。
6. システムボードから残りのコンポーネントを取り外した後、システムボードを取り外します。
7. スペアのシステムボードを取り付けます。

8(i) **重要:** 故障したシステムボードで使用されていたのと同じ構成を持つすべてのコンポーネントを取り付けます。

故障したシステムボードから取り外したすべてのコンポーネントを取り付けます。

DIMMとpersistent memory modulesを古いシステムボードと同じ場所に必ず取り付けてください。

9. アクセスパネルを取り付けます。
10. サーバーの電源を入れます。
11. 最新のドライバーを確実に使用するために、オプションカードや内蔵デバイスを含むすべてのファームウェアが同じバージョンにアップデートされていることを確認してください。
12. 必要に応じて、サーバーのシリアル番号と製品IDを再入力します。

詳しくは、Hewlett Packard Enterpriseの次のWebサイトにあるサーバーのメンテナンス&サービスガイドを参照してください。

- HPE ProLiant Gen10 Plusサーバー (<https://www.hpe.com/info/proliantgen10plus-docs>)
- HPE Synergy Gen10 Plusコンピュートモジュール (<https://www.hpe.com/info/synergy-docs>)

persistent memory modulesの移行

(i) 重要:

データを保存しておく必要がある場合、Hewlett Packard Enterpriseでは、persistent memory modules上にあるすべてのユーザーデータについて手動でバックアップを取ってから、目標構成の変更または再配置の手順を実行することを強くお勧めします。

ローカルキー管理で暗号化されたpersistent memory modulesの移行

このプロセスを使用して、ローカルキー管理で暗号化されたpersistent memory modulesを移行します。リモートキー管理が有効になっている場合は、リモートキー管理で暗号化されたpersistent memory modulesの移行を参照してください。

前提条件

- 暗号化されたpersistent memory modulesを移行する前に、Persistent Memoryモジュールの再配置のガイドラインをよく読んで、従ってください。
- 暗号化された persistent memory modulesを移行するには、次のいずれかを実行して、暗号化された persistent memory modulesのパスワードを入手する必要があります。
 - パスワードファイルをUSBキーにエクスポートします（推奨）。
 - サーバーの各persistent memory modulesのパスワードを手動で取得し記録します。

手順

1. persistent memory modulesの移行元となるサーバー上で、POST中にF9キーを押して、システムユーティリティにアクセスします。
2. パスワードファイルをUSBキーにエクスポートするため、次の操作を行います。
 - 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 > デバイス暗号化エクスポートオプションを選択します。
 - b. パスワードを一時パスフレーズ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persistent memory modulesを復元するときに、入力する必要があります。
 - c. ファイルを選択し、USBキーの場所を参照します。
 - d. 暗号化設定のエクスポートを選択して、ファイルを作成しエクスポートします。
3. persistent memory modulesのパスワードを手動で記録するには、次の操作を行います。
 - 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 > デバイス暗号化のステータスを選択します。
 - b. 各persistent memory modulesの隣に表示されているパスワードと場所を記録します。

移転後に暗号化されたpersistent memory modulesを復元するときに、同じ場所にこれらのパスワードを入力する必要があります。
4. サーバーの電源を切ります。
5. 各DIMMとpersistent memory modulesが取り付けられているスロットの位置をメモした後、サーバーからコンポーネントを取り外します。
6. DIMMとpersistent memory modulesを新しいサーバーまたは新しいシステムボードに取り付けます。

DIMMとpersistent memory modulesを取り付けるときは、必ず再配置のガイドラインに従ってください。
7. サーバーの電源を入れます。
8. POST中にF9キーを押してシステムユーティリティにアクセスします。
9. 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 > デバイス暗号化リカバリオプションを選択します。
10. USBキーにエクスポートしたファイルを使用してpersistent memory modulesのロックを解除するには、次の操作を行います。
 - a. USBキーを接続します。
 - b. USBデバイスからのパスフレーズのリストアを選択します。
 - c. ファイルのエクスポート時に作成された一時パスフレーズを入力します。
 - d. ファイルを選択し、USBキー上のパスワードファイルの場所に移動します。

- e. 暗号化設定のリストアを選択して、ファイルをインポートします。
11. パスワードが手動で記録されたpersistent memory modulesのロックを解除するには、次の操作を行います。
- a. デバイスを手動でロック解除を選択します。
 - b. persistent memory modulesを選択し、パスフレーズを入力します。
 - c. Enterを押します。
 - d. リストに記載されている暗号化されたpersistent memory modulesそれぞれについて、この手順を繰り返します。
12. 変更を保存して終了するには、F12キーを押します。

