



Hewlett Packard
Enterprise

HPE OneView 4.1 (HPE Synergy 用) リリースノート

摘要

本書では、HPE OneView 4.1 (HPE Synergy 用) の新機能、インストールとアップデート手順、および既知の制限事項について説明します。このリリースは、HPE OneView を搭載した HPE Synergy コンポーザーを使用する HPE Synergy 上のコンピュータモジュール、インターコネクト、およびストレージシステムの構成、管理、およびトラブルシューティングを行う管理者を対象としています。

部品番号: P01319-192
発行: 2018 年 6 月
版数: 1

ご注意

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、または複製については、HPE 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・ソフトウェア資料、および商業用製品の技術情報は、ベンダー標準の商業用ライセンスのもとで米国政府に使用許諾が付与されます。

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。HPE 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。HPE は本文書中の技術的あるいは校正上の誤り、省略に対して、いかなる責任も負いかねますのでご了承ください。

商標

Microsoft® および Windows® は、Microsoft Corporation の商標です。

VMware® は、VMware Inc. の登録商標です。

保証

Hewlett Packard Enterprise は購入日から 90 日以内であれば、問題のある配布メディアを交換します。

目次

リリースの説明とインストール手順	6
はじめに.....	6
HPE OneView 4.1 (HPE Synergy 用) で提供される主な変更点.....	6
HPE OneView 4.1 (HPE Synergy 用) の新機能.....	7
アプライアンスのインストールおよびアップデート手順.....	11
アップデート後のアプライアンスのバックアップ.....	11
問題と推奨処置	12
iLO の CNSA モードの制限事項.....	12
イメージストリーマーは FIPS/CNSA に準拠せず、HPE Synergy コンポーザーで FIPS/CNSA を有効にするとサポートされない.....	12
HPE OneView 4.1 にアップデートすると、緊急ローカルログイン機能が無効になる.....	12
高可用性アプライアンスのクラスターでは HPE OneView 4.10 のアップデートが失敗する.....	12
英語以外のディレクトリサーバーのグループ名を処理における制限事項.....	13
日本語版と中国語版で 4.1 バージョンの代わりに、HPE OneView 4.0 オンラインヘルプが含まれている.....	13
ヘルプボタン (「?」) の誤動作により、たくさんの「404 Not Found」ページが表示される.....	13
Virtual Connect (VC) インターコネクトモジュールのファームウェアアップデートが完了する前に構成を変更すると、接続が不正または無効なステータスになる.....	13
ハイパーバイザークラスタープロファイルの UI を使用した OS 展開設定のパスワード変更が有効ではない.....	13
ファームウェアのベースラインが設定されないまま、クラスターが HPE OneView に存在する場合、論理エンクロージャー (LE) のファームウェアアップデートに失敗する.....	14
論理エンクロージャーのファームウェアアップデートページに、HPE Virtual Connect 16Gb 24ポートファイバーチャネルモジュールの不正なファームウェアバージョンが表示される.....	15
間違ったパスワードエラーのため、ハイパーバイザークラスタープロファイルの作成または拡張が断続的に失敗する.....	15
ハイパーバイザークラスターのプロファイルをトークンを使用して、クラスター内の各ハイパーバイザーホストに対して固有のホスト名を作成できない.....	15
HPE OneView UI のハイパーバイザークラスターのプロファイルには、ハイパーバイザープロファイルを削除するための強制オプションがない.....	16
ハイパーバイザークラスターを作成すると、作成されたすべてのホストに同じホスト名が使用される.....	17
クラスターのプロファイルにボリュームを追加した後、サーバープロファイルのページを読み込めない.....	17
プロファイルを適用してはならない場合、プロファイルは誤ってプログラムされた HPE Synergy 480 Gen9 Multi MXM 拡張モジュールに適用される.....	18
サーバープロファイルまたはサーバープロファイルのテンプレートでブート可能とマークされた iSCSI ボリュームを削除できない.....	18
接続およびローカルストレージにプロファイルを適用すると内部エラーが発生し、接続の定義がプロファイルから削除される.....	18
複数の手動 Remote Support コレクションを同時に実行すると、HPE OneView がメモリ制限およびフェイルオーバーになる可能性がある.....	19
ネットワーク URI が変更された場合、不正な検証エラーが発生する.....	19
SAN 自動ゾーニング機能の問題.....	20
CHAP 名の長さ制限.....	20
論理インターコネクトファームウェアのアップデート実行時に発生するサーバーの電源状態の問題.....	20
BIOS 設定の編集ページの UEFI iSCSI ブートポリシーフィールドが適用されない.....	20

単一の HPE Synergy コンポーザー構成では、高可用性 (HA) の警告アラートをクリア不可能	20
HPE OneView のリストア操作後、Remote Support に失敗する	21
サーバーハードウェアの取り外しと挿入中に、Remote Support のデータコレクションが失敗する	21
サーバーが挿入された後に Remote Support が有効にならない	21
HPE Synergy コンポーザーの初期セットアップ中の問題	21
サーバーの電源を投入すると、アクティビティページに重複するアラートが表示される	22
サーバーハードウェアを取り外して再挿入すると、SAN 構成からブートする設定が失われる	22
サーバープロファイルの作成/編集ダイアログボックスで[作成/作成+OK]ボタンが動作しない	22
FCoE VLAN について推奨される Cisco トップオブラックスイッチ構成	22
オンラインヘルプのサーバーハードウェア画面で、ヘッダーにポートではなくアダプターと表記される	23
アクティブなフレームリンクモジュール (FLM) を同じバージョンのファームウェアを実行している FLM と置き換えると、HPE OneView で「アップデート」エラーが報告される	23
HPE OneView がオフラインの場合、アップデートしても、ベイが変更されたブレードについて報告されない	23
異なるインターコネクトモジュールにケーブルで直接接続された 3PAR Persistent Ports ポートペアがサポートされない	23
HPE Synergy Gen10 サーバーで iSCSI ポリシー BIOS をデフォルト以外の値に変更すると、起動が失敗する	24
削除されたネットワークで接続が引き続き使用されているというアラート	24
Smart アレイメザニンコントローラーの内蔵ドライブを選択すると、プロファイル作成に失敗する	24
アップリンクセットからネットワークを削除してもアラート、不正なプロファイルと接続状態が表示されない	24
リモートコンソールウィンドウが表示されるが、サーバーに接続されていない	25
HPE Synergy コンポーザー 4.1 によって管理されるフレームの削除	25
接続が、DHCP およびマネージドボリュームを使用している 2 つの iSCSI ブート接続のいずれかであった場合、接続を iSCSI ブート可能接続に戻すことができない	25
サーバーが iLO のリセット直後に更新すると、iLO5 の HPE OneView SNMP 構成が破損する	25
HPE OneView によって Gen10 ハードウェアが検出されない	26
アプライアンスの Web サーバー証明書の有効期限が切れていると、HPE OneView 4.1 へのアップデートに失敗する	26
スタックされたインターコネクトモジュールのいずれかまたは両方が取り外され、再度挿入されると、不正なスタッキングヘルスアラートが発生する	27
中国語ローカリゼーションを採用した HDD ドライブタイプを使用して論理 JBOD を作成すると、エラーが発生する	27
ネットワークの削除がサーバープロファイルで検出されない	27
SAN ボリュームアタッチメントがサーバープロファイルテンプレートから削除されると、誤った整合性警告アラートが表示される	28
ホスト名が数値のみで構成されている場合、アプライアンスネットワークの設定が失敗する	28
サブタスクが完了しても、Remote Support マスタータスクが完了しない	28
ルート CA 「iLO/iLO 3/iLO 4/iLO 5 デフォルト発行元 (信頼しない)」を信頼する	29
ドメインの完全な DNS 名でエンタープライズディレクトリサーバーを構成する	29
ホスト名の検証問題は、ドメインの完全な DNS 名を使用して、エンタープライズディレクトリサーバーを構成して通信するときに発生する	29
Active Directory サーバーの構成には TLS v1.2 を使用	30
ネットワークサブネットマスク設定の変更が UI で反映されない場合、「展開サーバーの追加」に失敗する	30
ファームウェアアップデート後、HPE Synergy コンピュータモジュールでファイルシステムが読み取り専用になる	30
スキャンツールによって脆弱な SSH 暗号の問題が報告される	30

HPE OneView 4.1 (HPE Synergy 用) に関する注意..... 31

ドキュメントの補足.....	32
HPE OneView 4.1 へのアップデート中および自動ハードウェア検出中の証明書の処理.....	32
iLO の有効期限が切れた証明書の修正.....	32
ルート証明書または中間証明書の有効期限が切れたときの回復オプション.....	33
セキュリティ.....	33
HPE OneView API リファレンス.....	33
ハイパーバイザーのサポート.....	33
3PAR ストレージレイとの FC 直接接続.....	33
HPE Synergy コンポーザーから受け取った Remote Support イベントの表示.....	34
API バージョンのサポートを削除.....	34
Gen10 サーバーに関する ESXi OS のファームウェアとドライバーのアップデート.....	34
HPE Synergy のドキュメントおよびトラブルシューティングの資料.....	35
HPE Synergy のドキュメント.....	35
HPE Synergy 構成および互換性ガイド.....	35
HPE Synergy フレームリンクモジュールユーザーガイド.....	35
HPE OneView (HPE Synergy 用) ユーザーガイド.....	35
HPE OneView Global Dashboard.....	35
HPE Synergy イメージストリーマーユーザーガイド.....	35
HPE Synergy Image Streamer GitHub.....	36
HPE Synergy Software Overview Guide.....	36
HPE Synergy ファームウェアとドライバーアップデートのためのベストプラクティス.....	36
HPE OneView (HPE Synergy 用) サポートマトリックス.....	36
HPE Synergy イメージストリーマーサポートマトリックス.....	36
HPE Synergy 用語集.....	36
HPE Synergy のトラブルシューティング資料.....	36
HPE OneView でのトラブルシューティング.....	37
HPE Synergy トラブルシューティングガイド.....	37
HPE ProLiant Gen10 サーバーおよび HPE Synergy エラーメッセージガイド.....	37
HPE OneView ヘルプと HPE OneView API リファレンス.....	37
HPE Synergy QuickSpecs.....	37
HPE Synergy ドキュメントの概要 (ドキュメントマップ)	38
サポートと他のリソース.....	39
Hewlett Packard Enterprise サポートへのアクセス.....	39
アップデートへのアクセス.....	39
Web サイト.....	40
リモートサポート (HPE 通報サービス)	40
カスタマーセルフリペア (CSR)	40
ドキュメントに関するご意見、ご指摘.....	41

リリースの説明とインストール手順

はじめに

このドキュメントでは、HPE OneView 4.1（HPE Synergy 用）のリリース情報を提供します。

対象読者	関連情報
すべてのユーザー	<ul style="list-style-type: none">・ 主な特徴・ ドキュメントの補足・ 関連製品および技術ドキュメントの見つけかたに関するサポートと他のリソース
新しいアプライアンスをインストールするユーザー	<ul style="list-style-type: none">・ アプライアンスのインストール手順・ HPE OneView 4.1（HPE Synergy 用）の使用に関する問題と推奨処置

最新のアップデート情報については、[Hewlett Packard Enterprise Information Library](#) をご覧ください。

HPE OneView 4.1（HPE Synergy 用）で提供される主な変更点

HPE Synergy バージョン用の HPE OneView 4.1 は、次の目的で設計されています。

- ・ HPE OneView へのアップデート後、サーバープロファイルテンプレートで編集時にエラーが発生する問題を解決する。
- ・ サーバープロファイルテンプレートのサーバープロファイルの変更によって、接続エラーメッセージが表示される問題を解決する。
- ・ カスタムダッシュボードパネルがスコープで動作せず、アクティビティが結果をフィルターしない問題を解決する。
- ・ 署名済み証明書をインポートするときに、証明書のインポートに失敗する問題を解決する。
- ・ iLO で HPE Synergy IP アドレスプールとドメインが設定されていない問題を解決する。
- ・ HPE Synergy 論理インターコネクトの HPE Virtual Connect SE 16Gb FC モジュールが存在する場合、1 から 2 への冗長化 HA の拡張が失敗する問題を解決する。
- ・ ロケールが日本語に設定され、再起動するたびに HPE OneView にディスクパーティションエラーのための不正なアラートが表示され、イメージストリーマーの起動に失敗する問題を解決する。
- ・ サーバープロファイルを作成しても次のクリティカルアラートを受信する問題を解決する。**サーバーアダプターの構成情報を読み取ることができません。**
- ・ HPE OneView のアップデートに失敗した後、アプライアンスが以前の動作状態に戻らない問題を解決する。
- ・ 論理エンクロージャーを追加するときに、**各デバイスおよびインターコネクトの IP を割当てするための IPv4 アドレスプール内の IP アドレスが不足しています。**という間違っただアラートを受信する問題を解決する。
- ・ HPE Synergy 論理エンクロージャーをインストールする際に、エンクロージャーのミッドプレーンの 1 つがデフォルトの 0000010 シリアル番号であるために発生する問題を解決する。

