Hewlett Packard
Enterprise

HPE iLO6 1.30ユーザーガイド

部品番号: 30-7A345B12-003-ja-JP
発行: 2023年3月
版数: 4

HPE iLO6 1.30ユーザーガイド

摘要

このガイドは、 HPE iLO6ファームウェアを使用したサポートされる HPE ProLiantサーバーの構成、アップデート、および操作に関する情報を提供します。本書は、 iLO6が含まれている Hewlett Packard Enterpriseサーバーの構成と使用に関係するシステム管理者、 Hewlett Packard Enterpriseの担当者、および Hewlett Packard Enterprise認定チャネルパートナーを対象としています。

部品番号: 30-7A345B12-003-ja-JP
発行: 2023年3月
版数: 4

ご注意

本書の内容は、将来予告なしに変更されることがあります。Hewlett Packard Enterprise製品およびサービスに対する保証については、当該製品およびサービスの保証規定書に記載されています。本書のいかなる内容も、新たな保証を追加するものではありません。本書の内容につきましては万全を期しておりますが、本書中の技術的あるいは校正上の誤り、脱落に対して、責任を負いかねますのでご了承ください。

本書で取り扱っているコンピューターソフトウェアは秘密情報であり、 その保有、使用、または複製には、Hewlett Packard Enterprise から使用許諾を得る必要があります。 FAR 12.211 および 12.212 に従って、商業用コンピューターソフトウェア、コンピューターソフトウェアドキュメンテーション、および商業用製品の技術データ (Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items) は、ベンダー標準の商業用使用許諾のもとで、米国政府に使用許諾が付与されます。

他社の Web サイトへのリンクは、Hewlett Packard Enterprise の Web サイトの外に移動します。 Hewlett Packard Enterprise は、Hewlett Packard Enterprise の Web サイト以外の情報を管理する権限を持たず、また責任を負いません。

商標

Microsoft®およびWindows®は、米国および/またはその他の国におけるMicrosoft Corporationの登録商標または商標です。

Java®およびOracle®は、Oracleおよび/またはその関連会社の登録商標です。

Google™は、Google Inc.の商標です。

Google Chrome™は、Google Inc.の商標です。

Linux®は、Linus Torvaldsの米国およびその他の国における登録商標です。

Red Hat®は、米国およびその他の国におけるRed Hat, Inc.の商標または登録商標です。

VMware®は、VMware, Inc.の米国および各国での登録商標または商標です。

Intel®、インテル、およびインテル®Xeon®はインテルコーポレーションまたはその子会社のアメリカ合衆国およびその他の国における商標または登録商標です。

SDはSD-3Cの米国およびその他の国における商標または登録商標です。

すべてのサードパーティのマークは、それぞれの所有者に帰属します。

改訂履歴

部品番号	発行日	版数	変更の概要
30-7A345B12-003-ja-JP	3月	4	iLO6 1.30は、Gen11 IntelおよびGen11 AMDプラットフォーム用iLO6の統合リリースです。
30-7A345B12-002-ja-JP	1月	3	iLO6 1.20は、Gen11 Intelプラットフォーム用iLO6の最初のリリースです。 iLO 6 1.20はGen11 AMDプラットフォームもサポートします。
30-7A345B12-001a-ja-JP	1月	2	前付のアップデート
30-7A345B12-001	12月	1	iLO6 1.10は、Gen11 AMDプラットフォーム用iLO6の最初のリリースです。

目次

        - iLOの再起動（リセット）方法
        - Webインターフェイスを使用したiLOプロセッサーの再起動（リセット）
        - iLOのiLO6構成ユーティリティを使用した再起動（リセット）
        - サーバーのUIDボタンによる正常なiLOの再起動の実行
        - サーバーのUIDボタンによるハードウェアiLOの再起動の実行
    - アプライアンスのイメージの再構築
    - システム診断
        - NMIの生成
        - システムセーフモードでの起動
        - インテリジェント診断モードで起動
        - 工場デフォルト設定のリストア
        - システムデフォルト設定のリストア
        - POST中のUEFIシリアルデバッグメッセージのActive Health Systemログへの保存
- 全般的なシステム情報の表示
    - ヘルスサマリー情報の表示
        - 冗長ステータス
        - サブシステムおよびデバイスのステータス
        - サブシステムおよびデバイスステータスの値
    - プロセッサー情報の表示
        - プロセッサーの詳細
    - メモリ情報の表示
        - アドバンストメモリプロテクションの詳細
        - メモリの概要
        - 物理メモリ詳細
        - メモリ詳細ペイン（物理メモリ）
    - ネットワーク情報の表示
        - 物理ネットワークアダプター
        - 論理ネットワークアダプター
    - デバイスインベントリの表示
        - デバイスインベントリの詳細
        - スロットの詳細ペイン
        - デバイスステータスの値
        - MCTP検出の構成
        - MCTP工場出荷時リセットの開始
    - ストレージ情報の表示
        - サポート対象のストレージコンポーネント
        - サポートされるストレージ製品
        - ストレージ詳細
            - コントローラー
            - ボリューム
            - ドライブ
            - ドライブエンクロージャー（Smartアレイのみ）
        - ステータスの値と定義
        - ドライブの電源の管理
            - ドライブの電源ボタンオプション
- ファームウェアおよびソフトウェアの表示および管理

    - サーバーの電源オン
    - 電圧低下からの復旧
    - 正常なシャットダウン
    - 電力効率
    - 電源投入時の保護
    - 電力割り当て（ブレードサーバーおよびコンピュートモジュール）
    - サーバー電源の管理
        - 仮想電源ボタンのオプション
    - システム電源リストア設定の構成
        - 自動電源オン
        - 電源オン遅延
    - サーバー電力使用量の表示
    - 電力設定
        - パワーレギュレーターの設定
            - パワーレギュレーターモード
        - 消費電力上限の構成
            - 消費電力上限の注意事項
        - バッテリバックアップユニット設定の構成
            - バッテリバックアップユニットのオプション
        - 電力しきい値設定超過のSNMPアラートの構成
            - 電力しきい値超過によるSNMPアラートのオプション
        - マウスとキーボードの持続接続の設定
            - その他の設定オプション
    - 電力情報の表示
    - 冷却機能の構成と表示
    - 温度情報
        - 温度グラフの表示
            - 温度グラフの詳細
        - 温度センサーデータの表示
            - 温度センサーの詳細
        - 温度の監視
    - RESTfulインターフェイスツールを使用したユーザー定義のしきい値の構成
- パフォーマンス管理機能の使用
    - パフォーマンス監視
        - パフォーマンスデータの表示
            - パフォーマンスデータの詳細
            - パフォーマンス監視のグラフ表示オプション
        - パフォーマンスアラートの構成
            - パフォーマンスアラートの設定オプション
    - ワークロードアドバイザー
        - サーバーワークロード詳細の表示
            - サーバーワークロードの詳細
        - パフォーマンスチューニングオプションの構成
            - パフォーマンスチューニングの設定
- iLOネットワーク設定の構成
    - iLOネットワーク設定

        - 自動証明書登録の有効化
        - 証明書の登録設定のアップデート
        - 自動的に管理されるSSL証明書の更新
        - 登録サービスの無効化
        - SSL証明書の削除
    - iLOのディレクトリの認証と認可設定
        - 認証およびディレクトリサーバー設定を構成するための前提条件
        - iLOでKerberos認証の設定を構成します
            - Kerberosの設定
        - iLOにおけるスキーマフリーディレクトリ設定の構成
            - スキーマフリーディレクトリの設定
        - iLOにおけるHPE拡張スキーマディレクトリ設定の構成
            - HPE拡張スキーマディレクトリの設定
        - ディレクトリユーザーコンテキスト
        - ディレクトリサーバーCA証明書
        - ディレクトリサーバーCA証明書の削除
        - Kerberos認証およびディレクトリ統合によるローカル ユーザー アカウント
        - ディレクトリテストの実行
            - ディレクトリテストの入力値
            - ディレクトリテストのステータス値と制御
            - ディレクトリテスト結果
            - iLOディレクトリテスト
    - iLOセキュリティ状態
    - iLO暗号化設定
        - 本番環境セキュリティ状態の有効化
        - 高セキュリティセキュリティ状態の有効化
        - FIPSおよびCNSAセキュリティ状態を有効にする
        - 高いセキュリティ状態を使用する場合のiLOへの接続
        - iLOによるFIPS承認済み環境の構成
        - FIPSセキュリティ状態の無効化
        - CNSAセキュリティ状態の無効化
        - iLOセキュリティ状態
        - SSH暗号、キー交換、およびMACのサポート
        - サポートされるSPDMアルゴリズム
        - SSL暗号およびMACのサポート
    - HPE SSO
        - HPE SSO用のiLOの設定
            - シングルサインオン信頼モードオプション
            - SSOユーザー権限
        - 信頼済みの証明書の追加
        - HPE SIM SSO証明書の取得
        - 直接DNS名のインポート
        - 信頼済みの証明書とレコードの表示
            - 信頼済みの証明書およびレコードの詳細
        - 信頼済みの証明書とレコードの削除
    - ログインセキュリティバナーの構成

- HPE Compute Ops Management
- ライフサイクル管理機能の使用
  - Always On Intelligent Provisioning
  - One-buttonセキュア消去
  - iLOのバックアップとリストア
- iLOと他のソフトウェア製品およびツールとの使用
  - iLOおよびリモート管理ツール
    - iLOからのリモート管理ツールの起動
    - リモートマネージャー構成の削除
    - iLOでのHPE OneViewの使用
      - サーバー署名（Synergyコンピュートモジュールのみ）
    - ホットフィックスを追加してHPE OneViewカスタムファームウェアバンドルを作成する
  - IPMIサーバー管理
    - Linux環境でのIPMIツールの高度な使用方法
  - HPE SIMでのiLOの使用
    - HPE SIMの機能
    - HPE SIMでのSSOの確立
    - iLOの識別および関連付け
      - HPE SIMでのiLOステータスの表示
      - HPE SIMでのiLOリンク
      - HPE SIMのシステムリストでのiLOの表示
    - HPE SIMでのSNMPアラートの受信
    - iLOとHPE SIMのHTTPポート一致要件
    - HPE SIMでのiLOライセンス情報の確認
- Kerberos認証とディレクトリサービスの設定
  - iLOでのKerberos認証
    - Kerberos認証の設定
    - Kerberos認証用のiLOホスト名とドメイン名の構成
      - Kerberos認証のiLOホスト名とドメイン名の要件
    - ドメインコントローラーでのKerberosサポートの準備
    - Windows環境でのiLO用キータブファイルの生成
      - Ktpass
      - Setspn
    - ご使用の環境がKerberos認証の時刻要件を満たしていることの確認
    - サポートされるブラウザーでのシングルサインオンの設定
      - Mozilla Firefoxでのシングルサインオンの有効化
      - Google Chromeでのシングルサインオン
      - Microsoft Edgeでのシングルサインオンの有効化
      - シングルサインオン（Zeroサインイン）設定の確認
      - 名前によるログインが動作していることの確認
  - ディレクトリ統合の利点
  - iLOで使用するディレクトリ構成の選択
  - スキーマフリーディレクトリ認証
    - ディレクトリ統合の設定（スキーマフリー構成）
    - スキーマフリーディレクトリ統合を使用するための前提条件
  - HPE拡張スキーマディレクトリ認証

iLO

iLO6は、HPEサーバーおよびコンピュートモジュールのシステムボードに組み込まれたリモートサーバー管理プロセッサーです。iLOでは、リモートの場所からサーバーを監視および制御できます。iLO管理は、サーバーをリモートで構成、アップデート、監視、および修復するための複数の方法を提供する強力なツールです。

サブトピック

iLO機能

iLOには、次の標準機能およびライセンスされた機能が含まれています。これらの機能のライセンス要件を確認するには、iLOのライセンスガイドを参照してください。

- **Active Health Systemログ** – ログをHPE InfoSight for Serversにアップロードして、ログデータを表示したり、有効な保証またはサポート契約に基づくサーバーのサポートケースを作成したりできます。詳しくは、次のWebサイトにあるHPE InfoSight for Serversのドキュメントを参照してください：https://www.hpe.com/support/infosight-servers-docs。
- **Agentless Management** – Agentless Managementとともに、管理ソフトウェア（SNMP）はホストOSではなくiLOファームウェア内で動作します。この構成により、ホストOS上のメモリおよびプロセッサーリソースがサーバーアプリケーション用に解放されます。iLOはすべての重要な内部サブシステムを監視し、ホストOSがインストールされていない場合でも、中央管理サーバーに直接SNMPアラートを送信できます。
- **展開とプロビジョニング** – 展開およびプロビジョニングの自動化などのタスクに仮想電源および仮想メディアを使用します。
- **組み込みリモートサポート** – サポート対象サーバーをHPEリモートサポートに登録できます。
- **ファームウェア管理** – iLOレポジトリ、インストールセット、インストールキューなどを含むiLOファームウェア機能を使用して、ファームウェアのアップデートを管理します。
- **ファームウェアの検証とリカバリ** – スケジュール済みまたはオンデマンドでファームウェアの検証スキャンを実行して、問題が検出されたときに実装するリカバリ操作を設定します。
- バックアップ**iLOバックアップとリストア** – iLOの構成をバックアップして、同じハードウェア構成のシステムに復元できます。
- **iLO連携管理** – iLO連携機能を使用して、一度に複数のサーバーを検出および管理します。
- **iLOインターフェイスの管理** – セキュリティを強化するために、選択したiLOインターフェイスおよび機能を有効または無効にします。
- **iLO RESTful APIおよびRESTfulインターフェイスツール（iLOREST）** – iLO6には、Redfish API準拠であるiLO RESTful

APIが含まれています。

- **iLOサービスポート** – サポート対象のUSBイーサネットアダプターを使用してクライアントをiLOサービスポートに接続し、サーバーに直接アクセスします。Hewlett Packard Enterpriseは、HPE USBイーサーネットアダプター（部品番号Q7Y55A）を使用することをお勧めします。また、USBキーを接続して、Active Health Systemログをダウンロードすることもできます。
- **インテグレーテッドマネジメントログ** – サーバーイベントを表示し、SNMPアラート、リモートsyslog、およびメールアラート経由での通知を設定します。
- **統合リモートコンソール** – サーバーとのネットワーク接続があれば、安全で高パフォーマンスのコンソールにより、世界中どこからでもサーバーにアクセスして管理できます。
- **IPMI** – iLOファームウェアは、IPMIバージョン2.0仕様に基づくサーバー管理を提供します。
- **詳細情報へのリンク** – サポート対象イベントのトラブルシューティング情報がインテグレーテッドマネジメントログページに表示されます。
- **One-buttonセキュア消去** – サーバーを安全に使用停止にしたり、別の用途のために準備したりします。
- **消費電力と電力設定** – サーバーの消費電力を監視し、サーバーの電力を設定し、サポートされているサーバーの消費電力上限を設定します。
- **電源管理** – リモートから安全に管理対象サーバーの電源状態を制御できます。
- **安全なリカバリ** – 電源の作動時にiLOファームウェアを検証します。ファームウェアが無効な場合、iLOファームウェアは自動的にフラッシュされます（iLO Standardライセンス）。

  サーバーの起動時に、システムROMを検証します。有効なシステムROMが検出されないと、サーバーは起動できません。リカバリオプションには、アクティブおよび冗長ROMのスワッピングや、ファームウェアの検証スキャンとリカバリアクションの起動などがあります。スケジュール済みのファームウェア検証スキャンと自動リカバリを行うには、iLO Advancedのライセンスが必要です。
- **セキュリティログ** – iLOファームウェアによって記録されたセキュリティイベントのレコードを表示します。
- **セキュリティダッシュボード** – 重要なセキュリティ機能のステータスを表示したり、潜在的なリスクがあるかどうか設定を評価したりします。リスクが検知されたら、詳細情報とシステムセキュリティを向上させる方法についてのアドバイスを見ることができます。
- **セキュリティ状態** – ご使用の環境に合ったセキュリティ状態を設定します。iLOは、本番稼働（デフォルト）のセキュリティ状態や、高セキュリティ、FIPS、CNSAなどのより高いセキュリティ状態をサポートします。
- **サーバーヘルスの監視** – iLOはサーバー内部の温度を監視し、修正信号をファンに送信して適切なサーバー冷却を維持します。さらに、インストールされているファームウェアとソフトウェアのバージョン、および他の監視対象のサブシステムとデバイスのステータスも監視します。
- **システム診断** – セーフモードまたはインテリジェント診断モードで起動してシステムを診断します。工場デフォルト設定またはシステムデフォルト設定をリストアできます。
- **Two-Factor認証** – Two-Factor認証は、KerberosおよびCAC Smartcard認証でサポートされます。
- **ユーザーアクセス** – ローカルまたはディレクトリベースのユーザーアカウントを使用してiLOにログインします。ローカルまたはディレクトリベースのアカウントでCAC Smartcard認証を使用できます。
- 仮想NIC – ホストオペレーティングシステムからiLOに安全にアクセスします。
- **仮想メディア** – リモートから高性能仮想メディアデバイスをサーバーにマウントできます。
- ワークロードアドバイザー – 選択されたサーバーワークロード特性を表示します。監視対象データに基づき、推奨のパフォーマンスチューニング設定を表示したり、構成したりできます。
- **Workload Matching** – 構成済みのワークロードプロファイルを使用して、サーバーのリソースを微調整できるようにします。

iLO Webインターフェイス

iLO Webインターフェイスを使用して、サポートされるブラウザーを介してiLOにアクセスし、管理対象サーバーを監視および構成できます。

詳しくは

iLO Webインターフェイスの概要

ROMベースの構成ユーティリティ

UEFIシステムユーティリティのiLO6構成ユーティリティを使用すると、ネットワークパラメーター、グローバル設定、およびユーザーアカウントを構成できます。

iLO6構成ユーティリティは、初期のiLOセットアップのために設計されていて、継続的なiLO管理のためのものではありません。このユーティリティはサーバーが起動するときに起動でき、リモートコンソールを使用してリモートから実行できます。

