



Hewlett Packard
Enterprise

HPE 向けインテル Optane Persistent Memory 100 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 100 シリーズのインストール、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 および HPE Synergy システムのインストール、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。Hewlett Packard Enterprise では、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。

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

はじめに	6
HPE 向けインテル Optane Persistent Memory 100 シリーズ.....	6
不揮発性メモリモード.....	6
メモリキャッシュ比率.....	6
セキュリティ機能	8
パスワード.....	8
暗号化.....	9
サニタイズ.....	9
署名されたファームウェア.....	10
ファームウェアロールバック保護.....	11
コンポーネントの識別	12
HPE 向けインテル Optane Persistent Memory 100 シリーズラベルの識別.....	12
取り付け	13
システム要件.....	13
メモリ取り付け情報.....	14
Persistent Memory モジュールの取り扱いのガイドライン.....	14
DIMM または persistent memory modules の取り付け.....	15
システムの構成	17
構成の概要.....	17
構成ツール.....	17
目標構成の設定.....	17
UEFI システムユーティリティを使用した目標構成の設定.....	18
ipmctl を使用した目標構成の設定.....	19
HPE Persistent Memory 管理ユーティリティを使用した目標構成の設定.....	19
HPE iLO RESTful API を使用した目標構成の設定.....	20
ネームスペースの作成.....	21
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.....	21
ipmctl を使用したネームスペースの作成.....	21
ndctl を使用したネームスペースの作成 (Linux)	21
キー管理の有効化.....	22
ローカルキー管理を使用した persistent memory modules の暗号化.....	23
リモートキー管理を使用した persistent memory modules の暗号化.....	24
他の BIOS/プラットフォーム構成 (RBSU) オプション.....	29
管理ツール	31
HPE 向けインテル Optane Persistent Memory の管理.....	31
UEFI システムユーティリティ.....	31
UEFI システムユーティリティを使用した目標構成の変更.....	31
UEFI システムユーティリティを使用した目標構成の削除.....	32
persistent memory modules パスワードの変更.....	33

persistent memory modules ステータスの表示.....	33
キー管理モードの変更.....	34
キー管理の無効化.....	35
persistent memory modules の暗号化の無効化.....	35
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.....	36
HPE iLO RESTful API.....	37
HPE iLO RESTful API の概要.....	37
RESTful インターフェイスツール.....	46
RESTful インターフェイスツールの起動.....	47
検出コマンド.....	47
構成コマンド.....	50
HPE Persistent Memory 管理ユーティリティ.....	54
HPE Persistent Memory 管理ユーティリティの取り付け.....	54
HPE Persistent Memory 管理ユーティリティへのサインイン.....	55
ナビゲーション.....	55
ipmctl ツール.....	63
ipmctl のインストール (Linux)	63
ipmctl を使用した persistent memory modules 構成の表示.....	64
ipmctl を使用した目標構成の削除.....	64
ipmctl によるメモリモードの判断.....	64

メンテナンス.....65

Persistent Memory モジュールの再配置のガイドライン.....	65
persistent memory modules データの手動でのバックアップ.....	66
DIMM または persistent memory modules の取り外し.....	67
システムボードの交換.....	69
persistent memory modules の移行.....	70
ローカルキー管理で暗号化された persistent memory modules の移行.....	70
リモートキー管理で暗号化された persistent memory modules の移行.....	71
persistent memory modules のサニタイズ.....	73
サニタイズポリシー.....	73
サニタイズガイドライン.....	74
UEFI システムユーティリティを使用したサニタイズ.....	75
HPE iLO RESTful API を使用したサニタイズ.....	75
ipmctl を使用したサニタイズ.....	76
パスワードを紛失した persistent memory modules の撤去.....	76
persistent memory modules ファームウェアのアップデート.....	77

HPE 向けインテル Optane Persistent Memory 100 シリーズの Linux サポート..... 78

nmem デバイス.....	78
nmem デバイスのプロパティ.....	78
nmem デバイスの一覧表示.....	79
領域.....	79
領域のプロパティ.....	79
領域の一覧表示.....	80
ネームスペース.....	80
ネームスペースのプロパティ.....	81
ネームスペースの作成.....	82
すべてのネームスペースを一覧表示する.....	82
ネームスペースモードの変更.....	82
ネームスペースの削除.....	83
pmem デバイスの初期化.....	83
システムのメモリ容量の表示.....	83

ファイルシステム.....	83
I/O の統計情報.....	84
HPE 向けインテル Optane Persistent Memory 100 シリーズの VMware サポート.....	85
HPE 向けインテル Optane Persistent Memory 100 シリーズの Windows Server サポート.....	86
トラブルシューティング.....	87
既知の問題.....	87
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.....	87
トラブルシューティングの資料.....	87
Web サイト.....	89
サポートと他のリソース.....	90
Hewlett Packard Enterprise サポートへのアクセス.....	90
アップデートへのアクセス.....	90
リモートサポート（HPE 通報サービス）.....	91
カスタマーセルフリペア（CSR）.....	91
保証情報.....	91
規定に関する情報.....	92
ドキュメントに関するご意見、ご指摘.....	92



はじめに

HPE 向けインテル Optane Persistent Memory 100 シリーズ

HPE 向けインテル Optane Persistent Memory 100 シリーズは、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）としてメモリを展開する柔軟性を提供し、最大 3.0 TB 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 100 シリーズは、第 2 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 は、3 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せん。

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。詳しくは、「メモリのキャッシュ比率」を参照してください。

メモリモードでは、各メモリコントローラー下での対称 DIMM と persistent memory modules の取り付けが必要とされます。

混合モード

混合モードに設定されている場合、persistent memory modules の一部の容量は揮発性メモリとして機能し、残りは不揮発性メモリとして機能します。DRAM 容量はすべて、キャッシュとして動作します。

詳しくは

[メモリキャッシュ比率](#)

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。

- 2:1 - 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。
- 4:1
- 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。

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。

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。

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
768 GB	6 x 128 GB	96 GiB	6 x 16 GiB	8:1
		192 GiB	6 x 32 GiB	4:1
		384 GiB	6 x 64 GiB	2:1 ²
		768 GiB	6 x 128 GiB	1:1 ²
1.5 TB	6 x 256 GB	96 GiB	6 x 16 GiB	16:1
		192 GiB	6 x 32 GiB	8:1
		384 GiB	6 x 64 GiB	4:1
		768 GiB	6 x 128 GiB	2:1 ²
3 TB	6 x 512 GB	96 GiB	6 x 16 GiB	32:1 ³
		192 GiB	6 x 32 GiB	16:1
		384 GiB	6 x 64 GiB	8:1
		768 GiB	6 x 128 GiB	4:1

