



Hewlett Packard
Enterprise

HPE OneView 4.0 (HPE Synergy 用) リリースノート

摘要

本書では、HPE OneView 4.0 (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 上のコンピューティングモジュール、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: P01319-191
発行: 2017 年 12 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

Google®は、Google Inc.の登録商標です。Microsoft®およびWindows®は、Microsoft グループ企業の商標です。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 4.0 (HPE Synergy 用) で提供される主な変更点.....	6
HPE OneView 4.0 (HPE Synergy 用) の新機能.....	6
アプライアンスのインストール/アップデート手順.....	9
アップデート後のアプライアンスのバックアップ.....	9
問題と推奨処置.....	11
SAN 自動ゾーニング機能の問題.....	11
CHAP 名の長さ制限.....	11
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.....	11
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.....	11
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.....	11
サーバーハードウェアの取り外しと挿入中に、Remote Support のデータ収集が失敗する.....	12
サーバーが挿入された後に Remote Support が有効にならない.....	12
HPE Synergy コンポーザーの初期セットアップ中の問題.....	12
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.....	12
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可能性がある.....	12
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.....	13
Active Directory 認証エラーメッセージ.....	13
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.....	13
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.....	14
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.....	14
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.....	14
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.....	14
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.....	14
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.....	15
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.....	15
アップリンクセットからネットワークを削除しても、アラートが表示されず、不適切なプロファイルおよび接続状態が表示される.....	15
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.....	15
HPE Synergy コンポーザー 4.0 によって管理されるフレームの削除.....	16
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.....	16
リモートの FLM 証明書が、手動での削除後も HPE OneView によって再度受け入れられる.....	16
サーバーが iLO のリセット直後にアップデートされると、iLO5 の HPE OneView SNMP 構成が破損する.....	16
HPE OneView によって Gen10 ハードウェアが検出されない.....	17
オンラインヘルプページの「サーバープロファイルの作成」で、NIC チェッキングオプションを指定できない.....	17
ソフトウェア管理者の役割を使用する場合の制限事項.....	17

証明書の期限切れアラートが、警告アラートではなく重大なロックされたアラートとして誤って生成される.....	18
関連付けられた証明書が削除されると、証明書に関連するアラートをクリアまたは削除できない.....	18
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を取り外すと、不適切なスタッキングヘルスアラートが発生する.....	18
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.....	19
デバイス証明書チェーンに期限切れの CA ルート証明書および中間証明書があると、通信問題が発生する.....	19
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.....	19
イメージストリーマーの展開プランを使用して作成したサーバープロファイルに正しいパスワードフィールドが反映されない.....	19
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.....	20
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、誤った一貫性警告アラートが表示される.....	20
ホスト名が数字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.....	20
一回限りの追加セットアップを行って下位互換性を確保しないと、古いクライアントに対する REST リクエストが失敗する.....	20
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.....	21
新しいエンクロージャーに移動した後、アプライアンスクラスターを形成できず、可用性が高くなる.....	22
ルート CA 「ILO/iLO3/iLO4 デフォルト発行元 (信頼しない)」を信頼する.....	23
アップロードされた CRL は即座に有効になるが、UI に表示されるまで 1 時間かかる.....	23
Active Directory サーバーの構成には TLS v1.2 を使用.....	23
トラストストアに証明書が存在するにもかかわらず、管理対象デバイスとの通信が失敗する.....	23
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.....	23
ファームウェアアップデート後、Synergy コンピューティングモジュールでファイルシステムが読み取り専用になる.....	24
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.....	24

HPE OneView 4.0 (HPE Synergy 用) に関する注意..... 25

ドキュメントの補足..... 26

セキュリティ.....	26
HPE OneView API リファレンス.....	26
3PAR ストレージレイとの FC 直接接続.....	26
HPE Synergy コンポーザーから受け取った Remote Support イベントの表示.....	26
API バージョンのサポートを削除.....	26
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.....	26
REST API を使用する際のリモートログインのセキュリティ保証.....	26

ドキュメントに関する正誤表..... 28

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..... 29

HPE Synergy のドキュメント.....	29
HPE Synergy 構成および互換性ガイド.....	29
HPE Synergy フレームリンクモジュールユーザーガイド.....	29
HPE OneView (HPE Synergy 用) ユーザーガイド.....	29
HPE OneView Global Dashboard.....	29
HPE Synergy イメージストリーマーユーザーガイド.....	29