ユーザーがiLO6構成ユーティリティにアクセスするときにログインを要求するようにiLOを構成できます。または、すべてのユーザー用のユーティリティを無効にすることもできます。これらの設定は、アクセス設定ページで構成できます。iLO6構成ユーティリティを無効にすると、iLOセキュリティを無効にするようにシステムメンテナンススイッチが設定されないかぎり、ホストからの再構成を防止します。

iLO6構成ユーティリティにアクセスするには、POSTの実行時にF9キーを押してUEFIシステムユーティリティを起動します。システム構成、iLO 6構成ユーティリティの順にクリックします。

詳しくは

iLOアクセス設定の構成

iLO RESTful API

iLOには、Redfish API準拠であるiLO RESTful APIが含まれています。iLO RESTful APIは、基本的なHTTPS操作（GET、PUT、POST、DELETE、およびPATCH）をiLO Webサーバーに送信することで、サーバー管理ツールからサーバーの構成、インベントリ、および監視を実行できる管理インターフェイスです。

iLO RESTful APIについて詳しくは、Hewlett Packard EnterpriseのWebサイト（https://www.hpe.com/support/restfulinterface/docs）を参照してください。

iLO RESTful APIを使用したタスクの自動化について詳しくは、https://www.hpe.com/info/redfishにあるライブラリとサンプルコードを参照してください。

詳しくは、Redfish & How it works with HPE Server Managementのビデオを見てください。

RESTfulインターフェイスツール

RESTfulインターフェイスツール（iLOREST）は、HPEサーバー管理タスクを自動化するためのスクリプティングツールです。これは、iLO RESTful APIを利用する、簡素化されたコマンドのセットを提供します。ツールは、ご使用のコンピューターにインストールしてリモートで使用することも、WindowsまたはLinuxオペレーティングシステムを搭載するサーバーにローカルでインストールすることもできます。RESTfulインターフェイスツールでは、自動化時間を短縮するための対話型モード、スクリプト可能なモード、およびCONREPのようなファイルベースモードが提供されます。

詳しくは、次のWebサイトを参照してください。https://www.hpe.com/info/resttool

iLOスクリプティングとコマンドライン

iLOスクリプティングとコマンドライン

iLOスクリプティングツールを使用して、複数のサーバーを設定したり、展開プロセスに標準設定を組み込んだり、サーバーやサブシステムを制御したりできます。

iLOスクリプティングおよびCLIガイドには、コマンドラインインターフェイスまたはスクリプティングインターフェイスを通じてiLOを使用するために利用できる構文およびツールに関する説明が記載されています。

iLO Amplifier Pack

iLO Amplifier Packは、高度なサーバーインベントリおよびファームウェアおよびドライバーのアップデートソリューションです。iLO Advanced機能を使用して高速検出、詳細なインベントリレポート、およびファームウェアとドライバーのアップデートを有効にします。iLO Amplifier Packは、ファームウェアとドライバーの大規模アップデートを目的として、サポートされている数千台のサーバーの迅速なサーバー検出およびインベントリを実行します。

iLO Amplifier Packについて詳しくは、次のWebサイトを参照してください。https://www.hpe.com/servers/iloamplifierpack

HPE InfoSight for Servers

HPE InfoSightポータルは、HPEによってホストされている安全なWebインターフェイスで、サポートされているデバイスをグラフィカルインターフェイスによって監視できます。

HPE InfoSight for Servers：

- HPE InfoSightの機械学習と予測分析を、Active Health System（AHS）およびHPE iLOのヘルスとパフォーマンス監視と組み合わせて、パフォーマンスを最適化し、問題を予測して防止します
- AHSからのセンサーデータとテレメトリデータを自動的に収集および分析し、インストールベースの動作から洞察を導き出して、問題の解決とパフォーマンスの向上に関する推奨事項を提供します

HPE InfoSight for Serversを使用するための準備について詳しくは、https://www.hpe.com/info/infosight-servers-docsを参照してください。

iLOのセットアップ

サブトピック

iLOをセットアップするための準備

このタスクについて

iLO管理プロセッサーをセットアップする前に、ネットワークとセキュリティの処理方法を決める必要があります。以下の質問に回答していくと、iLOの設定方法が明らかになります。

手順

1. iLOはどの方法でネットワークに接続しますか。
2. 共有ネットワークポート構成でNICチーミングを使用しますか。
3. iLOはどの方法でIPアドレスを取得しますか。
4. どのようなアクセスセキュリティおよびユーザーアカウントと権限が必要ですか。
5. iLOの設定にどのようなツールを使用しますか。

サブトピック

iLOネットワーク接続オプション

共有ネットワークポート構成によるNICチーミング

iLO IPアドレスの取得

iLOアクセスセキュリティ

iLO構成ツール

その他のiLO構成ツール

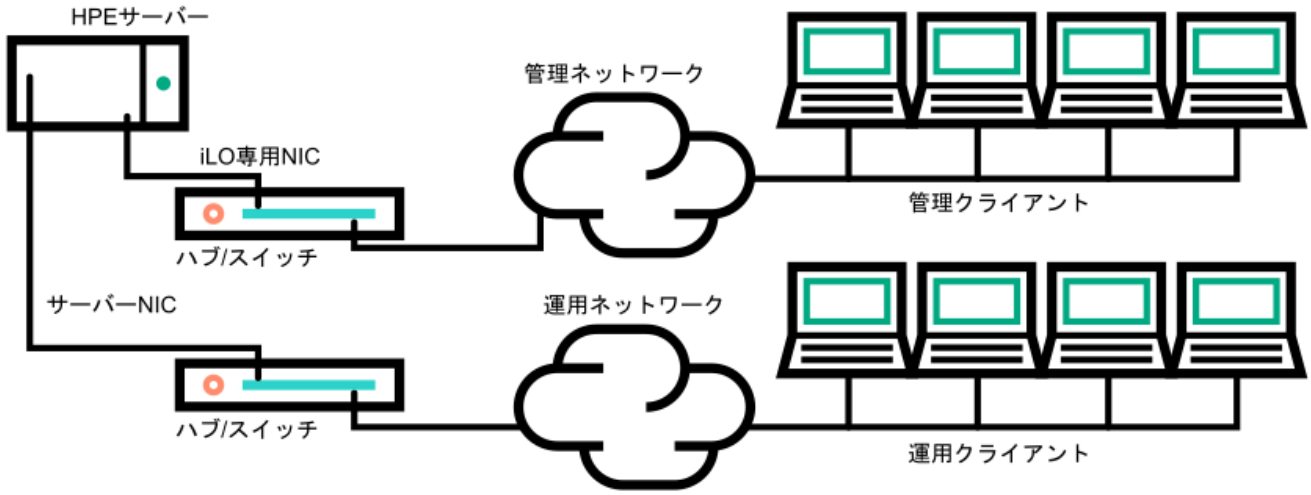
iLOネットワーク接続オプション

iLOは、専用の管理ネットワークまたは本番環境ネットワークの共有接続を使用してネットワークに接続できます。

専用管理ネットワーク

この設定では、独立したネットワークにiLOポートを配置します。ネットワークが独立しているため、性能が向上し、どのワークステーションをネットワークに接続するかを物理的に制御できるので、セキュリティが強化されます。また、本番環境ネットワーク内のハードウェアに障害が発生した場合には、サーバーへの冗長アクセスが提供されます。この構成では、本番環境ネットワークから直接iLOにアクセスすることはできません。専用管理ネットワークは、優先されるiLOネットワーク構成です。

図 1. 専用管理ネットワーク



本番環境ネットワーク

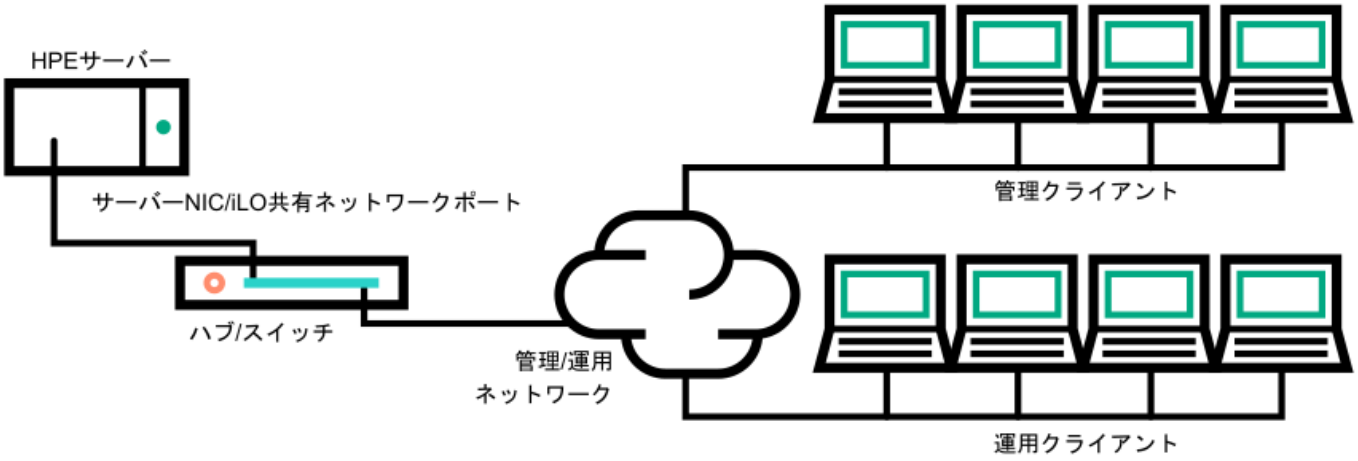
この設定では、NICとiLOポートの両方を本番環境ネットワークに接続します。iLOで、このタイプの接続は、共有ネットワークポート構成と呼ばれます。特定のHewlett Packard Enterprise内蔵NICとアドオンカードが、この機能を提供します。この接続により、ネットワークのどこからでもiLOにアクセスできます。共有ネットワークポート構成を使用すると、iLOをサポートするために必要なネットワークハードウェアやインフラストラクチャの量が減ります。

この設定の使用にはいくつかの欠点があります。

- 共有ネットワーク接続では、トラフィックによって、iLOのパフォーマンスが低下することがあります。
- サーバーの起動時、およびオペレーティングシステムNICドライバーのロードおよびアンロード時に、短時間（2～8秒）、ネットワークからiLOにアクセスできません。この短い時間の経過後に、iLOの通信がリストアされ、iLOがネットワークトラフィックに応答します。

  このようなシチュエーションが起きた場合は、リモートコンソールと、接続されているiLO仮想メディアデバイスが切断されることがあります。
- ネットワークコントローラーのファームウェアをアップデートまたはリセットすることも、iLOが短期間、ネットワーク経由で到達不能に陥る原因となる可能性があります。
- iLO共有ネットワークポート接続は、100 Mbpsを超える速度では動作できません。iLO仮想メディアを介したデータ転送などのネットワーク集約型タスクは、iLO専用ネットワークポートを使用する構成で実行される同じタスクよりも遅くなる場合があります。

図 2. 共有ネットワーク接続



iLOネットワーク有効化モジュール

一部のサーバーでは、専用管理ネットワーク（デフォルト）または共有ネットワーク接続によるリモート管理のサポートを追加するために、オプションのiLOネットワーク有効化モジュールが必要です。iLOネットワーク有効化モジュールがインストールされていない場合、iLOアクセスは、ホストベース（インバンド）のアクセス方式でのみサポートされます。サポートされているホストベースのアクセス方式の例には、iLO RESTful API、UEFIシステムユーティリティ、iLOサービスポート（利用可能な場合）、および仮想NICが含まれます。

サーバーでサポートされているネットワーク接続を確認するには、サーバーのユーザーガイドを参照してください。

共有ネットワークポート構成によるNICチーミング

NICチーミングは、サーバーNICのパフォーマンスと信頼性を向上させるために使用できる機能です。

サブトピック

NICチーミングの制限

Hewlett Packard Enterprise NICチーミングモード

NICチーミングの制限

iLOで共有ネットワークポートを使用するように構成する際に、チーミングモードを選択した場合：

- 次の状況でiLOネットワーク通信がブロックされます。
  - 選択されたNICチーミングモードによって、iLOが接続されているスイッチは、iLOが共有するように構成されているサーバーNIC/ポートからのトラフィックを無視するようになります。
  - 選択されたNICチーミングモードによって、iLO宛てのすべてのトラフィックが、iLOが共有するように構成されていないNIC/ポートに送信されます。
- iLOとサーバーは同じスイッチポートで送受信するため、選択されたNICチーミングモードでは、スイッチが同じスイッチポートでの2つの異なるMACアドレスを持つトラフィックを許容するようにする必要があります。LACP（802.3ad）の一部の実装では、同じリンク上の複数のMACアドレスを許容しません。

Hewlett Packard Enterprise NICチーミングモード

サーバーでHewlett Packard Enterprise NICチーミングを使用するように構成した場合、次のガイドラインに従ってください。

ネットワークフォールトトレランス（NFT）

サーバーは1つだけのNIC（プライマリアダプター）で送受信します。チームに含まれる他のNIC（セカンダリアダプター）はトラフィックを送信せず、受信したトラフィックを無視します。このモードにより、iLO共有ネットワークポートが正常に動作します。

iLOが優先プライマリアダプターとして使用するNIC/ポートを選択します。

送信ロードバランシング（TLB）

サーバーは、複数のアダプターで送信しますが、プライマリアダプターでのみ受信します。このモードにより、iLO共有ネットワークポートが正常に動作します。

iLOが優先プライマリアダプターとして使用するNIC/ポートを選択します。

スイッチアシストロードバランシング（SLB）

このモードタイプは、以下のことを指します。

- HPE ProCurveポートトランキング

- Cisco Fast EtherChannel/Gigabit EtherChannel（静的モードのみ、PAgPなし）
- IEEE 802.3adリンクアグリゲーション（静的モードのみ、LACPなし）
- ベイネットワークマルチリンクトランキング
- Extreme Network Load Sharing

このモードでは、プライマリアダプターとセカンダリアダプターの概念はありません。すべてのアダプターはデータを送受信する目的で等しいと見なされます。このモードは、iLO宛のトラフィックを受信できるサーバーNIC/ポートが1つだけであるため、iLO共有ネットワークポート構成で最も問題となる可能性があります。スイッチアシストロードバランシングの実装に対するスイッチベンダーの制限を判断するには、スイッチベンダーのドキュメントを参照してください。

サーバーで、別のNICチーミングの実装を使用する場合のNICチーミングモードの選択については、NICチーミングの制限およびベンダーのドキュメントを参照してください。

iLO IPアドレスの取得

iLOがネットワークに接続されてからアクセスを可能にするには、 iLOマネジメントプロセッサーがIPアドレスとサブネットマスクを取得する必要があります。動的アドレスまたは静的アドレスを使用することができます。

動的IPアドレス

動的IPアドレスは、デフォルトで設定されます。iLOは、DNSまたはDHCPサーバーからIPアドレスとサブネットマスクを取得します。この方法が最も簡単です。

DHCPを使用する場合：

- iLO管理ポートは、DHCPサーバーに接続されたネットワークに接続する必要があります。また、iLOをネットワークに接続してから電源を入れなければなりません。DHCPは、電源が投入されるとただちに要求を送信します。iLOが最初に起動したときにDHCPの要求に対する回答がない場合、DHCPは、90秒間隔で要求を再発行します。
- DHCPサーバーは、DNSおよびWINS名前解決を提供するように設定しなければなりません。

静的IPアドレス

ネットワークでDNSまたはDHCPサーバーを使用できない場合、静的IPアドレスが使用されます。静的IPアドレスは、iLO6構成ユーティリティを使用して構成できます。

静的IPアドレスの使用を予定する場合は、iLOセットアッププロセスを開始する前にIPアドレスが必要です。

iLOアクセスセキュリティ

次の方法でiLOへのアクセスを管理できます。

ローカルアカウント

iLOには、最大12のユーザーアカウントを格納できます。この構成は、研究所や中小企業のような小規模環境に最適です。

ローカルアカウントによるログインセキュリティはiLOアクセス設定およびユーザー権限によって管理します。

ディレクトリサービス

13ユーザー以上をサポートするには、ディレクトリサービスを使用してアクセスの認証や権限付与を行うようiLOを構成します。この構成により、ユーザーの数の制限がなくなります。また、この構成は、エンタープライズ内のiLOデバイスの数に合わせて、簡単に拡張できます。