¹ 1 プロセッサあたりの容量

² 非推奨。キャッシュの恩恵が受けられない

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

詳しくは

[サニタイズ](#)

[暗号化](#)

[パスワード](#)

[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 をサニ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せんが、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 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。

詳しくは

[キー管理の有効化](#)
[パスワード](#)

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）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 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せん。

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。

詳しくは

[persistent memory modules ファームウェアのアップデート](#)



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。

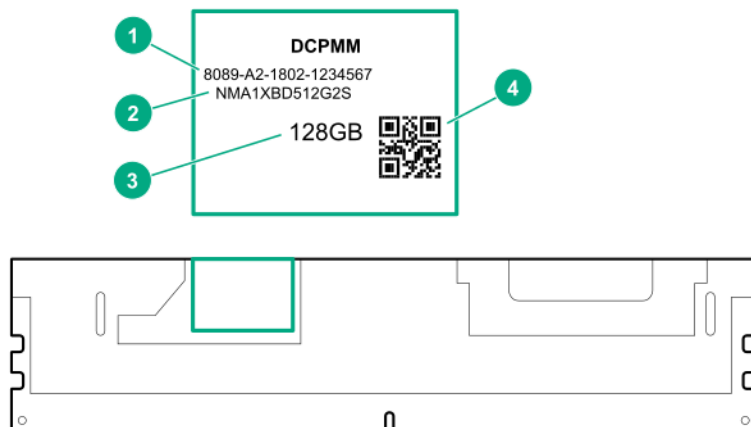
詳しくは

[persistent memory modules ファームウェアのアップデート](#)



コンポーネントの識別

HPE 向けインテル Optane Persistent Memory 100 シリーズ ラベルの識別



番号	説明	例
1	固有の ID 番号	8089-A2-1802-1234567
2	モデル番号	NMA1XBD512G2S
3	容量	128 GB 256 GB 512 GB
4	QR コード	部品番号およびシリアル番号を含む

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。



取り付け

システム要件

- ① **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 100 シリーズ
- 第 2 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 2.10 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 04.01.04.296
- HPE iLO 5 ファームウェアバージョン 1.43
- HPE Innovation Engine ファームウェアバージョン 2.1 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 2012 R2（Hewlett Packard Enterprise persistent memory ドライバー搭載）
- Windows Server 2016（Hewlett Packard Enterprise persistent memory ドライバー搭載）
- Windows Server 2019
- Red Hat Enterprise Linux 7.6 以降
- Red Hat Enterprise Linux 8.0 以降
- SUSE Linux Enterprise Server 12 SP4 以降
- SUSE Linux Enterprise Server 15（SUSE-SU-2019:0224-1 以降にカーネルアップデート必要）
- SUSE Linux Enterprise Server 15 SP1（SUSE-SU-2019:1550-1 以降にカーネルアップデート必要）
- VMware vSphere 6.7 U2 + Express パッチ 10（ESXi 670-201906002）以降（App Direct モードとメモリモードをサポート）
- VMware vSphere 6.5 U3 以降（メモリモードをサポート）

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。
 - メモリモード - 揮発性容量は persistent memory modules 容量の一部または全部です。
- 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。

❗ **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。
詳しくは、[メモリキャッシュ比率](#)を参照してください。

特定の取り付けと構成情報については、Hewlett Packard Enterprise の Web サイト (<https://www.hpe.com/docs/memory-population-rules>) にあるメモリの取り付けガイドラインを参照してください。

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 を取り付けの際は、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 persistent memory modules 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 サーバー (<https://www.hpe.com/info/proliantgen10-docs>)
- HPE Synergy Gen10 コンピュートモジュール (<https://www.hpe.com/info/synergy-docs>)

❗ **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 (<https://www.hpe.com/docs/server-memory>) 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。

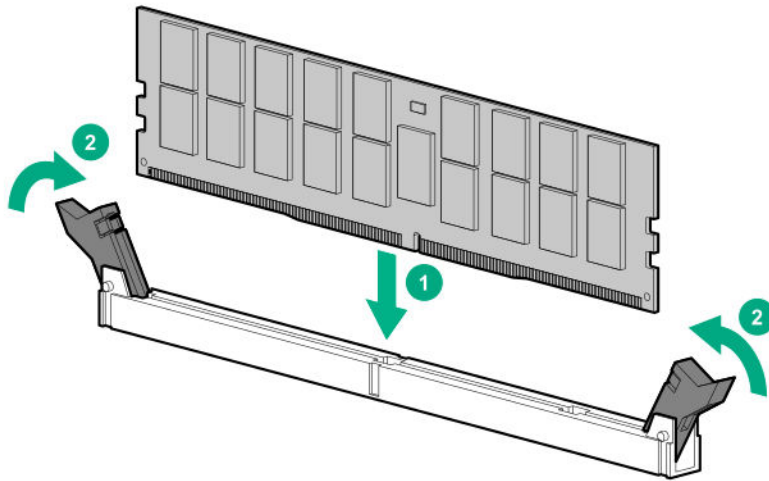
⚠ **注意:** DIMM および persistent memory modules は適切な配置のために重要です。コンポーネントを取り付ける前に、DIMM または persistent memory modules のノッチを対応するスロットのノッチに合わせてください。DIMM または persistent memory modules をスロットに押し込まないでください。正しく取り付けられた場合、必ずしもすべての DIMM または persistent memory modules が同じ方向に向く訳ではありません。

⚠ **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。

システムの構成

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。

❗ **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。

詳しくは

[目標構成の設定](#)

[キー管理の有効化](#)

[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](#)

[ネームスペースの作成](#)

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
- HPE Persistent Memory 管理ユーティリティ
- 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 の場合)

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す。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。次回の起動時に、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。

❗ **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。

❗ **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

❗ **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。
 - **メモリコントローラーインターリーブ** - 自動
 - **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。
 - **混合モード** - ゼロ以外の値を選択します。残量は、インターリーブが選択された状態で不揮発性メモリに割り当てられます。
これらの値は推奨される**メモリキャッシュ比率**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。
 - **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、次回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 Persistent Memory 管理ユーティリティを使用した目標構成の設定