HPE Synergy イメージストリーマー GitHub.....	30
HPE Synergy Software Overview Guide.....	30
HPE Synergy ファームウェアアップデートの概要.....	30
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.....	30
HPE OneView (HPE Synergy 用) サポートマトリックス.....	30
HPE Synergy イメージストリーマーサポートマトリックス.....	30
HPE Synergy 用語集.....	30
HPE Synergy のトラブルシューティング資料.....	31
HPE OneView でのトラブルシューティング.....	31
HPE Synergy トラブルシューティングガイド.....	31
Error Message Guide for HPE ProLiant Gen10 servers and HPE Synergy.....	31
HPE OneView ヘルプと HPE OneView API リファレンス.....	31
HPE Synergy QuickSpecs.....	31

HPE Synergy ドキュメントの概要 (ドキュメントマップ) 32

サポートと他のリソース..... 33

Hewlett Packard Enterprise サポートへのアクセス.....	33
アップデートへのアクセス.....	33
Web サイト.....	34
リモートサポート (HPE 通報サービス)	34
カスタマーセルフリペア (CSR)	34
ドキュメントに関するご意見、ご指摘.....	35

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 4.0（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">• 主な機能• 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 4.0（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 4.0（HPE Synergy 用）で提供される主な変更点

- Chrome バージョン 53.0 を使用する場合の、ダイアログボタンに関する問題を解決する。
- すべてのスタッキングリンクがダウンし、HPE Synergy インターコネクトモジュール（ICM）でデュアルユニットスタッキングが構成されている場合にマルチモジュールリンクアグリゲーション（MLAG）の潜在的なトラフィックロスを解決する。
- 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ていないことで起きる問題を解決する。
- HPE OneView が、論理インターコネクト（LI）および論理エンクロージャー（LE）ビューページで、HPE Synergy D3940 ストレージモジュールの I/O アダプターのファームウェアバージョン番号を誤表示する問題を解決する。
- 複数の SAS 論理インターコネクトに対して同時にファームウェアアップデートを実行すると、最初のファームウェアのみがアップデートされ、残りのファームウェアをアップデートできない問題を解決する。

HPE OneView 4.0（HPE Synergy 用）の新機能

セキュリティ

- スコープベースのアクセス制御
SBAC は、アプライアンスによって管理されるリソースのサブセットのみで機能する役割（サーバー、ストレージ、ネットワーク管理者など）を制限することにより、現在の役割ベースのアクセス制御を拡張します。リソースのサブセットは、リソースの論理グループであるスコープ機能によって定義されます。たとえば、Sarah という名前のサーバー管理者は、「実稼動」スコープのサーバーのみを管理できます。
- Two-Factor 認証（CAC/PIV）

スマートカードを使用して認証する機能を提供します。サポートされているスマートカードには、Common Access Card (CAC) や Personal Identity Verification (PIV) カードがあります。この機能は、HPE OneView の Active Directory サポートに統合されています。ユーザーは、PIN および証明書をスマートカードに指定し、これらの情報がディレクトリ内のアカウントと照合/検証されます。

- 証明書の管理

証明書の管理は、証明書ベースの信頼を管理するためのポリシーと手順を改善します。たとえば、HPE OneView 証明書トラストストアの管理機能、証明書失効に対するサポート、自己署名証明書の管理などがあります。

HPE OneView 4.0 で追加された包括的な証明書の管理機能は次のとおりです。

- iLO、Onboard Administrator、フレームリンクモジュール、リモートリポジトリ、プロキシサーバーなどの証明機関 (CA) 署名証明書のサポート
- 証明書失効リスト (CRL) のサポート
- 初回デバイス検出中に自己署名証明書を自動的に信頼
- HPE OneView 証明書ストアの管理
- 証明書の期限切れに関連するイベントのアラート
- 証明書の検証の厳密さを管理するためのセキュリティ設定

- SNMPv3

以前のバージョンの HPE OneView では、サーバーハードウェアのヘルスの監視に SNMPv1 を使用します。HPE OneView 4.0 では、さらに安全性の高い SNMPv3 プロトコルを介してヘルスを監視することができます。この機能は、iLO4 以降を使用しているサーバーで利用可能です。HPE OneView は、サーバーの次回のアップデートイベント (HPE OneView の再起動やサーバーの明示的なアップデートなど) の際に SNMPv3 を使用するように自動でアップデートされます。HPE OneView では、SNMPv3 を使用して SNMP トラップを転送することもできます。これには、管理対象デバイスまたは監視対象デバイスからの受信 SNMPv1 トラップが含まれます。このトラップは SNMPv3 に自動的に変換され、転送されます。SNMPv1 を経由した転送のサポートは下位互換性のために保持されます。