- ・ Web UI の再起動後に HPE OneView が起動しない問題を解決する。
- ・ リング拡張シナリオでイメージストリーマーハングの 2 番目のペアと共に論理エンクロージャーが作成される問題を解決する。
- ・ 起動時にタイムアウトが発生し、DNS と NTP が同期の確認を行う問題を解決する。
- ・ 1 つ以上のピリオド文字を含む共通プロビジョニンググループ (CPG) を使用して HPE 3PAR を追加すると、jQuery エラーが発生し、**ストレージシステムの追加ダイアログ**が表示されなくなる問題を解決する。
- ・ イメージストリーマー **FIPS/CNSA 互換性レポート**タスクが **FIPS/CNSA 互換性レポート**の親タスクのサブタスクではない問題を解決する。
- ・ 3PAR VMware 仮想ボリュームを使用すると、**非管理ボリュームのプロファイルアクセス**のアラートが発生し、HPE OneView によって管理されていないボリュームへのアクセスが削除される問題を解決する。
- ・ プロファイル操作中およびサーバーの電源をオンにしている間、接続障害のアラートが過渡に発生する問題を解決する。
- ・ HPE OneView 3.10.07 から 4.00.05 にアップデートした後、アプライアンスに名前のない証明書がある問題を解決する。
- ・ Gen10 サーバー プラットフォームの CPU 利用率が HPE OneView で正しく表示されない問題を解決する。
- ・ 制約違反のために HPE OneView のアップデートがデータベースのアップデートに失敗する問題を解決する。
- ・ 値が提供されていないにもかかわらず、サーバープロファイルテンプレートの**編集**ページにパスワード値が暗号化された形式で表示される問題を解決する。
- ・ イメージストリーマーの OS 展開プランでパスワードを後で編集しようと空白にしておくと、パスワードが設定されたと誤って示される問題を解決する。
- ・ CA の署名済み証明書に関連する IP またはホスト名が HPE OneView で変更された場合、FLM が HPE OneView との通信に失敗する問題を解決する。

HPE OneView 4.1 (HPE Synergy 用) の新機能

セキュリティ

・ HPE OneView 暗号化のサポート

HPE OneView には、管理アプライアンスを連邦情報処理標準 FIPS-140-2 (FIPS 140-2) および Commercial National Security Algorithm (CNSA) 標準に準拠するように構成するか、レガシー暗号化モードを引き続き使用するオプションがあります。FIPS 140-2 および CNSA モードでは、アプライアンスがプロトコルバージョン、暗号スイート、およびデジタル証明書強度をそれぞれ、FIPS 140-2 および CNSA に準拠したものに制限します。

・ iLO セキュリティモードのサポート

すべての HPE iLO セキュリティ状態がサポートされています。

- iLO 5 高度なセキュリティ、FIPS、および CNSA (スイート B) モード
- すべての iLO 5 セキュリティモードでサポートされているオンラインおよびオフラインのファームウェアアップデート
- iLO 4 を搭載した Gen9 サーバー (FIPS のみサポート)

・ Gen10 高度なセキュリティ/FIPS モードのファームウェアとドライバーのアップデート

SUT 2.2.0 および SUM 8.2.0 では、iLO が高度なセキュリティモードまたは FIPS モードの場合、ファームウェアとドライバーのアップデートがサポートされます。

注記: Gen10 サーバーの場合、SUT バージョンは iSUT 2.3.0 以降が必要です。

- ・ **カスタマイズ可能な TLS バージョン**

TLS1.0/TLS1.1 を選択的に無効にする REST API

- ・ **Spectre および Meltdown の脆弱性に対応**

HPE OneView 仮想アプライアンスは、最近公開された Spectre および Meltdown の脆弱性 (CVE-2017-5754、CVE-2017-5753、CVE-2017-5715、CVE-2018-3640、および CVE-2018-3639) での脆弱性はありません。これらの脆弱性は、OS へのローカルアクセスを必要とし、HPE OneView はアプライアンス上でユーザーがローカルで実行することを許可しません。HPE OneView は直接的な脆弱性はありませんが、適切な OS レベルの軽減が適用されています。これらの軽減策の一部は、対応するベンダーのハイパーバイザーのパッチによって異なります。

プライバシー

- ・ HPE OneView リモートサポート - 個人情報 (PII) は暗号化されています。
- ・ 基本データコレクションは、リモートサポート UI で表示できなくなりました。この新機能により、暗号化されていない PII データは公開されず、プライバシー規制に準拠します。HPE サポートに問い合わせ、収集データの例を参照するか、<http://www.hpe.com/info/insightremotesupport/docs> からセキュリティおよびプライバシーのホワイトペーパーを参照してください。

テンプレート/プロファイルの機能強化

- ・ **サーバーの電源をオンにして BIOS 設定をアップデートする**

サーバーハードウェアの電源が入っている間のみ、BIOS の設定を修正できます。

この新しい機能は Gen9 以降のサーバーでサポートされています。新しい BIOS 設定は、次回の電源投入時に有効になります。

- ・ **電源をオンにした時、HPE Synergy サーバーにプロファイル (ファームウェアと BIOS のみ) を割り当てる**

HPE OneView は現在、既存のサーバーで HPE OneView を採用しようとするお客様をサポートしていますが、製品ワークロードがオフラインのままプロファイルを適用することはできません。特定の構成のサーバープロファイルは、サーバーハードウェアの電源が入っている間に割り当てても、割り当ての解除もできません。

このサポートは次の場合に利用できます。

- Gen8 以降のサーバーで、すべての管理対象に Smart Update ツールを使用したファームウェア管理
- Gen9 以降のサーバーで、すべての管理対象の BIOS 設定管理
- HPE Synergy の物理シリアル番号/UUID

- ・ **ファームウェアのローリングアップデート**

論理エンクロージャーのファームウェアアップデートは、共有インフラストラクチャとサーバープロファイルを更新するとき、**統合インターコネクティブモード**を選択した場合、クラスター対応の方法で行われます。

関連するハイパーバイザープロファイルを持つ論理エンクロージャーのサーバープロファイルは、ローリング方式でファームウェアをアップデートします。これにより、製品ワークロードを実行しているサーバー上のファームウェアを中断せずにアップデートする場合に役立ちます。

関連するハイパーバイザープロファイルを持つ各サーバープロファイルについて、ハイパーバイザーはメンテナンスモードに置かれ、仮想マシンを移行し、ファームウェアや OS ドライバーをアップデートし、ハイパーバイザーがメンテナンスから抜けて仮想マシンのスケジュールを実行できます。このプロセスは、ハイパーバイザークラスターのプロファイルの一部である、論理エンクロージャーの各サーバープロファイルに順次繰り返されます。

関連するハイパーバイザープロファイルを持たないサーバープロファイルは、動作の変更がないままファームウェアがアップデートされます。

ハイパーバイザークラスタープロファイル

- ・ ハイパーバイザークラスターのプロファイルを使用して、HPE OneView によって管理されるサーバ上で実行されるハイパーバイザーのクラスターを展開および管理する機能です。ハイパーバイザークラスタープロファイルにより、サーバーノードからハイパーバイザークラスターまでの一貫した構成が調整し、同じワークロードを共有します。ハイパーバイザークラスタープロファイルでは、サーバープロファイルテンプレートをベースとして使用して、サーバーノードとハイパーバイザーの構成を定義します。
 - ハイパーバイザークラスタープロファイルは、VMware vCenter サーバーを利用して、VMware ESXi ベースのハイパーバイザークラスターを管理できます。
- ・ ハイパーバイザークラスタープロファイルを使用して、ハイパーバイザークラスターを作成することも、既存のハイパーバイザークラスターを HPE OneView にインポートして、ハイパーバイザークラスタープロファイルを使用して管理することもできます。
- ・ ハイパーバイザークラスターの拡張または縮小などのライフサイクル操作の管理、構成の変更、整合性チェックやローリングアップデート、サーバーノードでの中断を伴わないファームウェアアップデートができます。
 - HPE Synergy イメージストリーマー OS 展開プランを含むハイパーバイザークラスタープロファイルを使用すると、クラスターを拡張するための追加のハイパーバイザーをプロビジョニングすることができます。OS 展開プランで設定されていないハイパーバイザークラスタープロファイルの場合は、サーバープロファイルを作成し、外部ツールを使用してクラスターに vSphere を展開およびハイパーバイザーを追加し、ハイパーバイザーをハイパーバイザークラスタープロファイルにインポートして、不整合を修復することで、クラスターを拡張できます。

ファームウェア

- ・ **iLO レポジトリベースのオフラインアップデート (Gen10)**

この新しいアプローチでは、すべてのコンポーネントが iLO レポジトリにステージングされ、ビットをステージングするために 1GB のスペースが提供されます。

 - 各コンポーネントは、信頼できる HPE シグネチャーの iLO によって検証されます。有効なシグネチャーが見つからない場合、コンポーネントはフラッシュされません。
 - ファームウェアのアップデートで、iLO と UEFI シェルはネイティブフラッシュ機能を提供し、最大 80% までコンポーネントに対応します。SUT が必要なコンポーネントは、たとえば HDD など、ほんのわずかです。

- この新しいファームウェアアップデートアーキテクチャーは、特に SPP ブートが不要な場合、ファームウェアアップデートに要する時間を最大 30%まで節約することで、Gen10 サーバー プラットフォームのファームウェアアップデート時間を短縮します。
- この新しいアプローチは、HPE OneView へのサーバーの接続が遅い場合に役立ちます。HPE OneView は、アップデートが必要なコンポーネントのみを iLO レポジトリへアップロードします。

ストレージ

・ 3PAR 大容量および圧縮のサポート

HPE OneView は、ボリュームの有効期間全体を通して 3PAR ボリュームの圧縮状態を管理し、最大サイズ 64TiB (16TiB から増加) の 3PAR ボリュームをサポートします。

・ SAN ストレージボリューム管理でサポートされる Brocade FC インターコネクトモジュール

HPE OneView は、Brocade ファイバーチャネルのインターコネクトモジュールを使用している場合、サーバープロファイルとサーバープロファイルテンプレートベースによる SAN ストレージの自動ボリュームプロビジョニングと接続管理をサポートします。サポートされる構成には、Brocade FC 8Gb に接続された HPE Synergy Gen9 以降のサーバーおよび 3PAR ストレージに接続された外部 Brocade SAN にアップリンクした 16Gb インターコネクトモジュールが含まれます。この構成では、お客様がサーバーの接続を定義してサーバーポートのネットワーク/SAN を選択することにより、データボリュームを管理できます。現時点では、SAN からのブートはサポートされていません。お客様は、選択したネットワーク/SAN が Brocade のダウンリンクポートにプロビジョニングされていることを確認する必要があります。Brocade FC インターコネクトモジュールを含む Brocade SAN は、HPE OneView SAN 管理機能の一環として HPE OneView によって自動ゾーニングできます。

バーチャルコネク

- ・ ダウンリンクでのポートのミラーリング
- ・ Cisco ACI 統合

イメージストリーマーアプライアンス要求の機能強化

このリリースでは、イメージストリーマーが要求した関連タスクとアラートが、HPE OneView ユーザーインターフェイスの**エンクロージャー**ページに表示されます。要求プロセスに問題がある場合は、**エンクロージャー**ページに問題の詳細に関するアラートが表示されます。このアラートの工場出荷時のリセットリンクを使用すると、イメージストリーマーアプライアンスの工場出荷時のリセットを実行し、工場出荷時のリセットが完了した後で要求プロセスを再初期化できます。この機能は、失敗した要求の操作を再試行するために、以前のリリースを必要とするラボ訪問または SSH からメンテナンスコンソールへのアクセスを回避するときに役立ちます。