リモートキー管理で暗号化されたpersistent memory modulesの移行

このプロセスを使用して、リモートキー管理で暗号化されたpersistent memory modulesを移行します。ローカルキー管理が有効になっている場合は、ローカルキー管理で暗号化されたpersistent memory modulesの移行を参照してください。

前提条件

暗号化されたpersistent memory modulesを移行する前に、Persistent Memoryモジュールの再配置のガイドラインをよく読んで、従ってください。

手順

1. HPE iLOにログインします。
2. ナビゲーションツリーで管理をクリックして、キーマネージャータブをクリックします。
3. 次のキーマネージャースerverのエントリをメモします。
この情報は、移行を完了するために必要です。
 - プライマリキーサーバーアドレス
 - プライマリキーサーバーポート
 - セカンダリキーサーバーアドレス（入力された場合）
 - セカンダリキーサーバーポート（入力された場合）
4. キーマネージャ構成の下のグループ名をメモします。
この情報は、移行を完了するために必要です。
5. サーバーの電源を切ります。
6. 各DIMMとpersistent memory modulesが取り付けられているスロットの位置をメモした後、サーバーからコンポーネントを取り外します。
7. DIMMとpersistent memory modulesを新しいサーバーまたは新しいシステムボードに取り付けます。
DIMMとpersistent memory modulesを取り付けるときは、必ず再配置のガイドラインに従ってください。
8. サーバーの電源を入れます。
9. HPE iLOにログインします。
10. ナビゲーションツリーで管理をクリックして、キーマネージャータブをクリックします。
11. キーマネージャサーバーの下にある次の項目を入力します。
この情報は、古いサーバーから記録された情報と一致していなければなりません。
 - プライマリキーサーバーアドレス
 - プライマリキーサーバーポート
 - セカンダリキーサーバーアドレス（入力された場合）
 - セカンダリキーサーバーポート（入力された場合）
12. キーマネージャ構成の下のグループ名を入力します。
この項目は、古いサーバーから記録されたグループ名と一致していなければなりません。
13. サーバーを再起動します。
14. POST中にF9キーを押してシステムユーティリティにアクセスします。
15. 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。
16. キー管理メニューからリモートを選択します。
17. F12キーを押して変更を保存し、終了します。

サニタイズポリシー

再起動時のサニタイズ/消去後のポリシーに対するサニタイズオプションのシステムユーティリティのメニュー項目には、次のオプションがあります。

- サニタイズ/消去およびシステムの再起動 - このポリシーは以下のシナリオで使用します。
 - 新しいpersistent memory modulesをサーバーに追加した後。
 - エラーが原因でpersistent memory modulesがマップから除外され、再度persistent memory modulesを使用したい場合。
 - 以前に別のサーバーで使用したpersistent memory modulesを新しいサーバーに移動した後。
新しいサーバーのすべてが以前のサーバーと完全に一致する場合は、persistent memory modulesをサニタイズする必要はありません。
- サニタイズ/消去およびシステムの電源オフ - このポリシーは以下のシナリオで使用します。
 - persistent memory modulesの運用廃止。
 - persistent memory modulesの撤去（データを保持する必要がない場合に別のサーバーに移動する）。
- 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 - このポリシーを使用して、persistent memory modules内のデータが同じ方法で解釈されなくなるようにBIOS/プラットフォーム構成（RBSU）設定を変更します。例としては、不揮発性メモリのインターリーブがあります。
- 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 - このポリシーは、persistent memory modulesの使用を中止するか、またはpersistent memory modulesをHewlett Packard Enterpriseに返却する（サービス交換）場合に使用します。

サニタイズポリシーと1つ以上のpersistent memory modulesを選択すると、システムは、すべてのウォームリセット要求をコールドリセットにアップグレードします。最初のコールドリセットでは、以下のことを行います。

1. プロセッサの書き込みバッファにまだ保留している書き込みデータをDRAMにフラッシュします。
2. persistent memory modulesをマップアウトします。
3. サニタイズコマンドをpersistent memory modulesに送信します。

サニタイズポリシー

サニタイズコマンドが完了した後のシステムの動作：

サニタイズ/消去およびシステムの再起動	サニタイズコマンドが完了した後、サーバーを再起動します。
サニタイズ/消去およびシステムの電源オフ	サニタイズコマンドの完了後に電源オフ。
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	別のコールドリセットを実行して、再度persistent memory modulesでマッピング。
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	サニタイズコマンドの完了後に電源オフ。