ストレージ

- SAN 構成負荷分散からのブート - 接続とターゲット

SAN (BFS) 構成からのブートをサーバープロファイルやサーバープロファイルテンプレートで指定し、SAN およびストレージシステムターゲットに対して、接続のプライマリ/セカンダリ割り当ておよびストレージシステムターゲットポートの選択構成を均等に負荷分散することで、SAN およびストレージシステムインフラストラクチャを自動的に最大限活用できるようになります。複数のストレージプロファイルテンプレートを管理する必要がなくなるため、管理者はサーバー全体のブート構成の切り替えを追跡する必要もなくなります。

- ボリュームテンプレートと SP/SPT とのプロパティロックの統合

すべての HPE OneView を通じてボリュームを管理する、一貫性のある統合されたストレージボリューム管理機能を提供します。ボリュームテンプレート、プロパティロック、およびすべてのボリューム設定は、ボリュームテンプレート、ボリューム、サーバープロファイル、およびサーバープロファイルテンプレートを使用して管理することができます。

- iSCSI CHAP 認証情報の再生成

サーバーおよびストレージシステム間で iSCSI データバス CHAP 認証情報を再生成し、データセンターのパスワードローテーションポリシーをサポートします。

Virtual Connect

- s チャンネルの LACP - アップリンクポート上のマルチモジュール LAG (MLAG) と組み合わせると、コンピュータノードからアップストリームネットワークインフラストラクチャまでの本格的なエンドツーエンドのリンクアグリゲーションを提供します。この機能は、マスター/サテライトアーキテクチャにおける、フリクションレスなファームウェアアップデートに欠かせない要素です。これにより、アダプターポート間でシームレスなフェイルオーバーが実現し、トラフィックの負荷分散が強化されます。これを使用すると、サーバー管理者はスイッチアシスト NIC チューニングポリシーを利用することができます。
- 混在速度のマスター/サテライト ICM 構成 - この機能を使用すると、Synergy をご利用のお客様は、最大 4 つの Synergy フレームをラックに取り付け、フレームおよびインターコネクットの同じセット内に 10 Gb トラフィックと 20 Gb トラフィックを組み合わせながら、自身のアプリケーションのニーズに合わせてコンピューティングモジュールの帯域幅要件をカスタマイズすることができます。
- SmartLink および非冗長構成 - Synergy の VC の場合、アクティブ/アクティブ構成はイーサネットネットワーク構成です。この構成では、同じ VLAN 上のアクティブトラフィックで複数の VC インターコネクットモジュールを退出させることができるほか、すべてのアップリンクポート（スタンドバイモードではアップリンクポートなし）を最大限に活用し、SmartLink 機能と組み合わせる場合に、冗長性を維持しながら利用可能な帯域幅を倍増させます。また、インターコネクットのアップリンクポートのいずれかが実稼動ネットワークから切断された場合もシームレスなフェイルオーバーを提供します。SmartLink は VC モジュールに不可欠です。これによって、VC モジュールは、接続に割り当てられているネットワークがアップリンクポートを失った場合に、リンクをサーバープロファイル接続に自動で落とします。
- Pause Flood 検出および保護 - イーサネットスイッチインターフェイスでは、休止フレームベースのフロー制御メカニズムを使用してリンクパートナーからのデータフローを絞ります。休止フレームをフロー制御対応インターフェイスで受信すると、送信操作は停止されます。その他のすべてのトラフィックはキューに入れます。一定のストリームの休止フレームを長時間にわたって受信すると、キューリソースが消耗する原因となります。この状態は、すべてのインターフェイスでの切替操作と制御プロトコルトラフィックを処理する切替機能に大きな影響を与えます。この機能は、一時停止フラッディング状態のすべてのスイッチポートを監視し、スイッチのリソース消費を防ぎます。
- Synergy 無停止ファームウェアアップデート - 冗長サーバープロファイル接続構成、冗長アップストリームスイッチコネクティビティ、動的な「パスフェイルオーバー」を可能にする LAG を使用した論理インターコネクットアップリンクセットなどの本格的なエンドツーエンドの冗長性を提供する構成の場合、この機能は、無停止ファームウェアアップデートを提供します。無停止ファームウェアアップデートでは、ホストコンピューティングモジュールで実行されるアプリケーションについてネットワークエラーやネットワークパフォーマンスの低下を引き起こすことなく、Synergy ネットワーキングインフラストラクチャをアップデートできます。
- プライベートネットワークのサポート - プライベートネットワークでは、所定のネットワークのサーバー間トラフィックフローを制限することでネットワークセキュリティが保証されます。プライベートネットワークに関連付けられたサーバーポートやサーバープロファイル接続では、同じレイヤー 2 イーサネットドメイン内で互いに直接通信することはできません。デスティネーションとして別のサーバーを持つすべてのトラフィックはアップリンクポートを通じて出ていき、外部のレイヤー 3 ルーター経由で転送される必要があります。
- ネットワークセットの VLAN スケールを増大 - 明示的な VLAN の数が多いほど、特に Cisco ACI との相互運用性などの Synergy ネットワーキングユースケースが向上します。この機能は、ネットワークセットごとに 162 という限界を引き上げ、LIG/LI のサイズに基づいてネットワークセットの限界を動的に押し上げることができます。
 - 1×フレーム LIG/LI - 1000 VLAN
 - 2×フレーム LIG/LI - 500 VLAN