アプライアンスのメンテナンスコンソールを使用して、イメージストリーマーアプライアンスを工場出荷時の状態にリセットする場合は、手動で要求プロセスを初期化する必要があります。API を使用してイメージストリーマーアプライアンスの要求プロセスを初期化することができます。

API の詳細情報については、[HPE 情報ライブラリ](#)にある **HPE Synergy イメージストリーマー REST API リファレンスの OS 展開サーバー**を参照してください。

サポート可能性/リモートサポート

- ・ ケース用のメール通知のオープンまたはクローズ

メール通知は、ケースおよび契約期限を送信します。ユーザーは、サポートケースの作成、サポートケースのクローズ、および契約/保証が期限切れから 90、60、30 日間、またはすでに期限切れになったときに、メールを送信するように設定できます。

・ サポート技術者のリモートデバイスへのアクセス

お客様の許可を得て、認定されたサポート技術者がリモートデバイスへのアクセスを提供します。HPE サポート技術者は、トラブルシューティングおよび解決のために、HPE OneView アプライアンスにリモートで安全に接続できます。

新しい機能および追加ドキュメントの関連情報の詳細情報については、[HPE Synergy のドキュメントおよびトラブルシューティングの関連情報](#)を参照してください。

アプライアンスのインストールおよびアップデート手順

インストール手順については、www.hpe.com/info/synergy-docs のドキュメントを参照してください。

アップデートイメージファイルは、www.hpe.com/downloads/synergy の HPE Synergy ソフトウェアリリースで入手できます。

アップデート後のアプライアンスのバックアップ

アプライアンスをアップデートした後、忘れずに新しいバックアップファイルを作成してください。バックアップをリストアするには、プラットフォームタイプ、ハードウェアモデル、アプライアンスのファームウェアのメジャーおよびマイナー番号が一致している必要があります。アプライアンスのファームウェアバージョンの形式は次のとおりです。

majornumber.minornumber.revisionnumber-buildnumber

リビジョン番号とビルド番号は一致しなくても構いません。

リストアできるのは、ハードウェアモデルが同一の HPE Synergy コンポーザーについて、HPE OneView 4.1 で作成されたバックアップファイルのみです。

問題と推奨処置

ここでは、このリリースの問題と既知の制限事項について説明します。

iLO の CNSA モードの制限事項

管理対象サーバーの iLO が Commercial National Security Algorithm (CNSA) モード、またはスイート B モードの場合、HPE OneView コンソールから iLO ユーザーインターフェイスまたはコンソールにアクセスすることはできません。

イメージストリーマーは FIPS/CNSA に準拠せず、HPE Synergy コンポーザーで FIPS/CNSA を有効にするとサポートされない

イメージストリーマーは連邦情報処理規格 (FIPS) または Commercial National Security Algorithm (CNSA) に準拠しないため、HPE Synergy コンポーザーで有効になっている FIPS/CNSA ではサポートされていません。この確認は強制ではありませんが、構成はサポートされている製品構成ではありません。

HPE OneView 4.1 にアップデートすると、緊急ローカルログイン機能が無効になる

問題

非常にまれなシナリオでは、HPE OneView 4.1 にアップデートすると、緊急ローカルログイン機能が無効になります。

推奨処置

1. 緊急ローカルログインの設定は、**[設定 > のセキュリティページ**で確認してください。
2. ローカルログインを有効にすると、アプライアンスは緊急ローカルログインを暗黙的に有効にします。ローカルログインが無効になっている場合は、**設定 > のセキュリティページ**から緊急ローカルログインを再度有効にします。

高可用性アプライアンスのクラスターでは HPE OneView 4.10 のアップデートが失敗する

問題

高可用性アプライアンスのクラスターでは HPE OneView 4.10 のアップデートが失敗します。アプライアンスがアップグレード前の状態に戻し、スタンバイアプライアンスを「接続なし」状態のままにします。

推奨処置

1. アプライアンスの高可用性をリストアするには、**設定 > アプライアンス > のアクションメニュー**からスタンバイの削除アクションを開始します。
2. アプライアンスの同期を待つと、ステータスが「接続」に戻ります。
3. アップデートを再試行してください。

英語以外のディレクトリサーバーのグループ名を処理における制限事項

アクティブディレクトリサーバーまたは Open LDAP などのディレクトリサーバーが、中国語や日本語など、英語以外のグループ名で構成されている場合、HPE OneView のサポートはそのような名前の選択、表示、および使用をサポートします。Firefox バージョン 57 以降、または Chrome バージョン 64 以上を使用している場合、中国語または日本語のグループ名を選択した後に、グループの追加操作で構成されたグループのリストが表示されません。グループは追加されましたが、GUI がそのグループに関する情報を表示できません。グループは API を通じてのみ削除できます。Microsoft Internet Explorer または Microsoft Edge を使用している場合は、そのようなグループ名が正しく表示されます。

日本語版と中国語版で 4.1 バージョンの代わりに、HPE OneView 4.0 オンラインヘルプが含まれている

HPE OneView 4.1 オンラインヘルプでは、日本語と中国語の翻訳は利用できません。HPE OneView 4.1 製品には、日本語と中国語バージョンの HPE OneView 4.0 オンラインヘルプが含まれています。

ヘルプボタン（「？」）の誤動作により、たくさんの「404 Not Found」ページが表示される

問題

翻訳されたオンラインヘルプ（日本語または中国語 - 簡体字）を表示すると、ユーザーインターフェイスにオンラインヘルプトピックが表示されないリンクがあります（404 エラー）。

推奨処置

[Hewlett Packard Enterprise 情報ライブラリ](#)で最新の英語版オンラインヘルプにアクセスし、完了しようとしているタスク、または画面に関連するキーワードを使用して検索してください。

Virtual Connect（VC）インターコネクトモジュールのファームウェアアップデートが完了する前に構成を変更すると、接続が不正または無効なステータスになる

Virtual Connect（VC）インターコネクトモジュールのファームウェアアップデートが完了する前に HPE OneView の構成を変更すると、接続が不正または無効なステータスになるなどの予期しない動作が発生する可能性があります。

推奨処置

VC インターコネクトモジュールのファームウェアアップデートを実行するときは、HPE OneView 内の構成を論理インターコネクトに変更しようとする前に、モジュールが完全にアップデートされて、新しいファームウェアがアクティブになるまで待ちます。ここでいう変更には、ネットワーク、ファブリック、プロファイル、および共有アップリンクセットの追加または編集が含まれます。

ハイパーバイザークラスタープロファイルの UI を使用した OS 展開設定のパスワード変更が有効ではない

問題

一部のシナリオでは、ハイパーバイザークラスタープロファイル UI を使用して OS 展開設定のパスワードを変更できません。

症状

UI を使用してハイパーバイザークラスタープロファイルを編集し、OS 展開設定でパスワードのみを変更すると、タスクは正常に完了されても、新しいパスワードがハイパーバイザークラスタープロファイルに保存されません。HPE OneView REST API には、この問題はありません。

原因

ハイパーバイザークラスタープロファイルの OS 展開設定で設定された新しいパスワードは、ハイパーバイザークラスタープロファイルに追加される新しいハイパーバイザーにのみ適用されます。既存のクラスターメンバーは新しいパスワードがアップデートされないことがあります。これは予想される動作です。既存のクラスターメンバーを変更する必要がある場合は、パスワードを ESXi コンソールから直接変更するか、ハイパーバイザープロファイルを使用してハイパーバイザーを再展開します。

注記: この問題は、イメージストリーマーを搭載した HPE Synergy ハードウェアでのみ発生します。

推奨処置

パスワードは、次のメカニズムを使用して既存のクラスターメンバーで変更できます。

1. HPE OneView UI を使用してハイパーバイザークラスタープロファイルを編集します。
2. パスワードを変更し、ハイパーバイザークラスタープロファイルにハイパーバイザーを追加します。UI を使用してハイパーバイザークラスターを拡張する場合は、OS 展開設定を変更できます。
3. ハイパーバイザークラスタープロファイル REST API を使用して、パスワード OS 展開設定を変更することもできます。

ファームウェアのベースラインが設定されないまま、クラスターが HPE OneView に存在する場合、論理エンクロージャー (LE) のファームウェアアップデートに失敗する

問題

ハイパーバイザークラスタープロファイルで論理エンクロージャー (LE) をアップデートし、統合アップデートオプションを使用した場合、ファームウェアベースラインを「手動で管理」にすると、削除に失敗します。

症状

ユーザーは、ハイパーバイザークラスタープロファイルを編集し、不要になったハイパーバイザープロファイルを削除することにより、ハイパーバイザークラスターを縮小することができます。再試行で編集操作が失敗した場合、HPE OneView UI はハイパーバイザープロファイルを削除する強制オプションを提供しません。

原因

HPE OneView 以外のファームウェアを管理する場合は、LE ファームウェアのベースラインを「手動で管理する」にしてアップデートできます。LE サーバープロファイルのいずれかがハイパーバイザークラスタープロファイルによって使用されている場合、統合ファームウェアアップデートを使用されていると、ファームウェアベースラインを削除する LE アップデート操作に失敗する可能性があります。

推奨処置

統合アップデートオプションを使用して LE のファームウェアベースラインを削除する必要がある場合は、LE の共有インフラストラクチャのみをアップデートします。この編集を投稿すると、LE のすべてのサーバープロファイルがファームウェアベースラインを削除します。つまり、手動で管理するオプションでファームウェアベースラインをアップデートします。

論理エンクロージャーのファームウェアアップデートページに、HPE Virtual Connect 16Gb 24 ポートファイバーチャネルモジュールの不正なファームウェアバージョンが表示される

問題

SPP 2016.06.0 から HPE Virtual Connect 16Gb 24 ポートファイバーチャネルモジュールコンポーネントを使用して、カスタム SPP を作成すると、論理エンクロージャーのファームウェアアップデートページに、コンポーネントの不正なバージョンが表示されます。

推奨処置

動作の変更は必要ありません。UI に間違ったファームウェアバージョンが表示されても、必要に応じて正しいファームウェアをインストールします。インストールが完了すると、インターコネクトおよび論理インターコネクトページに、インストールされたファームウェアバージョンが表示されます。

間違ったパスワードエラーのため、ハイパーバイザクラスタープロファイルの作成または拡張が断続的に失敗する

問題

間違ったパスワードエラーのため、ハイパーバイザクラスタープロファイルの作成または拡張が断続的に失敗します。

症状

ホストが誤ったパスワードエラーで VMware vCenter を追加できないため、ハイパーバイザーのホストプロファイルが正しく構成されていません。

原因

イメージストリーマーで OS ビルドプランを使用すると、一連の手順で OS を構成できます。管理 NIC の構成後にパスワード構成手順を実行すると、断続的に問題が観測されます。

注記: この問題は、イメージストリーマーを搭載した HPE Synergy ハードウェアでのみ発生します。

推奨処置

1. 操作を再試行してください。
2. または、管理 NIC が OS ビルドプランで構成される前に、パスワードが最初の手順として構成されていることを確認してください。

注記: VMware ESXi 用の最新のイメージストリーマーのアーティファクトバンドルにはすでにこの変更が適用されています。

ハイパーバイザークラスターのプロファイルをトークンを使用して、クラスター内の各ハイパーバイザーホストに対して固有のホスト名を作成できない

問題

このリリースでは、ハイパーバイザークラスターのプロファイルをトークンを使用して、クラスター内の各ハイパーバイザーホストに対して固有のホスト名を作成する機能を利用できません。

症状

ハイパーバイザークラスタープロファイルを作成すると、サーバープロファイルテンプレートでホスト名が指定されていない場合、ハイパーバイザークラスタープロファイルの **OS 展開設定** セクションにホスト名を入力するオプションが表示されます。ここには静的なテキストしか入力できません。入力すると、すべてのハイパーバイザーが同じホスト名で構成されます。

原因

ホスト名は OS 展開設定の 1 つであり、ハイパーバイザークラスタープロファイルの **OS 展開設定** セクションに入力するか、ハイパーバイザーごとに異なるホスト名を指定することができます。ハイパーバイザークラスタープロファイル UI および REST API は、指定トークンをサポートしないため、ハイパーバイザークラスタープロファイルの **OS 展開設定** セクションで静的テキストが指定されているかどうかについて検証しません。