ディレクトリサービスを使用する場合でも、代替アクセスとして少なくとも1つのローカル管理者アカウントを有効にしておきます。

ディレクトリによりiLOデバイスとユーザーを集中的に管理することができ、より強力なパスワードポリシーを適用できます。

CAC Smartcard認証

ローカルアカウントとディレクトリサービスと共にCommon Access Smartcardを設定して、iLOユーザーアクセスを管理できます。

詳しくは

iLOのディレクトリの認証と認可設定
iLOユーザーアカウント
CAC Smartcard認証
iLOアクセス設定の構成

iLO構成ツール

iLOは、設定と操作用にさまざまなインターフェイスをサポートしています。このガイドで説明する主なインターフェイスは、次のとおりです。

iLO Webインターフェイス

iLOのWebインターフェイスは、Webブラウザーを使用してネットワーク上のiLOに接続できる場合に使用します。また、iLO管理プロセッサーの設定を変更する場合も、この方法を使用できます。

ROMベースセットアップ

システム環境がDHCP、DNS、またはWINSを使用しない場合は、iLO6構成ユーティリティを使用します。

その他のiLO構成ツール

このガイドでは説明しませんが、以下のiLO構成オプションがあります。

Intelligent Provisioning

Intelligent Provisioningを起動するには、POST中にF10キーを押します。

iLOのWebインターフェイスからAlways On Intelligent Provisioningにアクセスすることもできます。詳しくは、Intelligent Provisioningのユーザーガイドを参照してください。

iLO RESTful API

サーバー管理ツールから使用することでiLO経由でサポート対象サーバーの構成、インベントリ、および監視を実行できる管理インターフェイスです。詳しくは、次のWebサイトを参照してください。**https://www.hpe.com/info/redfish**

HPE OneView

iLO管理プロセッサーと対話してProLiantサーバーまたはSynergyコンピュートモジュールを構成、監視、および管理をする管理ツールです。詳しくは、HPE OneViewユーザーガイドを参照してください。

HPE Scripting Toolkit

このツールキットは、サーバーの無人/自動での大量インストールを可能にする、ITエキスパート向けのサーバーインストール製品です。詳しくは、WindowsまたはLinux用のScripting Toolkitユーザーガイドを参照してください。

スクリプティング

スクリプティングを使用して複数のiLO管理プロセッサーを設定できます。スクリプトは、RIBCLと呼ぶスクリプティング言語用に記述されたXMLファイルです。iLOは、RIBCLスクリプトを使用して設定できます。ネットワーク経由での設定、初期展開の際の設定、展開済みのホストからの設定などさまざまな設定が可能です。

以下の方法を使用できます。

- **HPQLOCFG** - ネットワーク経由でRIBCLスクリプトをiLOに送信するWindowsコマンドラインユーティリティです。
- **HPONCFG** - ホスト上で実行され、RIBCLスクリプトをローカルのiLOに転送する、ローカルでのオンラインのスクリプトによるセットアップユーティリティです。
- **カスタムスクリプティング環境（LOCFG.PL）** - iLOスクリプティングサンプルには、RIBCLスクリプトをネットワーク経由でiLOに送信するために使用できるPerlサンプルが含まれています。

- **SMASH CLP** – SSHまたは物理シリアルポートからコマンドラインにアクセスできるときに使用できるコマンドラインプロトコルです。

これらの方法について詳しくは、iLOスクリプティング/コマンドラインガイドを参照してください。

iLOのサンプルスクリプトは、次のWebサイトから入手できます。https://www.hpe.com/support/ilo6

初期セットアップ手順

このタスクについて

iLOはデフォルト設定のままでも、ほとんどの機能を使用できます。ただしiLOでは、複数の企業環境のために柔軟なカスタム設定が可能です。この章では、初期のiLOセットアップ手順について説明します。

手順

1. iLOのセットアップと使用方法については、一般的なセキュリティガイドラインを参照してください。
2. iLOをネットワークに接続します。
3. 動的IPアドレスを使用しない場合は、ROMベースセットアップユーティリティを使用して静的IPアドレスを設定します。
4. ローカルアカウント機能を使用する場合は、ROMベースセットアップユーティリティを使用してユーザーアカウントの追加（iLO6構成ユーティリティ）を行います。
5. 必要に応じて、iLOドライバーをインストールします。
6. （オプション）iLOライセンスをインストールします。

   iLO（Standard）は、追加コストまたはライセンスなしでHewlett Packard Enterpriseサーバーに事前設定されています。生産性を向上させる機能にはライセンスが必要です。詳しくは、https://www.hpe.com/support/ilo-docsにあるiLOライセンスガイドを参照してください。

iLOネットワークに接続する

このタスクについて

本番環境ネットワークまたは専用の管理ネットワークを使用してiLOをネットワークに接続します。

iLOは、標準Ethernetケーブル（RJ-45コネクターの付いたCAT 5 UTPケーブルなど）を使用します。標準的なEthernetハブまたはスイッチへのハードウェアリンクを確立するには、ストレートケーブルが必要です。

ハードウェアのセットアップについて詳しくは、サーバーのユーザーガイドを参照してください。

詳しくは

iLOネットワーク接続オプション

iLO6構成ユーティリティを使用したiLOのセットアップ

Hewlett Packard Enterpriseは、初めてiLOをセットアップする場合と、DHCP、DNS、またはWINSを使用しない環境にiLOのネットワークパラメーターを構成する場合に、iLO6構成ユーティリティを使用することをおすすめします。

サブトピック

静的IPアドレスの構成（iLO6構成ユーティリティ）

静的IPアドレスの構成（iLO6構成ユーティリティ）

このタスクについて

この手順は、静的IPアドレスを使用する場合にのみ必要です。動的IPアドレスを使用する場合は、DHCPサーバーによってiLOのIPアドレスが自動的に割り当てられます。

インストールを簡単にするために、Hewlett Packard EnterpriseはiLOでDNSまたはDHCPを使用することをおすすめします。

手順

1. （オプション）サーバーにリモートアクセスする場合、iLOリモートコンソールセッションを開始します。
2. サーバーを再起動するかまたは電源を入れます。
3. サーバーのPOST画面でF9キーを押します。

   UEFIシステムユーティリティが起動します。
4. システム構成をクリックします。
5. iLO 6構成ユーティリティをクリックします。
6. DHCPを無効にします。
   a. ネットワークオプションをクリックします。
   b. DHCP有効メニューでオフを選択します。

      IPアドレス、サブネットマスク、およびゲートウェイIPアドレスボックスが編集可能になります。DHCP有効がオンに設定されている場合は、これらの値を編集できません。
7. IPアドレス、サブネットマスク、およびゲートウェイIPアドレスボックスに値を入力します。
8. 変更を保存して終了するには、F12キーを押します。

   iLO6構成ユーティリティによって、保留中の構成変更を保存するか確認するメッセージが表示されます。
9. 保存して終了するには、はい - 変更を保存しますをクリックします。

   iLO6構成ユーティリティから、変更を反映するためにiLOをリセットする必要があることが通知されます。
10. OKをクリックします。

    iLOがリセットされ、iLOセッションが自動的に終了します。約30秒で再接続することができます。
11. 通常の起動プロセスを再開します。
    a. iLOリモートコンソールを起動します。

       iLO6構成ユーティリティは、前のセッションから開いたままになっています。
    b. ESCキーを数回押して、システム構成ページに移動します。
    c. システムユーティリティを終了し、通常のブートプロセスを再開するには、システムを終了して再起動をクリックします。

iLO6構成ユーティリティを使用したローカルユーザーアカウントの管理

サブトピック

ユーザーアカウントの追加（iLO6構成ユーティリティ）

手順

1. （オプション）サーバーにリモートアクセスする場合、iLOリモートコンソールセッションを開始します。
2. サーバーを再起動するかまたは電源を入れます。
3. サーバーのPOST画面でF9キーを押します。

   UEFIシステムユーティリティが起動します。
4. システム構成、iLO 6構成ユーティリティ、ユーザー管理、ユーザーの追加の順にクリックします。
5. 新しいユーザーの権限を選択します。

   権限を割り当てるには、権限名の横にあるメニューではいを選択します。権限を削除するには、いいえを選択します。

   ログイン権限はデフォルトですべてのユーザーに割り当てられるため、iLO6構成ユーティリティでは表示されません。

   リカバリセット権限はiLO6構成ユーティリティを通じて割り当てることができないため、リストにありません。
6. 新しいユーザー名ボックスとログイン名ボックスにユーザー名とログイン名を入力します。
7. パスワードを入力します。
   a. カーソルをパスワードボックスに移動し、Enterキーを押します。

      新しいパスワードを入力しますボックスが開きます。
   b. パスワードを入力して、Enterキーを押します。

      新しいパスワードを確認してくださいボックスが開きます。
   c. 確認のためもう一度パスワードを入力して、Enterキーを押します。

   iLO6構成ユーティリティは、新しいアカウントの作成を確認します。
8. 確認ダイアログボックスを閉じるには、OKをクリックします。
9. 必要な数のユーザーアカウントを作成し、F12キーを押して変更を保存し、システムユーティリティを終了します。
10. 変更を確認するよう求められた場合は、はい - 変更を保存しますをクリックしてユーティリティを終了し、ブートプロセスを再開します。

詳しくは

iLOユーザーアカウントの権限
iLOユーザーアカウントオプション
パスワードに関するガイドライン

ユーザーアカウントの編集（iLO6構成ユーティリティ）

このタスクについて

注記: Hewlett Packard Enterpriseでは、システムが電源投入時セルフテスト（POST）状態にあるときにiLOで構成変更を実行すると iLOがリセットされるため、避けることをおすすめします。POST中にそのような構成変更を行うと、 iLOが工場出荷時のデフォルト設定にリセットされる可能性があります。

手順

1. （オプション）サーバーにリモートアクセスする場合、iLOリモートコンソールセッションを開始します。
2. サーバーを再起動するかまたは電源を入れます。
3. サーバーのPOST画面でF9キーを押します。

   UEFIシステムユーティリティが起動します。
4. システム構成、iLO 6構成ユーティリティ、ユーザー管理、ユーザーの編集/削除の順にクリックします。
5. 編集または削除するユーザー名のアクションメニューを選択し、編集を選択します。

   アカウントのプロパティが表示されます。
6. ログイン名をアップデートします。
7. パスワードをアップデートします。
   a. カーソルをパスワードボックスに移動し、Enterキーを押します。

      新しいパスワードを入力しますボックスが開きます。
   b. パスワードを入力して、Enterキーを押します。

      新しいパスワードを確認してくださいボックスが開きます。
   c. 確認のためもう一度パスワードを入力して、Enterキーを押します。
8. ユーザーアカウントの権限を変更します。

   権限を割り当てるには、権限名の横にあるメニューではいを選択します。権限を削除するには、いいえを選択します。

   ログイン権限はデフォルトですべてのユーザーに割り当てられるため、iLO6構成ユーティリティでは利用できません。

   リカバリセット権限はiLO6構成ユーティリティを通じて割り当てることができないため、リストにありません。
9. 必要な数のユーザーアカウントをアップデートし、F12キーを押して変更を保存し、システムユーティリティを終了します。
10. 変更を確認するよう求められた場合は、はい - 変更を保存しますをクリックしてユーティリティを終了し、ブートプロセスを再開します。

ユーザーアカウントの削除（iLO6構成ユーティリティ）

手順

1. （オプション）サーバーにリモートアクセスする場合、iLOリモートコンソールセッションを開始します。
2. サーバーを再起動するかまたは電源を入れます。
3. サーバーのPOST画面でF9キーを押します。

   システムユーティリティが起動します。
4. システム構成、iLO 6構成ユーティリティ、ユーザー管理、ユーザーの編集/削除の順にクリックします。
5. 削除するユーザーのアクションメニューで、削除を選択します。

   このページで変更を保存するときに削除するユーザー名にマークが付けられます。

6. 必要に応じて、削除する他のユーザーアカウントにマークを付けてからF12キーを押して変更を保存し、システムユーティリティを終了します。
7. 変更を確認するよう求められた場合は、はい - 変更を保存しますをクリックしてユーティリティを終了し、ブートプロセスを再開します。

Webインターフェイスによるi LOのセットアップ

Webブラウザーを使用してネットワーク上のiLOに接続できる場合は、iLO Webインターフェイスを使用してiLOを構成できます。また、iLO管理プロセッサーの設定を変更する場合も、この方法を使用できます。

サポートされているブラウザーを使用して、デフォルトのDNS名、ユーザー名、およびパスワードを入力して、リモートのネットワーククライアントからiLOにアクセスします。

詳しくは

サポートされているブラウザー
iLO Webインターフェイスの使用

iLOに初めてログインする方法

手順

`https://<iLOホスト名またはIPアドレス>`
を入力します。

iLOのWebインターフェイスのアクセスにはHTTPS（SSL暗号セッションで交換されるHTTP）が必要です。

2. デフォルトのユーザー認証情報を入力して、ログインをクリックします。

> **ヒント:**
> 初めてiLOにログインした後、Hewlett Packard Enterpriseは、デフォルトのユーザーアカウントのパスワードを変更することをおすすめします。

詳しくは

ローカルユーザーアカウントの編集
パスワードに関するガイドライン

iLOのデフォルトのDNS名とユーザーアカウント

iLOファームウェアは、デフォルトのユーザー名、パスワード、およびDNS名が設定されています。デフォルトの情報は、iLOマネジメントプロセッサーを搭載するサーバーに取り付けられているシリアルラベルプルタブに記載されています。これらの値を使用し、Webブラウザーを使用して、ネットワーククライアントからリモートでiLOにアクセスしてください。

- **ユーザー名** - Administrator
- **パスワード** - ランダムな8文字の文字列または共通のデフォルトパスワード。パスワードのタイプは工場出荷時に定義されており、サーバーの注文に含まれるSKU番号によって異なります。

  一般的なデフォルトパスワードSKU番号はP08040-B21です。詳しくは、以下のWebサイトにあるiLO QuickSpecドキュメントを参照してください。**https://www.hpe.com/info/qs**。
- **DNS名** - ILOXXXXXXXXXXXX（**X**は、サーバーのシリアル番号）

重要:

Hewlett Packard Enterpriseは、初めてiLOにログインした後で、デフォルトのパスワードを変更することをお勧めします。

iLOを工場出荷時のデフォルト設定にリセットした場合は、リセット後にデフォルトのiLOアカウント認証情報（シリアルラベルプルタブに表示）を使用してログインします。

iLOドライバーのサポート

iLOは、内蔵のオペレーティングシステムを実行する独立したマイクロプロセッサーです。このアーキテクチャーでは、ホストのオペレーティングシステムとは関係なく、iLOのほとんどの機能を使用できます。iLOドライバーは、HPONCFGやAgentless Management ServiceなどのソフトウェアがiLOと通信できるようにします。インストールされているOSとシステム構成によって、インストール要件が決定します。

Windows

iLOでWindowsを使用する場合は、以下のドライバーを使用できます。

- iLO 6 Channel Interfaceドライバー for Windows - このドライバーは、Agentless Management Service、HPONCFG、ファームウェアのフラッシュコンポーネント、および他のユーティリティがiLOと通信する場合に必要です。SUMはこのドライバーを使用して、システムのファームウェアのインベントリを実行します。すべての構成でこのドライバーをインストールしてください。
- iLO6自動サーバー復旧ドライバー - このドライバーは、オペレーティングシステムがクラッシュまたはロックアップした場合にサーバーをリセットするASRハードウェアタイマーを管理します。

Linux

iLOでLinuxを使用する場合は、`hpilo` 1.5.0以降のドライバーを使用できます。

このドライバーは、エージェントおよびツールアプリケーションのiLOへのアクセスを管理します。

`hpilo`は、このバージョンのiLOファームウェアでサポートされているすべてのサーバーオペレーティングシステム用のLinuxカーネルの一部です。

`hpilo`は起動時に自動的にロードされます。

VMware

iLOでVMwareを使用する場合は、`ilo`ドライバーを使用できます。

このドライバーは、Agentless Management Service、WBEMプロバイダー、およびツールアプリケーションのiLOへのアクセスを管理します。これは、カスタマイズされたHewlett Packard Enterprise VMwareイメージに含まれています。元のVMwareイメージを使用するには、手動でドライバーをインストールする必要があります。

iLOドライバーのインストール

手順

1. お使いのOS用のiLOドライバーを入手します。
   - **Windowsの場合** - **SPPをダウンロード**するか、Hewlett Packard Enterpriseサポートセンター（**https://www.hpe.com/support/ilo6**）からドライバーをダウンロードします。
   - **VMwareの場合** - **SPPをダウンロード**するか、Hewlett Packard EnterpriseSoftware Delivery RepositoryのWebサイト（**https://www.hpe.com/support/SDR-Linux**）のvibsdepotセクションからドライバーをダウンロードします。

注記:

iLOドライバーはRed Hat Enterprise LinuxとSUSE Linux Enterprise Serverの両方のLinuxディストリビューションに含まれています。