- 3×フレーム LIG/LI - 333 VLAN
- 4×フレーム LIG/LI - 250 VLAN
- 5×フレーム LIG/LI - 200 VLAN
- 割り当てられているネットワークのない接続 - サーバー管理者は、サーバー「ポート」を予約し、後で、サーバー電源がオンになっている間にネットワークを割り当てることができます。これによって、次のユースケースが促進されます。
 - サーバー接続の事前プロビジョニング - お客様は、サーバーが必要とする接続（NIC ポート）の数を知っていますが、OS のプロビジョニング時に実稼動ネットワークでサーバーが「Chatty」になることは望みません。
 - サーバーの電源を切ってから実稼動ワークロードに接続を追加する必要性を省きます。
 - サーバー取得および OS インストールの前に仮想 MAC および WWN を割り当てることで、顧客プロセスがさらに最適化されます。
 - サーバーの電源をオフにしなくてもプロファイル接続を無効にすることができます。
- 構成パフォーマンスの向上 - 従来のリリースよりも Synergy リソースを迅速に検出して構成する機能が改善したため、論理エンクロージャーの作成時間が 60%短縮され、サーバープロファイルの作成にかかる時間も 75%短縮されます。
- Remote Support - Synergy インターコネクトをリモートでサポートします。ハードウェアに障害が発生すると、サポートケースが自動的にトリガーされます。
- HPE Synergy ファームウェア（4.00.33 以上が必要）用 HPE Virtual Connect SE 16Gb 24 ポートファイバーチャンネルモジュール
 - HPE Virtual Connect SE 16Gb FC モジュール（HPE Synergy ポートランキング用） - この機能は、IO パフォーマンスを最大限に高め、単一または複数のリンク障害によるダウンタイムを削減します。また、1 つの物理リンク上の IO 完了のスループット依存を排除し、トランクに参加するすべてのリンクについて総合パフォーマンスを向上させます。単一または複数の障害点を排除しながら、トランク内の 1 つまたは複数のリンクに障害が起きてもトラフィックの流れを継続させることができます。
 - ポートの監視に関するサポートが追加されています。
 - 旧式で脆弱な SSH および TLS 暗号（aes128-cbc、3des-cbc、aes192-cbc、aes256-cbc、DES-CBC3-SHA など）の使用を省きます。
 - CVE-2016-0800、CVE-2016-6515、CVE-2015-8325、CVE-2015-0291、および CVE-2016-2183 のセキュリティの脆弱性を解決します。

アプライアンスのインストール/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。

アップデート手順は、www.hpe.com/downloads/synergy にあるリリースセットに記載されています。

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。

復元できるのは、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 4.0 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。

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) と互換性がありません。

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 4.0 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、この設定が無視される。

推奨処置

RBSU を起動し、ネットワークブートオプションで iSCSI ポリシーの設定を変更してください。

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。

サーバーハードウェアの取り外しと挿入中に、Remote Support のデータ収集が失敗する

定期の Remote Support のデータ収集中に、サーバーハードウェアの取り外しと挿入を実行すると、収集が失敗することがある。

推奨処置

サーバーハードウェアの取り外しと挿入のスケジュールを、定期のデータ収集操作期間から外すか、または定期収集のスケジュールを変更します。

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ことがある。

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可能性がある

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ない可能性がある。

- ブートデバイスがリモート。たとえば、Storage Area Network (SAN) デバイス、またはゾーンのローカルストレージから起動。
- サーバープロファイルのブートモードが Unified Extensible Firmware Interface (UEFI)。
- 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