推奨処置

ハイパーバイザークラスタープロファイルの操作中に、固有のホスト名を作成するためには、次の手順を実行します。

1. ハイパーバイザークラスタープロファイルの **OS 展開設定** セクションでホスト名を指定しないでください。ハイパーバイザーを追加すると、追加される各ハイパーバイザーのホスト名を入力するように求められます。固有の有効なホスト名を入力できます。
2. トークンまたはトークンとテキストの組み合わせを使用して、サーバープロファイルテンプレートでホスト名を指定することもできます。
 - ・ 例 1: エンクロージャーとエンクロージャーのベイトークンを組み合わせ、その間に {enclosure}- {enclosurebay} のようにハイフンを入力します。エンクロージャー名が **Enc1** で、プロファイルがベイ 2 に適用されている場合、結果的にホスト名は **Enc1-2** になります。
 - ・ 例 2: ハイパーバイザークラスタープロファイルの **ハイパーバイザーテンプレート** セクションで、ハイパーバイザープロファイル名プレフィックスを指定できます。作成されたプロファイルごとに、プロファイル名プレフィックスに連番が追加されます。 **ESXi-Profile-** をプロファイル名プレフィックスに指定した場合、プロファイルの名前は **ESXi-Profile-1**、**ESXi-Profile-2** などとなります。 **OS 展開設定** セクションで、ホスト名を指定して {profile} トークンを使用すると、結果的にホスト名がプロファイル名と同一になります。

HPE OneView UI のハイパーバイザークラスターのプロファイルには、ハイパーバイザープロファイルを削除するための強制オプションがない

問題

HPE OneView UI のハイパーバイザークラスターのプロファイルには、ハイパーバイザープロファイルを削除するための強制オプションがない

症状

ユーザーは、ハイパーバイザークラスタープロファイルを編集し、不要になったハイパーバイザープロファイルを削除することにより、ハイパーバイザークラスターを縮小することができます。再試行で編集操作が失敗した場合、HPE OneView UI はハイパーバイザープロファイルを削除する強制オプションを提供しません。

注記: この問題は、REST API ユーザーには適用されません。ハイパーバイザーマネージャーのタスクが失敗した場合でも、REST API が、ハイパーバイザープロファイルを削除する要求に強制パラメーターを渡すことをサポートするためです。

原因

HPE OneView UI は、ハイパーバイザークラスタープロファイルからハイパーバイザーの強制削除をサポートしていません。

推奨処置

ハイパーバイザープロファイルが、ハイパーバイザーマネージャーによって報告された問題のためにハイパーバイザープロファイルを削除する操作を編集できない場合は、強制クエリパラメーターを true に設定して、これらのハイパーバイザープロファイルを削除するために REST API を使用します。REST API 仕様を参照してください。

ハイパーバイザークラスターを作成すると、作成されたすべてのホストに同じホスト名が使用される

問題

このリリースでは、ハイパーバイザークラスターのプロファイルトークンを使用して、クラスター内の各ハイパーバイザーホストに対して固有のホスト名を作成する機能を利用できません。

推奨処置

1. ハイパーバイザークラスタープロファイルの **OS 展開設定** セクションでホスト名を指定しないでください。ハイパーバイザーを追加すると、アプライアンスが追加される各ハイパーバイザーのホスト名を入力するように求めます。固有の有効なホスト名を入力できます。
2. トークンまたはトークンとテキストの組み合わせを使用して、サーバープロファイルテンプレートでホスト名を指定することもできます。
 - a. 例 1: エンクロージャーとエンクロージャーのベイトークンを組み合わせ、その間に `{enclosure}-` `{enclosurebay}` のようにハイフンを入力します。エンクロージャー名が Enc1 で、プロファイルがベイ 2 に適用されている場合、結果的にホスト名は Enc1-2 になります。
 - b. 例 2: ハイパーバイザークラスタープロファイルの **ハイパーバイザーテンプレート** セクションで、プロファイル名プレフィックスを指定できます。作成されたプロファイルごとに、プロファイルプレフィックスに連番が追加されます。「ESXi-Profile-」をプロファイル名プレフィックスに指定した場合、プロファイルの名前は「ESXi-Profile-1」、「ESXi-Profile-2」などとなります。**OS 展開設定** セクションで、ホスト名を指定して `{profile}` トークンを使用すると、結果的にホスト名がプロファイル名と同一になります。

クラスターのプロファイルにボリュームを追加した後、サーバープロファイルのページを読み込めない

問題

まれなシナリオでは、共有ボリュームをハイパーバイザークラスタープロファイルに追加した後、サーバープロファイルページを読み込めません。

推奨処置

1. ブラウザーページを更新します。
2. ページがまだロードされていない場合は、ブラウザを閉じて HPE OneView を再度開きます。

プロファイルを適用してはならない場合、プロファイルは誤ってプログラムされた HPE Synergy 480 Gen9 Multi MXM 拡張モジュールに適用される

問題

プロファイルを適用してはならない場合、HPE OneView がインポートされ、プロファイルは誤ってプログラムされた HPE Synergy 480 Gen9 Multi MXM 拡張モジュールに適用される。

症状

複数の MXM 拡張モジュールを備えた HPE Synergy 480 Gen9 のサーバーハードウェアページの**プロファイルを作成**ダイアログから新しいプロファイルを作成すると、失敗と共にこのエラーが表示されます。Device bay XX of enclosure {"name":"XXXXXX", "uri":"/rest/enclosures/ XXXXXXX"} is unavailable for a profile to be assigned.

さらに、ブレードを取り外し、プロファイルを作成してベイに割り当てられた後、ブレードが同じベイに再度挿入した場合、プロファイルの適用は完了しますが、サーバーに間違えて適用されます。

原因

この問題の主な原因は、HPE Synergy 480 Gen9 Multi MXM 拡張モジュールのフィールド交換ユニット (FRU) の誤ってプログラムされた「フォームファクター」によるものです。

推奨処置

FRU 問題を修正するために、認定 HPE サポート担当者にお問い合わせください。

サーバープロファイルまたはサーバープロファイルのテンプレートでブート可能とマークされた iSCSI ボリュームを削除できない

問題

HPE OneView の **SAN ストレージ**ページのサーバープロファイルまたはサーバープロファイルテンプレートでブート可能とマークされた iSCSI ボリュームを削除すると、次のエラーが返されます。

不明なタイプエラー: 「ターゲット」未定義のプロパティを読み取ることができません

注記: この問題は、HPE OneView UI を使用してボリュームを削除する場合にのみ発生します。

推奨処置

削除する iSCSI ボリュームを起動できないものとしてマークし、削除操作を再実行します。

接続およびローカルストレージにプロファイルを適用すると内部エラーが発生し、接続の定義がプロファイルから削除される

問題

接続およびローカルストレージにプロファイルを適用すると内部エラーが発生し、接続の定義がプロファイルから削除される。

推奨処置

操作を再度実行してください。エラーが続く場合は、認定サポート担当者に連絡し、サポートダンプを提供してください。

この失敗は、要求を満たすことができないサーバーにプロファイルを適用したために発生しました。具体的には、RAID 1 論理ドライブを構成し、既存の論理ドライブの自動インポートを選択するプロファイルです。そのプロファイルが、新しい RAID 1 論理ドライブを作成するために十分なドライブを持たないサーバーに適用されている場合、このエラーが表示され、操作を再試行することができません。

その場合は、次の回避策を実行してください。

1. サーバーのドライブを増設する
2. 新しい論理ドライブを構成しないようにプロファイルを変更し、既存の論理ドライブをインポートするオプションを保持します。

複数の手動 Remote Support コレクションを同時に実行すると、HPE OneView がメモリ制限およびフェイルオーバーになる可能性がある

問題

お客様が複数の手動 Remote Support コレクションを同時に実行し、論理エンクロージャー (LE) サポートダンブを実行すると、システムはメモリ制約になり、フェイルオーバーされます。

推奨処置

手動 Remote Support コレクションを実行する場合は、一度に1つの手動コレクションしか実行しないことをお勧めします。一度に複数のコレクションを実行すると、HPE OneView アプライアンスに過大な負荷をかけることとなります。手動コレクションの実行が完了すると、そのデバイスの **Remote Support** のデータセクションで、コレクションステータスが「完了」から「提出済み」に変わります。

ネットワーク URI が変更された場合、不正な検証エラーが発生する

問題

ユーザーがプロファイルテンプレートと関連プロファイルで使用されているネットワークを削除すると、ネットワークを作成したり、既存のネットワークを割り当てたり、テンプレートをアップデートしたり、影響を受けるプロファイルにテンプレートを再度適用したりすることはできません。その結果、ネットワークが削除されたことを示すエラーが発生します。

推奨処置

エラーを解決するためにユーザーが実行したいルートに応じて、このエラーに対する2つの回避策が考えられます。最初の回避策は、HPE OneView ユーザーインターフェイスを使用する方法です。影響を受ける各プロファイルを編集して接続をアップデートし、プロファイルを再度保存する必要があります。もう一つの回避策は、影響を受ける各プロファイルに対してスクリプト化できる REST インターフェイスによる方法です。スクリプトには以下のことが予想されます。

1. 影響を受けるプロファイルの URI を使用して GET 操作を実行し、現在のプロファイル設定を取得します。
2. 影響を受ける接続のネットワーク URI をアップデートし、ネットワーク名を削除するようにペイロードを変更します。
3. PUT 操作でプロファイルをアプライアンスに保存します。

SAN 自動ゾーニング機能の問題

SAN 自動ゾーニング機能は、HPE Smart SAN for 3PAR の Target Driven Peer Zoning (TDPZ) と互換性はありません。

推奨処置

HPE OneView SAN 自動ゾーニングを使用する場合は、3PAR Smart SAN ゾーニングと同時に SAN をゾーン化しないでください。

CHAP 名の長さ制限

QLogic または Broadcom アダプターを含むサーバーのサーバープロファイルで iSCSI 接続を構成する場合、CHAP 名は 128 文字以下で指定する必要があります。これらのアダプターの CHAP 名の最大長は、HPE OneView 4.1 によって強制されていませんが、最大長を超えた場合、ブレードによるストレージへの接続が失敗する可能性があります。

論理インターコネクトファームウェアのアップデート実行時に発生するサーバーの電源状態の問題

並列アクティブ化の方法を使用して論理インターコネクトファームウェアのアップデートを実行すると、サーバーの電源状態が確認されず、いずれかのサーバーが電源オン状態でもアップデートが実行される。論理インターコネクトファームウェアのアップデート画面では、すでに潜在的な機能停止について明確な指示を表示しています。

推奨処置

論理インターコネクトファームウェアのアップデートは、論理エンクロージャーのファームウェアアップデートアクションで、共有インフラストラクチャオプションを選択して実施するか、または並列アクティブ化の方法を使用した論理インターコネクトファームウェアのアップデートの前にサーバーの電源をオフします。

BIOS 設定の編集ページの UEFI iSCSI ブートポリシーフィールドが適用されない

HPE OneView には、BIOS 設定の編集ページの iSCSI ブートポリシーフィールドを設定および表示する機能が用意されているが、この設定を無視する。

推奨処置

UEFI システムユーティリティを起動し、ネットワークブートオプションで iSCSI のポリシーの設定を変更します。

単一の HPE Synergy コンポーザー構成では、高可用性 (HA) の警告アラートをクリア不可能

Hewlett Packard Enterprise は、HPE Synergy システムを承認済みの高可用性構成 (HPE Synergy コンポーザー) で構成することを強くお勧めします。システムを意図的に単一の HPE Synergy コンポーザーで構成すると、ロックされた高可用性の警告 (黄色) アラートが表示され、その構成である限りそのアラートをクリアすることはできません。

推奨処置

なるべく早く高可用性構成に移行してください。現在のところ、HA に準拠した構成を採用するまでは、アラートを無効にする方法はありません。

HPE OneView のリストア操作後、Remote Support に失敗する

症状

HPE Synergy スケールのバックアップリストア操作を実行すると、HPE OneView は正常にリストアされますが、HPE OneView IPv4 ネットワーク構成はリストアされません。

原因

HPE OneView のリストアアクションでは、Remote Support によるバックエンドの有効化と接続を妨げる IPv4 ネットワーク構成が再適用されません。