サニタイズガイドライン

記載されているすべてのシナリオでは、DIMMおよびpersistent memory modulesの取り付けガイドラインが順守されていることを想定しています。

persistent memory modulesを使用する前にサニタイズが必要なシナリオ

- 新しいpersistent memory modulesをシステムに追加した場合は、新しいpersistent memory modulesを使用する前にそのpersistent memory modulesをサニタイズします。
- 不揮発性メモリのインターリーブが有効に設定されたサーバーからpersistent memory modulesを取り外すときは、persistent memory modulesが取り外されたプロセッサのすべてのpersistent memory modulesをサニタイズします。
- 以前使用していたpersistent memory modulesをシステムに追加した場合は、次のいずれかを実行します。
 - 不揮発性メモリのインターリーブ設定が有効に設定されている場合は、persistent memory modulesを使用する前にそのプロセッサのすべてのpersistent memory modulesをサニタイズします。
 - 不揮発性メモリのインターリーブ設定が無効に設定されている場合は、サニタイズは不要です。
- 不揮発性メモリのインターリーブ設定を変更したときは、サーバーのすべてのpersistent memory modulesをサニタイズします。

サニタイズが不要な可能性があるシナリオ

これらのシナリオでは、データを保持しながら、新しいサーバーでそのデータにアクセスできるように、persistent memory modulesを移行する方法について説明します。

- persistent memory modulesが、ハードウェアとシステムユーティリティの両方の設定で新しいサーバーに対応する別のサーバーで使用されていた。
- 新しいサーバーの、元のサーバー内の同じDIMMスロットにpersistent memory modulesが取り付けられている。
- 不揮発性メモリのインターリーブが、有効に設定されている状態でpersistent memory modulesが使用される場合は、インターリーブセットのすべてのpersistent memory modulesを新しいサーバーの同じDIMMスロットに取り付けます。
- 不揮発性メモリのインターリーブが、無効に設定されている状態でpersistent memory modulesが使用される場合は、persistent memory modulesをサーバーの任意のスロットに取り付けます。

UEFIシステムユーティリティを使用したサニタイズ

persistent memory modules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 > PMEM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：
 - アクションなし
 - 暗号による消去
 - メディアの上書き
 - 暗号による消去の後、メディアの上書き
 - 再起動時のサニタイズ/消去後のポリシー：
 - 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persistent memory modules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persistent memory modules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persistent memory modules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persistent memory modules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。

HPE iLO RESTful APIを使用したサニタイズ

HPE iLO RESTful APIを使用してpersistent memory modulesをサニタイズするには、関連するコマンドを使用します。

コマンド	システムユーティリティオプション
PmmSanitizeOperation	再起動時のサニタイズ/消去操作
NoAction	アクションなし
CryptoErase	暗号による消去
Overwrite	メディアの上書き
CryptoEraseOverwrite	暗号化による消去およびメディアの上書き
PmmSanitizePolicy	再起動時のサニタイズ/消去後のポリシー
SanitizeAndRebootSystem	サニタイズ/消去およびシステムの再起動
SanitizeAndShutdownSystem	サニタイズ/消去およびシステムの電源オフ
SanitizeAndBootToFirmwareUI	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
SanitizeToFactoryDefaults	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
SanitizeAllPmm	サニタイズ/消去操作の対象メモリ: システム内のすべてのpersistent memory modules
SanitizeProcXPmm1	サニタイズ/消去操作の対象メモリ: プロセッサXのすべてのpersistent memory modules
SanitizeProcXPmmY1	サニタイズ/消去操作の対象メモリ: プロセッサX DIMM Y

¹ ここで、XとYはプロセッサとDIMMスロット番号を表します。例: `SanitizeProc1Pmm4`。

ipmctlを使用したサニタイズ

ipmctlツールを使用して、以下の条件下にある persistent memory modulesをサニタイズできます。

- Persistent Memoryモジュールは、次のどの状態にあってもなりません。
 - ロック解除、フリーズ
 - 無効、フリーズ
 - 超過
- 指定されたpersistent memory modulesに関連付けられているネームスペースがあれば、最初に削除される必要があります。

サーバーに取り付けられたすべてのpersistent memory modules上の不揮発性データを消去するには、次のコマンドを実行します。

```
ipmctl delete -dimm
```

パスワードを紛失したpersistent memory modulesの撤去

persistent memory modulesのパスワードが不明であり、保存されているデータの保持またはデータへのアクセスが必要な場合は、暗号による消去オプションでpersistent memory modulesをサニタイズしてモジュールを再利用します。