2. ドライバーをインストールします。
   - Hewlett Packard Enterpriseサポートセンターからドライバーをダウンロードした場合、ソフトウェアに付属のインストール手順を実行します。
   - SPPをダウンロードした場合、SPPドキュメント（https://www.hpe.com/info/spp/documentation）の指示に従ってください。

iLO Webインターフェイスの使用

サブトピック

サポートされているブラウザー

HPE iLO6は以下のブラウザーの最新バージョンをサポートします。

推奨ブラウザー

- Google Chromeモバイルおよびデスクトップのバージョン
- Mozilla Firefox
- Microsoft Edge

Chrome、Firefox、EdgeがHPE iLO6で最高のパフォーマンスを提供します。

ブラウザーの要件

- JavaScript - iLOはクライアントサイドJavaScriptを広範に使用します。
- Cookies - 一部の機能が正常に動作するために、Cookieを有効にする必要があります。
- ポップアップウィンドウ - 一部の機能が正常に動作するために、ポップアップウィンドウを有効にする必要があります。ポップアップブロックが無効になっていることを確認してください。
- **TLS** - WebブラウザーからiLOにアクセスするには、ブラウザーでTLS 1.2以降を有効にする必要があります。

iLO Webインターフェイスへのログイン

手順

`https://<iLOのホスト名またはIPアドレス>`
を入力します。

iLO Webインターフェイスにアクセスするには、HTTPSを使用する必要があります（HTTPSはSSL暗号セッションで交換されるHTTPです）。

iLOログインページが開きます。

- ログインセキュリティバナーが構成されている場合は、バナーテキストが通知セクションに表示されます。
- ヘルスLEDステータスが劣化またはクリティカルの場合は、ヘルスLEDアイコンがiLOホスト名の横に表示されます。
- iLOのヘルスステータスが劣化で、匿名データアクセスオプションが有効な場合は、ヘルスステータスと問題の説明がiLOのログインページに表示されます。セキュリティ侵害の可能性があるセルフテスト障害は、説明には表示されません。

2. ディレクトリまたはローカルアカウントログイン名とパスワードを入力して、ログインをクリックします。

   iLOがKerberosネットワーク認証用に設定されている場合は、ログインボタンの下に Zeroサインインボタンが表示されます。Zeroサインインボタンを使用して、ユーザー名とパスワードを入力せずにログインできます。

   iLOがCAC Smartcard認証用に設定されている場合は、ログインボタンの下にSmartcardでログインボタンが表示されます。スマートカードを接続して、Smartcardでログインボタンをクリックすることができます。CAC Smartcard認証を使用する場合、ログイン名とパスワードを入力しないでください。

詳しくは

iLOのデフォルトのDNS名とユーザーアカウント
CAC Smartcard認証
ログインセキュリティバナーの構成

ブラウザーインスタンスとiLOの間でのCookieの共有

iLOにアクセスし、ログインすると、1つのセッションCookieが、ブラウザーのアドレスバーでiLO URLを共有する、開いているすべてのブラウザーウィンドウで共有されます。この結果、開いているすべてのブラウザーウィンドウが1つのユーザーセッションを共有します。1つのウィンドウでログアウトすると、開いているすべてのウィンドウでユーザーセッションが終了します。新しいウィンドウで別のユーザーとしてログインすると、他のウィンドウでセッションが置き換えられます。

これは、ブラウザーの標準的な動作です。iLOは、同一クライアント上の同じブラウザー内の2つの異なるブラウザーウィンドウから複数のユーザーがログインすることをサポートしません。

共有インスタンス

iLOのWebインターフェイスが別のブラウザーウィンドウまたはタブ（ヘルプファイルなど）を開く場合、このウィンドウは、iLOへの同じ接続とセッションCookieを共有します。

iLOのWebインターフェイスにログインしているときに、手動で新しいブラウザーウィンドウを開くと、元のブラウザーウィンドウの複製インスタンスが開きます。アドレスバーのドメイン名が元のブラウザーセッションと一致する場合、新しいインスタンスは元のブラウザーウィンドウとセッションCookieを共有します。

Cookieの順序

ログイン時に、ログインページは、ウィンドウをiLOファームウェアの適切なセッションにリンクさせるブラウザーセッションCookieを作成します。ファームウェアは、ブラウザーログインを、セッションリストページに示される個別のセッションとして追跡します。

例えば、User1がログインすると、Webサーバーは、アクティブユーザーとしてUser1を示し、ナビゲーションペインにメ

ニュー項目を示し、右のペインにページデータを示す初期フレームビューを表示します。User1が各リンクをクリックすると、メニュー項目とページデータだけがアップデートされます。

User1がログインしているときに、User2が同じクライアントでブラウザーウィンドウを開いてログインすると、User1セッションで作成されたCookieは、2番目のログインによって上書きされます。User2が異なるユーザーアカウントである場合、異なる現在のフレームが作成され、新しいセッションが許可されます。2番目のセッションは、セッションリストページにUser2として表示されます。

2番目のログインによって、User1のログイン時に作成されたCookieが上書きされ、事実上、最初のセッションが親ブラウザーから切り離されています。この動作は、User1のブラウザーが、ログアウトせずに閉じられた場合と同じです。親ブラウザーから切り離されたUser1のセッションは、タイムアウトしたときに再要求されます。

ブラウザーのページ全体が強制的に更新されない限り、現在のユーザーのフレームは更新されないので、User1は、ブラウザーウィンドウを使用して操作を続けることができます。ただし、ブラウザーは、すぐに判別できない場合でも、すでにUser2のセッションCookie設定を使用して動作しています。

User1がこのモード（User2がログインしてセッションCookieをリセットしたためにUser1とUser2がプロセスを共有）で操作を続ける場合、以下の状態になることがあります。

- User1のセッションは、User2に割り当てられている権限を使用して継続的に動作します。
- User1が操作してもUser2のセッションは中断されませんが、User1のセッションはタイムアウトになる場合があります。
- どちらかのウィンドウがログアウトすると、両方のセッションが終了します。ログアウトしなかったほうのウィンドウでのその次の動作によって、ユーザーは、タイムアウトまたは早期タイムアウトが発生したかのように、ログインページに転送されることがあります。
- 2番目のセッション（User2）からログアウトすると、次の警告メッセージが表示されます。

  ```
  Logging out: unknown page to display before redirecting the user to the login page.
  ```

- User2が、ログアウトした後にUser3としてログインしなおすと、User1は、User3のセッションを共有します。
- User1がログインしているときにUser2がログインする場合、User1は、URLを変更してインデックスページに転送することができます。これにより、User1は、ログインせずにiLOにアクセスしているかのような状態になります。

これらの動作は、複製ウィンドウが開いている限り継続されます。すべての動作は、最後のセッションCookieセットを使用して、同じユーザーに帰属させられます。

現在のセッションCookieの表示

ログイン後にURLナビゲーションバーに次のように入力すると、ブラウザーに現在のセッションCookieが表示されます。

```
javascript:alert(document.cookie)
```

表示される最初のフィールドにセッションIDが示されます。異なるブラウザーウィンドウでセッションIDが同じである場合、これらのウィンドウはiLOセッションを共有しています。

F5キーを押すか、表示 > 最新の情報に更新の順に選択するか、表示の更新ボタンをクリックすることによって、ブラウザーの表示を更新して、ユーザーの本当のIDを表示することができます。

Cookieに関連する問題を回避するためのベストプラクティス

- ブラウザーのアイコンまたはショートカットをダブルクリックして、ログインごとに新しいブラウザーを起動します。
- ブラウザーウィンドウを閉じる前にiLOセッションをログアウトします。

iLO Webインターフェイスの概要

iLOのWebインターフェイスは、類似の作業をグループ化しており、容易なナビゲーションとワークフローを提供します。インターフェイスは、ナビゲーションツリーにまとめられています。Webインターフェイスを使用するには、ナビゲーションツリーで項目をクリックし、表示するタブの名前をクリックします。

以下のオプションは、サーバータイプや構成でサポートしている場合のみ、ナビゲーションツリーに表示されます。

- iLOでリモート管理ツールが使用されている場合は、<リモート管理ツール名>オプションが表示されます。

サブトピック

iLO制御のアイコン

iLOのWebインターフェイスにログインすると、iLO制御を任意のiLOページから使用できます。iLO制御のアイコンをクリックして、製品の機能または情報にアクセスできます。

- 電源アイコン – 仮想電源ボタン機能にアクセスするには、このアイコンを使用します。

  このアイコンの色は、現在の電源ステータスによって異なります。

- UIDアイコン – UID LEDをオンまたはオフに切り替えるには、このアイコンを使用します。

  このアイコンの色は、現在のUID LEDステータスによって異なります。

- 言語 – 現在のiLO Webインターフェイスセッションの言語を選択するには、このアイコンを使用します。

  言語設定を表示または変更するには、設定オプションを使用します。

  このアイコンを使用できるのは、1つまたは複数の言語パックがインストールされている場合だけです。

- ヘルスLEDアイコン – システムLEDステータスを示します。このアイコンの色は、現在のシステムLEDステータスによって変わります。

- サーバーヘルスアイコン – サーバーのヘルスステータスの概要を表示するには、このアイコンを使用します。このアイコンをクリックして、サーバーのファン、温度センサー、その他の監視対象サブシステムのヘルスステータスを表示できます。

  リスト内のほとんどのヘルスステータス値について、ステータスをクリックして詳細情報を表示できます。

  このアイコンは、概要が表示されているサーバーのヘルスステータスによって変わります。

- iLOヘルスアイコン – iLOのヘルスステータスを表示するには、このアイコンを使用します。表示される値は、OKまたは警告です。

- セキュリティアイコン – このアイコンはiLOのセキュリティ状態を示します。これは、セキュリティダッシュボードページからの結合した結果に基づいています。表示される値は、OK、無視、およびリスクです。

  このアイコンをクリックして、セキュリティダッシュボードページに移動できます。

  このアイコンの色は、セキュリティ状態によって異なります。

- ユーザーアイコン – このアイコンは次の操作をサポートしています。

  - ログアウトオプションを使用して、現在のiLO Webインターフェイスセッションからログアウトします。
  - セッションオプションを使用して、アクティブなiLOセッションを表示します。
  - 設定オプションを使用して、ユーザー管理ページでiLOユーザーアカウントを表示または変更します。

    現在のセッションユーザーの名前をクリックして、ユーザー管理ページに移動することもできます。

- ヘルプアイコン – 現在のiLO Webインターフェイスページのオンラインヘルプを表示するには、このアイコンを使用します。

> **ヒント:**
> オンラインヘルプで前後に移動するには、Alt + 左矢印またはAlt +右矢印を押します。

- ... 詳細アイコン – ブラウザーウィンドウが小さすぎるため完全なページが表示されない場合は、ファームウェア& OSソフトウェアページにこのアイコンが表示されます。

  ファームウェアのアップデートオプション、iLOレポジトリにアップロードオプション、およびキューに追加オプションにアクセスするには、このアイコンを使用します。

iLOナビゲーションペイン

iLOには、表示/非表示を切り替えることができる折りたたみ可能なナビゲーションペインがあります。

- ナビゲーションペインを非表示にするには、✕ をクリックします。

  ナビゲーションペインを非表示にすると、cookieに保存されているご使用の優先設定が次の操作を行う際も引き続き使用されます。

  - 別のページの表示
  - ブラウザーウィンドウのサイズ変更または更新
  - ログイン/ログアウト
- 非表示のナビゲーションペインを表示するには、 をクリックします。

iLOナビゲーションペインのリモートコンソールのサムネイル

ナビゲーションペインには、リモートコンソールのサムネイルが表示されます。

- リモートコンソールを起動するには、サムネイルをクリックし、メニューからコンソールオプションを選択します。
- HTML5 IRCを固定モードで実行する場合、スタティックリモートコンソールサムネイルが変わって、アクティブリモートコンソールセッションを表示します。
- モニターを備えたサーバーの場合：リモートコンソールのサムネイルをクリックし、Wake-Upモニターを選択することで、モニターのスリープモードを解除することができます。

ログインページからのリモート管理ツールの起動

前提条件

iLOはリモート管理ツールで制御されています。

手順

1. iLOログインページに移動します。

   iLOがリモート管理ツールの制御下にある場合、iLO Webインターフェイスに次のようなメッセージが表示されます。

   このシステムは以下によって管理されています：<リモート管理ツール名>。
   iLO内でローカルで変更すると、その変更は、集中管理された設定と同期が取れなくなります。

   リモート管理ツールの名前はリンクになっています。
2. リモート管理ツールのリンクをクリックします。

詳しくは

ログインページからの言語の変更

前提条件

言語パックがインストールされていること。

このタスクについて

言語パックがインストールされている場合は、ログイン画面の言語メニューを使用して、iLOセッション用の言語を選択します。この選択は、将来使用するために、ブラウザーのCookieに保存されます。

手順

1. iLOログインページに移動します。
2. 言語メニューから言語を選択します。

詳しくは

言語パック

iLO情報およびログの表示

サブトピック

iLOの概要情報の表示

セキュリティダッシュボードの使用

iLOセッションの管理

iLOイベントログ

インテグレーテッドマネジメントログ

セキュリティログ

Active Health System

iLOの概要情報の表示

手順

ナビゲーションツリーで情報をクリックします。

iLO概要ページは、サーバーとiLOサブシステムに関する高レベルな詳細情報を表示し、一般に使用される機能へリンクします。

サブトピック

サーバーの詳細

iLOの詳細

ステータスの詳細

サーバーの詳細

製品名

このiLOプロセッサーを統合する製品。

サーバー名

ホストOSによって定義されたサーバー名。

アクセス設定ページに移動するには、サーバー名リンクをクリックします。

オペレーティングシステム

サーバーのOSとバージョン。

OS情報は、Agentless Management Service（AMS）がインストールされ実行中であり、かつOSが使用可能になると表示されます。サーバーの電源がオフのときは、表示されません。

システムROM

アクティブなシステムROMのバージョン。

システムROM日付

アクティブなシステムROMの日付。

冗長化システムROM

冗長化システムROMのバージョン。冗長化システムROMは、システムROMのアップデートに失敗した場合や、システムROMがロールバックされる場合に使用されます。この値は、システムが冗長化システムROMをサポートする場合のみ表示されます。

冗長化システムROMオプションは、サポートされているプラットフォームでのみ使用できます。

サーバーシリアル番号

システムの製造時に割り当てられるサーバーシリアル番号。POST実行時にROMベースのシステムユーティリティを使用すると、この値を変更できます。

シリアル番号（論理）

ホストアプリケーションに提示されるシステムシリアル番号。この値は、他のソフトウェアによって設定された場合にのみ表示されます。この値により、OSとアプリケーションのライセンスが影響を受ける場合があります。シリアル番号（論理）の値は、システムに割り当てられている論理サーバープロファイルの一部として設定されます。論理サーバープロファイルを削除すると、シリアル番号の値がシリアル番号（論理）の値からサーバーシリアル番号の値に戻ります。シリアル番号（論理）の値が設定されていないと、この項目は表示されません。

製品ID

この値は、同じシリアル番号を持つ異なるシステムを区別します。製品IDは、システムの製造時に割り当てられます。POST実行時にROMベースのシステムユーティリティを使用すると、この値を変更できます。

UUID

ソフトウェアがこのホストを識別するために使用するUUID（Universally Unique Identifier）。この値は、システムの製造時に割り当てられます。

UUID(論理)

ホストアプリケーションに提示されるシステムUUID。この値は、他のソフトウェアによって設定された場合にのみ表示されます。この値により、OSとアプリケーションのライセンスが影響を受ける場合があります。UUID（論理）の値は、システムに割り当てられている論理サーバープロファイルの一部として設定されます。論理サーバープロファイルを削除すると、システムUUIDの値がUUID（論理）の値からUUIDの値に戻ります。UUID（論理）の値が設定されていないと、この項目は表示されません。

リモートコンソール

サーバーコンソールとのリモートアウトオブバンド通信のためにリモートコンソールを開始できます。

アクセス設定ページでリモートコンソールオプションが無効な場合、無効の値が表示されます。

現在のユーザーがリモートコンソール権限を割り当てられていない場合、利用不可の値が表示されます。

iLO統合リモートコンソールページに移動するには、リモートコンソールリンクをクリックします。

詳しくは

概要ページからのHTML5 IRCの起動
概要ページからの.NET IRCの起動

iLOの詳細

IPアドレス

iLOサブシステムのネットワークIPアドレス。

リンクローカルIPv6アドレス

iLOサブシステムのSLAACリンクローカルアドレス。ネットワークサマリーページに移動するには、リンクローカルIPv6アドレスリンクをクリックします。

iLOホスト名

iLOサブシステムに割り当てられた完全修飾ネットワーク名。デフォルトで、ホスト名はILO+システムのシリアル番号および現在のドメイン名です。この値はネットワーク名に使用され、一意である必要があります。

ネットワーク共通設定ページに移動するには、iLOホスト名リンクをクリックします。

iLO専用ネットワークポート

ネットワークインターフェイスのステータス（有効または無効）。サーバーがこのオプションをサポートしていない場合、この値は表示されません。

ネットワークの概要ページに移動するには、ネットワークインターフェイス名リンクをクリックします。

iLO共有ネットワークポート

ネットワークインターフェイスのステータス（有効または無効）。サーバーがこのオプションをサポートしていない場合、この値は表示されません。

ネットワークの概要ページに移動するには、ネットワークインターフェイス名リンクをクリックします。

iLO仮想NIC

iLO仮想NICセクションには、仮想NICからiLOに接続するときに使用するIPアドレスが表示されます。

この機能を構成できるアクセス設定ページに移動するには、iLO仮想NICをクリックします。

ライセンスタイプ

ライセンス済みiLOファームウェア機能性のレベル。

ライセンスページに移動するには、ライセンスタイプリンクをクリックします。

iLOファームウェアバージョン

インストールされているiLOファームウェアのバージョンと日付。

インストールされたファームウェアページに移動するには、iLOファームウェアバージョンリンクをクリックします。

iLO日付/時刻

iLOサブシステムの内蔵クロック。

SNTP設定ページに移動するには、iLO日付/時刻リンクをクリックします。

ステータスの詳細

サーバーヘルス

サーバーヘルスインジケーター。この値は、全体的なステータスや冗長性（障害処理能力）など、監視対象サブシステムの状態を要約します。起動時にいずれかのサブシステムが冗長でなくても、サーバーのヘルスステータスは劣化しません。表示される値は、OK、劣化、およびクリティカルです。