アクション

1. Remote Support をまだグローバルに利用できない場合は、無効にします。
2. ネットワークの IP アドレスを設定します。
3. Remote Support の再有効化:
4. エンクロージャーを更新します。

サーバーハードウェアの取り外しと挿入中に、Remote Support のデータコレクションが失敗する

定期の Remote Support のデータコレクション中に、サーバーハードウェアの取り外しと挿入を実行すると、コレクションが失敗する。

推奨処置

サーバーハードウェアの取り外しと挿入を、スケジュールされたコレクション操作以外の時間に設定するか、スケジュールされたコレクションの予定時間を変更します。

サーバーが挿入された後に Remote Support が有効にならない

Remote Support が有効なサーバーを取り外し、再度エンクロージャーに挿入したときに、サーバーハードウェアに対する Remote Support が再度有効にならないことがある。この状況は、サーバーハードウェアの Remote Support 構成を確認し、Remote Support ステータスが無効になっていることで判断できます。

推奨処置

Remote Support を再度有効にするために、サーバーハードウェアをアップデートします。

HPE Synergy コンポーザーの初期セットアップ中の問題

HPE Synergy コンポーザーの初期セットアップ時に、使用中の IP アドレスを入力すると、使用中の IP アドレスは使用されないが、ユーザーに対して高可用性 (HA) が有効でないことを警告するアラートが生成されない。

推奨処置

HPE Synergy コンポーザーの初期セットアップ時に構成されたすべての IP アドレスが、管理ネットワーク内で使用中でないことを確認します。

サーバーの電源を投入すると、アクティビティページに重複するアラートが表示される

サーバーの電源を投入すると、アクティビティページに重複した(最大 4 つの)サーバーの電源が入りましたおよびサーバーのリセットが検出されましたのライフサイクルアラートが表示される。

推奨処置

重複するライフサイクルアラートを無視してください。

サーバーハードウェアを取り外して再挿入すると、SAN 構成からブートする設定が失われる

次のすべてに該当する場合は、デフォルトのブートドライブ構成が失われ、サーバーが自動的に起動しません。

- ・ ブートデバイスがリモートにある。たとえば、Storage Area Network (SAN) デバイスまたはゾーン化されたローカルストレージから起動する。
- ・ サーバープロファイルのブートモードが UEFI ブートモードに設定されている。
- ・ 使用されているオペレーティング システムが SUSE Linux Enterprise Server 11 SP3、SP4 または Red Hat Enterprise Linux 6.x。

および、次のいずれかの事象が発生。

- ・ サーバーハードウェアが交換された。
- ・ サーバーハードウェアの NVRAM がクリアされた。
- ・ サーバープロファイルが、新しいサーバーハードウェアに移動された。

推奨処置

完全な詳細と修正操作については、CA [c05306567](#) を参照してください。

サーバープロファイルの作成/編集ダイアログボックスで[作成/作成+/OK]ボタンが動作しない

OS 展開プランを含むサーバープロファイルを作成、または編集した後、OS 展開プランを含まないサーバープロファイルを作成/編集すると、ダイアログボックスで作成/作成+/OK ボタンが動作しなくなることがある。

推奨処置

ブラウザを更新し、操作を再試行します。このような状況を防ぐためには、OS 展開プランに関連するいずれかの作成/編集操作の後では、ブラウザの更新を実行します。

FCoE VLAN について推奨される Cisco トップオブラックス イッチ構成

HPE OneView を使用して、FCoE VLAN で構成された HPE Synergy インターコネクトモジュールを管理する場合は、Cisco のトップオブラックスイッチを使用する場合は、VFC MAC アドレスを Cisco のトップオブラックスイッチと併用することをお勧めします。

推奨処置

この推奨事項は、HPE Synergy インターコネクトが Cisco スイッチに接続されている場合に適用されます。外部スイッチ構成の一環として、論理エンクロージャーから外部 Cisco スイッチへのマルチホップ FCoE を使用し

て、HPE OneView でサーバーを展開する場合は、各サーバーの MAC アドレスへの vSAN および VFC インターフェイスバインディングを手動で構成する必要があります。HPE OneView SAN ストレージ構成によって SAN のゾーニング構成が自動化される場合、SAN のエッジで構成されている VFC インターフェイスは構成されません。これらは、手動で構成する必要があります。

MAC アドレスバインディングに関する Cisco 欠陥 (CSCug84860) を回避するために、2016 年 3 月以降にリリースされた Cisco ファームウェアを使用してください。

サーバープロファイルの仮想 MAC アドレスを使用する場合は、プロファイルの適用後にサーバーごとに使用してください。物理 MAC アドレスを使用する場合は、VFC インターフェイスを一度だけ構成すれば、必要な数のプロファイルを適用することができます。

オンラインヘルプのサーバーハードウェア画面で、ヘッダーにポートではなくアダプターと表記される

オンラインヘルプのサーバーハードウェア画面で、ポートというセクションがアダプターと表記される。

推奨処置

ヘルプのアダプターページは、ポート UI 画面を指しています。

アクティブなフレームリンクモジュール (FLM) を同じバージョンのファームウェアを実行している FLM と置き換えると、HPE OneView で「アップデート」エラーが報告される

HPE OneView ユーザーがアクティブなフレームリンクモジュールを取り外し、スタンバイのフレームリンクモジュールがフレームを引き継ぐ前に交換モジュールを挿入すると、HPE OneView で「リフレッシュ」エラーが発生する。

推奨処置

エンクロージャーを手動でアップデートしてエラーをクリアします。

HPE OneView がオフラインの場合、アップデートしても、ベイが変更されたブレードについて報告されない

HPE OneView が動作していないときにベイ間でサーバーを移動すると、HPE OneView を起動した際にサーバーがエラーが報告される場合がある。

推奨処置

エラーが消去され、ブレードが適切な位置にあることが報告されるまでエンクロージャーをアップデートしてください。

異なるインターコネクต์モジュールにケーブルで直接接続された 3PAR Persistent Ports ポートペアがサポートされない

アプライアンスは、3PAR StoreServ アレイのポートのペアが Persistent Ports のフェールオーバー用に構成され、エンクロージャ上の 2 つの異なるインターコネクต์モジュールに直接接続するようにケーブル接続されているストレージ構成をサポートしていません。

推奨処置

3PAR StoreServ アレイの Persistent Port 機能 (アレイのすべてのポートで) を無効にするか、直接接続ケーブルを変更して、パートナーとなっているポートが同じインターコネクต์モジュールに確実に接続されるようにします。

HPE Synergy Gen10 サーバーで iSCSI ポリシー BIOS をデフォルト以外の値に変更すると、起動が失敗する

HPE Synergy Gen10 サーバー上で iSCSI ポリシー BIOS をデフォルト以外の値（アダプターイニシエーターなど）に変更すると、iSCSI ソフトウェアのブート試行はターゲットに接続できず、サーバーが起動しない。

推奨処置

UEFI システムユーティリティを起動し、ネットワークブートオプションからソフトウェアイニシエーターへで iSCSI のポリシーの設定を変更します。

削除されたネットワークで接続が引き続き使用されているというアラート

ネットワークを削除してサーバープロファイルテンプレートをアップデートすると、削除されたネットワークがまだ接続に割り当てられているというアラートが一部のサーバープロファイルに示される場合がある。プロファイルに変更が行われ、サーバープロファイルをアップデートすることによって変更がクリアされたことを踏まえると、これは間違ったアラートとなる。この操作は、プロファイルアップデートメニューから行われた可能性がある。

推奨処置

ユーザーインターフェイスのサーバープロファイルを更新のアクションで、影響を受けるサーバープロファイルを更新してください。

Smart アレイメザニンコントローラーの内蔵ドライブを選択すると、プロファイル作成に失敗する

「ローカルストレージ設定を適用できません。Smart Storage Administrator ツールが次のエラーメッセージで失敗しました：エラー (2829)。アレイを作成できません。ディスクがありません」というエラーが表示され、プロファイルが失敗する。これは、プロファイルで「内蔵ドライブ」は選択されていても、メザニンコントローラーで HPE プレミアムバックプレーンハードディスクドライブアップグレードキットが構成されていないことが原因です。

推奨処置

HPE プレミアムバックプレーンハードディスクドライブアップグレードキットがない場合は、Smart アレイメザニンコントローラーで「内蔵ドライブ」を選択しないでください。

アップリンクセットからネットワークを削除してもアラート、不正なプロファイルと接続状態が表示されない

論理インターコネクトグループの 2 つ以上のアップリンクセットからネットワークを削除し、削除されたネットワークに対する参照がアクティブになっているサーバープロファイルがあるグループのアップデートを実行すると、そのネットワークがインターコネクトから削除されても、一部のサーバープロファイルで正常に接続されていると引き続き表示される場合がある。

推奨処置

この方法によるネットワーク削除は、論理インターコネクトグループの 1 つのアップリンクセットに制限してください。また、1 つ以上のアップリンクセットからネットワークが削除されるように論理インターコネクトを直接編集し、その後、論理インターコネクトおよび論理インターコネクトグループが要件を満たすように、関連する論理インターコネクトグループを編集します。さらに、意図せず削除された場合は、論理インターコネクトグループにネットワークをリストアし、グループの 2 回目のアップデートを実行すると、すべての接続のコネクティビティを正常にリストアすることができます。

リモートコンソールウィンドウが表示されるが、サーバーに接続されていない

HPE OneView から iLO 5 リモートコンソールを起動すると、リモートコンソールウィンドウが開きますが、サーバーに接続できません。

推奨処置

iLO 5 Web インターフェイスにログインし、iLO 5 インターフェイスからリモートコンソールを起動してサーバーコンソールにアクセスします。

HPE Synergy コンポーザー 4.1 によって管理されるフレームの削除

HPE Synergy コンポーザー 4.1 によって管理されるフレームを削除しても、HPE OneView 内のフレームリンクモジュール (FLM) の自己署名証明書が削除されない。

推奨処置

自己署名証明書を HPE Synergy コンポーザーのコンソールから手動で削除するには、**設定 > セキュリティ > 証明書の管理**の順に移動します。FLM 名に関連付けられている証明書を検索します。

HPE OneView に自己署名証明書を残しても、他のフレームに対する HPE Synergy コンポーザー操作に影響はありません。

接続が、DHCP およびマネージドボリュームを使用している 2 つの iSCSI ブート接続のいずれかであった場合、接続を iSCSI ブート可能接続に戻すことができない

1 番目がプライマリブート可能であり、2 番目がブート不可である、2 つの iSCSI ブート接続を含むプロファイルを編集する場合に、DHCP およびマネージドボリュームを使用しているセカンダリブート可能 iSCSI 接続に 2 番目の接続を変更すると、「プロファイルをアップデートできません。」という検証エラーが発生します。解決策は、イーサネット機能タイプと iSCSI ブートパラメーターを使用したブート可能な接続はすべて、同じイニシエーター名を共有することです。

推奨処置

1. ブート不可接続を削除する
2. 新しい iSCSI ブート可能接続を追加する

サーバーが iLO のリセット直後に更新すると、iLO5 の HPE OneView SNMP 構成が破損する

管理対象サーバー上の iLO5 をリセットした直後に、HPE OneView によって管理されているサーバーハードウェアを更新すると、HPE OneView が iLO5 で設定する SNMP 構成が破損します。これにより、iLO 5 からの SNMP トラップが HPE OneView で受信されなくなります。これは、サーバーの監視と、プロファイル適用や電源制御などのサーバー管理のいくつかの側面に影響します。

推奨処置

iLO 5 が応答を開始した後約 1 分待ってから、HPE OneView でサーバーを再度更新してください。これにより、iLO の SNMP 設定がリストアされ、HPE OneView がサーバーの監視と管理を継続できるようになります。

HPE OneView によって Gen10 ハードウェアが検出されない

HPE OneView にエンクロージャーをインポートしたり、Gen10 コンピュートモジュールにエンクロージャーを追加したりするときは、HPE OneView のハードウェアセットアップ画面またはサーバーハードウェア画面に Gen10 ハードウェアのリストは表示されません。これは、以下のように、HPE Synergy で Gen10 ハードウェアの検出をサポートしていないソフトウェアまたはファームウェアのバージョンが実行されている場合に発生します。

- ・ HPE Synergy フレームリンクモジュールがファームウェアバージョン 1.x を実行しています。
- ・ HPE Synergy コンポーザーが 3.00.xx バージョンの HPE OneView を実行しています。

