Hewlett Packard Enterprise

HPE OneView 4.1 リリースノート

摘要

本書では、HPE OneView 4.1 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: P01318-192
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/アップデート手順

はじめに

このドキュメントでは、HPE OneView 4.1 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 4.1 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 4.1 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 4.1 仮想アプライアンスにおける変更

HPE OneView 4.1 バージョンは、次の目的で設計されています。

- 監視対象のエンクロージャーの 1 つに、古いバージョンの Virtual Connect ファームウェアで実行される Virtual Connect FC モジュールがあり、誤って管理エンクロージャーではない監視エンクロージャーに制限がかかっているため、HPE OneView アップデートが失敗する問題を解決する。
- HPE OneView 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。
- アプライアンスが HPE OneView 3.1 でのエンクロージャー移行の互換性テストのエラーを制限する問題を解決する。
- カスタムダッシュボードパネルでスコープが動作せず、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。
- FC 接続で HPE OneView 3.00.08 へのアップデート後にサーバープロファイルテンプレートを作成できない問題を解決する。
- HPE OneView アプライアンスのアップデートでストレージパスがダウンする問題を解決する。
- DL380 Gen9 サーバーの HPE OneView ファームウェアタブの下にすべてのハードディスクドライブが表示されない問題を解決する。
- 証明書認証トークンを作成できないため、HPE OneView のアップデートが失敗する問題を解決する。
- 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。
- Web UI の再起動後に HPE OneView が起動しない問題を解決する。

- 起動時に DNS と NTP の確認が同時に発生し、タイムアウトを引き起こす問題を解決する。
- 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。
- 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。
- DL ラックサーバーのシステムボードまたは Serial Peripheral Interface（SPI）ボードの交換後に予期しない問題が発生したため、ファームウェアのベースライン設定をクリアできない問題を解決する。
- HPE OneView バージョン 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 4.0 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。
- アップデート後に以下のアラートを受信する問題を解決する。**エイリアス名を持つ自己署名証明書のインフラストラクチャ管理認証機関–内部ルートの基本的な制約が有効ではありません。**

HPE OneView 4.1 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。

  注記: FIPS 140-2 および CNSA は、c7000 以外のハードウェアを管理する VM アプライアンスにのみ適用されます。

- **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

- **Gen10 高セキュリティ/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。

- **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。

  該当するベンダーのパッチをハイパーバイザー環境に適用することが重要です。以下に例を示します。VMware ESXi、Microsoft Hyper-V、および Red Hat の KVM。ハイパーバイザーに Spectre および Meltdown パッチを適用しなかった場合、HPE OneView 仮想マシンはハイパーバイザーホストの他のゲストからの攻撃に対して脆弱になります。

  Spectre および Meltdown 用ハイパーバイザーベンダーのパッチは、ホストとゲストの性能を低下させます。具体的な性能テストの詳細については、ハイパーバイザーベンダーのドキュメントを参照してください。HPE テストで、HPE OneView 仮想アプライアンスへのパフォーマンスは、実行される操作に応じて 2～20% の影響を与えます。追加リソースを HPE OneView 仮想アプライアンスに割り当てるか、ハイパーバイザーホストの競合する VM の数を減らす必要があります。

  VMware 環境では、HPE OneView 仮想アプライアンスはハードウェアバージョン 7 を使用します。VMware セキュリティアドバイザリ **VMSA-2018-0004.3** では、分岐ターゲットインジェクションの脆弱性である CVE-2017-5715 に対して、ESXi がゲストの移行を適用する前にゲスト VM のハードウェアバージョンを 9 以上にする必要があることに注意してください。HPE OneView は Spectre および Meltdown の脆弱性に対して脆弱ではありませんが、HPE OneView の今後のリリースでは、後者の ESXi ハードウェアバージョンをサポートする予定です。

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て、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。

ラックマネージャー

ラックマネージャープラットフォームは、マルチノードシステムです。ノードはラック内またはラック間に搭載され、管理コントローラーによって中央管理されます。

ラックマネージャープラットフォームは、以下によって構成されています。

- **1 つ以上のシャーシ** - シャーシは、システムやパーティションなどの論理コンポーネントを構築するために使用される個別ノードです。各シャーシは、コンピュート、ストレージ、またはネットワークノードのようなシステムコンポーネントの物理コンテナーです。