サーバーヘルスは、個々のサブシステムの情報をまとめたものです。サブシステムは次のとおりです。

- プロセッサー
- メモリ
- BIOS/ハードウェアヘルス
- ネットワーク
- ストレージ
- 電源装置
- 電源装置の冗長性
- ファン
- ファンの冗長性
- 液冷機能
- 液冷機能の冗長性
- 温度
- Smartストレージバッテリ

サーバーヘルスは、サブシステムのヘルスを集約したものです。サブシステムの最も高い重大度がサーバーヘルスとして示されます。

冗長性ファクターが障害の場合、サーバーヘルスの計算で考慮される冗長性ファクターの重大度は警告になります。

ヘルスサマリーページに移動するには、サーバーヘルスリンクをクリックします。

ヘルスLED

システムLEDステータスを示します。これは、サーバーの動作ステータスです。表示される値は、OK、劣化、およびクリティカルです。

インテグレーテッドマネジメントログページに移動するには、ヘルスLEDリンクをクリックします。

iLOヘルス

iLOヘルスステータス。iLO診断セルフテストを組み合わせた結果に基づいています。表示される値は、OKおよび劣化です。

診断ページに移動するには、iLOヘルスリンクをクリックします。

iLOセキュリティ

iLOのセキュリティ状態。セキュリティダッシュボードページからの結合した結果に基づいています。表示される値は、OK、無視、およびリスクです。

セキュリティダッシュボードページに移動するには、iLOセキュリティリンクをクリックします。

サーバー電源

電源 - サーバーの電源状態（オンまたはオフ）。

仮想電源ボタン機能にアクセスするには、サーバー電源アイコンをクリックします。

サーバー電源ページに移動するには、サーバー電源リンクをクリックします。

UIDインジケーター

UID LEDの状態。UID LEDを使用すると、特に高密度ラック環境でサーバーを特定し、その位置を見つけることができます。状態には、UIDオン、UIDオフ、およびUID点滅があります。

iLOサービスポートが使用中の場合は、UID点滅ステータスにサービスポートのステータスが含まれます。表示される可能性がある値は、UID点滅（サービスポートビジー）、UID点滅（サービスポートエラー）、およびUID点滅（サービスポート完了）です。

UID LEDをオンまたはオフに変更するには、UIDインジケーターアイコンをクリックするか、iLO Webインターフェイスの上部にあるUID制御をクリックします。

UIDが点滅していた後で点滅が停止すると、ステータスは前回の値（UIDオンまたはUIDオフ）に戻ります。UID LEDが点滅している間に新しい状態を選択すると、UID LEDが点滅を停止したときに新しい状態が有効になります。

注意:
UID LEDは自動的に点滅して、ホストでリモートコンソールのアクセスやファームウェアアップデートのような重大な操作が進行中であることを示します。UID LEDの点滅中は、絶対にサーバーの電源を切らないでください。

プラットフォームのRASポリシー

構成されたプラットフォームの耐障害性および保守性（RAS）ポリシー。

次の値が表示される可能性があります。

- Firmware First（デフォルト） - BIOSは訂正されたエラーを監視し、訂正されたエラーに対してアクションが必要な場合にイベントをログに記録します。この構成では、OSは訂正されたエラーの監視およびログへの記録を行いません。
- OS First - 訂正済みエラーはOSに対してマスクされず、OSがログ記録のためのポリシーを制御します。

注記:
エラー訂正は、当然起こるものと予想されます。BIOSもイベントをログに記録していない限り、訂正されたエラーのログに基づいてアクションを実行する必要はありません。

この設定は、UEFIシステムユーティリティでシステム構成 > BIOS/プラットフォーム構成（RBSU） > アドバンストオプションに移動して構成できます。Hewlett Packard Enterpriseとしては、デフォルト設定を使用することをお勧めします。

Trusted Platform ModuleまたはTrusted Module

TPMあるいはTMソケットまたはモジュールのステータス。

表示される可能性のある値は未サポート、未装着、または装着: 有効です。

Trusted Platform ModuleおよびTrusted Moduleは、プラットフォームの認証に使用される仕掛けを安全に格納するコンピューターチップです。これらの仕掛けには、パスワード、証明書、暗号鍵などが含まれます。また、TPMまたはTMを使用すると、プラットフォームの測定値を格納してプラットフォームの信頼性を保証することができます。

サポートされているシステムでは、ROMはTPMまたはTMレコードを復号化し、構成ステータスをiLOに渡します。

モジュールタイプ

TPMまたはTMの種類と仕様のバージョン。指定できる値は、TPM 1.2、TPM 2.0、TM 1.0、未指定、および未サポートです。この値は、サーバーにTPMまたはTMが存在する場合に表示されます。

microSDフラッシュメモリカード

内蔵SDカードのステータス。存在する場合、SDカードの容量が表示されます。

アクセスパネルステータス

アクセスパネルの状態。表示される可能性のある値は、OK（アクセスパネルが取り付けられている）および侵入（アクセスパネルが開いている）です。

HPEへの接続ステータス

このセクションでは、サポートされているサーバーに関するリモートサポート登録ステータスが表示されます。

表示される可能性があるステータスの値は、以下のとおりです。

- リモートサポートに登録済み - サーバーは登録されています。
- 未登録 - サーバーは登録されていません。
- HPE リモートサポート情報を取得できません - 登録ステータスが特定できませんでした。
- リモートサポート登録エラー - リモートサポートの接続エラーが発生しました。

ステータス値をクリックして、リモートサポート登録ページに移動できます。

AMS

Agentless Management機能はiLOハードウェアで動作し、オペレーティングシステムやプロセッサーに依存しません。Agentless Managementでは、ヘルス監視とアラート通知機能がシステムに内蔵され、サーバーに電源コードを接続するとただちに動作を開始します。

iLOと直接通信できないデバイスおよびコンポーネントから情報を収集するには、Agentless Management Service（AMS）をインストールします。このセクションには、AMSのステータスが表示されます。

Agentless Management Service（AMS）の詳細情報は表示できません。

表示される値は、OKまたは利用不可能です。

以下で管理

このセクションには、システムの管理に使用される外部マネージャーが表示されます。表示される値は、以下のとおりです。

- HPE OneView - システムがHPE OneViewによって管理されていることを示します。
- HPE GreenLake for Compute Ops Management - システムがCompute Ops Managementによって管理されていることを示します。

注記:

- システムは、HPE OneViewまたはCompute Ops Managementのいずれかで管理できます。
- 管理の情報は、システムがいずれかの外部マネージャーで管理されている場合にのみ表示されます。

詳しくは

HPE内蔵リモートサポート

セキュリティダッシュボードの使用

前提条件

無視オプションを構成するためのiLO設定の構成権限。

このタスクについて

セキュリティダッシュボードページには、重要なセキュリティ機能のステータス、システムの全体セキュリティステータス、セキュリティ状態およびサーバー構成ロック機能の現在の構成が表示されます。ダッシュボードを使用して、構成の潜在的なリスクについて評価します。リスクが検知されたら、詳細情報とシステムセキュリティを向上させる方法についてのアドバイスを見ることができます。

手順

1. ナビゲーションツリーで情報をクリックして、セキュリティダッシュボードタブをクリックします。
2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。
3. セキュリティダッシュボード表で検出されたリスクについて確認します。

   セキュリティ機能にリスクステータスが付いて表示されている場合は、ステータスの値をクリックすると詳細情報が表示されます。詳細情報には、リスクと可能な解決策についての情報が含まれています。
4. （オプション）無視オプションをセキュリティ機能に構成します。
   - 無視オプションは、デフォルトでは無効になっています。
   - 無視オプションをセキュリティ機能に対して有効にすると、iLOが全体セキュリティステータスを判定するときその機能のステータスは無視されます。セキュリティ機能のステータスを無視しても、セキュリティダッシュボード表のステータス値は変わりません。

   セキュリティ機能の無視値を変更すると、iLOが全体セキュリティステータスを再計算します。

サブトピック

セキュリティダッシュボード詳細

全体セキュリティステータス

- OK–iLOが監視対象のセキュリティ機能に関連したセキュリティリスクを検出しませんでした。
- リスク–iLOが1つ以上の監視対象セキュリティ機能に関連した潜在的セキュリティリスクを検出しました。
- 無視–iLOが1つ以上の監視対象セキュリティ機能に関連した潜在的セキュリティリスクを検出しました。影響を受けるすべての機能が全体セキュリティステータスから除外されるよう設定されています。

  このステータスは、概要ページとiLOのコントロールにも表示されます。

セキュリティ状態

構成されているセキュリティ状態。表示される値は、以下のとおりです。

- 本番稼働
- 高セキュリティ
- FIPS
- CNSA
- Synergyセキュリティモード

サーバー構成ロック

構成されるサーバー構成ロックの設定。この機能は、管理者にデバイスの置き換えまたは追加、ハードウェアの取り外し、セキュアブートの変更、ファームウェアのインストールのような作業について警告します。この機能をUEFIシステムユーティリティで構成したり、iLO RESTful APIを使用して構成することができます。

セキュリティダッシュボードページでサーバー構成ロック情報を表示するには、環境が以下の要件を満たしている必要があります。

- インストールされているシステムROM/BIOSファームウェアが、サーバー構成ロック機能をサポートしている。

  Intelベースのサーバーではバージョン2.00が必要で、AMDベースのサーバーではバージョン1.40が必要です。
- iLO6 1.40以降にアップグレードした後、サーバーを再起動した。
- セキュリティ状態を本番環境からより高いセキュリティ状態に変更した後、サーバーを再起動した。
- サーバー構成ロックを含むライセンスがインストールされている。

セキュリティダッシュボード表

- セキュリティパラメーター–監視対象のセキュリティ機能の名前。

  iLO Webインターフェイスで構成できる機能については、この列のリンクをクリックして関連するwebインターフェイスページに移動してください。
- ステータス–監視対象のセキュリティ機能のセキュリティステータス。
  - OK–iLOがこの機能に関連したセキュリティリスクを検出しませんでした。
  - リスク–iLOがこの機能に関連した潜在的なセキュリティリスクを検出しました。
- 状態–監視対象のセキュリティ機能の現在の状態。表示される値は、以下のとおりです。
  - 有効–機能は有効です。

- 無効–機能は無効です。
- 不十分–機能は有効ですが、推奨される構成は使用されていません。
- オフ–機能はオフに設定されています。
- オン–機能はオンに設定されています。
- OK–機能はiLOのセキュリティ推奨事項に準拠しています。
- 失敗–機能は障害を報告しました。
- 修正済み–機能は、修正された障害を報告しました。
- 真–機能は使用中です。
- 偽–機能は使用されていません。

- 無視–この列に表示されるスイッチを使って、機能を無視するよう設定できます。無視設定を有効にすると、監視対象の機能は全体セキュリティステータス値に含まれません。

  機能を無視しても、セキュリティダッシュボード表に表示されるステータス値は変わりません。

詳しくは

iLOセキュリティ状態

リスク詳細

セキュリティダッシュボードページでセキュリティ機能のリスク詳細を表示すると、以下の情報が利用可能です。

- 説明 – セキュリティ機能がリスクステータスになっている理由の説明。
- 推奨されるアクション – 推奨される解決策。

  無視オプションが有効になっている場合、この値は表示されません。
- 無視 – 無視オプションが有効になった日時。
- 以下によって無視 – 無視オプションを有効にしたユーザーの名前。

セキュリティリスク状態の原因

以下のセキュリティ機能がセキュリティダッシュボードページで監視されます。サーバーでサポートされない機能は表示されません。

アクセスパネルステータス

シャーシの侵入検知コネクターにより、アクセスパネルのステータスが侵入になっていることが報告されました。

この機能は、シャーシの侵入検知が構成されているサーバーでのみ使用できます。

Hewlett Packard Enterpriseでは、IMLとiLOイベントログに記録されたイベントを監査し、監視ビデオをチェックしてサーバーへの物理的な侵入活動がないかどうかを確認することをお勧めします。

認証失敗ログ

iLOは、認証の失敗を記録するように構成されていません。

Hewlett Packard Enterpriseでは、アクセス設定ページのこの機能を有効にすることをお勧めします。

デフォルトSSL証明書が使用中

iLOのデフォルト自己署名証明書が使用中です。

Hewlett Packard Enterpriseでは、信頼済みの証明書をSSL証明書カスタマイズページで構成することをお勧めしま

す。

IPMI/DCMI over LAN

IPMI/DCMI over LAN機能が有効になっています。これにより、サーバーは既知のIPMIセキュリティ脆弱性にさらされます。

Hewlett Packard Enterpriseでは、アクセス設定ページのこの機能を無効にすることをお勧めします。

最新のファームウェアスキャン結果

最新のファームウェア検証テストが失敗しました。ファームウェアコンポーネントが壊れているか、その整合性が損なわれています。

Hewlett Packard Enterpriseでは、影響のあるファームウェアコンポーネントを、検証済みのイメージにアップデートすることをお勧めします。

この機能を使用するには、ライセンスをインストールする必要があります。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

最小パスワード長

最小パスワード長が推奨の長さよりも短くなっています。これにより、サーバーは辞書攻撃に対して脆弱になります。

Hewlett Packard Enterpriseでは、アクセス設定ページでこの値を8（デフォルト）以上に設定することをお勧めします。

パスワードの複雑さ

iLOは、パスワードの複雑さのガイドラインを適用するように構成されていません。これにより、サーバーは辞書攻撃に対して脆弱になります。

アクセス設定ページでこの機能を有効にできます。

ホスト認証が必要

ホスト認証が必要機能は無効になっており、iLOは高セキュリティのセキュリティ状態を使用するように構成されています。この機能が無効になっていると、ホストベースの構成ユーティリティを使用して管理プロセッサーにアクセスするときに、iLO認証情報は必要ありません。

Hewlett Packard Enterpriseでは、アクセス設定ページのこの機能を有効にすることをお勧めします。

iLO RBSUへのログイン要求

iLOは、UEFIシステムユーティリティのiLO構成オプションへのアクセスにログイン認証情報を要求するようには構成されていません。この構成では、システムブート中にiLO構成への未認証のアクセスが許可されます。

Hewlett Packard Enterpriseでは、アクセス設定ページのこの機能を有効にすることをお勧めします。

セキュアブート

UEFIセキュアブートオプションが無効になっています。この構成では、UEFIシステムファームウェアは、信頼された署名がブートローダー、オプションROMファームウェア、およびシステムソフトウェアの実行ファイルにあるかどうかの検証をスキップします。これにより、電源オン時にiLOによって確立された信頼チェーンが壊れます。

Hewlett Packard Enterpriseでは、この機能を有効にすることをお勧めします。

詳しくは、UEFIシステムユーティリティのドキュメントを参照してください。

セキュリティオーバーライドスイッチ

サーバーのセキュリティオーバーライドスイッチ（システムメンテナンススイッチとも呼ばれる）が有効になっています。セキュリティオーバーライドスイッチを有効にすると、ログイン認証が不要なため、この構成は1つのリスクです。

Hewlett Packard Enterpriseでは、この機能を無効にすることをお勧めします。

SNMPv1

SNMPv1は有効になっています。この構成は、iLOでのSNMPv1要求の受信およびSNMPv1アラートの送信を許可します。SNMPv1を有効にすると、攻撃に対するシステムの脆弱性が増加します。

Hewlett Packard Enterpriseでは、SNMP設定ページでこの機能を無効にすることをお勧めします。

グローバルコンポーネントの完全性

SPDM認証が有効になっています。この構成により、iLOはSPDMを使用して、サーバー内の該当するすべてのコンポーネントを認証します。アクセス設定ページでグローバルコンポーネントの完全性を無効にすると、iLOのセキュリティステータスがリスクに変わります。

グローバルコンポーネントの完全性が無効になっている場合、iLOはSPDM認証のためにコンポーネントを検証せず、SPDMをサポートするカードであっても
未サポート
と報告されます。

アクセス設定ページでこの機能を有効にできます。

詳しくは

iLOアクセス設定の構成
iLOセキュリティを無効にする理由
ファームウェア検証

iLOセッションの管理

前提条件

ユーザーアカウント管理権限

手順

1. 情報ページに移動し、セッションリストタブをクリックします。

   セッションリストページには、アクティブなiLOセッションの情報が表示されます。

2. （オプション）セッションを切断するには、その横にあるチェックボックスをクリックして、セッションの切断をクリックします。

   iLOは、選択したセッションの切断を確認するプロンプトを表示します。

3. はい、切断しますをクリックします。

セッションリスト詳細

iLOで以下の詳細が現在のセッションとセッションリスト（*アクティブセッションの総数*）の各表に表示されます。

- ユーザー - iLOユーザーアカウント名。

  通常のユーザーアカウントが*ユーザー：ユーザーアカウント名*の形式で表示されます。サービスアカウントが*サービスユーザー：ユーザーアカウント名*の形式で表示されます。

- IP - iLOにログインするために使用するコンピューターのIPアドレス。
- ログイン時間 - iLOセッションが開始した日時。
- アクセス時刻 - iLOがセッションで最後にアクティブだった日時。
- 失効 - セッションが自動的に終了する日時。
- ソース - セッションのソース （たとえば、リモートコンソール、Webインターフェイス、ROMベースのセットアップユーティリティ、iLO RESTful API、SSHなど）。
- 権限のアイコン（現在のユーザーのみ） - 現在のユーザーアカウントに割り当てられている権限。チェックマークのアイコンは、権限が有効になっていることを示します。Xアイコンは権限が無効になっていることを示します。