推奨処置

1. HPE Synergy (3.10.Gen10.20170721 以降) の最新の Synergy ソフトウェアリリースをダウンロードします。
2. Synergy ソフトウェアリリースから HPE Synergy コンポーザーのファームウェアバンドルを解凍します。これには HPE OneView のアップデートが含まれています。
3. HPE OneView をアップデートします。
4. Synergy ソフトウェアリリースから Synergy Custom SPP を展開して、ファームウェアレポジトリに保存します。
5. **論理エンクロージャー**画面に移動して、フレームリンクモジュールのファームウェアをアップデートします。
6. フレームリンクモジュールが 2.0 (またはそれ以降) に正常にアップデートされると、Gen10 コンピュートモジュールが、確認のために**ハードウェアセットアップのインベントリ画面**または**サーバーハードウェアの概要画面**に表示されるはずですが、コンピューモジュールが表示されない場合は、エンクロージャーをアップデートして強制的に検出を実施してください。

アプライアンスの Web サーバー証明書の有効期限が切れていると、HPE OneView 4.1 へのアップデートに失敗する

問題

アプライアンスの Web サーバー証明書の有効期限が切れているか、アップデート前に期限切れになると、「不明なエラー」でアップデートに失敗し、サポートダンプの `/update/logs/update.log` ファイルに以下のメッセージが表示されます。

[エラー] アプライアンスの Web サーバー証明書の有効期限が切れているか、古い証明書に戻されています。アップグレードを続行できません。新しいアプライアンスの自己署名証明書を再生成するか、新しい CA 署名済みアプライアンスの証明書を再度インポートしてください。その後、アップグレードを再試行します。

原因

- ・ アップデート前にアプライアンスの証明書が期限切れになっている可能性があります。
- ・ アプライアンスがアップデート前またはアップデート中に期限切れの証明書を検出し、古い証明書に戻したり、新しい証明書を再生成したりした可能性があります。
- ・ アプライアンスの証明書が 24 時間以内に期限切れになる可能性があります。

推奨処置

1. アプライアンスの証明書が有効であることを確認します。以下の項目は、無効な証明書を示しています。

- ・ 証明書の有効期限が切れている場合、または証明書が 24 時間以内に期限切れになる場合。
 - ・ 証明書が SHA1 証明書の場合。
 - ・ 証明書で以前その証明書に対して構成された組織情報が失われている場合。アプライアンス証明書が期限切れになり、アップデートされた証明書をインストールする前にアプライアンスを再起動すると、一部の情報が失われる可能性があります。
 - ・ 以前は CA の署名済み証明書をインストールしていたものの、現在のアプライアンス証明書がインストール済みの証明書ではない場合。アプライアンス証明書が期限切れになり、アップデートされた証明書をインストールする前にアプライアンスを再起動すると、正しくない証明書が表示されることがあります。
- このような場合は、アプライアンスの自己署名証明書を再生成するか、新しい CA 署名済み証明書をインポートしてください。
2. アプライアンス証明書が無効な場合は、新しい証明書を再生成し、新しいアプライアンスの自己署名証明書を再生成するか、新しい CA 署名済みアプライアンス証明書を再インポートします。
 3. アップデートを再試行してください。

アップデートが正常に完了すると、アラートはクリアされます。

スタックされたインターコネクトモジュールのいずれかまたは両方が取り外され、再度挿入されると、不正なスタッキングヘルスアラートが発生する

スタックされたインターコネクトモジュールのいずれかまたは両方が取り外され、再度挿入されると、HPE OneView によって、論理インターコネクトページにレポートが報告される場合があります。このアラートは、スタッキングポートがインターコネクトページでリンクアップ状態になっていても、「スタッキングヘルスが切断された」ことを意味します。これは間違ったアラートとなります。

推奨処置

論理インターコネクトページで Q7 と Q8 のリンク状態を確認してください。ポートがリンクされている場合、スタッキングヘルスのアラートは誤りであり、クリアすることができます。論理インターコネクト画面に移動し、アクションメニューからアラートをクリアしてください。

中国語ローカリゼーションを採用した HDD ドライブタイプを使用して論理 JBOD を作成すると、エラーが発生する

中国語ローカリゼーションを採用した HDD ドライブタイプを使用して論理 JBOD を作成すると、ドライブタイプが null であることを示すエラーが発生します。

推奨処置

論理 JBOD を定義する場合、**ドライブ選択の基準**として**ドライブタイプオプション**を使用しないでください。代わりに、**サイズとテクノロジーオプション**を使用してください。この場合、表示されているフォームに**ドライブサイズとドライブテクノロジー**を手動で入力する必要があります。

ネットワークの削除がサーバープロファイルで検出されない

負荷の高い状態では、サーバープロファイルが使用しているネットワークの削除を検出できず、接続を失った場合でも問題がないと報告し続ける可能性があります。サーバープロファイルでアップデート操作を行うことで、通常、実際と一致しない場合のプロファイルの状態を修正することができます。アップデートを行うと、接続とサーバープロファイルの状態が正常にアップデートされますが、問題を説明するアラートは生成されません。

推奨処置

接続用に新しいネットワークを指定するか、サーバープロファイルから接続を削除します。

SAN ボリュームアタッチメントがサーバープロファイルテンプレートから削除されると、誤った整合性警告アラートが表示される

SAN ボリュームアタッチメントがサーバープロファイルテンプレートから削除されると、サーバープロファイルテンプレートに関連付けられた各サーバープロファイルで誤った整合性警告アラートが発生します。実際には（サーバープロファイルテンプレートの要件を超える）追加のボリュームは許容され、整合性に影響を与えないため、不整合は存在しません。

推奨処置

手動でアラートをクリアします。

ホスト名が数値のみで構成されている場合、アプライアンスネットワークの設定が失敗する

ホスト名が数値のみで構成されている場合、アプライアンスネットワークの設定が失敗する。

推奨処置

ホスト名には英数字の値を入力します。

サブタスクが完了しても、Remote Support マスタータスクが完了しない

最初の親の Remote Support の有効化タスクが正常に完了しないと表示される可能性があり、そのため、子タスクが正常に完了しても、6 時間後にタイムアウトエラーで終了します。この動作は、アプライアンスの再起動で表示される可能性があります。

推奨処置

対応する必要はありません。タイムアウトエラーメッセージは無視してもかまいません。

注記: PATCH が使用されている場合、スクリプティングは各サブタスク上で GET を実行して、成功または失敗したかどうかを確認する必要があります。このアプローチをとると、各タスクの成功または失敗はスクリプトによって判断できます。

PUT /rest/support/configuration を使用して Remote Support を有効にするスクリプトは、同期呼び出しであるため最長 6 時間待機する可能性があります。タイムアウトエラーの結果、内部サーバーエラー（タイムアウトではない）を示す HTTP エラーのリターンコードが発生します。正確な原因に関する情報は、サーバーエラーとともに送信されます。

同じ機能を実行するために、PATCH /rest/support/ を使用して enableRemoteSupport プロパティを置き換えるスクリプトは、タスク ID を使用して HTTP 202（通常の非同期応答）を取得します。通常、スクリプトは GET /rest/tasks/{id} を使ってポーリングを行い、タスクを完了します。タイムアウトの場合、ポーリングへの応答は、API ドキュメントで説明されているようにエラー終了を示します。

ルート CA「iLO/iLO 3/iLO 4/iLO 5 デフォルト発行元（信頼しない）」を信頼する

設定 > セキュリティ > 証明書の管理 > 証明書の追加画面を使用して、iLO の自己署名の証明書を信頼し、IP アドレスまたはホスト名からフェッチを選択する場合は必ず、**強制的にリーフ証明書を信頼するオプション**を有効にします。これにより、iLO のリーフ証明書のみがトラストストアに追加されるようになります。このオプションの使用を忘れた場合、iLO のデフォルト発行元（信頼しない）がトラストストアに追加されることがあります。この場合、デフォルト（信頼しない）の証明書を削除してください。これらの証明書はトラストストアに配置しないでください。配置された場合、エラーの原因となる可能性があります。

ドメインの完全な DNS 名でエンタープライズディレクトリサーバーを構成する

HPE OneView でエンタープライズディレクトリサーバーを構成する場合、ディレクトリサーバーは、サーバー証明書、1 つ以上の発行元、およびオプションでルート証明書を含む証明書チェーンを提示することがあります。サーバが証明書チェーンにルートを提示していない場合、HPE OneView では、ディレクトリサーバーを構成する前に、ルート証明書をアプライアンスに事前にインポートする必要があります。ディレクトリサーバーに接続すると、アプライアンスのトラストストアに対して信頼検証が実行されます。サーバーが信頼できると検出された場合、HPE OneView は接続中に証明書チェーンに表示されているすべての発行元を保存します。

ドメインの完全な DNS 名を使用して HPE OneView でディレクトリサーバーを構成する場合は、次の点に注意する必要があります。

1. HPE OneView が DNS 名を使用してディレクトリサーバーに接続しようとする場合、サーバーのルート証明書が HPE OneView に事前にインポートされていることが必須条件です。
2. このドメインで複数のディレクトリサーバーが構成されている場合は、各ディレクトリサーバーのすべての発行元証明書を HPE OneView に事前にインポートする必要があります。

ホスト名の検証問題は、ドメインの完全な DNS 名を使用して、エンタープライズディレクトリサーバーを構成して通信するときに発生する

HPE OneView では、ディレクトリサーバーの証明書のサブジェクト代替名（SAN）に次のいずれかが含まれていない場合、DNS 名を使用してエンタープライズディレクトリサーバーとの構成および通信が許可されません。

ドメイン名または解決された IP アドレス、またはドメイン名のワイルドカードエントリー

このシナリオでは、以下のエラーメッセージと解決方法が表示されます。

エラー：サーバーとの信頼できる通信を確立できません。ディレクトリサーバー証明書に、IP アドレスまたはホスト名が指定されていません。

解決方法：ディレクトリサーバーが有効な IP アドレスまたはホスト名が指定されている証明書で設定されていることを確認します。指定された証明書でディレクトリサーバーを設定した後、CA 署名済み証明書の場合は、ルート証明書と適切な中間証明書が HPE OneView のトラストストアに存在することを確認します。問題を解決するために新しいディレクトリサーバー自己署名証明書が生成された場合は、HPE OneView のトラストストアに当該証明書を追加します。サーバーを更新して、操作を再試行してください。下記のリンクを使用して、HPE OneView のトラストストアに証明書を追加します。

推奨処置

エンタープライズディレクトリサーバーの管理者は、サーバー証明書の SAN に、ドメイン名または解決された IP アドレス、またはドメイン名のワイルドカードエントリーのいずれかが含まれていることを確認する必要があります。

Active Directory サーバーの構成には TLS v1.2 を使用

安全性の低い TLS v1.0 または TLS v1.1 プロトコルではなく、TLS v1.2 を使用して HPE OneView が Active Directory と通信できるように、必ず、TLS v1.2 を使用して Active Directory サーバーを構成してください。

ネットワークサブネットマスク設定の変更が UI で反映されない場合、「展開サーバーの追加」に失敗する

HPE OneView アプライアンスのネットワークサブネットマスク設定が変更されると、HPE OneView アプライアンスの UI にこの変更が反映されず、展開サーバーの追加に失敗する。

推奨処置

設定 > アプライアンスページから HPE OneView アプライアンスを再起動します。

注記: 展開サーバーの追加は、HPE OneView アプライアンスを再起動してから行うと失敗しません。

ファームウェアアップデート後、HPE Synergy コンピュートモジュールでファイルシステムが読み取り専用になる

FCoE ネットワークに接続されたサーバープロファイルが含まれている HPE Synergy コンピュートモジュールで、Virtual Connect SE 40Gb F8 モジュールのファームウェアアップデート後に、ファイルシステムが読み取り専用になることがある。この問題は、FCoE ネットワークに接続されているサーバーでのみ発生し、イーサネット、iSCSI、または FC ネットワーク接続が任意に組み合わせられているサーバーには当てはまりません。

推奨処置

FCoE ネットワークに接続されているサーバーについて Virtual Connect SE 40Gb F8 モジュールのファームウェアアップデートを実行する際は、メンテナンスウィンドウが必要になります。ファームウェアアップデートが完了したら、各 FCoE 接続サーバーにアクセスしてサーバーのファイルシステムの現在の状態を検証することが重要です。ファイルシステムが読み取り専用とマークされている場合は、サーバーを再起動してファイルシステムを読み取り/書き込みモードに復元する必要があります。すべての FCoE サーバーを検証すると、メンテナンスウィンドウを終了することができます。この検証プロセスは、FCoE 接続を使用しているサーバーにのみ適用されます。FCoE 接続を使用していないサーバーを検証する必要はありません。