このプロセスでは、persistent memory modulesに以前保存されたデータの保持またはデータへのアクセスを行うことはできません。ハードウェアの再利用を可能にするのみです。

詳しくは、[persistent memory modulesのサニタイズ](#)を参照してください。

persistent memory modulesファームウェアのアップデート

persistent memory modulesのファームウェアをアップデートするには、次のいずれかの方法を使用します。

- Service Pack for ProLiant (SPP) – Service Pack for ProLiantクイックスタートガイド (<https://www.hpe.com/info/spp/documentation>) を参照してください。

SPPをダウンロードする場合は、Hewlett Packard EnterpriseのWebサイト (http://www.hpe.com/jp/servers/spp_dl) を参照してください。

- HPEオンラインフラッシュコンポーネント

HPE向けインテルOptane Persistent Memory 200シリーズのLinuxのサポート

Linuxは、次の表に示すデバイスタイプを使用して、persistent memory modulesを提示します。

Linuxデバイスパス

パス	名前	タイプ	メモ
/dev/pmem*	ファイルシステムDAXがある 不揮発性メモリ	ブロック型デバイス	
/dev/pmem*s	セクターアトミック	ブロック型デバイス	
/dev/dax*. *	デバイスDAX	キャラクター型デバイス	<ul style="list-style-type: none">• 専用ソフトウェア向け• ファイルシステムをサポートしない

次の表は、不揮発性メモリドライバーによって使用されるデバイスの中間層を示したものです。

Linuxドライバーのスタックデバイス

タイプ	パス	説明
nmem	/sys/bus/nd/devices/nmem*	persistent memory modulesを表します
領域	/sys/bus/nd/devices/region*	インターリーブされたpersistent memory modulesのセットまたは単一のpersistent memory modulesのいずれかによって表されるメモリ領域を表します。
ブロック型デバイス	/sys/block/pmem*	ファイルシステムDAXと通常のブロック型デバイスを表します。
デバイスDAX	/sys/class/dax/dax*	デバイスDAXのキャラクター型デバイスを表します。

nmemデバイス

Linuxでは、persistent memory modulesはnmemデバイスで表されます。

nmemデバイスのプロパティ

nmemデバイスには、次のようないくつかのプロパティがあります。

- Dev - Linuxドライバーのデバイス名 (nmem0など)。
- ID - 物理ラベルに印字されているシリアル番号。
- ハンドル - デバイスのシステムファームウェアによって生成された一意の識別子。
- Phys_id - 16進数でエンコードしたDIMMの位置。
- セキュリティ - persistent memory modulesのセキュリティ状態 (無効、ロック解除、ロック、フリーズ、または上書き)。

nmemデバイスの一覧表示

persistent memory modulesとそのプロパティのリストを表示するには、次のコマンドを実行します。

```
ndctl list --human --dimms
[
  {
    "dev": "nmem1",
    "id": "8089-a2-1839-12345678",
    "handle": "0x11",
    "phys_id": "0x27",
    "security": "disabled"
  },
  {
    "dev": "nmem3",
    "id": "8089-a2-1839-87654321",
    "handle": "0x101",
    "phys_id": "0x24",
    "security": "disabled"
  }
]:
]
```

領域

領域とは、1つ以上の persistent memory modulesから提示されるシステムメモリの一部のことです。領域は、次のいずれかで構成されます。

- 1つのインターリーブセット（各persistent memory modulesが同じ容量に貢献する）
- 単一のpersistent memory modules

Linuxでは、領域は目標構成によって設定されます。領域の名前はregionRRです。ここでRRは0以降の任意の数です。領域の最大数は、persistent memory modulesまたはインターリーブセットの個数です。

領域のプロパティ

領域デバイスには、いくつかのプロパティがあります。

- Dev - (このブート用の) 領域の識別子。
- Size - この領域によって提示された不揮発性メモリの容量。
- Available_size - 現在ネームスペースに割り当てられていないサイズ。
- Max_available_extent - ネームスペースに割り当てることができる最大連続サイズ。
- Type - 常に不揮発性メモリです。
- Numa_node - 領域の numa_node ID。このIDは、numactlを使用して、この領域に近い複数のプロセッサをバインドするために使用できます。
- Iset_id - 領域の世界的に一意的ID。

1組のpersistent memory modulesが他のサーバーに移動されても、このIDは変わらず、persistent memory modulesのフルセットは必ず一緒のままになります。

- Persistence_domain - HPE ProLiantおよびHPE Synergy Gen10 Plusサーバー製品では、常にメモリコントローラーに設定されます。

注記:

SUSE Linux Enterprise Server 15 GAは、サーバーに取り付けられた各persistent memory modulesに追加の領域番号を割り当てます。そして、これらには最も低い番号が割り当てられます。Hewlett Packard Enterpriseでは、この表記を修正するカーネルアップデートSUSE-SU-2019:0224-1をインストールすることをお勧めします。

領域の一覧表示

領域とそのプロパティのリストを表示するには、次のコマンドを実行します。

```
ndctl list --human --regions
[
  {
    "dev":"region1",
    "size":"502.00 GiB (539.02 GB)",
    "available_size":0,
    "max_available_extent":0,
    "type":"pmem",
    "numa_node":0,
    "iset_id":"0x12ccda9021308a22",
    "persistence_domain":"memory_controller"
  },
  {
    "dev":"region3",
    "size":"502.00 GiB (539.02 GB)",
    "available_size":"374.00 GiB (401.58 GB)",
    "max_available_extent":"374.00 GiB (401.58 GB)",
    "type":"pmem",
    "numa_node":0,
    "iset_id":"0x5ed6da900f318a22",
    "persistence_domain":"memory_controller"
  }
]:
]
```

ネームスペース

ネームスペースは、領域の一部です。Linuxでは、ネームスペースはndctlで管理されます。

ネームスペースは、namespace<regionRR>.<NN>のように番号が付けられます。ここで、

- regionRRは、ネームスペースの作成元の領域デバイス名です。
- NNはネームスペースの番号で、0~63の範囲です。

次の表に、Linuxカーネルの不揮発性メモリドライバでサポートされているネームスペースの種類を示します。

モード	名前	OS	説明
raw	未構成時	すべて	<ul style="list-style-type: none">• /dev/pmem0ブロックデバイスを作成します。• DAXオプションなしで、すべてのファイルシステムをサポートします。• BIOS/プラットフォーム構成 (RBSU) で、デフォルトネームスペースの適用が有効に設定されている場合、未構成の不揮発性メモリを提示します。
sector	セクターアトミック	すべて	<ul style="list-style-type: none">• /dev/pmem0sブロックデバイスを作成します。• DAXオプションなしで、すべてのファイルシステムをサポートします。• セクター (512バイトや4,096バイトなど) の原子性を提供するために使用されるブロック変換テーブル。• ブロックへの書き込み中に電源が失われると、以前の内容に戻ります。
fsdax	ファイルシステムDAX	Linux	<ul style="list-style-type: none">• /dev/pmem0ブロックデバイスを作成します。• DAXオプションを提供するファイルシステム (ext4とxfs) をサポートします。• -o daxオプションを指定してマウントすると、アプリケーションはI/Oパスからページキャッシュを削除して、不揮発性メモリに直接アクセスできます。
devdax	デバイスDAX	Linux	<ul style="list-style-type: none">• ソフトウェアのオーバーヘッドを最小限に抑えるために、不揮発性メモリ対応アプリケーション用に/dev/dax0.0キャラクター型デバイスを作成します。• ファイルシステムはサポートされていません。• read()とwrite()のサポートはなく、mmap()のみです。

ネームスペースのプロパティ

ネームスペースデバイスには、いくつかのプロパティがあります。

- Dev - 領域名に基づく、このネームスペースの一意のデバイス名 (namespace6.0など)。
- Mode - raw、sector、fsdax、またはdevdax。
- Size - このネームスペースの容量。
- uuid - ネームスペースの世界的に一意の識別子。

ネームスペースのデバイス名と領域名は、他の領域の存在次第で変わる可能性があるため、それらをスクリプトで使用するのには安全ではありません。

- Sector - 論理ブロックサイズ。
- Blockdev - このネームスペースを使用している/dev/pmemNNブロックデバイスの名前 (存在する場合)。
- Chardev - このネームスペースを使用している/dev/daxNN.MMキャラクター型デバイスの名前 (存在する場合)。
- Numa_node - ネームスペースのnuma_node ID。このIDは、numactlを使用して、このネームスペースに近い複数のプロセッサをバインドするために使用できます。

ネームスペースの作成

ネームスペースを作成するときには、サイズと領域のオプションを指定できます。サイズを指定しない場合、最大サイズが割り当てられます。

例：領域0から始まるfsdaxネームスペース全体を作成するには、次のコマンドを実行します。

```
$ sudo ndctl create-namespace -m fsdax -r region0
```

例：領域1から始まる32 GBの未定義のネームスペースを作成するには、次のコマンドを実行します。

```
$ sudo ndctl create-namespace -m raw -s 32G -r region1
```