詳しくは

iLOユーザーアカウント

iLOイベントログ

iLOイベントログ

イベントログは、iLOファームウェアが記録した重要なイベントを記録したものです。

ログに記録されるイベントの例には、サーバーの停電やサーバーのリセットなどのサーバーイベントがあります。ログに記録されるその他のイベントには、ログイン、仮想電源イベント、ログのクリア、一部の構成変更などがあります。

iLOにより、パスワードの安全な暗号化、すべてのログインのトラッキング、およびログインに失敗したときのすべての記録の管理が可能となります。 認証失敗ログ設定により、認証失敗のログ記録条件を設定できます。イベントログは、DHCP環境での監査機能を向上させるために記録したエントリーごとにクライアント名を取得し、アカウント名、コンピューター名、およびIPアドレスを記録します。

イベントログがいっぱいになると、新しいイベントごとにログ内の一番古いイベントが上書きされます。

イベントログに表示される可能性があるエラーのリストについては、ご使用のサーバーのエラーメッセージガイドを参照してください。

サブトピック

イベントログの表示

CSVファイルへのイベントログの保存

イベントログのクリア

イベントログの表示

手順

1. ナビゲーションツリーで情報をクリックし、iLOイベントログタブをクリックします。
2. （オプション）ソート、検索、およびフィルター処理機能を使用して、ログのビューをカスタマイズします。
3. （オプション）イベントリストを更新するには、 をクリックします。
4. （オプション）イベントをクリックして、イベントの詳細ペインを表示します。

サブトピック

イベントログビューのコントロール

イベントログの詳細

イベントログのアイコン

イベントログイベントペインの詳細

イベントログビューのコントロール

イベントのソート

列でログテーブルをソートするには、列見出しをクリックします。

表示を昇順または降順に変更するには、列見出しをもう一度クリックするか、列の横にある矢印アイコンをクリックします。

イベントリストの更新

ログエントリーのリストを更新するには、 をクリックします。

イベントの検索

日付、イベントID、または説明テキストに基づいてイベントを検索するには、 をクリックしてから、検索ボックスにテ

キストを入力します。

イベントフィルター

ログフィルターにアクセスするには、 をクリックします。

- 深刻度によってフィルターを適用するには、深刻度メニューから重大度レベルを選択します。
- カテゴリでフィルタリングするには、カテゴリメニューで値を選択します。
- 表示されるイベントの日付と時刻を変更するには、時刻メニューで値を選択します。以下から選択します。
  - デフォルト表示 - UTC時間を表示します。
  - ローカル時刻表示 - iLO Webインターフェイスのクライアント時間を表示します。
  - ISO時刻表示 - UTC時間をISO 8601形式で表示します。
- 最終アップデート日でフィルタリングするには、最終アップデートメニューで値を選択します。
- フィルターをデフォルト値に戻すには、フィルターのリセットをクリックします。

イベントログの詳細

イベントログを表示すると、記録されたイベントの合計数がフィルターログアイコンの上に表示されます。

ログフィルターを適用すると、フィルター条件を満たすイベントの数がフィルターアイコンの下に表示されます。

イベントごとに、次の詳細が表示されます。

- ID - イベントのID番号。イベントは生成された順番で番号付けされます。

  デフォルトでは、ログはIDでソートされ、最新のイベントが先頭になります。工場出荷時設定へのリセットによりカウンターがリセットされます。
- 深刻度 - 検出されたイベントの重要性。
- 説明 - この説明によって、記録されたイベントの特性が提供されます。

  iLOファームウェアが前のバージョンにロールバックされると、より新しいファームウェアによって記録されたイベントについて、`不明なイベントタイプ`という説明が表示される場合があります。この問題は、サポートされる最新バージョンのファームウェアにアップデートするか、ログをクリアすることによって解決できます。
- 最終アップデート - このタイプの最新のイベントの発生日時。この値は、iLOファームウェアによって保存された日時に基づきます。

  イベントがアップデートされた日時をiLOファームウェアが認識しなかった場合は、値が`NOT SET`と表示されます。
- 回数 - このイベントが発生した回数（サポートされている場合）。

  通常、重大なイベントは発生するたびにログエントリーを生成します。これらのイベントが1つのログエントリーにまとめられることはありません。

  重要度が低いイベントが繰り返し発生する場合、これらのイベントは1つのログエントリーにまとめられ、iLOによって回数および最終アップデートの値がアップデートされます。

  各イベントタイプは定義された間隔を備えており、繰り返し発生するイベントの処理（統合するのかそれとも新しいイベントを記録するのか）はこの間隔によって決定されます。
- カテゴリ - イベントのカテゴリ。例：管理、構成、セキュリティ。

イベントログのアイコン

- クリティカル – イベントはサービスの消失（またはサービスの消失が予期されること）を示しています。すぐに対処する必要があります。
- 警告 – イベントは重大ですが、性能の低下を示してはいません。
- 情報 – イベントは背景情報を提供します。

イベントログイベントペインの詳細

- 初期アップデート – このタイプの最初のイベントの発生日時。この値は、iLOファームウェアによって保存された日時に基づきます。

  イベントが最初に発生した日時をiLOが認識しなかった場合は、`NOT SET`と表示されます。
- イベントクラス – イベントクラスの一意識別子。

  この値は16進数形式で表示されます。
- イベントコード – イベントクラス内のイベントの一意識別子。

  この値は16進数形式で表示されます。
- 推奨されるアクション – 障害状態に対する推奨されるアクションの簡単な説明。

> **注記:**
> 推奨されるアクションのテキストは静的です。イベントステータスが変更されても、削除またはアップデートされません。修正アクションが完了したら、推奨アクションを無視してかまいません。

CSVファイルへのイベントログの保存

手順

1. ナビゲーションツリーで情報をクリックし、iLOイベントログタブをクリックします。
2. csv をクリックします。

   CSVアウトプットウィンドウが表示されます。
3. 保存をクリックし、ブラウザーのプロンプトに従ってファイルを保存するか、ファイルを開きます。

イベントログのクリア

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーで情報をクリックし、iLOイベントログタブをクリックします。
2. 🗑 をクリックします。

   iLOが要求を確認するように求めます。

3. はい、クリアしますをクリックします。

   これまで記録されたすべての情報のログがクリアされます。この操作はイベントログに記録されます。

インテグレーテッドマネジメントログ

IMLは、サーバーで発生した履歴イベントの記録です。イベントはシステムROMや、iLOドライバーなどのサービスによって生成されます。ログに記録されたイベントには、ヘルスおよびステータス情報、ファームウェアアップデート、オペレーティングシステム情報、ROMベースのPOSTコードなど、サーバー固有の情報が含まれます。

IMLのエントリーが問題の診断や発生する可能性がある問題の特定に役立つ可能性があります。サービスの中断を防止するために、予防的処置が役立つ場合があります。

iLOはIMLを管理するので、サーバーが稼働していない場合でも、サポートされているブラウザーを使用してIMLを参照できます。サーバーが稼働していない場合にログを表示できるので、リモートホストサーバーの問題のトラブルシューティングに役立ちます。

IMLがいっぱいになると、新しいイベントごとにログ内の一番古いイベントが上書きされます。

サブトピック

IMLイベントタイプの例

- ファンのアクションとステータス
- 電源のアクションとステータス
- 温度ステータスと自動シャットダウンのアクション
- ドライブ障害
- ファームウェアフラッシュアクション
- Smart Storage Energy Packステータス
- ネットワークアクションとステータス

IMLの表示

手順

1. ナビゲーションツリーで情報をクリックし、インテグレーテッドマネジメントログタブをクリックします。
2. （オプション）ソート、検索、およびフィルター処理機能を使用して、ログのビューをカスタマイズします。
3. （オプション）イベントリストを更新するには、 をクリックします。

4. （オプション）イベントをクリックして、イベントの詳細ペインを表示します。

サブトピック

IMLビューのコントロール

イベントのソート

列でログテーブルをソートするには、列見出しをクリックします。

表示を昇順または降順に変更するには、列見出しをもう一度クリックするか、列の横にある矢印アイコンをクリックします。

イベントリストの更新

ログエントリーのリストを更新するには、 をクリックします。

イベントの検索

日付、イベントID、または説明テキストに基づいてイベントを検索するには、 をクリックしてから、検索ボックスにテキストを入力します。

イベントフィルター

ログフィルターにアクセスするには、 をクリックします。

- 深刻度でフィルタリングするには、深刻度リストから重大度レベルを選択します。
- クラスでフィルタリングするには、クラスリストからクラスを選択します。
- カテゴリでフィルタリングするには、カテゴリリストで値を選択します。
- 表示されるイベントの日付と時刻を変更するには、時刻メニューで値を選択します。以下から選択します。
  - デフォルト表示 - UTC時間を表示します。
  - ローカル時刻表示 - iLO Webインターフェイスのクライアント時間を表示します。
  - ISO時刻表示 - UTC時間をISO 8601形式で表示します。
- 最終アップデート日付でフィルタリングするには、最終アップデートメニューで値を選択します。
- フィルターをデフォルト値に戻すには、フィルターのリセットをクリックします。

IMLの詳細

IMLを表示すると、記録されたイベントの合計数がフィルターログアイコンの上に表示されます。

ログフィルターを適用すると、フィルター条件を満たすイベントの数がフィルターアイコンの下に表示されます。

イベントごとに、次の詳細が表示されます。

- **修復可能なイベント** - Webインターフェイスの左側の最初の列には、ステータスがクリティカルまたは警告の各イベントの隣にアクティブなチェックボックスが表示されます。このチェックボックスは、修復済みとしてマークするイベン

トを選択するために使用されます。

- ID - イベントのID番号。イベントは生成された順番で番号付けされます。

  デフォルトでは、ログはIDでソートされ、最新のイベントが先頭になります。工場出荷時設定へのリセットによりカウンターがリセットされます。

- 深刻度 - 検出されたイベントの重要性。
- クラス - UEFI、環境、またはシステムのリビジョンなど、発生したイベントの種類を特定します。
- 説明 - この説明によって、記録されたイベントの特性が提供されます。

  iLOファームウェアがロールバックされると、より新しいファームウェアによって記録されたイベントについて、`不明なイベントタイプ`という説明が表示される場合があります。この問題は、サポートされる最新バージョンのファームウェアにアップデートするか、ログをクリアすることによって解決できます。

- 最終アップデート - このタイプの最新のイベントの発生日時。この値は、iLOファームウェアによって保存された日時に基づきます。

  イベントがアップデートされた日時をiLOが認識しなかった場合は、値が`NOT SET`と表示されます。

- 回数 - このイベントが発生した回数（サポートされている場合）。

  通常、重大なイベントは発生するたびにログエントリーを生成します。これらのイベントが1つのログエントリーにまとめられることはありません。

  重要度が低いイベントが繰り返し発生する場合、これらのイベントは1つのログエントリーにまとめられ、iLOによって回数および最終アップデートの値がアップデートされます。

  各イベントタイプは定義された間隔を備えており、繰り返し発生するイベントの処理（統合するのかそれとも新しいイベントを記録するのか）はこの間隔によって決定されます。

- カテゴリ - イベントのカテゴリ。例：ハードウェア、ファームウェア、管理

IMLアイコン

- クリティカル - イベントはサービスの消失（またはサービスの消失が予期されること）を示しています。すぐに対処する必要があります。
- 警告 - イベントは重大ですが、性能の低下を示してはいません。
- 情報 - イベントは背景情報を提供します。
- 修正済み - イベントは修正アクションを行いました。

IMLイベントペインの詳細

- 初期アップデート - このタイプの最初のイベントの発生日時。この値は、iLOファームウェアによって保存された日時に基づきます。

  イベントが最初に発生した日時をiLOが認識しなかった場合は、`NOT SET`と表示されます。

- イベントクラス - イベントクラスの一意識別子。

  この値は16進数形式で表示されます。

- イベントコード - イベントクラス内のイベントの一意識別子。

  この値は16進数形式で表示されます。

- さらに詳しくは – ここに表示されるリンクをクリックすると、サポートされているイベントのトラブルシューティング情報にアクセスできます。
- 推奨されるアクション – 障害状態に対する推奨されるアクションの簡単な説明。

> **注記:**
> 推奨されるアクションのテキストは静的です。イベントステータスが変更されても、削除またはアップデートされません。修正アクションが完了するか、イベントに修正済みステータスが表示されたら、推奨アクションを無視してかまいません。

IMLエントリーの修正済みへの変更

前提条件

iLOの設定を構成する権限

このタスクについて

IMLエントリーのステータスをクリティカルまたは警告から修正済みに変更するには、この機能を使用します。

> **注記:**
> 修理済みとしてマークされたIMLエントリーでは、指定されたIMLイベントの重大度が修理済みに設定されるだけです。このプロセスでは、対応する修理済みの重大度のSNMPトラップまたはRedfishイベントは生成されません。
> たとえば、イベントのクリティカルの重大度が上書きされ、手動で修理済みに設定された場合、iLOでは障害が修理済みであるか、特定のサーバー環境のために手動で変更されたのかを特定できません。したがって、イベントが手動で修理済みとしてマークされている場合、iLOでは常にIMLが修理済み状態に変更されますが、それ以上のアラートは要求されません。

手順

1. 問題を調べて修正します。
2. ナビゲーションツリーで情報をクリックし、インテグレーテッドマネジメントログタブをクリックします。
3. ログエントリーを選択します。

   IMLエントリーを選択するには、IMLテーブルの最初の列のエントリーの横のチェックボックスをクリックします。IMLエントリーの横にあるチェックボックスが表示されない場合、エントリーを修復済みとしてマークすることはできません。
4. をクリックします。

   iLO Webインターフェイスが更新され、選択したログエントリーのステータスが修正済みに変化します。

IMLにメンテナンスノートを追加する

前提条件

iLO設定の構成権限

このタスクについて

メンテナンスノートを使用して、次のような作業に関するログエントリーを作成します。
- アップグレード
- システムバックアップ

- 定期的なシステムメンテナンス
- ソフトウェアインストール

手順

1. ナビゲーションツリーで情報をクリックし、インテグレーテッドマネジメントログタブをクリックします。
2.  をクリックします。

   メンテナンスノートを入力ウィンドウが開きます。
3. ログエントリーとして追加するテキストを入力し、OKをクリックします。

   入力できるテキストの最大長さは227バイトです。テキストを入力せずにメンテナンスノートを送信することはできません。

   メンテナンスクラスの情報ログエントリーがIMLに追加されます。

CSVファイルへのIMLの保存

手順

1. ナビゲーションツリーで情報をクリックし、インテグレーテッドマネジメントログタブをクリックします。
2.  をクリックします。

   CSVアウトプットウィンドウが表示されます。
3. 保存をクリックし、ブラウザーのプロンプトに従ってファイルを保存するか、ファイルを開きます。

IMLのクリア

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーで情報をクリックし、インテグレーテッドマネジメントログタブをクリックします。
2.  をクリックします。

   iLOが要求を確認するように求めます。
3. はい、クリアしますをクリックします。

   これまで記録されたすべての情報のログがクリアされます。この操作はIMLに記録されます。

セキュリティログ

セキュリティログは、iLOファームウェアによって記録されたセキュリティイベントのレコードを提供します。

ログに記録されるイベントの例には、セキュリティ構成の変更や、セキュリティコンプライアンスの問題などがあります。ログに記録されるその他のイベントには、ハードウェアへの侵入、メンテナンス、サービス拒否攻撃などがあります。

セキュリティログは、記録されたすべてのセキュリティイベントの集中的なビューを提供します。いくつかの同じイベントは、iLOイベントログまたはIMLにも含まれます。

セキュリティログがいっぱいになると、新しいイベントごとにログ内の一番古いイベントが上書きされます。

セキュリティログの表示

手順

1. ナビゲーションツリーで情報をクリックして、セキュリティログタブをクリックします。
2. （オプション）ソート、検索、およびフィルター処理機能を使用して、ログのビューをカスタマイズします。
3. （オプション）イベントリストを更新するには、 をクリックします。
4. （オプション）イベントをクリックして、イベントの詳細ペインを表示します。

セキュリティログビューのコントロール

イベントのソート

列でログテーブルをソートするには、列見出しをクリックします。

表示を昇順または降順に変更するには、列見出しをもう一度クリックするか、列の横にある矢印アイコンをクリックします。

イベントリストの更新

ログエントリーのリストを更新するには、 をクリックします。

イベントの検索

日付、イベントID、または説明テキストに基づいてイベントを検索するには、 をクリックしてから、検索ボックスにテキストを入力します。

イベントフィルター

ログフィルターにアクセスするには、 をクリックします。

- 深刻度でフィルタリングするには、深刻度リストから重大度レベルを選択します。
- クラスでフィルタリングするには、クラスリストからクラスを選択します。
- カテゴリでフィルタリングするには、カテゴリリストで値を選択します。
- 表示されるイベントの日付と時刻を変更するには、時刻メニューで値を選択します。以下から選択します。
  - デフォルト表示 - UTC時間を表示します。
  - ローカル時刻表示 - iLO Webインターフェイスのクライアント時間を表示します。
  - ISO時刻表示 - UTC時間をISO 8601形式で表示します。
- 最終アップデート日付でフィルタリングするには、最終アップデートメニューで値を選択します。
- フィルターをデフォルト値に戻すには、フィルターのリセットをクリックします。

