Hewlett Packard Enterprise

HPE OneView 4.0 リリースノート

摘要

本書では、HPE OneView 4.0 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 の仮想アプライアンスを使用して HPE ProLiant サーバー、HPE Virtual Connect、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: P01318-191
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

はじめに

このドキュメントでは、HPE OneView 4.0 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	• **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**
新規でアプライアンスをインストールする、または HPE OneView の 1.20 以降のバージョンからアップグレードするユーザー	• **アプライアンスのインストール/アップデート手順** • HPE OneView 4.0 を使用するための**問題とその対策**

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 の導入では、前のリリースの問題は **HPE OneView ライフサイクルページ**で説明されているように対処されます。

HPE OneView 4.0 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動作する役割（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、「製品」スコープのサーバーのみを管理できます。

- 証明書の管理

  証明書の管理によって、証明書ベースの信頼を管理するためのポリシーと手順が向上します。たとえば、HPE OneView 証明書の信頼ストアの管理機能、証明書失効のサポート、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

- 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。

- SNMPv3

  HPE OneView の以前のバージョンでは、サーバーハードウェアの健全性監視に 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健全性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について利用可能です。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）中に SNMPv3 を使用するように自動的に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着信 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 経由での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一次/二次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できるようにすることで、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フル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り、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ための一貫性のある、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 データパス 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。

ライフサイクル管理

自動検出 - DL/ML/Apollo - IP 範囲の Ping に基づいてサーバーリソースの自動検出機能を提供します。

Virtual Connect

- HPE Virtual Connect 16Gb 24 ポート ファイバーチャネルモジュール for c-Class BladeSystem - ポートミラーリング、コネクター情報、デジタル診断のサポートが追加されました。

- Digital Diagnostic Monitoring（DDMI）では、温度、電力、電圧、および電流に関する情報が提供されます。接続のヘルスステータスに関する情報に簡単にアクセスできます。
- ポートミラーリングは、サポート担当者に、サーバー HBA と 16Gb FC モジュール間のトラフィックフローを分析する方法を提供します。

- SNMPv3 - c7000 VC モジュールの SNMPv3 のサポートが追加されました。これにより、VC モジュールから統計データを収集するための信頼性と安全性の高い方法と、SNMPv3 トラップおよびインフォームを使用した VC モジュールの監視機能が提供されます。
- Migration Manager の拡張機能- 新しいオンライン Migration Manager の拡張機能が含まれます。新しい拡張機能により、エンクロージャの移行を開始する前により深い分析と確認が可能になり、信頼性の高い自動的な移行が実現します。
- HPE Virtual Connect 16Gb 24 ポートファイバーチャネルモジュールファームウェア
  - SFP コネクターおよびデジタル診断のサポートが追加されました。
  - ポートの監視のサポートが追加されました。
  - 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。
  - HPE OneView によって設定されたホスト名が正しく設定されていなかった問題が解決されました。

アプライアンスのインストール/アップグレード手順

インストール/アップグレード手順については、**HPE OneView 4.0 インストールガイド**にある「アプライアンスのアップデート」の章を参照してください。アップデートには、アプライアンスの再起動が必要で、再起動などを含むアップデートの完了には約 60 分を要します。

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。

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。

iLO4 が共有ネットワークポートで構成されているサーバーの電源投入イベントが検出されない

iLO4 が共有ネットワークポート（SNP）で構成されているサーバーでは、サーバーの電源投入時に「電源オン」イベントが送信されない場合があります。これにより、HPE OneView においてサーバーの電源状態が実際のハードウェアの電源状態と一致しなくなるため、サーバーの電源投入が HPE OneView によって検出されなくなります。また、プロファイル適用時の障害など、HPE OneView で複数の問題を引き起こす可能性があります。

推奨処置

電源を入れた後、毎回サーバーを最新の状態にアップデートするか、推奨されているとおり常時専用ネットワークポートをご使用ください。

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。

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。

Cisco Nexus 5K/6K スイッチ管理に関する制限事項

B22HP Fabric Extender を使用する Cisco Nexus 5K/6K スイッチを HPE OneView が管理している場合、サーバプロファイル設定による SAN からの起動はサポートされません。