次のいずれかを使用して、HPE Persistent Memory 管理ユーティリティを使って目標構成を設定します。

- ガイド付き構成 - プリセットされ最適化された推奨比率の 1 つを使用して、不揮発性および揮発性のメモリ割り当てを定義します。
- 高度な設定 - サーバーのワークロード要件に基づいて、不揮発性および揮発性のメモリ割り当てのカスタム値を定義します。

ユーティリティの使用について詳しくは、[HPE Persistent Memory 管理ユーティリティ](#)を参照してください。

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と HPE Persistent Memory 管理ユーティリティ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/PROC1MemoryDomain/MemoryChunks",
  "body": {
    "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/"
      }
    }
  ]
}
```

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.
```

詳しくは

[HPE iLO RESTful API](#)

[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](#)

ネームスペースの作成

UEFI システムユーティリティを使用したネームスペースの作成

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

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 0x1
```

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-users-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. **パズフレーズのタイプ**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**パズフレーズ**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

iLO は以下のキーマネージャ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。
 - プライマリキーサーバーアドレス
 - プライマリキーサーバーポート
 - セカンダリキーサーバーアドレス
 - セカンダリキーサーバーポート
4. (オプション) プライマリおよびセカンダリキーサーバーを使用した構成でサーバーの冗長化を確認するには、**冗長化が必要**オプションを有効にします。
Hewlett Packard Enterprise では、このオプションを有効にすることをお勧めします。
5. **OK** をクリックします。
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

プライマリーサーバーアドレス

プライマリ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。

プライマリーサーバーポート

プライマリーサーバーポート。

セカンダリサーバーアドレス

セカンダリ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。

セカンダリサーバーポート

セカンダリサーバーポート。

冗長化が必要

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

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


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

キーマネージャー構成の詳細の追加

前提条件

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

手順

1. ナビゲーションツリーで**管理**をクリックして、**キーマネージャー**タブをクリックします。
2.  (キーマネージャー構成セクション内) をクリックします。
キーマネージャー構成設定を編集ページが開きます。
3. 次の情報をキーマネージャー上の iLO アカウントセクションに入力します。
 - **アカウントグループ**
 - (オプション) **キーマネージャーローカル CA 証明書名**

アカウント名の値は読み取り専用です。

4. 次の情報をキーマネージャー**管理者**アカウントセクションに入力します。

- ログイン名
- パスワード

5. OK をクリックします。

iLO は情報要求をキーマネージャーサーバーに送信します。

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

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

キーマネージャー構成の詳細

アカウント名

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

アカウントグループ

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

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

キーマネージャーローカル CA 証明書名

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

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

ログイン名

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

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

パスワード

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

キーマネージャー構成のテスト

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

- キーマネージャーソフトウェアのバージョンが iLO と互換性があることを確認します。
- TLS を使用してプライマリ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、iLO でキーマネージャーの構成が完了している。

手順

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

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

キーマネージャーイベントの表示

前提条件

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

手順

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

キーマネージャーログのクリア

前提条件

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

手順

1. ナビゲーションツリーで**管理**をクリックして、**キーマネージャ**タブをクリックします。
2. **キーマネージャログ**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。
 - 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
- **ノードインターリーブ** - このオプションは、プロセッサ間でメモリをインターリーブします。persistent memory modules ではサポートしていません。
 - 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 > ノードインターリーブ
 - iLO RESTful API のプロパティ名：NodeInterleaving
- **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

- **便宜的セルフリフレッシュ** - 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 > 便宜的セルフリフレッシュ
 - iLO RESTful API のプロパティ名：OpportunisticSelfRefresh
- **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
- **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、インテルパフォーマンスカウンターモニター (PCM) ツールは、チャンネルごとの帯域幅をレポートできます。

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

管理ツール

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
- HPE Persistent Memory 管理ユーティリティ
- ipmctl。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

詳しくは

[HPE iLO RESTful API](#)

[HPE Persistent Memory 管理ユーティリティ](#)

[UEFI システムユーティリティ](#)

[RESTful インターフェイスツール](#)

[ipmctl ツール](#)

UEFI システムユーティリティ

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。

- ❗ **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。
- ❗ **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。
- ❗ **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。
 - 混合モード - ゼロ以外の値を選択します。残量は、インターリーブが選択された状態で不揮発性メモリに割り当てられます。
 - **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、次のサーバー再起動時にのみ適用されます。

-
- ① **重要:** UEFI システムユーティリティに表示される、不揮発性メモリに関連するすべてのポップアップメッセージを確認してください。これらのメッセージの指示に従わないと、不揮発性メモリのデータが消失する可能性があります。
-
- ① **重要:** 最大限のアップタイムとデータ保護を確保するには、高可用性のベストプラクティスに関するソフトウェアアプリケーションプロバイダの推奨事項に常に従ってください。
-

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

- ❗ **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。

- ❗ **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。

- ❗ **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。

- ❗ **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

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

手順

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

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と HPE Persistent Memory 管理ユーティリティの使用をお勧めします。Postman、curl、wget などのサードパーティ製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。

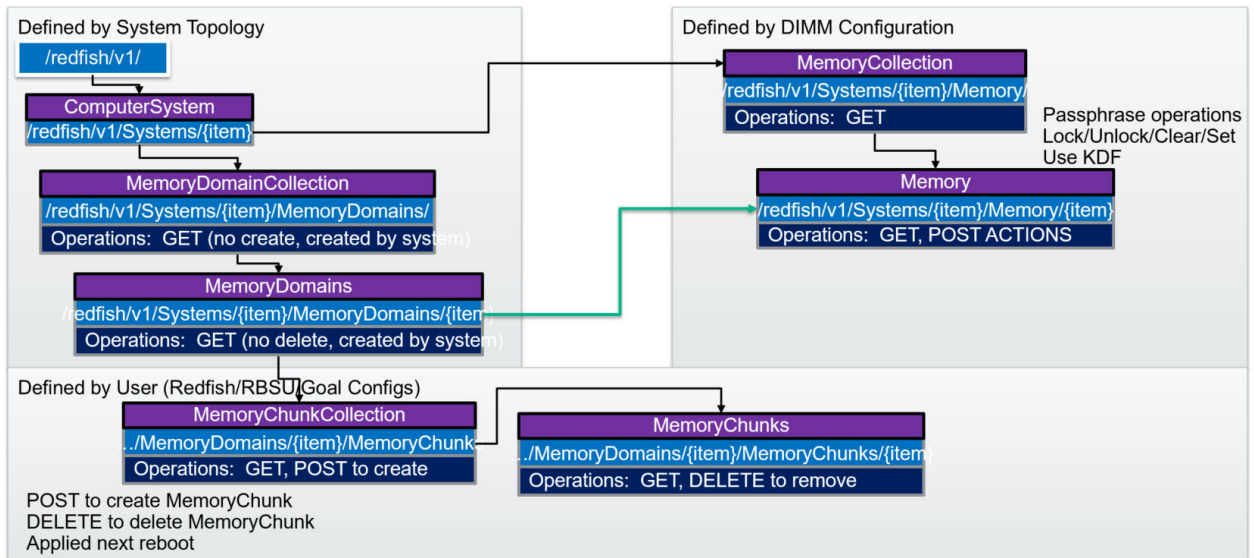
- メモリ
- メモリチャンク
- メモリドメイン
- メモリ領域

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=(',', ': ')))
```