スキャンツールによって脆弱な SSH 暗号の問題が報告される

脆弱性スキャンツール (Nessus) によって、HPE OneView が脆弱な SSH 暗号、aes-256-cbc をサポートしていると報告されます。

推奨処置

現時点では、対処は不要です。

この問題は、重大度が低いと評価されており、対処するための軽減策が SSH に適用されています。この暗号の使用は、管理ネットワークに制限されます。この問題は、将来のリリースで対処される予定です。

HPE OneView は、OpenSSH 5.3 を使用しています。これには、CVE-2008-5161 で説明されているように、CBC 暗号の使用に起因するプレーンテキストリカバリ成功の可能性を減らすための軽減策が含まれています。

CVE-2008-5161 に関する詳細については、以下を参照してください。

<http://community.arubanetworks.com/t5/Wireless-Access/SSH-and-AES-CBC/td-p/248919>

HPE OneView 4.1 (HPE Synergy 用) に関する注意

サポートされる iSCSI ブート構成

次のパラメーターがサポートされています。

- ・ IPv4 (IPv6 のサポートなし)
- ・ 静的 IP アドレスと DHCP 割当て済み IP アドレス
- ・ SW iSCSI (ソフトウェアイニシエーター) および HW-iSCSI (iSCSI オフロード、ハードウェア支援イニシエーター)
- ・ iSCSI を使用したブート可能なイーサネット接続は、物理ポート (ポート「a」など) の最初の仮想機能にのみ使用でき、HW-iSCSI 接続は、物理ポート (ポート「b」、つまりストレージ機能) の 2 番目の機能にのみ使用できます。

ファイバーチャネルの直接接続

HPE OneView 4.1 (HPE Synergy 用) では、ファイバーチャネルのファブリック接続および FCoE (Fibre Channel over Ethernet) ネットワーク接続をサポートしています。HPE OneView 4.1 では、3PAR ストレージ (FlatSAN) を含む DirectAttach をサポートしています。

ポートのミラーリング

ファームウェアバージョン 4.00.33 以降を実行している VC SE 16 Gb FC モジュールでは、双方向ミラーリングがサポートされています。

システムボードの交換

ベイ内のサーバーにプロファイルが割り当てられており、そのサーバーがメンテナンスのために取り外された場合、HPE Synergy は、ネットワークセキュリティなどの検証を行ってから電源が入るように、そのベイに対する電源を保留します。サーバーが挿入されると、HPE Synergy はサーバーを検出し、HPE Synergy が同一サーバーであるかどうか (UUID を使用)、および以前のサーバーと構成が同じかどうかを確認します。構成が同じである場合、電源保留は解除されます。構成が同じでない場合、プロファイルにはエラーのマークが付き、この時点でそのサーバー/ベイからプロファイルを削除することができます (または、ハードウェアタイプが同じであれば、編集して再適用することもできます)。

システムボードを交換する際はおそらく、プロファイルにとっても同一サーバーに見えるように、RBSU を通じて UUID を手動で再プログラミングする必要があります。この場合、電源保留を解除するには、プロファイルを編集して未割り当てとマークし、保存します。これで電源保留が解除され、サーバーに電源を入れられるようになり、必要に応じて再度プログラミングできます。変更が行われると、サーバーの POST サイクルが完了し、そのサーバー/ベイにプロファイルが再度割り当てられます。

ドキュメントの補足

次の情報は公開後に利用可能となったため、HPE OneView 4.0 のドキュメントでは表示されません。

HPE OneView 4.1 へのアップデート中および自動ハードウェア検出中の証明書の処理

HPE OneView 4.1 には、管理対象デバイスまたは監視対象デバイスとのすべての HTTPS/TLS 通信の証明書確認に関連するセキュリティ機能が改善が含まれています。これらの新しい機能の 1 つには、改善されたアラート機能と期限切れの証明書を持つデバイスとの通信を制御するポリシーが含まれています。4.1 の以前バージョンとの互換性を維持するために、HPE OneView 4.1 にアップデートすると、HPE OneView は期限切れの証明書を持つデバイスのアラートを送信しても、デフォルトでこれらのデバイスとの通信を継続します。たとえば、4.1 アップデート中に期限切れの証明書を持つサーバーハードウェア iLO でアラートが発生しても、これらのデバイスは引き続き監視または管理されます。これは HPE Synergy フレームリンクトポロジの初期ハードウェア設定など、自動デバイス検出の操作にも該当します。

期限切れの証明書がエラーまたは警告として扱われるかどうかを制御するポリシーが、**設定 > セキュリティ** 画面に表示されます。証明書の検証はデフォルトで有効になっており、またデフォルトでは**自己署名証明書の有効期限をチェックする**設定が無効になっています。このデフォルトは、期限切れの証明書がある場合 4.1 のアップデートおよび自動検出操作を簡素化することを目的としています。有効期限切れの証明書をできるだけ早くアップデートし、有効期限のチェックを有効にすることを強くお勧めします。

この緩和された有効期限チェックのユーザー設定は、一般に自己署名証明書に適用されますが、4.1 アップデートまたは自動検出操作中にのみ期限切れの CA 署名済み証明書に適用されます。ユーザーが外部ファームウェアレポジトリを追加する、またはサーバーハードウェアを追加するなど、デバイスの証明書の検証を必要とする操作は、期限切れの CA 証明書がエラーになるため、デバイスの信頼性を調整する前に修正する必要があります。

iLO で FIPS が有効になっている場合、iLO は新しい証明書を生成し、アプライアンスにインポートする必要があります。新しい証明書のインポートに失敗すると、HPE OneView はサーバーを管理対象外として報告します。

iLO の有効期限が切れた証明書の修正

iLO 2、iLO 3、iLO 4、および iLO 5 の期限切れの証明書を修復する場合、次のいずれかを実行します。

手順

1. 独自の公開キーインフラストラクチャ (PKI) を使用している場合は、iLO 証明書の署名要求を発行し、iLO に CA 署名済み証明書をインストールします。CA ルート証明書と中間証明書が HPE OneView トラストストアに置かれていることを確認します。**設定 > セキュリティ > 証明書の管理 > 証明書の追加**画面を使用して、base64 でエンコードされた CA ルート証明書およびすべての中間証明書を貼り付けます。サーバーハードウェアを更新して、再度追加してください。
2. 期限切れの自己署名証明書をアップデートします。iLO が工場出荷時のデフォルトにリセットされたり、iLO のホスト名が変更されたりすると、新しい自己署名 SSL 証明書が生成されます。証明書をアップデートしたら、**設定 > セキュリティ > 証明書の管理 > 証明書の追加**画面を使用して証明書を HPE OneView トラストストアに追加します。**IP アドレスまたはホスト名から証明書を追加**オプションを選択し、iLO およびポート 443 の IP アドレスまたはホスト名を指定します。また、**証明書を貼り付け**オプションを選択し、iLO 自己署名証明書を貼り付けることもできます。どちらの場合も、**強制的にリーフ証明書を信頼する**を選択することを忘れないでください。サーバーハードウェアを更新または再追加します。

注記: iLO 証明書には、**デフォルト発行元 (信頼しない)** の発行元フィールドが表示されます。これらの証明書は常に自己署名として扱われるため、PKI 発行の CA 署名済み証明書を使用しない iLO の場合、**強制的にリーフ証明書を信頼するオプション**が常に使用されます。

- 一部の iLO ファームウェアリビジョンには、デフォルトの自己署名証明書が期限切れになっている既知の問題があります。**有効期間の開始日**は証明書の**有効期間の終了日**よりも前です。この問題を解決するには、**Hewlett Packard Enterprise サポートセンター**にある該当する iLO カスタマーアドバイザーを参照してください。

ルート証明書または中間証明書の有効期限が切れたときの回復オプション

ルート証明書または中間証明書が期限切れになると、アプライアンスは有効期限が切れてから 60 日後に事前アラートを提供します。有効期限が切れる前に管理者が証明書を置き換えなかった場合、ユーザーはエンタープライズディレクトリの認証情報でログインし、Two-Factor 認証 (2FA) 証明書は機能しません。このイベントから復旧するには、管理者は緊急ローカルログインを使用してリモートログインし、アプライアンス証明書または 2FA 証明書に署名した、必要なアップデート済みの CA 証明書をインポートする必要があります。

リモートシステムからの緊急ローカルログインが無効になっている場合、管理者は以下を行う必要があります。

- キオスクを使用してログインし、緊急ログインをリモートで有効にする。
- リモートセッションを通じて証明書をインポートする。
- リモートシステムからの緊急ログインを再度無効にする。

セキュリティ

セキュリティに関する最新情報については、HPE OneView (HPE Synergy 用) ユーザーガイドの「アプライアンスのセキュリティ機能について」を参照してください。

HPE OneView API リファレンス

サポートされている最小 API バージョンは、将来のリリースで変更される可能性があります。Hewlett Packard Enterprise は、新しいバージョンの HPE OneView にアップグレードする際の互換性の問題を回避するため、できるだけ早く最新の API バージョンに移行することをお勧めします。

ハイパーバイザーのサポート

次のメジャーリリースでは、HPE OneView は ESXi 6.0 より以前バージョンの ESXi をサポートしません。Hewlett Packard Enterprise は、互換性の問題を回避するため、できるだけ早く ESXi 6.0 の最小バージョンに移行することをお勧めします。

3PAR ストレージアレイとの FC 直接接続

HPE Virtual Connect SE 40Gb F8 モジュール (HPE Synergy 用) のための 3PAR ストレージアレイとの FC 直接接続は、ToR/EoR SAN スイッチを使用する必要性をなくすことによって、Virtual Connect のお客様に簡素化および自動化されたストレージプロビジョニング体験を提供します。

HPE Synergy コンポーザーから受け取った Remote Support イベントの表示

HPE OneView で Remote Support が有効になっている場合、HPE Synergy コンポーザーから受信したイベントを表示し、Remote Support に自動転送できるようになりました。

API バージョンのサポートを削除

サポート対象外となる API バージョンについては、以下のドキュメントで詳しく説明しています。

- ・ HPE OneView サポートマトリックス
- ・ HPE OneView API リファレンス

Gen10 サーバーに関する ESXi OS のファームウェアとドライバーのアップデート

Gen10 サーバーでは、ESXi WBEM インベントリプロバイダのサポートは利用できなくなります。

HPE Synergy のドキュメントおよびトラブルシューティングの資料

HPE Synergy のドキュメント

Hewlett Packard Enterprise Information Library (<http://www.hpe.com/info/synergy-docs>) はタスクベースのレポジトリです。インストール手順、ユーザーガイド、メンテナンスとサービスガイド、ベストプラクティス、およびその他のリソースへのリンクが含まれています。この Web サイトを使用して、次のような最新のドキュメントを入手してください。

- ・ HPE Synergy テクノロジーについての学習
- ・ HPE Synergy のインストールおよびケーブル接続
- ・ HPE Synergy コンポーネントのアップデート
- ・ HPE Synergy の使用および管理
- ・ HPE Synergy のトラブルシューティング

HPE Synergy 構成および互換性ガイド

HPE Synergy 構成および互換性ガイドは、Hewlett Packard Enterprise Information Library (<http://www.hpe.com/info/synergy-docs>) から入手できます。HPE Synergy 管理とファブリックアーキテクチャーの概要、詳細なハードウェアコンポーネントの識別および構成、およびケーブルの接続例が示されています。

HPE Synergy フレームリンクモジュールユーザーガイド

HPE Synergy フレームリンクモジュールユーザーガイドは、Hewlett Packard Enterprise Information Library (<http://www.hpe.com/info/synergy-docs>) から入手できます。本ガイドでは、フレームリンクモジュールの管理、構成、およびセキュリティについて説明します。

HPE OneView (HPE Synergy 用) ユーザーガイド

HPE OneView (HPE Synergy 用) ユーザーガイドは、Hewlett Packard Enterprise Information Library (<http://www.hpe.com/info/synergy-docs>) から入手できます。リソース機能、プランニングタスク、クイックスタートタスクの構成、グラフィカルユーザーインターフェイスのナビゲーションツール、および HPE OneView のサポートと参照情報が示されています。

HPE OneView Global Dashboard

HPE OneView Global Dashboard は、HPE OneView によって複数のプラットフォームとデータセンターサイト間で管理される、ヘルス、アラート処理、およびキーリソースの統合ビューを提供します。HPE OneView Global Dashboard ユーザーガイドは、Hewlett Packard Enterprise Information Library (<http://www.hpe.com/info/synergy-docs>) から入手できます。HPE OneView Global Dashboard のインストール、構成、ナビゲーション、およびトラブルシューティングについて説明します。