バックアップからのリストア後に、サーバーハードウェアは、ロックされたアラートとして誤って報告されることがある

ロックされたアラートの時間が以前のバックアップ操作に対応することを確認することで、リストア後にこの状況を特定できます。リストアが完了した後に、ロックされたアラートのサーバーをアップデートします。アップデート操作が正常に行われなかったが、ロックされたアラートが残っている場合、これは期限切れのロックされたアラートである可能性があります。

推奨処置

1. エンクロージャまたはラックサーバーを削除し、再インポートします。アラートが表示されているサーバーハードウェアがブレードサーバーである場合、エンクロージャからブレードを削除し、そのエンクロージャ内のすべてのブレードも削除してから、エンクロージャを追加します（すべてのブレードを含む）。時間はかかりますが、一般的にこれがより安全な選択です。ラックサーバーの場合、エンクロージャ全体を削除する必要なく、サーバーを個別に削除できます。
2. より迅速な解決策は、バックアップ前に作成された期限切れのロックされたアラートを削除することです。これを行うには、次の管理者認証情報を使用して、次の REST API コールを発行します。

   DELETE https://<Appliance_IP>/rest/alerts/<ALERT_ID>?force=true

   <ALERT_ID>の数字を取得するには、UI のロックされたアラートを選択し、URI の末尾にある数字を記録します。たとえば、URI が **https://<Appliance_IP>/ #/server-hardware/show/activity/r/rest/server-hardware/<UUID>?f_sort=name%3Aasc& activityUri=%2Frest%2Falerts%2F26** である場合、アラート ID は「26」になります。

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。

アプライアンスの再起動後にエラーが発生すると、サーバーハードウェアにアラートが表示される

複数のエンクロージャを管理するときに HPE OneView アプライアンスを再起動すると、次のエラーメッセージが表示されることがあります。

- 内部エラーが発生しました。
- リソースの追加/アップデートに失敗しました。
- オブジェクトが無効である可能性があります。

推奨処置

HPE OneView アプライアンスは引き続き正常に動作し、アラートはクリアすることができます。

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。

リストア後の Remote Support

新しいアプライアンス IP アドレスにアプライアンスをリストアした後で、Remote Support のためにデバイスを再度有効にするには、セカンダリリフレッシュが必要な場合があります。

推奨処置

デバイスで Remote Support が有効になっている場合は、エンクロージャとサーバーハードウェアをリフレッシュして、アプライアンスとデバイス間の通信を再確立します。

HPE OneView 詳細ペインのスコープパネルには、スコープマスターペインに表示されるスコープのみが表示される

設定 > スコープページで検索フィルターを使用した後に、スコープフィルター選択と、選択したリソースに表示されるスコープの割り当てから、一部のスコープが欠落します。

推奨処置

ブラウザーをアップデートすると、この問題は解消されます。

Windows Server 2016 で Smart Update ツール（SUT）による Gen9 ファームウェアのアクティブ化に失敗する

Windows Server 2016 用 HPE Emulex 10/20 GbE ドライバーに SUM 7.6.0 ビルドが含まれていない場合に、Gen9 ファームウェアのアクティブ化に失敗します。

推奨処置

SUM 8.0.0 以降のバージョンを使用してカスタム SPP を作成するか、SPP の 2017.07.02 以降のバージョンを使用します。

自動ターゲット選択を使用して、新しいパスを追加したり既存のサーバープロファイルを変更したりすると、サーバープロファイルでさまざまなターゲットポートのセットが使用される

自動ターゲット選択を使用して、既存のサーバープロファイルに新しいパスまたは添付ファイルを追加するときに、サーバープロファイルの一部の既存のパスで、同じ SAN を使用するさまざまなターゲットポートのセットが使用される場合、エラーが発生します。これにより、HPE OneView は異なる SAN を使用して既存のパスからさまざまなターゲットを選択するため、結果としてパスが機能しなくなります。

推奨処置

プロファイルまたは添付ファイルを編集してから、手動ターゲットと適切なターゲット（場合によっては、選択可能なターゲットのみ）を選択します。

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。

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 を 3.00.08 から 4.0 にアップグレードした後のサーバープロファイルフラグエラー