ブラウザをアップデートし、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、ブラウザのアップデートを実行します。

Active Directory 認証エラーメッセージ

Active Directory 認証を HPE OneView に追加する際、Active Directory サーバーのアドレスが、数値の IP アドレスではなく DNS 名を使用して指定されていると、エラーが発生する場合があります。エラーメッセージは次のとおりです。

「ポート<ポート番号>が構成されているディレクトリサーバー<DNS 名>に到達できません。ディレクトリサーバー<DNS 名>に ping できません。」

推奨処置

ディレクトリサーバーを HPE OneView に追加する場合は、数値の IP アドレスを使用します。

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、VFC MAC アドレスバインディングを Cisco のトップオブラックス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witch 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witch 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てから交換モジュールを挿入し、その後、予備のフレームリンクモジュールがフレームを引き継ぐと、HPE OneView でエラーが発生する。

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

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ト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ト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 ソフトウェアを起動しても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

RBSU 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ります。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、**プロファイル操作メニュー**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アップデートアクションを行って、影響を受けるサーバープロファイルをアップデートしてください。

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、アラートが表示されず、不適切なプロファイルおよび接続状態が表示される

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ります。

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復元し、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復元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 iLO5 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ないことがあります。

推奨処置

iLO5 Web インターフェイスにログインし、iLO5 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 4.0 によって管理されるフレームの削除

HPE Synergy コンポーザー 4.0 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。

自己署名証明書を手動以外の方法で削除した場合、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 番目がプライムブート可能であり、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

リモートの FLM 証明書が、手動での削除後も HPE OneView によって再度受け入れられる

HPE OneView UI からリモートリング内の FLM 証明書を手動で削除した場合、その同じ FLM に再接続すると、HPE OneView はこの証明書を自動的に再度受け入れます。

サーバーが iLO のリセット直後にアップデートされると、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がリセットされると、HPE OneView が iLO5 で設定する SNMP 構成が破損する可能性があります。これにより、iLO5 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

iLO5 が応答を開始した後約 1 分待ってから、HPE OneView でサーバーを再びアップデートしてください。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 コンピューティング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) の最新のリリースセットをダウンロードします。
2. リリースセットから 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 (3.10.04 以降) 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. リリースセットから HPE Synergy Custom SPP バンドルを展開して、ファームウェアリ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 コンピューティングモジュールが、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、コンピューティング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。

オンラインヘルプページの「サーバープロファイルの作成」で、NIC チーミングオプションを指定できない

オンラインヘルプページの「サーバープロファイルの作成」で、OS 展開画面に NIC チーミングオプションが表示されない。

推奨処置

OS 展開画面では、チーム化された NIC 属性の 2 つの同類ネットワーク接続をチーム化することができます。NIC チーミングでは、2 つの NIC 属性を 1 つの NIC チーム属性にまとめ、いずれの接続も同じネットワークに対して確立することができます。また、OS/アプリケーションを正常に実行するにはチーミングをオプションとするか必須とするかを展開プランで指定することができます。さらに、展開プランで、OS に冗長 NIC トラフィックが発生しないように NIC チームを適切に構成することができます。

ソフトウェア管理者の役割を使用する場合の制限事項

ソフトウェア管理者の役割は、インフラストラクチャ管理者が、すべての HPE OneView リソース (エンクロージャー、LE、LIG、LI、ネットワーク、ユーザー、グループなど) を管理する権限をユーザーに付与することなく、HPE Synergy イメージストリーマーのリソース (展開プラン、ゴールドイメージ、OS ビルドプラン、プランスクリプト、アーカイブバンドルなど) の管理権限を委任できるようにするために作成されたものです。ただし、この場合はソフトウェア管理者の役割に制限が設けられます。たとえば、この役割が与えられたユーザーは、自分が開始したタスクの詳細や自分のリソースに関するアラートを見ることはできません。

推奨処置

インフラストラクチャ管理者権限をソフトウェア管理者に付与してください。特権を編集するには、次のリンクを参照してください。[ローカルユーザーアカウントの編集 \(インフラストラクチャ管理者として\)](#)