すべての名前スペースを一覧表示する

すべての名前スペースを一覧表示するには、次のコマンドを実行します。

```
$ ndctl list
```

名前スペースとそのプロパティの一覧を表示するには、次のコマンドを実行します。

```
# ndctl list --human --namespaces
[
  {
    "dev": "namespace1.0",
    "mode": "fsdax",
    "map": "dev",
    "size": "494.15 GiB (530.59 GB)",
    "uuid": "ff189419-de3d-406d-8f7f-812696a25ca8",
    "raw_uuid": "24841e1f-ab7e-43e5-a2fd-695af39bb682",
    "sector_size": 512,
    "blockdev": "pmem1",
    "numa_node": 0
  },
  {
    "dev": "namespace3.0",
    "mode": "raw",
    "size": "128.00 GiB (137.44 GB)",
    "uuid": "ba1733ea-782a-441a-91a3-e9c0af088752",
    "sector_size": 512,
    "blockdev": "pmem3",
    "numa_node": 0
  },
  :
]
```

ネームスペースモードの変更

このコマンドを実行して、既存のネームスペースのネームスペースモードを変更します。

例：既存のnamespace0.0を“fsdax”に変更するには、次のコマンドを実行します。

```
$ sudo ndctl create-namespace -f -e namespace0.0 -m fsdax
```

△ 注意：ネームスペースモードを変更すると、既存のデータがすべて破棄されます。モードを変更する前に、すべてのデータをバックアップしてください。

ネームスペースの削除

ネームスペースを削除するには、次のコマンドを実行します。

```
$ sudo ndctl disable-namespace namespace0.0  
$ sudo ndctl destroy-namespace --force namespace0.0
```

△ 注意: ネームスペースを削除すると、既存のデータがすべて破棄されます。ネームスペースを削除する前に、すべてのデータをバックアップしてください。

pmemデバイスの初期化

サーバーに取り付けられたpersistent memory modulesの個数と容量次第では、ログインプロンプトが表示されるまでに、persistent memory modulesが初期化を完了していない可能性があります。

初期化が完了するまで待ちます。 `list` コマンドを使用して、persistent memory modulesが初期化を完了したことを確認できます。

```
ndctl list
```

このコマンドは、persistent memory modulesが初期化を完了したときのネームスペースのリストを返します。このコマンドが情報をすぐに返さない場合、初期化はまだ進行中です。

システムのメモリ容量の表示

`free` コマンドは、システム内のメモリ容量を表示します。なお、プロセッサのページテーブル用に予約されているメモリは含みません。persistent memory modulesの容量が大きいと、これはかなり目立つようになります。

`-h` (または `--human`) オプションは、容量を人間が読み取れる形式で単位を付けて報告します (デフォルト単位は KiB です)。

```
$ free -h
```

	total	used	free	shared	buff/cache	available
Mem:	62G	423M	59G	2.1M	2.9G	61G
Swap:	7.8G	0B	7.8G			

数値は切り捨てられて丸められます。単位はGとして表示されますが、Giとして解釈してください。

`-b` オプションは、正確なサイズをバイト単位で出力します。

```
$ free -b
```

	total	used	free	shared	buff/cache	available
Mem:	67403063296	444485632	63883395072	2240512	3075182592	66085310464
Swap:	8388603904	0	8388603904			

ファイルシステム

pmemブロックデバイスには、任意のファイルシステム（ext4、xfs、btrfsなど）を配置できます。

ext4とxfsは、DAXマウントオプション（`-o dax`）をサポートします。これにより、アプリケーションはI/Oパスからページキャッシュを削除して、直接アクセスを実行できます。このDAXオプションを使用するには、pmemブロックデバイスをfsdaxネームスペースモードに設定する必要があります。

次の例では、3つのpmemブロックデバイス上にext4、xfs、およびbtrfsファイルシステムを作成し、DAXオプションでext4とxfsをマウントしています。

注記:

RHEL8を使用している場合は、まず `reflink` 機能を無効にしてください。この機能を無効にするには、次のコマンドを実行します。

```
sudo mkfs.xfs -m reflink=0 /dev/pmem0
```

```
$ sudo mkfs.ext4 -F /dev/pmem0
$ sudo mount -o dax /dev/pmem0 /mnt/pmem0

$ sudo mkfs.xfs -f /dev/pmem1
$ sudo mount -o dax /dev/pmem1 /mnt/pmem1

$ sudo mkfs.btrfs -f /dev/pmem2
$ sudo mount /dev/pmem2 /mnt/pmem2
```