HPE OneView を 3.00.08 から 4.0 にアップグレードした後に、無効なパスを含むサーバープロファイルのパスが、後で有効にされると、「イニシエーター'xx:xx:xx:xx:xx:xx:xx:xx'を使用するストレージパスの構成は SAN Manager で見つかりませんでした。」というエラーにフラグが設定されます。これにより、サーバープロファイルがクリティカル状態になります。

推奨処置

有効にするパスを削除して再作成すると、サーバープロファイルのパスを使用できるようになります。

論理スイッチを作成すると、Cisco Fabric Extender モジュールがエラー付きで追加済み状態に移行する

Cisco Nexus Top-of-Rack（ToR）スイッチが NX-OS 7.3（2）N1（1）を実行している場合、論理スイッチを作成すると、Cisco Nexus スイッチに接続されたすべての Cisco Fabric Extender B22 FEX モジュールが、**監視対象**または**構成済み**状態ではなく、**エラー付きで追加済み**状態に移行します。この場合、B22 FEX モジュールを HPE OneView で監視または管理することはできません。

HPE OneView は、NXOS 7.3（2）N1（1）を実行する Cisco Nexus スイッチからの XML 出力を解析できません。結果として、HPE OneView は ToR スイッチからの状態情報を読み取ることができず、ToR スイッチは**監視対象**または**構成済み**状態に移行できません。

推奨処置

このシナリオから回復するには、次のいずれかの操作を実行します。

- サポートされている以前のバージョンの NX-OS にダウングレードします。
- 論理スイッチリソースを削除し、Cisco ツールを使用して B22 FEX インターコネクトを監視または管理します。

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

SUT のインストール後に Sles12SP3 iSCSI OS が Service Pack for ProLiant 2017.10.0 でクラッシュする

サーバーがオンラインアップデートのために SUT を使用して iSCSI からブートすると、SLES12SP3 OS がクラッシュし、その後のブートの試行に失敗します。これは、Gen9 と Gen10 の両方のサーバーで発生します。SUT ファームウェアとドライバのインストールが完了した後、サーバーが数回再起動することがあります。

推奨処置

なし

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。

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。

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。

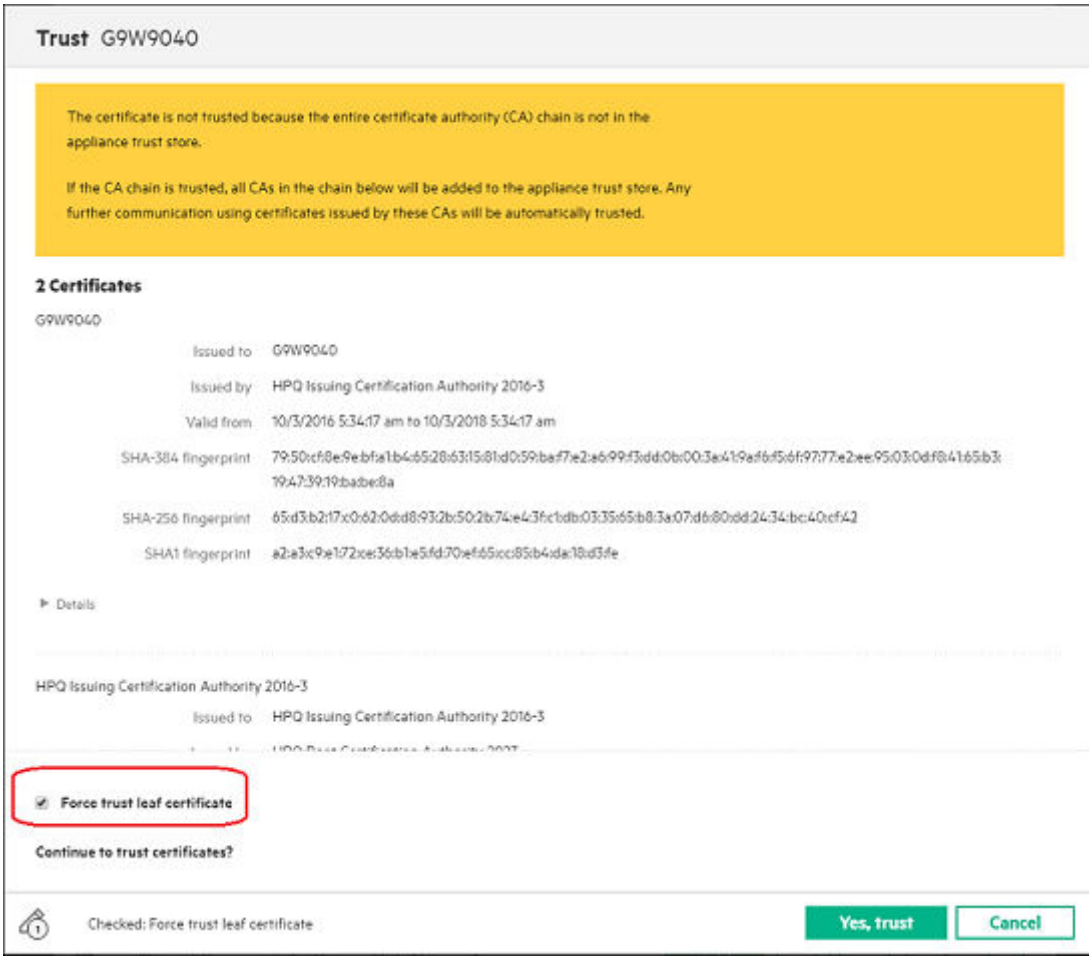
一回限りの追加セットアップを行って下位互換性を確保しないと、古いクライアントに対する REST リクエストが失敗する