証明書の期限切れアラートが、警告アラートではなく重大なロックされたアラートとして誤って生成される

HPE OneView には新しい証明書に関連するセキュリティ設定、「自己署名証明書の有効期限をチェックする」が含まれています。この設定は、デフォルトでは無効になっています。無効化されている場合、デバイスのリソースページ（サーバーハードウェアページなど）に期限切れの証明書のデバイスに関する警告アラートが表示されます。さらに、期限切れの証明書に関する個別のアラートが設定/アクティビティーページに表示されます。これら後者のアラートが、警告アラートではなく、自己署名証明書の重大なロックされたアラートとして誤って生成されます。

推奨処置

デバイスとの通信は、これら特定の重大なアラートによる影響を受けません。期限切れの証明書が修正されると、警告アラートと重大なアラートの両方が自動的にクリアされます。証明書アラートを解決するには、デバイスの新しい自己署名証明書を生成し、これを HPE OneView の証明書トラストストアに配置するか、証明書署名要求を実行し、デバイスに対して認証機関によって発行された証明書を使用します。

関連付けられた証明書が削除されると、証明書に関連するアラートをクリアまたは削除できない

証明書に関連するアラート（証明書の有効期限や失効など）はクリアされることはなく、元のアラートに関連する証明書が削除された場合、削除することができません。

推奨処置

自己署名証明書を使用するデバイスの場合、デバイスの標準的な手順に従って、証明書をアップデートし、結果の証明書を HPE OneView にアップロードします。必ず、元の証明書と同じエイリアスを使用してください。アラートに適切なエイリアスが表示されていることに注意してください。

有効期限が切れた自己署名証明書は、証明機関の署名付き証明書に置き換えられる場合、トラストストアにすでに存在する既存の有効な自己署名証明書が使用され、上記の適切なエイリアスを使用して一時的にアップロードされます。アラートをクリアした後は、一時的な自己署名証明書を削除できます。トラストストアにこの一時的な証明書が存在することが、セキュリティリスクを示すわけではありません。デバイスとの通信を有効にはしません。

上記のどちらのケースでも、有効期限について処理されるトラストストアの証明書アラートは、スケジュールされたバックグラウンドタスクを使用して実行されます。アラートがクリアされるまでに最長 1 時間を要することがあります。

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を取り外すと、不適切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。

デバイス証明書チェーンに期限切れの CA ルート証明書および中間証明書があると、通信問題が発生する

HPE OneView が HTTPS 接続を開始したときにリモートサーバー/デバイスがリーフ証明書または部分証明書チェーンのみを提供し、残りのチェーンを構成する HPE OneView トラストストアに格納されているルート証明書または中間証明書のいずれかが期限切れになっている場合、ユーザーは是正措置を講じるまで期限切れの証明書を使用してデバイスへの接続が引き続き信頼されます。

推奨処置

HPE OneView は、トラストストア内の証明書の期限より前にアラートを表示します。期限の 2 か月前から毎日アラートが表示されます。この問題を回避するには、アラートに示されている対処法に従ってください。

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

イメージストリーマー OS 展開プランがサーバープロファイルテンプレートで指定されている場合に、展開プランのカスタム属性のパスワード値を空白のままにすると、サーバープロファイルテンプレートを後で編集するときに、実際には未設定であるにもかかわらずパスワードが設定されているようにドットが表示される。

推奨処置

パスワードを設定することを意図したサーバープロファイルテンプレートを編集する場合は、表示されているものを盲信せず、フィールドをクリアしてパスワードを再入力するのが最善策です。

イメージストリーマーの展開プランを使用して作成したサーバープロファイルに正しいパスワードフィールドが反映されない

イメージストリーマーの展開プランを使用してサーバープロファイルテンプレートからサーバープロファイルを作成する際、カスタム属性パスワードフィールドの内容に、サーバープロファイルテンプレートで入力した値が反映されない。これは、存在すべき場所にパスワードがないか、存在してはならない場所にパスワードがあるかのいずれかが原因であると考えられます。

推奨処置

OS 展開プランでサーバープロファイルテンプレートからサーバープロファイルを作成する場合は、**サーバープロファイルの作成アクション**を通じてサーバープロファイルテンプレートからプロセスを開始してください。サーバープロファイルページまたはサーバーハードウェアページからプロセスを開始しないでください。このプロセスをサーバープロファイルページまたはサーバーハードウェアページから開始する場合は、サーバープロファイルのカスタム属性パスワードフィールドの内容に関係なく、必ずフィールドをクリアしてから必要なパスワードを入力してください。