  HPE Superdome Flex サーバーで、シャーシは、CPU、メモリ、I/O、電源装置、およびファンを備えたコンピュートノードを表す 5U ノードです。

- **1 つ以上のシステムまたはパーティション** - システムはサーバーとして機能し、サービスをホストするオペレーティングシステムの単一インスタンスを実行する論理エンティティです。HPE OneView で、パーティションはサーバーハードウェアリソースとしてモデル化されています。

HPE Superdome Flex サーバーでは、システムをパーティションとも呼びます。パーティションは、超高速ファブリックで相互接続された 1 つ以上のコンピューターシャーシで構成されます。各パーティションはベースシャーシから始まり、拡張シャーシを使用して拡張して大量システムを形成することができます。

- **1 つ以上のマネージャー** - ラックマネージャープラットフォームを管理し、管理コントローラーの機能をホストする、マネージャーコンポーネントです。HPE OneView は、この管理コントローラーを介してラックマネージャーと通信し、ラックマネージャープラットフォームのシステム管理、制御、およびプラットフォーム管理を可能にします。一部のプラットフォームには、冗長性をサポートする複数のマネージャーコンポーネントがあります。

  HPE Superdome Flex サーバーで、マネージャーコンポーネントはラック管理コントローラー（RMC）と呼ばれます。RMC は DMTF Redfish API をホストします。

- **1 つ以上のラック** - ラックには、すべてのラックマネージャープラットフォームのコンポーネントが物理的に含まれています。

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、DL/XL/ML 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も、割り当ての解除もできます。

  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 OneView BladeSystem 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アップデートするとき、**統合**インターコネクトアクティベーション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。このアップデートにより、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インポート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、ワークロードを共用します。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。

  - サーバープロファイルを作成し、vSphere を展開し、外部ツールを使用してクラスターに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 c-Class 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、Boot from SAN 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。

Virtual Connect

- ダウンリンクでのポートのミラーリング
- Cisco ACI 統合

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 OneView 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

インストールとアップデートの手順については、**Hewlett Packard Enterprise 情報ライブラリ**の HPE OneView インストールガイドで「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。

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。

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。

MD5 デジタル署名を使用した管理対象デバイス証明書の非推奨通知

iLO 2 管理プロセッサーを搭載したサーバーなどの古いデバイスでは、MD5 ハッシュアルゴリズムに基づくデジタル署名付きのトランスポート層セキュリティ（TLS）証明書を使用できます。このような証明書は深刻なセキュリティリスクをもたらします。MD5 アルゴリズムは、モデム証明書のデジタル署名用の SHA-256 などのセキュアハッシュアルゴリズム（SHA）スイートに置き換えられています。HPE OneView の将来のバージョンでは、これらのレガシー証明書を使用するデバイスはサポートされません。

iLO 2 では、すべての HPE OneView iLO 2 ファームウェアバージョンが SHA ベースの証明書をサポートしています。ただし、iLO ファームウェアのアップグレードでは、デバイスの既存の証明書は変更されません。iLO の工場出荷時のリセット操作と iLO のホスト名を変更する場合のみ、iLO の自己署名証明書を再生成できます。同様に、認証機関が発行した証明書にも MD5 デジタル署名が含まれている可能性があり、アップデートされた証明書を取得するには新しい iLO 証明書の署名要求が必要です。詳しくは、iLO ユーザーガイドを参照してください。

HPE OneView /rest/証明書の REST API を使用すると、MD5 デジタル署名で証明書を使用しているデバイスを決定できます。HPE OneView PowerShell インターフェイス、POSH-HPOneView は **https://hewlettpackard.github.io/POSH-HPOneView** から入手して、使用できます。以下に例を示します。

- `Connect-HPOVMgmt -Hostname <your appliance> -Username <OneView username> [-AuthLoginDomain <AD or LDAP domain>]`
- `$certs = Send-HPOVRequest "/rest/certificates"`
- `$md5certs = @()`

- `$certs.members | foreach-object {$md5certs += New-Object PSObject -property @{commonName=$_.certDetails.commonName; aliasName=$_.aliasName; signature= $_.certDetails.signatureAlgorithm }}`
- `$md5certs | ? {$_.signature -match "MD5" } | format-table`