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したときの 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。



このオプションは、ディレクトリのリーフ証明書を HPE OneView トラストストアに直接インポートします。すでにディレクトリ統合を設定している場合は、設定->セキュリティ->証明書の管理->証明書の追加を使用してディレクトリサーバーのリーフ証明書を手動で追加することもできます。

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）。

オンラインヘルプ内のリンクの問題

ラベルテキストの編集に関する情報への直接リンクは、オンラインヘルプでは利用できません。

推奨処置

オンラインヘルプで情報を検索するには、*ラベルの割り当てによるグループへのリソースの編成*を参照してください。

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。

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

処置は不要です。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。

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

HPE OneView 4.0 に関する注意事項

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 割り当て IP アドレス
- HW-iSCSI (iSCSI オフロード、ハードウェア支援によるイニシエーター)
- ブート可能な HW iSCSI は、物理ポート(ストレージ機能であるポート"b")の 2 番目の機能でのみ接続できます。

iLO4 デバイスの管理

iLO4 を搭載するデバイスを管理する場合、HPE OneView 3.0 以降は、iLO4 ファームウェアバージョン 2.55 以降で最適に動作します。お客様のデバイスに iLO4 ファームウェアのバージョン 2.3x をお持ちの場合は、お持ちの iLO4 ファームウェアをバージョン 2.55 以降にアップグレードされてから HPE OneView 3.0 以降を用いたデバイス管理を開始されることを強くお勧めします。

アダプターポートの設定

レガシー BIOS モードでサーバーブレードを使用した SAN（FC または iSCSI）から起動するサーバープロファイル接続を新規作成する場合は、アダプターのポート 1 が設定されている必要があります（ポート 1、ポート 2 両方が設定されていてもかまいません）。ポート 2 のみ設定を行うと、誤ったデバイス（通常はローカルディスク）からサーバーが起動される原因となる場合があります。この動作は、Emulex アダプターモデル 554M、650M、554FLB、556FLB、および 650FLB に影響を与えます。

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なく電源が入らないよう、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 を使用して）、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場合、プロファイルにとっても同一サーバーに見えるよう、RBSU を通じて UUID を手動で再プログラミングしなければならない可能性が高くなります。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これを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、それ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 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。