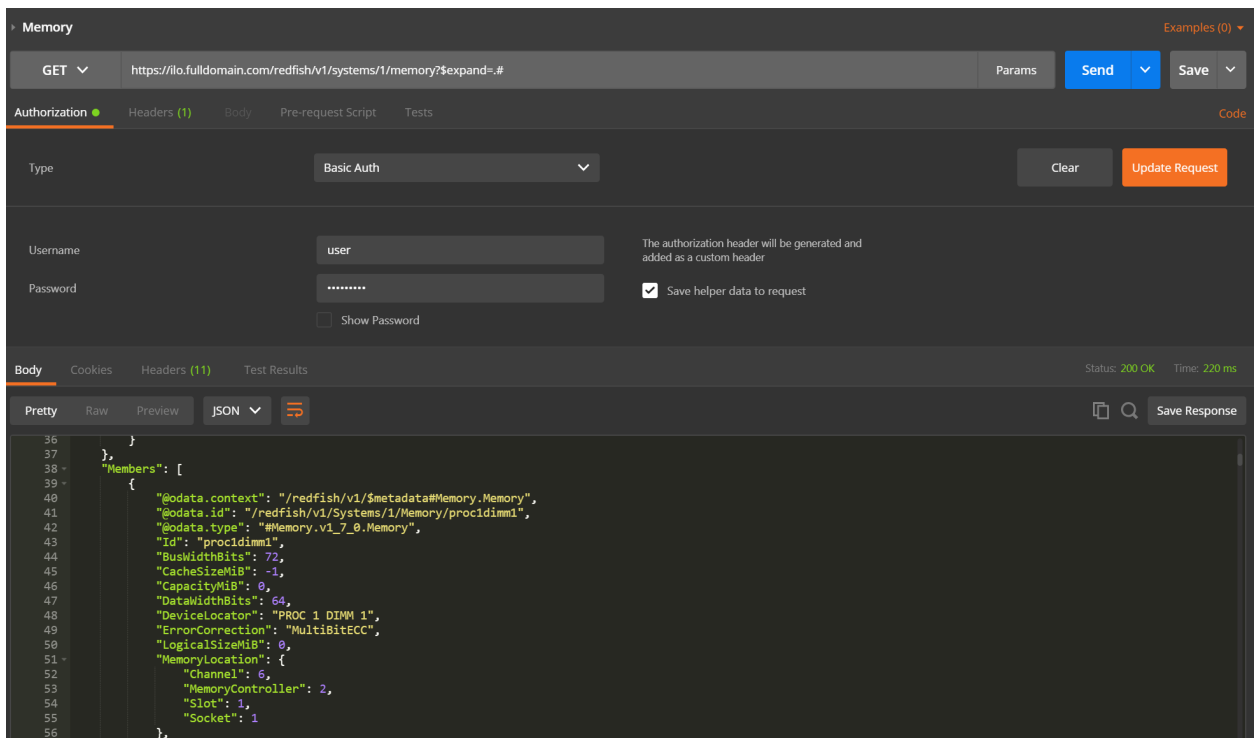
Postman を使用した拡張メモリコレクションの取得

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=.#





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）
LatencyOptimized	レイテンシに最適化
PmmQos	サービス品質
Disabled	無効（デフォルト）
Profile1	プロファイル 1
Profile2	プロファイル 2
Profile3	プロファイル 3
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）

表は続く



コマンド	システムユーティリティオプション
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	操作なし
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。

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す。
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/PROC1MemoryDomain/MemoryChunks",
  "body": {
    "AddressRangeType": "PMEM",
    "Oem": {
      "Hpe": {
        "MemoryChunkSizePercentage": 100
      }
    },
    "InterleaveSets": [{
      "Memory": {
        "@odata.id": "/redfish/v1/Systems/1/Memory/proc1dim6/"
      }
    }
  ]
}
```

```

    }, {
"Memory": {
"@odata.id": "/redfish/v1/Systems/1/Memory/procldimm7/"
    }
    }
  ]
}
}
}

```

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。

- ❗ **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/proc1dim6/" }
    },
    {
      "Memory": { "@odata.id": "/redfish/v1/Systems/1/Memory/proc1dim7/" }
    }
  ]
}

# 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")))

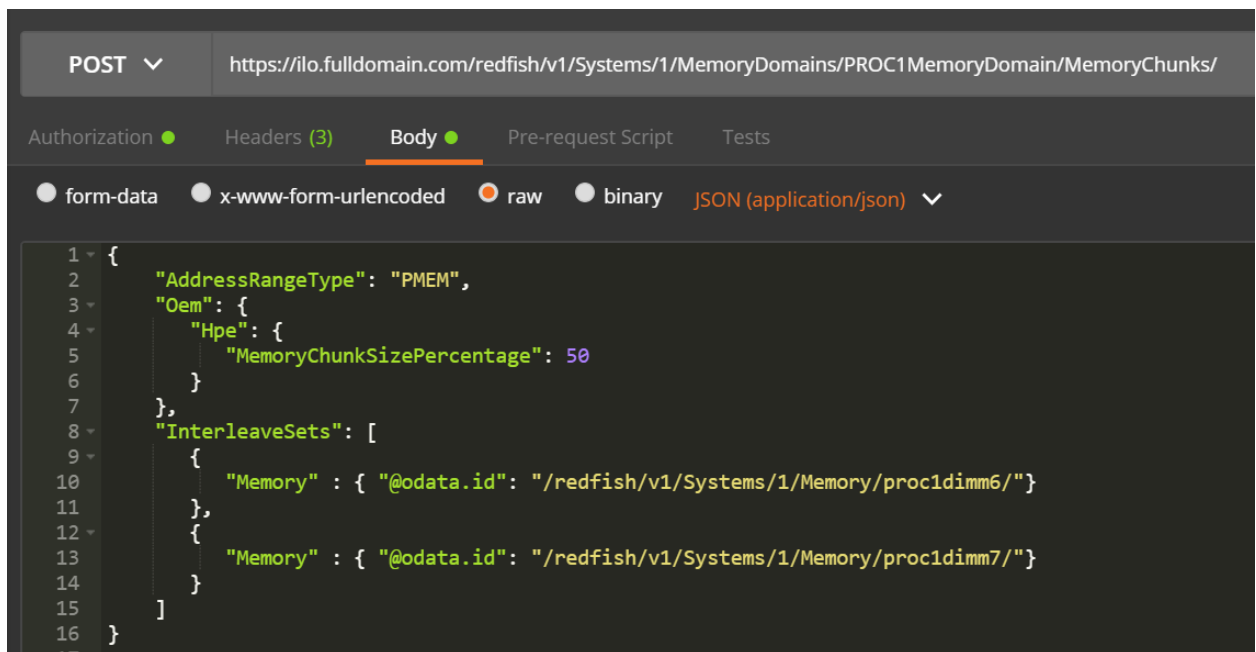
```