HPE Synergy イメージストリーマーユーザーガイド

HPE Synergy イメージストリーマーユーザーガイドは、Hewlett Packard Enterprise Information Library (<http://www.hpe.com/info/synergy-docs>) から入手できます。このユーザーガイドでは、イメージストリーマーを使用した OS 展開プロセス、イメージストリーマーの機能、およびイメージストリーマーアーティファクトの目的とライフサイクルについて説明します。また、認証、権限、およびイメージストリーマーのトラブルシューティングに関する情報も含まれます。

HPE Synergy Image Streamer GitHub

HPE Synergy Image Streamer GitHub レポジトリ (<https://github.com/HewlettPackard>) には、サンプルアーティファクトと、サンプルアーティファクトの使用法に関するドキュメントが含まれます。また、イメージストリーマーを使用して実行できる展開手順について説明するテクニカルホワイトペーパーも含まれます。

HPE Synergy Software Overview Guide

HPE Synergy Software Overview Guide は、Hewlett Packard Enterprise Information Library (<http://www.hpe.com/info/synergy-docs>) から入手できます。HPE Synergy をサポートするさまざまなソフトウェアおよび構成ユーティリティの概要と詳細な参考資料について説明します。このガイドは、タスクベースであり、かつ以下について利用可能な、サポートされるすべてのソフトウェアおよび構成ユーティリティに関するドキュメントとリソースについて説明しています。

- ・ HPE Synergy のセットアップと構成
- ・ OS の展開
- ・ ファームウェアのアップデート
- ・ トラブルシューティング
- ・ リモートサポート

HPE Synergy ファームウェアとドライバーアップデートのためのベストプラクティス

HPE Synergy ファームウェアとドライバーアップデートのためのベストプラクティスは、Hewlett Packard Enterprise Information Library (www.hpe.com/info/synergy-docs) から入手できます。ファームウェアのアップデート方法、および HPE OneView が提供する HPE Synergy コンポーザーを介してファームウェアおよびドライバーをアップデートするための推奨のベストプラクティスに関する情報が記載されています。

HPE OneView (HPE Synergy 用) サポートマトリックス

HPE OneView (HPE Synergy 用) サポートマトリックスは、Hewlett Packard Enterprise Information Library (<http://www.hpe.com/info/synergy-docs>) から入手できます。HPE OneView のソフトウェアおよびファームウェアの最新の要件、サポートされるハードウェア、および構成の上限を維持します。

HPE Synergy イメージストリーマーサポートマトリックス

HPE Synergy イメージストリーマーサポートマトリックスは、Hewlett Packard Enterprise Information Library (<http://www.hpe.com/info/synergy-docs>) から入手できます。HPE Synergy イメージストリーマーのソフトウェアおよびファームウェアの最新の要件、サポートされるハードウェア、および構成の上限を維持します。

HPE Synergy 用語集

Hewlett Packard Enterprise Information Library (<http://www.hpe.com/info/synergy-docs>) 内の HPE Synergy 用語集では、HPE Synergy に関連する一般的な用語を定義します。

HPE Synergy のトラブルシューティング資料

HPE Synergy トラブルシューティング資料は、HPE OneView 内および Hewlett Packard Enterprise Information Library (<http://www.hpe.com/info/synergy-docs>) から入手できます。

HPE OneView でのトラブルシューティング

HPE OneView グラフィカルユーザーインターフェイスには、HPE OneView 内のトラブルシューティングのための、アラート通知およびオプションが含まれています。UI は、リソースのステータスとメッセージの潜在的な問題の解決を示す色の付いたアイコンを含む、HPE Synergy コンポーネントの複数のビューを示します。

検出されたすべての HPE Synergy ハードウェアのステータスをすばやく表示するには、エンクロージャービューおよびマップビューも使用できます。

HPE Synergy トラブルシューティングガイド

HPE Synergy トラブルシューティングガイドは、Hewlett Packard Enterprise Information Library (<http://www.hpe.com/info/synergy-docs>) から入手できます。HPE Synergy ハードウェアおよびソフトウェアコンポーネントの両方に対し、一般的な問題の解決のための情報、障害の分離と識別のための手順、問題の解決、および保守を提供します。

HPE ProLiant Gen10 サーバーおよび HPE Synergy エラーメッセージガイド

HPE ProLiant Gen10 サーバーおよび HPE Synergy エラーメッセージガイドは、Hewlett Packard Enterprise Information Library (<http://www.hpe.com/info/synergy-docs>) から入手できます。HPE Synergy ハードウェアおよびソフトウェアコンポーネントの両方で受け取った特定のエラーメッセージに関連する、一般的な問題を解決するための情報を提供します。

HPE OneView ヘルプと HPE OneView API リファレンス

HPE OneView ヘルプおよび HPE OneView API リファレンスは、HPE OneView のユーザーインターフェイスで利用できる、アクセスしやすい組み込み型のオンラインヘルプです。これらのヘルプファイルには、HPE Synergy 内の一般的な問題、および問題のトラブルシューティング手順と例への「詳細情報」リンクが含まれています。

このヘルプファイルは、Hewlett Packard Enterprise Information Library (www.hpe.com/info/synergy-docs) から入手できます。

HPE Synergy QuickSpecs

HPE Synergy には、システムの仕様のほか、個々の製品およびコンポーネントの仕様があります。仕様の完全な情報については、Hewlett Packard Enterprise の Web サイト (<http://www.hpe.com/info/qs>) から入手できる HPE Synergy および個々の HPE Synergy 製品の QuickSpecs を参照してください。

HPE Synergy ドキュメントの概要（ドキュメントマップ）

<http://www.hpe.com/info/synergy-docs>

プランニング

- ・ HPE Synergy 12000 Frame Site Planning Guide
- ・ HPE Synergy 構成および互換性ガイド
- ・ HPE OneView（HPE Synergy 用）サポートマトリックス
- ・ HPE Synergy イメージストリーマーサポートマトリックス
- ・ Setup Overview for HPE Synergy
- ・ HPE Synergy Software Overview Guide

ハードウェアの取り付け

- ・ HPE Synergy はじめに（フレームに付属）
- ・ HPE Synergy 12000 フレームセットアップ/インストールガイド
- ・ HPE ラックレールインストール手順 HPE Synergy 12000 フレーム用（フレームに付属）
- ・ HPE Synergy 12000 Frame Rack Template（フレームに付属）
- ・ フードラベル
- ・ ユーザーガイド類
- ・ HPE Synergy Cabling Interactive Guide
- ・ HPE OneView（HPE Synergy 用）ヘルプ — ハードウェアセットアップ

管理および監視の構成

- ・ HPE OneView（HPE Synergy 用）ヘルプ
- ・ HPE OneView（HPE Synergy 用）ユーザーガイド
- ・ HPE OneView API Reference for HPE Synergy
- ・ HPE OneView REST API スクリプティングヘルプ（HPE Synergy 用）
- ・ ユーザーガイド

管理

- ・ HPE OneView（HPE Synergy 用）ユーザーガイド
- ・ HPE Synergy イメージストリーマーヘルプ
- ・ HPE Synergy イメージストリーマーユーザーガイド
- ・ HPE Synergy イメージストリーマー API リファレンス
- ・ HPE Synergy イメージストリーマー展開ワークフロー
- ・ HPE Synergy Frame Link Module User Guide

監視

- ・ HPE OneView（HPE Synergy 用）ユーザーガイド
- ・ HPE OneView Global Dashboard ユーザーガイド

メンテナンス

- ・ Product maintenance and service guides
- ・ HPE Synergy ファームウェアとドライバ更新のためのベストプラクティス
- ・ HPE OneView（HPE Synergy 用）ヘルプ
- ・ HPE OneView（HPE Synergy 用）ユーザーガイド
- ・ HPE Synergy Appliances Maintenance and Service Guide for HPE Synergy Composer and HPE Synergy Image Streamer

トラブルシューティング

- ・ HPE OneView アラートの詳細
- ・ HPE Synergy トラブルシューティングガイド
- ・ HPE ProLiant Gen10 サーバーおよび HPE Synergy エラーメッセージガイド
- ・ Integrated Management Log Messages and Troubleshooting Guide for HPE ProLiant Gen10 and HPE Synergy
- ・ HPE OneView API Reference for HPE Synergy
- ・ HPE Synergy イメージストリーマー API リファレンス

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の場合、「Contact Hewlett Packard Enterprise Worldwide」の Web サイト(www.hpe.com/assistance)にアクセスします。
- ・ 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 (www.hpe.com/support/hpesc)にアクセスします。

必要な情報

- ・ 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、およびシリアル番号
- ・ オペレーティングシステム名とバージョン
- ・ 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とログ
- ・ 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、**Synergy の Software Depot** に移動します。
- ・ お客様の資格を表示したりアップデートしたり、契約や保証をお客様のプロファイルにリンクしたりするには、Hewlett Packard Enterprise サポートセンターの **More Information on Access to Support Materials** ページにアクセスします。

www.hpe.com/support/AccessToSupportMaterials

- ⓘ **重要:** 一部のアップデートにアクセスするには、Hewlett Packard Enterprise サポートセンターからアクセスするときに製品の権利付与情報が必要になる場合があります。関連する権利付与情報を使って HP パスポートをセットアップしておく必要があります。

Web サイト

Web サイト	リンク
Hewlett Packard Enterprise Information Library	www.hpe.com/info/enterprise/docs
Hewlett Packard Enterprise サポートセンター	www.hpe.com/support/hpesc
Hewlett Packard Enterprise Worldwide の連絡先	www.hpe.com/assistance
HPE OneView ドキュメント	www.hpe.com/info/oneview/docs
サブスクリプションサービス/サポートのアラート	http://www.hpe.com/support/e-updates-ja
カスタマーセルフリペア	www.hpe.com/support/selfrepair
HPE OneView FAQ ドキュメントの Remote Support	Remote Support のドキュメント (英語)
Single Point of Connectivity Knowledge (SPOCK) ストレージ互換性マトリックス	www.hpe.com/storage/spock
HPE 3PAR StoreServ ストレージ	www.hpe.com/info/storage
HPE Integrated Lights-Out	http://www.hpe.com/jp/servers/ilo
ストレージのホワイトペーパーおよび分析レポート	www.hpe.com/storage/whitepapers

リモートサポート (HPE 通報サービス)

リモートサポートは、保証またはサポート契約の一部としてサポートデバイスでご利用いただけます。リモートサポートは、インテリジェントなイベント診断を提供し、ハードウェアイベントを Hewlett Packard Enterprise に安全な方法で自動通知します。これにより、ご使用の製品のサービスレベルに基づいて、迅速かつ正確な解決が行われます。ご使用のデバイスをリモートサポートに登録することを強くおすすめします。

ご使用の製品にリモートサポートの追加詳細情報が含まれる場合は、検索を使用してその情報を見つけてください。

リモートサポートおよびプロアクティブケア情報

HPE 通報サービス

www.hpe.com/services/getconnected

HPE プロアクティブ ケアサービス

<http://www.hpe.com/services/proactivecare-ja>

HPE プロアクティブケアサービス : サポートされている製品のリスト

www.hpe.com/services/proactivecaresupportedproducts

HPE プロアクティブケアアドバンスドサービス : サポートされている製品のリスト

www.hpe.com/services/proactivecareadvancedsupportedproducts

カスタマーセルフリペア (CSR)

Hewlett Packard Enterprise カスタマーセルフリペア (CSR) プログラムでは、ご使用の製品をお客様ご自身で修理することができます。CSR 部品を交換する必要がある場合、お客様のご都合のよいときに交換できるよう

直接配送されます。一部の部品は CSR の対象になりません。Hewlett Packard Enterprise もしくはその正規保守代理店が、CSR によって修理可能かどうかを判断します。

ドキュメントに関するご意見、ご指摘

Hewlett Packard Enterprise では、お客様により良いドキュメントを提供するように努めています。ドキュメントを改善するために役立てさせていただきますので、何らかの誤り、提案、コメントなどがございましたら、ドキュメントフィードバック担当 (docsfeedback@hpe.com) へお寄せください。この電子メールには、ドキュメントのタイトル、部品番号、版数、およびドキュメントの表紙に記載されている刊行日をご記載ください。オンラインヘルプの内容に関するフィードバックの場合は、製品名、製品のバージョン、ヘルプの版数、およびご利用規約ページに記載されている刊行日もお知らせください。