DAXマウントオプションが有効であったことを確認するには、有効なマウントオプションについて検討します。pmemブロックデバイスが、fsdaxモードに設定されていない場合、ファイルシステムはDAXオプションを削除することがあります。

```
$ mount | grep pmem
/dev/pmem0 on /mnt/pmem0 type ext4 (rw,relatime,dax,data=ordered)
/dev/pmem1 on /mnt/pmem1 type xfs (rw,relatime,attr2,dax,inode64,noquota)
/dev/pmem2 on /mnt/pmem2 type btrfs (rw,relatime,ssd,space_cache,subvolid=5,subvol=)
```

I/Oの統計情報

パフォーマンスのオーバーヘッドを考慮して、iostatsはデフォルトで無効になっています（たとえば、12M IOPSが25%低下して9M IOPSになります）。iostatsはsysfsで有効にできます。

iostatsは、パーティションごとではなく、ベースのpmemデバイスについてのみ収集されます。DAXパスを通過するI/Oはカウントされないため、`-o dax`でマウントされたファイルシステム内のファイルへのI/Oについては、何も収集されません。

```
$ echo 1 > /sys/block/pmем0/queue/iostats
$ echo 1 > /sys/block/pmем1/queue/iostats
$ echo 1 > /sys/block/pmем2/queue/iostats
$ echo 1 > /sys/block/pmем3/queue/iostats

$ iostat -mxy 1
avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           21.53    0.00   78.47    0.00    0.00    0.00

Device:            rrqm/s   wrqm/s         r/s     w/s    rMB/s    wMB/s avgrq-sz avgqu-sz   await
r_await w_await  svctm  %util
pmem0              0.00    0.00 4706551.00    0.00 18384.95    0.00    8.00    6.00    0.00
0.00    0.00    0.00 113.90
pmem1              0.00    0.00 4701492.00    0.00 18365.20    0.00    8.00    6.01    0.00
0.00    0.00    0.00 119.30
pmem2              0.00    0.00 4701851.00    0.00 18366.60    0.00    8.00    6.37    0.00
0.00    0.00    0.00 108.90
pmem3              0.00    0.00 4688767.00    0.00 18315.50    0.00    8.00    6.43    0.00
0.00    0.00    0.00 117.
```

HPE向けインテルOptane Persistent Memory 200シリーズのVMwareのサポート

HPE ARSエラー処理の実装向けインテルOptane Persistent Memory 200シリーズでは、特定の障害シナリオで物理メモリの可用性が大きな影響を受ける可能性があります。すべてのネームスペースの最初の2MBは、ESXiで物理メモリの重要なメタデータを格納するために使用されます。通常、VMKernel物理メモリでは、ARSクリアエラーDSMが正常に実行されることが想定されています。HPEに固有の設計によって、ESXiでARSエラーをクリアできず、この2MB領域でARSエラーが発生した場合に、ESXiではそれらのネームスペースのDIMMで物理メモリファイルシステムを再フォーマットおよび作成できません。1つのネームスペースをフォーマットできなくなると、ESXiでエラーが発生し、ホスト上に物理メモリデータストアを作成できず、ホスト内のすべての物理メモリを使用できなくなります。

ESXiで物理メモリデータストアが作成される前に、ネームスペースの最初の2MBで訂正不能エラーが発生したモジュールを交換する必要があります。メモリモジュールで訂正不能エラーが検出されると、HPE IMLログにイベントが記録されます。IMLログを使用すれば、どの物理メモリに欠陥があり、交換する必要があるのかを判断できます。部品の交換すると、大幅なシステムのダウンタイムが発生する可能性があります。詳しくは、HPEにお問い合わせください。

すべての物理メモリの実装では、OSから物理メモリへのアクセスが許可される前に、すべてのエラーが検出および報告されるように、物理メモリの整合性チェックを実行する必要があります。物理メモリの実装は、このような整合性チェックが実行されるタイミングと方法によって異なります。HPEシステムのBIOSでは、必要に応じて起動時（致命的なエラーが原因でシステムリセットが発生した場合など）に、物理メモリの整合性チェックが実行されます。HPEシステムにインストールされている物理メモリの量によっては、物理メモリの整合性チェックが完了するまでに長い時間がかかる場合があります。たとえば、6TBの物理メモリを備えた2ソケットシステムでは、物理メモリの整合性チェックが完了するまでに1.5時間かかる場合があります。

VMwareでのHPE向けインテルOptane Persistent Memory 200シリーズの使用については、[VMware文書のWebサイト](#)を参照してください。