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



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って、HPE 向けインテル Optane Persistent Memory 100 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
-D, --device	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。
-C, --config	persistent memory modules の構成を表示します。
-L, --logical	不揮発性インターリーブセットを表示します。
-M, --summary	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
-h, --help	コマンドのヘルプを表示します。
-I, --dimm	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 P@S 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。1@1,1@12。
-j, --json	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
-h, --help	コマンドのヘルプを表示します。
-I, --dimm	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 P@S 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。1@1,1@12。
-j, --json	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
-h, --help	コマンドのヘルプを表示します。
-j, --json	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 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。

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
-h, --help	コマンドのヘルプを表示します。
-j, --json	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。

構成コマンド

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。

```
showpmmpendingconfig [-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
-h, --help	コマンドのヘルプを表示します。
-j, --json	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 > showpmmpendingconfig
```

- 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 > showpmmpendingconfig --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
-h, --help	コマンドのヘルプを表示します。
-C, --config	適用する configID を指定します。
--list	使用可能なすべての configID とその説明をリストします。
-f, --force	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、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
-h, --help	コマンドのヘルプを表示します。
-m, --memory-mode	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。
-i --pmem-interleave	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 on または off です。
-p --proc	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。
-f, --force	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 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。

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。

```
clearpmmpendingconfig [-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
-h, --help	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 > clearpmmpendingconfig
```

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
-h, --help	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。

HPE Persistent Memory 管理ユーティリティ

HPE Persistent Memory 管理ユーティリティは、サーバーに取り付けられた不揮発性メモリをリモートに構成したり評価したりできるようにするデスクトップアプリケーションです。

❗ **重要:** HPE Persistent Memory 管理ユーティリティは、サポートされている persistent memory modules が取り付けられている HPE サーバーでのみ使用されることを意図しています。

HPE Persistent Memory 管理ユーティリティの取り付け

HPE iLO を介してマネージドサーバーネットワークにアクセスでき、かつ HPE iLO v1.43 以降を実行しているコンピューターに HPE Persistent Memory 管理ユーティリティをインストールします。

手順

1. Hewlett Packard Enterprise ウェブサイト (<https://www.hpe.com/support/hpesc>) から HPE Persistent Memory 管理ユーティリティをダウンロードします。
2. Windows または Linux 用の適切なインストーラーファイルを実行して、インストールを完了します。

- Windows : ダウンロードディレクトリからインストーラーファイルを見つけて実行します。
- Linux:
 - ダウンロードしたパッケージをご使用のローカルドライブディレクトリにコピーし、そのディレクトリに移動します。
 - ご使用の Linux ディストリビューションの標準手順を使用して、RPM をインストールします。以下に例を示します。

Red Hat Enterprise Linux - yum localinstall hpepmm-{version}.x86_64.rpm

rpm -iv hpepmm-{version}.x86_64.rpm を使用する場合、依存関係を手動でインストールする必要があります。

3. ユーティリティを起動します。

- Windows :
 - スタートメニューで Hewlett Packard Enterprise の下のアイコンを見つけます。
 - インストールディレクトリ C:\Program Files (x86)\Hewlett Packard Enterprise\Persistent Memory Management Utility で目的のアイコンを見つけます。
- Linux : hpepmm を実行します。

HPE Persistent Memory 管理ユーティリティへのサインイン

手順

1. HPE Persistent Memory 管理ユーティリティを開きます。
2. 構成するサーバーの HPE iLO のホスト名または IP アドレスを入力します。
3. HPE iLO のユーザー名とパスワードを入力します。
ユーザー名には、BIOS および iLO の構成設定を修正する特権が付与されていることが必要です。







ナビゲーション

ユーティリティ内を移動するには、画面左側のメニュー項目または画面上部のツールバーをクリックします。

- ツールバーのアイコン
- 概要
- ガイド付き構成
- 詳細設定
- 構成タスク
- バージョン情報



ツールバーのアイコン

アイコン	説明
	画面上のデータ表示を更新します
	アプリケーションメニューを開きます
	ログインユーザー名とログアウトボタンを表示します
	ウィンドウを最小化します
	ウィンドウを最大化します
	ウィンドウを閉じます

概要

Overview 画面には、サーバーに取り付けられた不揮発性メモリの構成のスナップショットが表示されません。



Physical タブ

The screenshot displays the 'Physical' tab of the HPE-ProLiant Manage HPE Persistent Memory interface. It shows a table of installed HPE Persistent Memory Modules with columns for Location, Status, Security State, Firmware Version, Capacity, and Allocation. All modules are in 'Good, In Use' status with a 'Disabled' security state. An 'Allocation Summary' on the right shows a total of 2016 GB, split into 1008 GB Persistent and 1008 GB Volatile.