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、接続損失がない場合でも、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、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、誤った一貫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一貫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、一貫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

アラートは手動でクリアすることができます。

ホスト名が数字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

ホスト名が数字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します。

推奨処置

ホスト名には英数字の値を入力します。

一回限りの追加セットアップを行って下位互換性を確保しないと、古いクライアントに対する REST リクエストが失敗する

HPE OneView 4.0 のインストールをエンタープライズディレクトリに統合した場合、バージョン 4.0 では認証機関によって発行された証明書チェーンでディレクトリを使用するときの HTTPS 証明書のチェック機能が改善されました。これらの改善されたセキュリティチェックでは、旧バージョンの HPE OneView のディレクトリ構成関連の REST API を使用してスクリプトや製品との互換性を維持するために、一回限りの追加セットアップが必要です。追加セットアップが実行されるまで、古いクライアント（バージョン 500 以前を指定する API 呼び出しを使用するクライアントなど）では、/rest/logindetails などの REST リクエストは失敗します。

この問題は、新しいバージョン 4.0 のインストールに固有の問題です。以前のリリースからアップグレードする場合、追加の手順は不要であり、下位互換性は自動的に保持されます。自己署名証明書を使用するディレクトリは影響を受けません。

推奨処置

エンタープライズディレクトリ統合とレガシーの HPE OneView クライアントを使用する新しい HPE OneView 4.0 インストールでは、ディレクトリサーバーを構成する際に、以下のように強制的にリーフ証明書を信頼するオプションをオンにしてください。

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。

同じ関数を実行するために、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。

新しいエンクロージャーに移動した後、アプライアンスクラスターを形成できず、可用性が高くなる

論理エンクロージャー（LE）の拡張操作の実行、推奨される HA アクションごとの関連するスタンバイアプライアンスの新しいエンクロージャー（Synergy フレーム）への移動、その後での設定 > アプライアンス > スタンバイを削除の選択、アップグレード操作の実行、復元の実行後、HPE OneView アプリケーションクラスターの形成が失敗し、クラスターの可用性が高くなる場合があります。

イメージストリーマーを同じ LE に追加すると、イメージストリーマーの展開サーバーの追加に失敗したり、LE のグループタスクからのアップデートがハングしたりする可能性があります。また、フレームリンクモジュール（FLM）ファームウェアをアップデートした後や、FLM モジュールが失敗すると、「**イメージストリーマー展開アプライアンスでストレージシステムにクォーラムが構成されていません**」というアラートが HPE OneView に表示される場合があります。

推奨処置

HPE OneView アプライアンスのクラスターの問題、またはイメージストリーマーのクォーラムアラートの発生後にこれらに対処するには、最寄りの HPE サポート窓口にお問い合わせして fixme.bin を入手するか、次の手順を実行してください。

1. HPE コンポーザーのスタンバイアプライアンスをアクティブなアプライアンスと同じフレームに移動します。アプライアンスが同期されたら、アクティブアプライアンスとスタンバイアプライアンスが、設定 > アプライアンスページに**接続済み**と表示されていることを確認します。
2. 「**Two appliances in an appliance cluster should not be in same frame (アプライアンスクラスター内の 2 つのアプライアンスは、同じフレーム内に存在してはなりません)**」という後続のアラートを解決するには、スタンバイアプライアンスを新しいフレームに移動します。アプライアンスが同期されたら、アクティブアプライアンスとスタンバイアプライアンスが、設定 > アプライアンスページに**接続済み**と表示されていることを確認します。

論理エンクロージャーで発生したイメージストリーマーの**展開サーバーの追加の失敗**や**グループからアップデートのハング**の問題の発生後に解決するには、最寄りの HPE サポート窓口にお問い合わせして fixme.bin（前述と同じバージョン）を入手してください。fixme.bin を適用してから、以下の手順を実行します。

1. 工場出荷時設定にリセットし、OS 展開サーバーのアプライアンスペアを再挿入します。
2. 当初失敗した操作を再度実行します。

ルート CA「iLO/iLO3/iLO4 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。

アップロードされた CRL は即座に有効になるが、UI に表示されるまで 1 時間かかる

認証機関の証明書失効リスト（CRL）をアップロードすると、CRL は HPE OneView から処理され、すぐにすべての後続の TLS 接続に適用されます。ただし、1 時間単位の証明書ステータスのスケジュール済みジョブが実行され、UI でステータスがアップデートされた場合に、アップロードされた CRL が証明書の管理 UI で有効であると表示されるまで最長 1 時間かかる可能性があります。