セキュリティログの詳細

セキュリティログを表示すると、記録されたイベントの合計数がフィルターログアイコンの上に表示されます。

ログフィルターを適用すると、フィルター条件を満たすイベントの数がフィルターアイコンの下に表示されます。

イベントごとに、次の詳細が表示されます。

- ID - イベントのID番号。イベントは生成された順番で番号付けされます。

  デフォルトでは、ログはIDでソートされ、最新のイベントが先頭になります。工場出荷時設定へのリセットによりカウンターがリセットされます。
- 深刻度 - 検出されたイベントの重要性。
- クラス - UEFI、環境、またはシステムのリビジョンなど、発生したイベントの種類を特定します。

- 説明 – この説明によって、記録されたイベントの特性が提供されます。

  iLOファームウェアがロールバックされると、より新しいファームウェアによって記録されたイベントについて、`不明なイベントタイプ`という説明が表示される場合があります。この問題は、サポートされる最新バージョンのファームウェアにアップデートするか、ログをクリアすることによって解決できます。
- 最終アップデート – このタイプの最新のイベントの発生日時。この値は、iLOファームウェアによって保存された日時に基づきます。

  イベントがアップデートされた日時をiLOが認識しなかった場合は、値が`NOT SET`と表示されます。
- 回数 – このイベントが発生した回数（サポートされている場合）。

  通常、重大なイベントは発生するたびにログエントリーを生成します。これらのイベントが1つのログエントリーにまとめられることはありません。

  重要度が低いイベントが繰り返し発生する場合、これらのイベントは1つのログエントリーにまとめられ、iLOによって回数および最終アップデートの値がアップデートされます。

  各イベントタイプは定義された間隔を備えており、繰り返し発生するイベントの処理（統合するのかそれとも新しいイベントを記録するのか）はこの間隔によって決定されます。
- カテゴリ – イベントのカテゴリ。たとえば、セキュリティ、メンテナンス、または構成。

セキュリティログアイコン

- クリティカル – イベントはサービスの消失（またはサービスの消失が予期されること）を示しています。すぐに対処する必要があります。
- 警告 – イベントは重大ですが、性能の低下を示してはいません。
- 情報 – イベントは背景情報を提供します。

セキュリティログイベントペインの詳細

- 初期アップデート – このタイプの最初のイベントの発生日時。この値は、iLOファームウェアによって保存された日時に基づきます。

  イベントが最初に発生した日時をiLOが認識しなかった場合は、値が`NOT SET`と表示されます。
- イベントクラス – イベントクラスの一意識別子。

  この値は16進数形式で表示されます。
- イベントコード – イベントクラス内のイベントの一意識別子。

  この値は16進数形式で表示されます。
- 推奨されるアクション – 障害状態に対する推奨されるアクションの簡単な説明。

注記:

推奨されるアクションのテキストは静的です。イベントステータスが変更されても、削除またはアップデートされません。修正アクションが完了したら、推奨アクションを無視してかまいません。

CSVファイルへのセキュリティログの保存

手順

1. ナビゲーションツリーで情報をクリックして、セキュリティログタブをクリックします。
2. CSV をクリックします。

   CSVアウトプットウィンドウが表示されます。
3. 保存をクリックし、ブラウザーのプロンプトに従ってファイルを保存するか、ファイルを開きます。

セキュリティログのクリア

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーで情報をクリックして、セキュリティログタブをクリックします。
2. 🗑 をクリックします。

   iLOが要求を確認するように求めます。
3. はい、クリアしますをクリックします。

   これまで記録されたすべての情報のログがクリアされます。この操作はセキュリティログに記録されます。

Active Health System

Active Health Systemは、サーバーハードウェアとシステム構成の変化を監視し、記録します。

Active Health Systemは、以下の機能を提供します。

- 1,600を超えるシステムパラメーターの継続的なヘルス監視
- すべての構成変更のログの取得
- ヘルスおよびサービス通知の統合（正確なタイムスタンプ付き）
- アプリケーションのパフォーマンスに影響を与えないエージェントレスの監視

サブトピック

Active Health Systemのデータ収集

Active Health Systemでは、ユーザーの経営、財務、顧客、従業員、またはパートナーに関する情報を収集しません。

収集される情報の例を示します。

- サーバーモデルとシリアル番号
- プロセッサーのモデルと速度
- ストレージの容量と速度

- メモリの容量と速度
- ファームウェア/BIOSおよびドライバーのバージョンと設定

Active Health Systemは、サードパーティのエラーイベントログ活動（たとえば、OSを介して作成し、渡した内容）からOSデータを解析したり、変更したりしません。

Active Health Systemログ

Active Health Systemが収集したデータはActive Health Systemログに保存されます。データは、安全に記録され、オペレーティングシステムから分離され、しかも顧客データから独立しています。ホストのリソースは、Active Health Systemデータの収集およびロギングで消費されることはありません。

Active Health Systemログが満杯になると、ログ内の最も古いデータが新しいデータで上書きされます。

Active Health Systemログがダウンロードされ、サポート担当者に送信されて、担当者がお客様の問題の解決をサポートするのにかかる時間は5分以内です。

Active Health Systemデータをダウンロードし、Hewlett Packard Enterpriseに送信することで、お客様は、分析、技術的な解決、および品質改善のためにデータが使用されることに同意したものと見なされます。収集されるデータは、Privacy Statement（https://www.hpe.com/info/privacyに掲載されています）に従って管理されます。

ログをHPE InfoSight for Serversにアップロードして、ログデータを表示したり、有効な保証またはサポート契約に基づくサーバーのサポートケースを作成したりできます。詳しくは、次のWebサイトにあるHPE InfoSight for Serversのドキュメントを参照してください：https://www.hpe.com/support/infosight-servers-docs。

Active Health Systemログのダウンロード方法

Active Health Systemログをダウンロードするには、次の方法を使用できます。

- **iLO Webインターフェイス**–Active Health Systemログページから日付の範囲のログをダウンロードするか、ログ全体をダウンロードします。
- **iLOサービスポート**–サーバーの前面のiLOサービスポートにUSBフラッシュドライブを接続して、ログをダウンロードします。
- **cURLユーティリティ**–cURLコマンドラインツールを使用して、ログをダウンロードします。
- **Intelligent Provisioning** – 手順については、Intelligent Provisioningユーザーガイドを参照してください。
- **iLO RESTful APIおよびRESTfulインターフェイスツール** – 詳しくは、https://www.hpe.com/support/restfulinterface/docsを参照してください。

詳しくは

日付範囲を指定したActive Health Systemログのダウンロード
Active Health Systemログ全体のダウンロード
cURLを使用したActive Health Systemログのダウンロード
iLOサービスポート経由でのActive Health Systemログのダウンロード
Active Health Systemログ（iLOREST）のダウンロード

日付範囲を指定したActive Health Systemログのダウンロード

手順

1. iLO UIのナビゲーションツリーで情報をクリックし、Active Health Systemログタブをクリックします。

   Active Health Systemログのダウンロードが進行中の場合、ログにアクセスできません。

2. ログに含める日付の範囲を入力します。デフォルト値は7日間です。
   a. 開始ボックスをクリックします。

      カレンダーが表示されます。
   b. カレンダーで範囲の開始日を選択します。
   c. 終了ボックスをクリックします。

      カレンダーが表示されます。
   d. カレンダーで範囲の終了日を選択します。

   デフォルト値の範囲をリセットするには、↩ をクリックします。
3. （オプション）ダウンロードしたファイルに含める以下の情報を入力します。
   - サポートケース番号（最大14文字）
   - 連絡者名
   - 電話番号（最大39文字）
   - メールアドレス
   - 会社名

   入力した連絡先情報は、Hewlett Packard Enterpriseのプライバシーに関する声明に準拠して取り扱われます。この情報は、サーバーに保存されるログデータには記録されません。
4. ダウンロードをクリックします。
5. ファイルを保存します。
6. 開いているサポートケースがある場合は、ログファイルをメールでサポート技術者に送信できます。

   メールの件名は、次のように表記してください。CASE:〈ケース番号〉。

   25 MBを超えるファイルは、圧縮してFTPサイトにアップロードする必要があります。必要に応じて、FTPサイトについてHewlett Packard Enterpriseにお問い合わせください。
7. （オプション）ファイルをHPE InfoSight for Serversにアップロードします。

   HPE InfoSight for ServersでAnalyze Logsページにアクセスするには、Compute見出しの下のInfrastructure > Analyze Logsを選択します。

   詳しくは、次のWebサイトにあるHPE InfoSight for Serversユーザーガイドを参照してください：https://www.hpe.com/support/infosight-servers-docs

Active Health Systemログ全体のダウンロード

このタスクについて

Active Health Systemログ全体のダウンロードには、かなり時間がかかる場合があります。技術的な問題のためにActive Health Systemログをアップロードする必要がある場合、Hewlett Packard Enterpriseは、問題が発生した特定の日付範囲のログをダウンロードすることをお勧めします。

手順

1. ナビゲーションツリーで情報をクリックして、Active Health Systemログタブをクリックします。

   Active Health Systemログのダウンロードが進行中の場合、ログにアクセスできません。
2. アドバンスト設定を表示をクリックします。

3. （オプション）ダウンロードしたファイルに含める以下の情報を入力します。
   - サポートケース番号（最大14文字）
   - 連絡者名
   - 電話番号（最大39文字）
   - メールアドレス
   - 会社名

   入力した連絡先情報は、Hewlett Packard Enterpriseのプライバシーに関する声明に準拠して取り扱われます。この情報は、サーバーに保存されるログデータには記録されません。
4. すべてのログをダウンロードをクリックします。
5. ファイルを保存します。
6. 開いているサポートケースがある場合は、ログファイルをメールでサポート技術者に送信できます。

   メールの件名は、次のように表記してください。CASE:〈ケース番号〉。

   25 MBを超えるファイルは、圧縮してFTPサイトにアップロードする必要があります。必要に応じて、FTPサイトについてHewlett Packard Enterpriseにお問い合わせください。
7. （オプション）ファイルをHPE InfoSight for Serversにアップロードします。

   HPE InfoSight for ServersでAnalyze Logsページにアクセスするには、Compute見出しの下のInfrastructure > Analyze Logsを選択します。

   詳しくは、次のWebサイトにあるHPE InfoSight for Serversユーザーガイドを参照してください：https://www.hpe.com/support/infosight-servers-docs

cURLを使用したActive Health Systemログのダウンロード

このタスクについて

手順

1. cURLをインストールします。
2. cURLは以下のWebサイトからダウンロードできます。http://curl.haxx.se/
3. コマンドウィンドウを開きます。
4. `curl`ディレクトリに変更します。
5. 以下の例に似たコマンドを実行します。

   重要:

   これらのコマンドを入力するときは、スペースやその他のサポートされていない文字を使用しないでください。

   コマンドライン環境でアンパサンドなどの特殊文字が必要な場合、この文字の前にエスケープ文字を付ける必要があります。詳しくは、このコマンドライン環境のドキュメントを参照してください。

   - 日付範囲を指定してActive Health Systemログをダウンロードする場合：

     ```
     curl "https://<iLO_IP_address>/ahsdata/ahs.ahs?from=<yyyy-mm-dd>&to=
     <yyyy-mm-dd>" -k -v -u <username>:<password> -o <filename>.ahs
     ```

   - 過去7日間のActive Health Systemログをダウンロードし、Hewlett Packard Enterpriseサポートケース番号をログ

ヘッダーに追加する場合：

```
curl "https://<iLO_IP_address>/ahsdata/ahs.ahs?days=<number_of_days>
&case_no=<number>" -k -v -u <username>:<password> -o <filename>.ahs
```

- 過去7日間のActive Health Systemログをダウンロードし、ケース番号と連絡先情報を含める場合：

```
curl "https://<iLO_IP_address>/ahsdata/ahs.ahs?days=<number_of_days>
&case_no=<number>&contact_name=<name>&phone=<phone_number>&email=
<email_address>&co_name=<company>" -k -v -u <username>:<password>
-o <filename>.ahs
```

- Active Health Systemログ全体をダウンロードする場合：

```
curl "https://<iLO_IP_address>/ahsdata/ahs.ahs?downloadAll=1" -k -v
-u <username>:<password> -o <filename>.ahs
```

6. ファイルは指定したパスに保存されます。
7. コマンドウィンドウを閉じます。
8. （オプション）開いているサポートケースがある場合は、ログファイルをメールでサポート技術者に送信できます。

   メールの件名は、次のように表記してください。CASE:〈ケース番号〉。

   25 MBを超えるファイルは、圧縮してFTPサイトにアップロードする必要があります。必要に応じて、FTPサイトについてHewlett Packard Enterpriseにお問い合わせください。
9. （オプション）ログファイルをHPE InfoSight for Serversにアップロードして、ログデータを表示したり、有効な保証またはサポート契約に基づくサーバーのサポートケースを作成したりできます。

   詳しくは、次のWebサイトにあるHPE InfoSight for Serversのドキュメントを参照してください：https://www.hpe.com/support/infosight-servers-docs。

サブトピック

iLOでのcURLコマンドの使用法

iLOでのcURLコマンドの使用法

cURLを使用してActive Health Systemログを抽出する場合、コマンドコンポーネントには以下が含まれます。

オプション

`<iLO IP address>`

iLO IPアドレスを指定します。

`from=<yyyy-mm-dd>&to=<yyyy-mm-dd>`

ログの開始と終了の日付範囲を示します。`year-month-day`の形式で日付を入力してください。たとえば、2017/07/29は、2017-07-29と入力します。

`days=<number of days>`

今日の日付から過去`<number of days>`日間のログファイルをダウンロードすることを指定します。

`downloadAll=1`

ログ全体をダウンロードすることを指定します。

`-k`

HTTPS警告が無視されるように指定します。これにより、接続が安全でなくなる可能性があります。

`-v`

指定すると、詳細な出力が表示されます。

-u <username>:<password>

iLOユーザーアカウント認証情報を指定します。

-o <filename>.ahs

出力ファイルの名前とパスを指定します。

case_no=<HPE support case number>

ログヘッダーに追加するHewlett Packard Enterpriseサポートケース番号を指定します。

ダウンロードしたログに連絡先情報を追加するためのオプション

phone=<phone number>

ログヘッダーに追加する電話番号を指定します。

email=<email address>

ログヘッダーに追加する電子メールアドレスを指定します。

contact_name=<contact name>

ログヘッダーに追加する連絡先の名前を指定します。

co_name=<company name>

ログヘッダーに会社名を挿入します。

Active Health Systemログ（iLOREST）のダウンロード

前提条件

- RESTfulインターフェイスツールがインストールされている。
- iLOの設定を構成する権限

手順

1. RESTfulインターフェイスツールを起動します。

   ```
   ilorest
   ```
   と入力します。

3. iLOシステムにログインします。

   ```
   iLOrest > login iLO host name or IP address -u iLO user name -p iLO password
   ```

4. 手順3でログインしたサーバーのActive Health Systemログをダウンロードします。

   - 直近の7日間のログをダウンロードするには、次のようなコマンドを入力します。

     ```
     iLOrest > serverlogs --selectlog=AHS --directorypath=ディレクトリパス
     ```

   - 指定された期間のログをダウンロードするには、次のようなコマンドを入力します。

     ```
     iLOrest > serverlogs --selectlog=AHS --directorypath=ディレクトリパス
     --customiseAHS="from=YYYY-MM-DD&&to=YYYY-MM-DD"
     ```

   - すべてのActive Health Systemログをダウンロードするには、次のようなコマンドを入力します。

     ```
     iLOrest > serverlogs --selectlog=AHS --downloadallahs --directorypath=ディレクトリパス
     ```

   ログは次のファイル名でダウンロードされます。`HPE_サーバーのシリアル番号_YYYYMMDD.ahs`

5. （オプション）開いているサポートケースがある場合は、ログファイルをメールで**gsd_csc_case_mngmt@hpe.com**に送信

できます。

メールの件名は、次のように表記してください。CASE:〈ケース番号〉。

25 MBを超えるファイルは、圧縮してFTPサイトにアップロードする必要があります。必要に応じて、FTPサイトについてHewlett Packard Enterpriseにお問い合わせください。

6. （オプション）ログファイルをHPE InfoSight for Serversにアップロードして、ログデータを表示したり、有効な保証またはサポート契約に基づくサーバーのサポートケースを作成したりできます。

   詳しくは、次のWebサイトにあるHPE InfoSight for Serversのドキュメントを参照してください：https://www.hpe.com/support/infosight-servers-docs。

サブトピック

iLOREST serverlogコマンドの使用法

iLOREST serverlogコマンドの使用法

`--selectlog=AHS`

Active Health Systemログタイプで処理することを指定します。

`--directorypath=`*`ディレクトリパス`*

出力ファイルのパスを指定します。

`--customiseAHS="from=`*`YYYY-MM-DD`*`&&to=`*`YYYY-MM-DD`*`"`

ログの開始と終了の日付範囲を示します。`year-month-day`の形式で日付を入力してください。たとえば、2017/07/29は、2017-07-29と入力します。

`--downloadallahs`

ログ全体をダウンロードすることを指定します。

詳しくは、RESTfulインターフェイスツールのドキュメントを参照してください。

Active Health Systemログの消去

前提条件

- iLOの設定を構成する権限
- Active Health Systemログを有効は、Active Health Systemログページのアドバンスト設定を表示セクションで有効になっています。