Location	Status	Security State	Firmware Version	Capacity	Allocation
PROC 1 DIMM 6	Good, In Use	Disabled	01.02.00.5375	252 GB	126 GB Persistent, 126 GB Volatile
PROC 1 DIMM 7	Good, In Use	Disabled	01.02.00.5375	252 GB	126 GB Persistent, 126 GB Volatile
PROC 2 DIMM 6	Good, In Use	Disabled	01.02.00.5375	252 GB	126 GB Persistent, 126 GB Volatile
PROC 2 DIMM 7	Good, In Use	Disabled	01.02.00.5375	252 GB	126 GB Persistent, 126 GB Volatile
PROC 3 DIMM 6	Good, In Use	Disabled	01.02.00.5375	252 GB	126 GB Persistent, 126 GB Volatile
PROC 3 DIMM 7	Good, In Use	Disabled	01.02.00.5375	252 GB	126 GB Persistent, 126 GB Volatile
PROC 4 DIMM 6	Good, In Use	Disabled	01.02.00.5375	252 GB	126 GB Persistent, 126 GB Volatile
PROC 4 DIMM 7	Good, In Use	Disabled	01.02.00.5375	252 GB	126 GB Persistent, 126 GB Volatile

Physical タブをクリックして、サーバーに取り付けられた各 persistent memory modules のステータス、セキュリティ状態、ファームウェアバージョン、容量、および割り当て（不揮発性メモリ対揮発性メモリ）を表示します。

セキュリティ状態

説明



無効 - サーバーでキー管理が無効です。



ロック解除 - サーバーでローカルまたはリモートのキー管理が有効です。

パスワードを使用して、persistent memory modules のロック解除に成功しました。



ロック - サーバーでローカルまたはリモートのキー管理が有効です。

persistent memory modules のロック解除に失敗しました。この状態は以下の場合に発生する可能性があります。

- persistent memory modules がサーバーに移行され、パスワードがまだ入力またはインポートされていません。
- persistent memory modules がサーバーに移行され、誤ったパスワードが入力されました。

Logical タブ

The screenshot displays the 'Logical' tab in the HPE-ProLiant Manage HPE Persistent Memory interface. The main content area is titled 'Persistent Memory Regions' and lists three processors:

- Processor 1:** 252 GB Persistent Memory. PMMs in Region: PROC 1 DIMM 6, PROC 1 DIMM 7.
- Processor 2:** 252 GB Persistent Memory. PMMs in Region: PROC 2 DIMM 6, PROC 2 DIMM 7.
- Processor 3:** 252 GB Persistent Memory. PMMs in Region: PROC 3 DIMM 6, PROC 3 DIMM 7.

The right-hand side features an 'Allocation Summary' section with a donut chart and a table:

Category	Value
Persistent	1008 GB
Volatile	1008 GB
Total	2016 GB

Logical タブをクリックして、現在の不揮発性メモリ領域に含まれるサイズ、ステータス、および DIMM を表示します。すべての persistent memory modules がメモリモードにある場合は、不揮発性メモリ領域は存在しません。



ガイド付き構成

HPE-ProLiant - Manage HPE Persistent Memory

Configure all HPE Persistent Memory Modules

Select Allocation

Choose one of the recommended allocations below. The allocations are determined by installed memory and supported volatile to cache ratios. For more options, use Advanced Configuration.

Allocation Option	DRAM Cache	System Memory	PMEM	Total
Option 1 (Orange)	256 GB	2016 GB	0 GB	2272 GB
Option 2 (Teal)	256 GB	1008 GB	1008 GB	2272 GB
Option 3 (Light Blue)	0 GB	256 GB	2016 GB	2272 GB

Options

- Interleave persistent memory regions
- Create default namespaces for persistent memory regions

Configure [Configuration Tasks](#)

Guided Configuration 画面を使用して、サーバーの目標構成を作成または変更します。

Hewlett Packard Enterprise では、プリセットされ最適化された比率の 1 つを使用して、不揮発性および揮発性のメモリ割り当てを定義することをお勧めします。これらの値は、サーバーの合計メモリ割り当て量を表します。

ガイド付き構成を使用した目標構成の設定

前提条件

- HPE iLO を介してターゲットサーバーを管理するためのアクセス権があるコンピューターにユーティリティをインストールします。
- BIOS と HPE iLO の構成権限を持つアカウントを使用して、ユーティリティにログインします。
- 有効になっている場合は、ローカルまたはリモートのキー管理を無効にします。詳しくは、[キー管理の無効化](#)を参照してください。

手順

1. Guided Configuration 画面で、サーバー向けに最適化されたプリセット比率の 1 つを選択します。
2. メモリ構成の要件に応じて、次のいずれかまたは両方のオプションを有効にします。
 - **Interleave persistent memory regions**
 - **Create default namespaces for persistent memory regions**
3. **Configure** をクリックします。

- この目標構成をサーバーにすぐに適用するには、**Configuration Tasks** を選択し、**Reboot** をクリックします。
- 再起動する前に、新しい不揮発性メモリ領域のためにデフォルトのネームスペースを作成しておかなかった場合は、このユーティリティか、または UEFI システムユーティリティや `ndctl` など、他の利用可能な方法のいずれかを使用してください。

❗ **重要:** VMware vSphere がある persistent memory modules を使用しているシステムでは、この手順は必須でなく、推奨もされていません。

詳細設定

Advanced Configuration 画面を使用して、サーバーの目標構成を作成または変更します。

Hewlett Packard Enterprise では、Guided Configuration 画面を使用して、目標構成を設定することをお勧めします。Guided Configuration 画面で定義されたプリセットの最適化された比率が、サーバーのニーズを満たしていない場合は、この画面でプロセッサごとに揮発性メモリのカスタム割り当てを指定できます。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。

詳細設定を使用した目標構成の設定

前提条件

- HPE iLO を介してターゲットサーバーを管理するためのアクセス権があるコンピューターにユーティリティをインストールします。
- BIOS と HPE iLO の構成権限を持つアカウントを使用して、ユーティリティにログインします。
- 有効になっている場合は、ローカルまたはリモートのキー管理を無効にします。詳しくは、[キー管理の無効化](#)を参照してください。

手順

1. Advanced Configuration 画面で、各プロセッサの揮発性メモリ割り当ての値を入力します。残りのパーセンテージは、不揮発性メモリとして割り当てられます。

[+]ボタンと[-]ボタンを使用して、値を手動で増減できます。

入力されるこれらの値は推奨される**メモリキャッシュ比率**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。