SPP カスタムダウンロードを使用してカスタム SPP を作成するために必要なフィルタ

使用する任意のフィルターを選択します。ただし、有効なカスタム SPP を作成する場合、次のフィルターは必須です。

- **バンドルフォーマット**：**ブート可能 ISO（SUM を含む）**を選択します。
- **オペレーティングシステム**: すべての **RHEL** オペレーティングシステムを選択します。
- **デバイス**：**OA**、**Virtual Connect（VC）**、および **iLO** を選択します。
- **サーバーモデル**：1 つ以上の Gen8/9 ブレードサーバーモデルおよび 1 つの Gen10 ブレードサーバーモデルを選択します。

オンラインヘルプでサーバープロファイルを使用する

次の情報が「どのようなときにサーバープロファイルを使用するか」に追加されました。

- Smart Update ツールベースのインストール方法のアクティブ化操作スケジュールを指定します。
- Gen8 以降の世代のサーバーモデルでサポートされています。

現在「管理ボリューム」オプションを使用した FC 接続に選択されるターゲットポートはロードバランシングされる

HPE OneView 3.0 で、**管理対象ボリューム**オプションを使用して FC 接続にブートターゲットを設定した場合、複数のポートが使用できる場合でも、HPE OneView は常にストレージシステムが公開した最初のターゲットポートを選択します。HPE OneView 3.10 以降では、HPE OneView は、ブート用のターゲットポートを選択するときに最も使用されていないターゲットポートを選択します。このロードバランスは、作成されるプロファイルが増えると、それにあわせて自動的に行われます。この機能を使用しない場合は、**ブートターゲットの指定** FC ブートオプションを使用する必要があります。

Gen10 Service Pack for ProLiant（SPP）のすべての G7 サーバーサポートの削除

2017 年 4 月以降の Service Pack for ProLiant（SPP）では、すべての **G7 サーバー**はベースライン（「フリーズ」）になり、Gen10 からサポート対象外となります。

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す。

- 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。

ファームウェアがすでに最新状態である場合のファームウェアアップデートのスキップ

基準バージョンに従ってプロファイルがすでに最新である場合、ファームウェアのアップデートはスキップされます。これにより、HPE OneView の高速実行が可能になり、プロファイル全体の適用時間を最大で 15〜20 分削減できます。これは、Gen10 サーバーにのみ適用されます。

未割り当てのサーバープロファイル／サーバープロファイルテンプレートの作成

同じ FC 接続で新しいサーバープロファイルテンプレートの作成を試みる前に、FC 接続がある各サーバープロファイルに関連付けられている、論理インターコネクトグループをアップデートします。サーバープロファイルテンプレートの割り当て解除を試みる前に、FC 接続があるサーバープロファイルに関連付けられている、論理インターコネクトグループをアップデートします。

HPE OneView 4.0 のドキュメントに関する正誤表

ストレージボリュームの作成と編集に関するオンラインヘルプは、StoreVirtual ストレージシステムに適用可能なプロビジョニングタイプとして「Thin Deduplication」にリストされていますが、このタイプは StoreServ でのみサポートされています。

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アップデート方法を確認してください。
- 製品のアップデートをダウンロードするには、以下のいずれかに移動します。
  - Hewlett Packard Enterprise サポートセンターのメールニュース配信登録ページ：

    www.hpe.com/support/e-updates

  - Software Depot の Web サイト：

    www.hpe.com/support/softwaredepot

- 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** ページに移動します。

  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資格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**
Contact Hewlett Packard Enterprise Worldwide	**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	**www.hpe.com/support/e-updates**
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 Virtual Connect のユーザーガイド HPE Virtual Connect のコマンドラインリファレンス	**www.hpe.com/info/virtualconnect**
HPE 3PAR StoreServ ストレージ	**www.hpe.com/info/storage**
HPE Integrated Lights-Out	**www.hpe.com/info/ilo**
HPE BladeSystem エンクロージャー	**www.hpe.com/servers/bladesystem**
HPE ProLiant サーバーハードウェアの Web サイト	• 一般的な情報：**www.hpe.com/info/servers** • BL シリーズサーバーブレード：**www.hpe.com/info/blades** • DL シリーズラックマウント型サーバー：**www.hpe.com/ servers/dl**
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トサービス：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。