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。

トラストストアに証明書が存在するにもかかわらず、管理対象デバイスとの通信が失敗する

まれに、トラストストアに証明書が存在するにもかかわらず、**信頼された通信を確立できません**というアラートにより管理対象デバイスとの通信が失敗する場合があります。証明書を追加するための解決方法は失敗します。

推奨処置

設定 > セキュリティ > 証明書の管理画面から、以下を行います。

- 通信が失敗したデバイス証明書を削除する
- 同じエイリアス名を使用するデバイス証明書を追加する

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、Synergy コンピューティング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 Synergy コンピューティングモジュールで、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 4.0 (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) の最初の仮想関数にのみ使用でき、HW-iSCSI 接続は、物理ポート (ポート「b」、つまりストレージ関数) の 2 番目の関数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 4.0 (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 4.0 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 OneView (VC など) 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。ブレードが挿入されると、HPE OneView はブレードを検出し、ブレード/OA をチェックしてそれが同一サーバーであるかどうか (UUID を使用)、および以前のブレード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。構成が異なる場合は、プロファイルに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。

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 4.0 (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

注記: サポートされる API の最小バージョンは今後のリリースで変更されることがあります。このため、HPE OneView の新しいバージョンへのアップグレード時の互換性の問題を回避するためご都合のよいときに、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。

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 コンポーザーから送信され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 1 つまたは複数のドキュメントで詳しく説明していません。

- HPE OneView 4.0 リリースノート
- HPE OneView 4.0 サポートマトリックス
- HPE OneView 4.0 API スクリプティングヘルプ

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。

REST API を使用する際のリモートログインのセキュリティ保証

`/rest/login-sessions/smartcards` を使用してアプライアンスにリモートでログインするには、通常実行されるサーバー証明書認証に加えて、プライベートキーとクライアント証明書認証をサポートするクライアントライブラリを使用する必要があります。クライアントライブラリを評価する場合は、クライアントのプライベートキーがサーバーに渡されないことを確認してください。

この REST API を使用してセキュアなリモートログインを行う方法には、Curl バージョン 7.54.1-1 以降を使用する方法が考えられます。この結果として libssh2 が使用されます ([curl man page](#) を参照)。

ドキュメントに関する正誤表

- HPE OneView のオンラインヘルプでは、**OS ボリューム > 全般**セクションに、OS ボリュームの状態が表示されると記載されていますが、これは間違いです。OS ボリュームの状態は、HPE Synergy イメージストリーマーのユーザーインターフェイスの**展開アプライアンス > ストレージ**セクションに表示されます。
- HPE OneView オンラインヘルプの「**複数の論理インターコネクトグループを持つエンクロージャーグループの有効な構成**」セクションで、下記の注記の「Virtual Connect SE 40Gb F8 モジュールが複数のフレームで冗長性のために構成されている場合、HPE Synergy イメージストリーマー展開はサポートされません。」という部分は、HPE OneView 4.0 には適用されません。

注記: 高可用環境でのオペレーティングシステム展開に HPE Synergy イメージストリーマーを使用するには、Synergy の Virtual Connect SE 40Gb F8 モジュールと Synergy フレームのインターコネクトリンクモジュールのセットごとに、Synergy イメージストリーマーアプライアンスのペアが必要です。論理エンクロージャーに含めることができるイメージストリーマーアプライアンスは、1 台までです。

Virtual Connect SE 40Gb F8 モジュールが複数のフレームで冗長性のために構成されている場合、HPE Synergy イメージストリーマー展開はサポートされません。

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 イメージストリーマー GitHub

HPE Synergy イメージストリーマー 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 通報サービス)

HPE Synergy ファームウェアアップデートの概要

*HPE Synergy ファームウェアアップデートの概要*は、Hewlett Packard Enterprise Information Library (<http://www.hpe.com/info/synergy-docs>) から入手できます。本書では、HPE Synergy のファームウェアをアップデートする方法について説明します。

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 (<http://www.hpe.com/info/synergy-docs>) から入手できます。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。

Error Message Guide for HPE ProLiant Gen10 servers and HPE Synergy

Error Message Guide for HPE ProLiant Gen10 servers and HPE Synergy 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アップデート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*
- *Error Message Guide for HPE ProLiant Gen10 servers and HPE Synergy*
- *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。