2. メモリ構成の要件に応じて、次のいずれかまたは両方のオプションを有効にします。
 - **Interleave persistent memory regions** - プロセッサごとにこのオプションを有効にします。
 - **Create default namespaces for persistent memory regions**
3. **Configure** をクリックします。
4. この目標構成をサーバーにすぐに適用するには、**Configuration Tasks** を選択し、**Reboot** をクリックします。
5. 再起動する前に、新しい不揮発性メモリ領域のためにデフォルトのネームスペースを作成しておかなかった場合は、このユーティリティか、または UEFI システムユーティリティや `ndctl` など、他の利用可能な方法のいずれかを使用してください。

❗ **重要:** VMware vSphere がある persistent memory modules を使用しているシステムでは、この手順は必須でなく、推奨もされていません。

構成タスク

State	Status	Operation	Allocation	Affected PMMs
*		DELETE	252 GB Persistent, 252 GB Volatile	PROC 1 DIMM 6, PROC 1 DIMM 7
*		DELETE	252 GB Persistent, 252 GB Volatile	PROC 2 DIMM 6, PROC 2 DIMM 7
*		DELETE	252 GB Persistent, 252 GB Volatile	PROC 3 DIMM 6, PROC 3 DIMM 7
*		DELETE	252 GB Persistent, 252 GB Volatile	PROC 4 DIMM 6, PROC 4 DIMM 7
*		CREATE	252 GB Persistent, 252 GB Volatile	PROC 1 DIMM 6, PROC 1 DIMM 7
*		CREATE	252 GB Persistent, 252 GB Volatile	PROC 2 DIMM 6, PROC 2 DIMM 7
*		CREATE	252 GB Persistent, 252 GB Volatile	PROC 3 DIMM 6, PROC 3 DIMM 7







Configuration Tasks ページには、サーバーの再起動によってまだ確定されていない不揮発性メモリ構成に加えられた変更が表示されます。

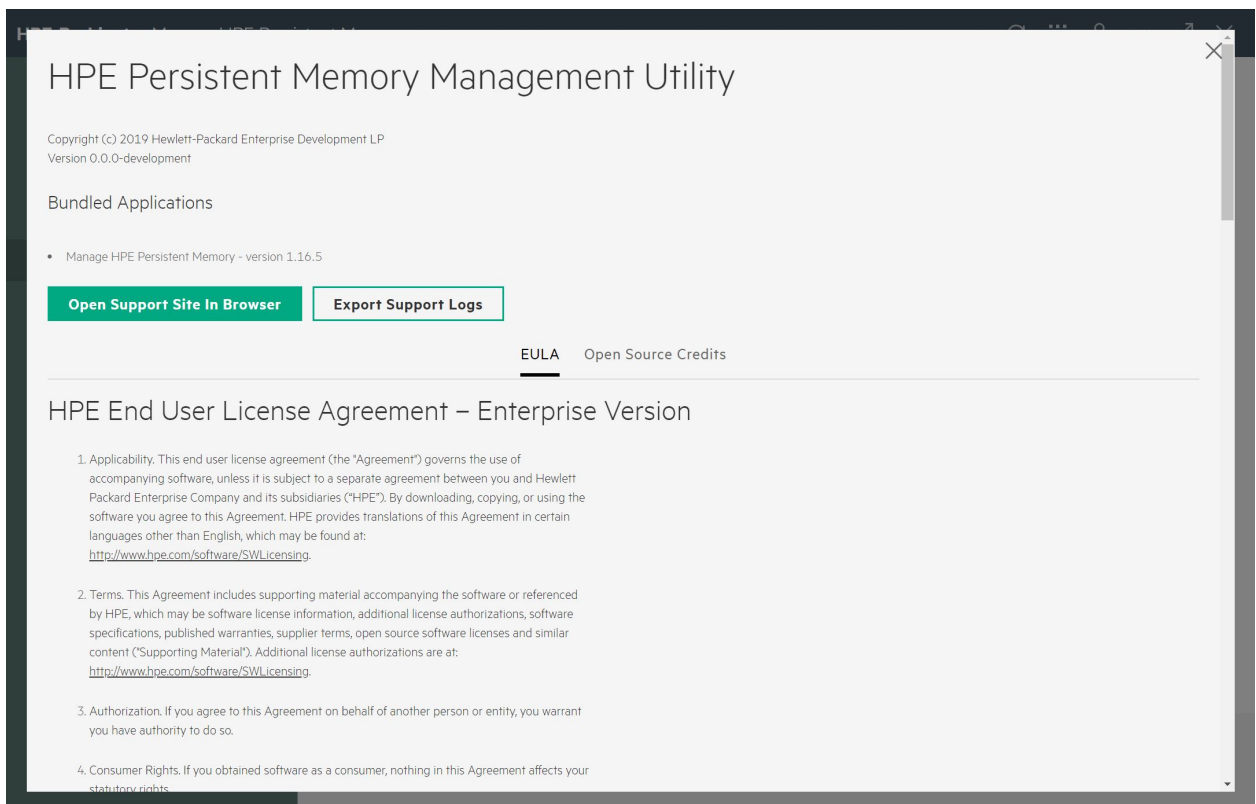
タスクをクリアすると、保留中の目標構成を元に戻すことができます。これにより、目標構成を設定するためのタスクが削除され、サーバーは以前の不揮発性メモリ構成設定を保持します。

保留中の構成タスクをすぐに確定するには、**Reboot** をクリックします。

ステータスアイコンを解釈するには、次の表を使用します。

ステータス	説明
	新しい構成
	完了済み。構成が適用されました。
	構成が適用されていない
	保留中のタスク。目標構成は正常にステージングされ、現在は変更を適用中です。

バージョン情報




About 画面を使用して、次のことを行います。



- HPE エンドユーザー使用許諾契約書を確認し同意します。
- ブラウザで Hewlett Packard Enterprise サポートセンターを開きます。
- サポートログをエクスポートします。

ログファイルのエクスポート

手順

1. ツールバーにある Application メニューアイコン  をクリックします。

2. **About** を選択した後、**Export Support Logs** をクリックします。

ログファイル (zookeeper-<タイムスタンプ>.debug.zip) は、次の場所に作成されます。

- Windows - C:\Users\<ユーザー名> (Windows エクスプローラーが自動的にこの場所を開きます)
- Linux - /home /<ユーザー名>

ipmctl ツール

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 | 01.02.00.5375
0x0011 | 502.5 GiB | Disabled | Healthy | 01.02.00.5375
0x0021 | 502.5 GiB | Disabled | Healthy | 01.02.00.5375
```

```
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 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。