HPE向けインテルOptane Persistent Memory 200シリーズで認定されたVMware PMEMであるHewlett Packard Enterpriseサーバーを見つけるには、[VMware Compatibility Guide](#)を参照してください。

HPE向けインテルOptane Persistent Memory 200シリーズのWindows Serverのサポート

Windows ServerでのHPE向けインテルOptane Persistent Memory 200シリーズの使用に関する情報は、[Hewlett Packard Enterprise Webサイト](#)にあるテクニカルホワイトペーパー、Deploying HPE Persistent Memory on Microsoft Windows Server 2012 R2, Server 2016, and Server 2019を参照してください。



不揮発性メモリファイルシステムが原因でシステムブートが失敗する

症状

大量の不揮発性メモリが取り付けられている場合、およびfsdaxを使用してネームスペースが作成されている場合、システムは緊急プロンプト/リカバリシェルを起動します。

解決方法 1

原因

PMEMデバイスが、次のバージョンを実行しているシステムの/etc/fstabファイルで定義されている自動マウント時間内に初期化されません。

- Red Hat Enterprise Linux 7.x
- Red Hat Enterprise Linux 8.0 ([RRHSA-2019:1959](#)なし)
- SUSE Linux Enterprise Server 12 SPx
- SUSE Linux Enterprise Server 15

アクション

この問題を回避するには、

```
/etc/systemd/system.conf
```

ファイルのDefaultTimeoutStartSecの値を、
1200s

など、十分に大きな値に増加させます。

システムブートのタイムアウトが発生しなくなります。

解決方法 2

原因

SUSE Linux Enterprise Server 12 SP4を実行しているシステムでは、大量のPMEMデバイスを構成すると、

btrfs

モジュールのロードで遅延が発生する可能性があります。

アクション

次のエントリーを

```
/etc/modprobe.d/99-local.conf
```

に追加することで、

libnvdimm

モジュールのロードが

btrfs

カーネルモジュールの後になるよう強制します。

```
# Load btrfs before libnvdimm
```

```
softdep libnvdimm pre: btrfs
```

詳しくは、<https://www.suse.com/support/kb/doc/?id=7024085>を参照してください。

トラブルシューティングの資料

トラブルシューティングの資料は、以下のドキュメントのHPE Gen10およびGen10 Plusサーバー製品で使用できます。

- 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では、一般的な問題を解決するための手順を紹介し、障害を特定し識別するための一連の包括的な対策、問題の解決方法、ソフトウェアのメンテナンスについて説明しています。
- HPE ProLiant Gen10サーバー、Gen10 Plusサーバー、およびHPE Synergy用のインテグレートドマネジメントログメッセージおよびトラブルシューティングガイドでは、クリティカルおよび警告IMLイベントを解決するためのIMLメッセージおよび関連するトラブルシューティング情報を提供しています。

お使いの製品のトラブルシューティングの資料にアクセスするには、[Hewlett Packard EnterpriseのWebサイト](#)を参照してください。

Webサイト

全般的なWebサイト

不揮発性メモリに関するWebサイト

不揮発性メモリに関するHewlett Packard Enterprise Information Library

www.hpe.com/info/persistentmemory-docs

HPE Persistent Memoryポータル

www.hpe.com/info/persistentmemory

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。

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>

- お客様のエンタイトルメントを表示およびアップデートするには、または契約と標準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 More Information on Access to Support Materialsページをご覧ください。

<https://www.hpe.com/support/AccessToSupportMaterials>

(i) 重要:

Hewlett Packard Enterpriseサポートセンターからアップデートにアクセスするには、製品エンタイトルメントが必要な場合があります。関連するエンタイトルメントでHPEパスポートをセットアップしておく必要があります。

リモートサポート（HPE通報サービス）

リモートサポートは、保証またはサポート契約の一部としてサポートデバイスでご利用いただけます。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に基づいて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/hpalert>

HPE Pointnext Tech Care

<https://www.hpe.com/jp/ja/services/tech-care>

HPE Complete Care

<https://www.hpe.com/jp/ja/services/complete-care>

カスタマーセルフリペア (CSR)

Hewlett Packard Enterpriseカスタマーセルフリペア (CSR) プログラムでは、ご使用の製品をお客様ご自身で修理することができます。CSR部品を交換する必要がある場合、お客様のご都合のよいときに交換できるよう直接配送されます。一部の部品はCSRの対象になりません。Hewlett Packard Enterpriseの正規保守代理店が、CSRによって修理可能かどうかを判断します。

CSRについて詳しくは、お近くの正規保守代理店にお問い合わせください。

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、プロセスによってキャプチャーされます。