注記: この方法では、HPE OneView トラストストアに存在する証明書のみを識別します。証明書には、認証機関のルート証明書と中間証明書、およびデバイスの自己署名証明書が含まれます。CA ルートおよび中間証明書の場合、デバイスのリーフ証明書は HPE OneView トラストストアに存在しません。

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。

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。

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、ブラウザーを閉じて HPE OneView を再度開きます。

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、削除操作を再試行します。

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 4.1 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。

HPE Virtual Connect 16Gb 24 ポートのファイバーチャネルモジュールで、HPE OneView 4.10 でカスタム SPP を使用した論理エンクロージャーファームウェアアップデートに失敗する

問題

c7000 環境には複数の論理インターコネクトがあり、論理インターコネクトには HPE Virtual Connect 16Gb 24 ポートファイバーチャネルモジュールが含まれている場合があります。このシナリオでは、HPE Virtual Connect 16Gb 24 ポートファイバーチャネルモジュールにバンドルされた SPP を使用して、論理インターコネクトで論理エンクロージャーのファームウェアアップデートをすると失敗する可能性があります。

推奨処置

1. 警告アラートを受信した論理インターコネクトで、論理インターコネクトファームウェアのアップグレードを再試行します。
2. それでも問題が解決しない場合は、SPP を削除してからもう一度追加し、論理インターコネクトファームウェアのアップグレードを再試行してください。

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

iLO 4 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ません。この問題により、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更新するか、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。

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。

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

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。

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、セカンダリ更新が必要です。

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更新して、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 バージョン 2017.07.02 以降を使用します。

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、STRM コードは異なる 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 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。

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。

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、SLES 12 SP3 が SPP 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、SLES 12 SP3 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

対応する必要はありません。

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**/updatelogs/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。

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。

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 API /rest/login-sessions/smartcards を使用してリモートでアプライアンスにログインできます。通常行われるサーバー証明書の認証に加えて、この API のクライアント証明書認証も要求する必要があります。従って、通常の REST クライアント/ライブラリはこの REST API を使用できません。クライアント証明書の認証をサポートするクライアント/ライブラリを使用します。クライアント/ライブラリを使用するには、クライアントはクライアント証明書に関連する秘密キーもまた必要とします。この秘密キーは、クライアントが秘密キーの所有を証明するために使用します。クライアントは、どんな場合も有線でキーを渡すことはできません。クライアント秘密キーがサーバーに渡されない場合の使用法と確認の詳細については、クライアント/ライブラリのドキュメントを参照してください。

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-7.54.1-1 バージョン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 を使用してクライアント認証行う場合、詳細については **curl メインページ**を参照してください。

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、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。

HPE OneView 4.1 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、Hewlett Packard Enterprise 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、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。自動デバイス検出の操作も同じく適用されます。

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。

3. 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リ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。

1. 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。
2. リモートセッションを通じて証明書をインポートする。
3. 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。

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。

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。

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。

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

プロファイルがベースラインバージョンごとにすでに最新の場合、ファームウェアアップデートはスキップされ、HPE OneView の実行速度が向上するため、プロファイルの適用タイミング全体で最大 15～20 分を節約できます。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 のドキュメントおよびトラブルシューティングの資料

Hewlett Packard Enterprise 情報ライブラリは、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 OneView のテクノロジーについて
- HPE OneView アプライアンスのインストールとケーブル接続
- HPE OneView コンポーネントのアップデート
- HPE OneView の使用と管理
- HPE OneView のトラブルシューティング

HPE OneView ユーザーガイド

HPE OneView ユーザーガイドは、**Hewlett Packard Enterprise 情報ライブラリ**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 サポートマトリックス

HPE OneView サポートマトリックスは、**Hewlett Packard Enterprise 情報ライブラリ**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 OneView のトラブルシューティングガイド

HPE OneView トラブルシューティングガイドは、**Hewlett Packard Enterprise 情報ライブラリ**から入手できます。HPE OneView 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 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 OneView 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。

ヘルプファイルは、**Hewlett Packard Enterprise 情報ライブラリ**からも入手可能です。

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。