メンテナンス

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。

❗ **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。

詳しくは

[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](#)
[UEFI システムユーティリティを使用したサニタイズ](#)
[DIMM または persistent memory modules の取り外し](#)
[DIMM または persistent memory modules の取り付け](#)
[メモリ取り付け情報](#)
[構成の概要](#)

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ー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 サーバー (<https://www.hpe.com/info/proliantgen10-docs>)
- HPE Synergy Gen10 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。

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。

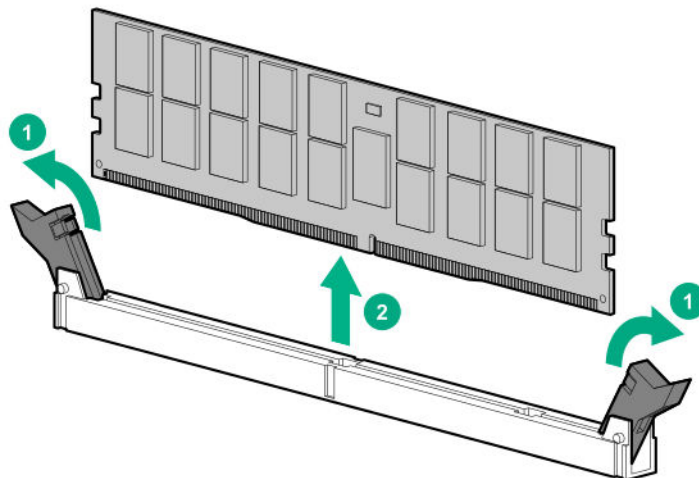
- HPE ProLiant Gen10 サーバー (<https://www.hpe.com/info/proliantgen10-docs>)
- HPE Synergy Gen10 コンピュートモジュール (<https://www.hpe.com/info/synergy-docs>)

前提条件

- DIMM または persistent memory modules の取り扱いは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 サーバー (<https://www.hpe.com/info/proliantgen10-docs>)
- HPE Synergy Gen10 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.  **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 サーバー (<https://www.hpe.com/info/proliantgen10-docs>)
- HPE Synergy Gen10 コンピュートモジュール (<https://www.hpe.com/info/synergy-docs>)

persistent memory modules の移行

- ❗ **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**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、次の操作を実行します。
 - a. USB キーを接続します。
 - b. **USB デバイスからのパズ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**一時パズフレーズ**を入力します。
 - d. **ファイルを選択**を選択して、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、パズ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。

詳しくは

[Persistent Memory モジュールの再配置のガイドライン](#)

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サーバーのエントリーをメモします。
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. キーマネージャー構成の下の**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. キーマネージャー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. キーマネージャー構成の下の**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) > サーバークセキュリティ > 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。

詳しくは

[Persistent Memory モジュールの再配置のガイドライン](#)

persistent memory modules のサニタイズ

サニタイズポリシー

次回の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があります。
- 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 > PMM オプション > サニタイズオプションを選択し、以下を選択します。
 - 再起動時のサニタイズ/消去操作：
 - 操作なし
 - 暗号による消去
 - メディアの上書き
 - 暗号化による消去およびメディアの上書き
 - 再起動時のサニタイズ/消去操作後のポリシー：
 - サニタイズ/消去およびシステムの再起動
 - サニタイズ/消去およびシステムの電源オフ
 - サニタイズ/消去およびシステムユーティリティの再起動
 - 工場出荷時設定へのサニタイズ/消去およびシステムの電源オフ
2. サニタイズ/消去操作の対象メモリ選択肢を有効にします。
3. サニタイズする 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。

詳しくは

[サニタイズ](#)

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	操作なし
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**必要ない**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 100 シリーズの Linux 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	注記
/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	• 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 - 現在名前スペースに割り当てられていないサイズ。
- Max_available_extent - 名前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。
- lset_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 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ー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 - この名前空間を使用している/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 - 名前空間の numa_node ID。この ID は、numactl を使用して、この名前空間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。

名前空間の作成

名前空間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 名前空間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 の未定義の名前空間を作成するには、次のコマンドを実行します。

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

すべての名前空間を一覧表示する

すべての名前空間を一覧表示するには、次のコマンドを実行します。

```
$ ndctl list
```

名前空間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
  },
  :
]
```

名前空間モードの変更

このコマンドを実行して、既存の名前空間の名前空間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/pmem0/queue/iostats
$ echo 1 > /sys/block/pmem1/queue/iostats
$ echo 1 > /sys/block/pmem2/queue/iostats
$ echo 1 > /sys/block/pmem3/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 100 シリーズの VMware サポート

VMware と HPE 向けインテル Optane Persistent Memory 100 シリーズを組み合わせる使用する方法について詳しくは、[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 100 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 100 シリーズの Windows Server サポート

Windows Server での HPE 向けインテル Optane Persistent Memory 100 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。



トラブルシューティング

既知の問題

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 ポートフォリオ

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。



サポートと他のリソース

Hewlett Packard Enterprise サポートへのアクセス

- ライブアシスタンスについては、Contact Hewlett Packard Enterprise Worldwide の Web サイトにアクセスします。

<https://www.hpe.com/info/assistance>

- ドキュメントとサポートサービスにアクセスするには、Hewlett Packard Enterprise サポートセンターの Web サイトにアクセスします。

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

ご用意いただく情報

- テクニカルサポートの登録番号（該当する場合）
- 製品名、モデルまたはバージョン、シリアル番号
- オペレーティングシステム名およびバージョン
- ファームウェアバージョン
- エラーメッセージ
- 製品固有のレポートおよびログ
- アドオン製品またはコンポーネント
- 他社製品またはコンポーネント

アップデートへのアクセス

- 一部のソフトウェア製品では、その製品のインターフェイスを介してソフトウェアアップデートにアクセスするためのメカニズムが提供されます。ご使用の製品のドキュメントで、ソフトウェアの推奨されるソフトウェアアップデート方法を確認してください。
- 製品のアップデートをダウンロードするには、以下のいずれかにアクセスします。

Hewlett Packard Enterprise サポートセンター

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

Hewlett Packard Enterprise サポートセンター：ソフトウェアのダウンロード

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

マイ HPE ソフトウェアセンター

<https://www.hpe.com/software/hpesoftwarecenter>

- eNewsletters およびアラートをサブスクライブするには、以下にアクセスします。

<https://www.hpe.com/support/e-updates>

- 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。



- ❶ **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、製品エントタイトルメントが必要な場合があります。関連するエントタイトルメントで 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。