このタスクについて

ログファイルが壊れた場合、またはログを消去して再開する場合は、Active Health Systemログを消去してください。

手順

1. ナビゲーションツリーで情報をクリックして、Active Health Systemログタブをクリックします。

   ダウンロードのログが進行中の場合、Active Health Systemログにアクセスできません。

2. アドバンスト設定を表示をクリックします。
3. ログをクリアセクションまでスクロールしてから、クリアをクリックします。
4. 要求を確認するメッセージが表示されたら、はい、クリアしますをクリックします。

ログがクリア中であることがiLOによって通知されます。

5. iLOをリセットします。

   一部のActive Health Systemデータは iLOの起動中にのみログに記録されるため、iLOをリセットする必要があります。この手順を行うことにより、データー式が確実にログに記録されます。

6. サーバーを再起動します。

   サーバーの起動時にオペレーティングシステムの名前とバージョンなど、一部の情報がログに記録されるため、サーバーの再起動が必要です。この手順を行うことにより、データー式が確実にログに記録されます。

iLOとシステム診断の使用

サブトピック

iLOセルフテスト結果の表示

iLOの再起動（リセット）

アプライアンスのイメージの再構築

システム診断

iLOセルフテスト結果の表示

このタスクについて

iLOセルフテスト結果セクションには、テスト名、ステータス、ノートを含め、内部のiLO診断テストの結果が表示されます。

どのようなテストが実行されるかは、システムによって異なります。すべてのシステムですべてのテストが実行されるわけではありません。システムで実行されるテストを確認するには、診断ページで一覧を参照してください。

テストに関してステータスが報告されていない場合、そのテストは表示されません。

手順

1. ナビゲーションツリーで情報をクリックし、診断タブをクリックします。
2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

サブトピック

iLOセルフテストの詳細

iLOセルフテストの種類

iLOセルフテストの詳細

iLOヘルス

　iLOヘルスステータス。iLO診断セルフテストを組み合わせた結果に基づいています。

セルフテスト

テスト済みの機能。

ステータス

テストのステータス。

- パス – テストが成功しました。
- 劣化 – テストで問題が検出されました。再起動、ファームウェアやソフトウェアのアップデート、またはサービスが必要になる場合があります。

  セルフテストでこのステータスが報告された場合は、IMLをチェックして詳細を確認してください。

  サポートケースを開始する場合は、Active Health Systemログをダウンロードし、このログを含めます。

  Secure Elementのステータスが劣化の場合は、サポートに連絡し、AHSと注記の詳細を提供してください。
- 情報 – テストされたシステムに関する補足データが注記列に提供されます。

注記

注記列にテストの補足情報が含まれる場合があります。

テストによっては、他のシステムプログラマブルロジック（システムボードPALなど）またはPower Management Controllerのバージョンがこの列に示されます。

iLOセルフテストの種類

どのようなテストが実行されるかは、システムによって異なります。すべてのシステムですべてのテストが実行されるわけではありません。実行される可能性があるテストを次に示します。

- Cryptographic – セキュリティ機能をテストします。
- NVRAM data – 不揮発性の構成データ、ログ、および設定を保持するサブシステムをテストします。
- Embedded Flash – 構成、プロビジョニング、およびサービス情報を保存できるシステムの状態をテストします。
- Host ROM – BIOSをチェックし、管理プロセッサーと比較してBIOSのバージョンが古くないかどうかを確認します。
- Supported Host – 管理プロセッサーのファームウェアをチェックし、サーバーハードウェアに対してファームウェアのバージョンが古くないかどうかを確認します。
- Power Management Controller – 電力測定値、消費電力上限、および電力管理に関連する機能をテストします。
- CPLD – サーバーのプログラマブルハードウェアをテストします。
- EEPROM – 製造工程で割り当てられた基本iLOプロパティを保存しているハードウェアをテストします。
- Secure Element – 製造工程で割り当てられた基本iLOプロパティを保存しているハードウェアをテストします。

  サポートされているプラットフォームに応じて、Secured ElementまたはEEPROMが表示されます。
- **ASIC Fuses** – iLOチップに組み込まれていることが予想されるデータと既知のデータパターンを比較して、チップが適切に製造され、動作設定が許容範囲を満たしていることを確認します。

iLOの再起動（リセット）

場合によっては、iLOを再起動しなければならないことがあります。たとえば、iLOがブラウザーに応答しない場合などです。

リセットオプションはiLOの再起動を開始します。構成が変更されることはありませんが、iLOファームウェアへのアクティブな接続がすべて終了します。ファームウェアファイルのアップロードが進行中の場合、アップロードは強制的に終了します。ファームウェアのフラッシュが進行中の場合、このプロセスが終了するまでiLOをリセットできません。

これらのどのリセット方法も利用できないか、予想どおりに機能しない場合は、サーバーの電源を切り、電源装置を切断します。

サブトピック

iLOの再起動（リセット）方法

iLOのWebインターフェイス

診断ページのリセットボタンを使用します。

iLO6構成ユーティリティ

UEFIシステムユーティリティのiLO6構成ユーティリティを使用します。

iLO RESTful API

詳しくは、次のWebサイトを参照してください。https://www.hpe.com/support/restfulinterface/docs

コマンドラインとスクリプトツール

詳しくは、HPE iLO 6スクリプティング/コマンドラインガイドを参照してください。

IPMI

詳しくは、HPE iLO 6 IPMIユーザーガイドを参照してください。

サーバーのUID

サポートされているサーバーのサーバーUIDボタンを使用して、 正常な再起動またはハードウェアの再起動を開始します。

この方法は、他のリセット方法が使用できない、または期待どおりに機能しない場合に使用できます。

Webインターフェイスを使用したiLOプロセッサーの再起動（リセット）

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーで情報をクリックし、診断タブをクリックします。
2. リセットをクリックします。

   iLOが要求を確認するように求めます。

   サーバーが電源投入時セルフテスト（POST）プロセスにある場合は、リセットすると予期しない動作（iLOが工場出荷時のデフォルト設定にリセットされるなど）が発生する可能性があることをiLOが警告します。iLOリセットの完了後に、システムの再起動が必要になる場合があります。
3. はい、iLOをリセットしますをクリックします。

   iLOがリセットされ、ブラウザー接続が閉じます。

iLOのiLO6構成ユーティリティを使用した再起動（リセット）

前提条件

iLOの設定を構成する権限

手順

1. （オプション）サーバーにリモートアクセスする場合、iLOリモートコンソールセッションを開始します。
2. サーバーを再起動するかまたは電源を入れます。
3. サーバーのPOST画面でF9キーを押します。

   UEFIシステムユーティリティが起動します。
4. システムユーティリティ画面で、システム構成、iLO 6構成ユーティリティの順にクリックします。
5. iLOをリセットメニューではいを選択します。

   iLO6構成ユーティリティからリセットを確認するように求められます。
6. OKをクリックします。
7. iLOがリセットされ、すべてのアクティブな接続が終了します。iLOをリモートで管理している場合は、リモートコンソールセッションが自動的に終了します。

   iLOをリセットすると、次のサーバー再起動までiLO6構成ユーティリティを使用できなくなります。
8. ブートプロセスを再開します。
   a. （オプション）iLOをリモート管理している場合は、iLOのリセットが完了するのを待ってから、iLOリモートコンソールを起動します。

      以前のセッションのUEFIシステムユーティリティが開いています。
   b. メインメニューが表示されるまでEscキーを押します。
   c. システムを終了して再起動をクリックします。
   d. 要求の確認を求めるメッセージが表示されたら、OKをクリックしてユーティリティを終了し、通常のブートプロセスを再開します。

サーバーのUIDボタンによる正常なiLOの再起動の実行

このタスクについて

サポートされているサーバーのUIDボタンを使用して、適切なiLOの再起動を開始できます。

正常なiLOリブートを開始すると、iLOファームウェアがiLOのリブートを開始します。

正常なiLOのリブートを開始しても構成が変更されることはありませんが、iLOへのすべてのアクティブ接続が終了します。ファームウェアファイルのアップロードが進行中の場合、その処理が終了します。ファームウェアのフラッシュが進行中の場合、このプロセスが終了するまでiLOをリブートできません。

手順

正常なiLOリブートを開始するには、UIDボタンを5～9秒間押し続けます。

UIDボタン/LEDが青色で毎秒4回点滅し、正常なiLOリブートが実行中であることを示します。

サーバーのUIDボタンによるハードウェアiLOの再起動の実行

このタスクについて

サポートされているサーバーのUIDボタンを使用して、iLOハードウェアの再起動を開始できます。

ハードウェアiLOの再起動を開始すると、サーバーハードウェアによってiLOの再起動が開始されます。

手順

ハードウェアiLOの再起動を開始するには、UIDボタンを10秒以上押し続けます。

> **注意:**
> ハードウェアiLOの再起動を開始しても構成が変更されることはありませんが、iLOへのすべてのアクティブ接続が終了します。ファームウェアのフラッシュが進行中の場合、フラッシュデバイスでデータの破損が発生する可能性があります。フラッシュデバイスでデータの破損が発生した場合は、セキュアリカバリまたはiLOネットワークのフラッシュエラーリカバリ機能を使用します。ハードウェアiLOの再起動中にデータの損失やNVRAMの破損が発生する可能性があります。
> トラブルシューティングの他のオプションが使用可能な場合は、ハードウェアの再起動を開始しないでください。

UIDボタン/LEDが青色で毎秒8回点滅し、ハードウェアiLOの再起動が実行中であることを示します。

アプライアンスのイメージの再構築

前提条件

- ログイン権限
- リモートコンソール権限
- 仮想電源およびリセット権限
- 仮想メディア権限

このタスクについて

アプライアンスハードウェアに直接アクセスできない場合、iLOを使用して、サポートされているアプライアンス向けにイメージの再構築プロセスを開始することができます。

> **警告:**
> アプライアンスのイメージの再構築を行うと、イメージの再構築プロセスが完了するまでオフラインになります。

手順

1. iLO仮想メディア機能を使用して、アプライアンスのソフトウェアイメージを含むUSBデバイスを接続します。

   イメージには、HPE OneViewまたはHPEイメージストリーマーソフトウェアが含まれている必要があります。
2. ナビゲーションツリーで情報をクリックし、診断タブをクリックします。
3. 再構築 をクリックします。

   iLOが要求を確認するように求めます。
4. はい、アプライアンスのイメージを再イメージをクリックします。

詳しくは

仮想ドライブ（クライアントPC上の物理ドライブ）の使用

システム診断

以下のシステム診断機能が利用できます。機能のサポートは、サーバーモデルとiLOのバージョンによって異なります。サーバーでサポートされていない機能は、診断ページに表示されません。

- NMIを生成する
- 工場デフォルト設定にリストアする
- デフォルトシステム設定をリストアする
- UEFIシリアルデバッグメッセージをActive Health Systemログに保存する

重要:
複数のシステム診断操作を同時に開始しないでください。同時に複数の操作を実行すると、予期しない結果が生じる可能性があります。

サブトピック

NMIの生成

システムセーフモードでの起動

インテリジェント診断モードで起動

工場デフォルト設定のリストア

システムデフォルト設定のリストア

POST中のUEFIシリアルデバッグメッセージのActive Health Systemログへの保存

NMIの生成

前提条件

仮想電源およびリセット権限

このタスクについて

NMIを生成機能で、オペレーティングシステムをデバッグのために停止できます。

この機能は、システムが起動せず、OS前の状態（例えば、POST中）でハングする場合に役立ちます。NMIを使用すると、システムROM例外ハンドラーが有効になり、問題が発生したコードのトレースをキャプチャーできます。

注意:
診断とデバッグのツールとしてのNMIの生成は、主にオペレーティングシステムが使用不能になった場合に使用します。通常のサーバーの運用では、NMIを使用しないでください。NMIの生成ではオペレーティングシステムは適切にはシャットダウンされず、オペレーティングシステムがクラッシュします。このため、サービスとデータは失われます。NMIを生成ボタンは、OSが正常に動作せず、経験のあるサポート組織がNMIを推奨する極端なケースのみに使用してください。

手順

1. ナビゲーションツリーで情報をクリックし、診断タブをクリックします。
2. システム診断を表示をクリックします。
3. NMIを生成をクリックします。

   iLOが要求を確認するように求めます。

△ **注意:**

NMIを生成すると、データ損失やデータ破壊の原因となる可能性があります。

4. はい、続行しますをクリックします。

   iLOは、NMIが送信されたことを確認します。

システムセーフモードでの起動

前提条件

- ホストBIOS構成権限
- 仮想電源およびリセット権限
- iLOの設定を構成する権限
- サーバープラットフォームでこの機能がサポートされている。
- サーバーの電源がオフになっている。

このタスクについて

システムセーフモードオプションを使用して、最小構成でシステムを起動して、ブートプロセッサーとメモリの1つのチャネルが正しく動作しているかどうかを確認します。他のすべてのデバイスは、構成から迅速かつ安全に削除されます。

手順

1. ナビゲーションツリーで情報をクリックし、診断タブをクリックします。
2. システム診断を表示をクリックします。
3. セーフモードで起動をクリックします。

   iLOが要求を確認するように求めます。
4. はい、続行しますをクリックします。

   セーフモードでサーバーの起動に成功すると、ブートプロセッサーと1つのメモリチャネルが正常に動作していることが示されます。

   このアクションの結果はIMLに記録されます。

インテリジェント診断モードで起動

前提条件

- ホストBIOS構成権限
- 仮想電源およびリセット権限
- iLOの設定を構成する権限
- サーバープラットフォームでこの機能がサポートされている。
- サーバーの電源がオフになっている。

このタスクについて

サポートされているシステムでインテリジェント診断モードに入ると、POST中のブート障害が自動的に診断されます。

手順

1. ナビゲーションツリーで情報をクリックし、診断タブをクリックします。
2. システム診断を表示をクリックします。
3. インテリジェント診断モードで起動をクリックします。

   iLOが要求を確認するように求めます。
4. はい、続行しますをクリックします。

   システムがインテリジェント診断モードであることがiLOから通知されます。

   ブート障害の原因を特定するために、サーバーは一連の再起動を開始します。原因が識別されると、影響を受けるデバイスが無効化され、ブートプロセスが再開されます。

   注記:
   このプロセスは、完了までに長時間かかることがあります。ブート障害の原因を特定するために、複数のサーバーの再起動が必要になる場合があります。インテリジェント診断モードに入ったら、プロセスを中断せずに完了させます。

   ステータスを監視するには、サーバーのPOST画面を確認します。

   このアクションの結果はIMLに記録されます。
5. 問題が検出された場合は、必要な手順を実行して問題を解決してください。

工場デフォルト設定のリストア

前提条件

- ホストBIOS構成権限
- 仮想電源およびリセット権限
- iLOの設定を構成する権限
- サーバープラットフォームでこの機能がサポートされている。
- サーバーの電源がオフになっている。

このタスクについて

すべてのBIOS構成設定を工場デフォルト値にリセットするには、工場デフォルト設定のリストアオプションを使用します。

このプロセスにより、ブート構成、セキュアブートのセキュリティキー（セキュアブートが有効な場合）、構成された日付時刻の設定など、すべてのUEFI不揮発性変数が削除されます。

一部のUEFI設定を保持するオプションを使用するには、デフォルトのシステム設定の復元オプションを検討してください。

この機能を使用すると、不揮発性メモリに保存されたiLO IPアドレスおよびiLO設定が保持されます。

手順

1. （オプション）UEFIシステムユーティリティでユーザーデフォルトの保存オプションをはい、保存します。に設定します。

   このオプションを有効にすると、工場デフォルト設定をリストアするときに、現在のBIOS設定がデフォルト設定として使用されます。

   詳しくは、UEFIシステムユーティリティのユーザーガイドを参照してください。
2. ナビゲーションツリーで情報をクリックし、診断タブをクリックします。

3. システム診断を表示をクリックします。
4. 工場デフォルト設定のリストアをクリックします。

   iLOにより、要求の確認を求められます。また、セキュアブートの設定など、以前に構成した設定がデフォルト値にリセットされることが警告されます。
5. はい、続行しますをクリックします。

   UEFI不揮発性変数がデフォルト値にリセットされ、サーバーが再起動します。

   ステータスを監視するには、サーバーのPOST画面を確認します。

   このアクションの結果はIMLに記録されます。

システムデフォルト設定のリストア

前提条件

- ホストBIOS構成権限
- 仮想電源およびリセット権限
- iLOの設定を構成する権限
- サーバープラットフォームでこの機能がサポートされている。
- サーバーの電源がオフになっている。

このタスクについて

システムデフォルト設定のリストアオプションを使用すると、すべてのBIOS構成設定がデフォルト値にリセットされ、サーバーは再起動します。

このオプションを選択すると、以下を除くすべてのプラットフォーム設定をリセットします。

- セキュアブートBIOS設定
- 日付と時刻の設定
- プライマリおよび冗長のROMの選択（サポートされる場合）
- オプションカードやiLOなどの他のエンティティは、個別にリセットする必要があります。

  この機能を使用すると、不揮発性メモリに保存されたiLO IPアドレスおよびiLO設定が保持されます。

手順

1. （オプション）UEFIシステムユーティリティでユーザーデフォルトの保存オプションをはい、保存します。に設定します。

   このオプションを有効にすると、デフォルトのシステム設定をリストアするときに、現在のBIOS設定がデフォルト設定として使用されます。

   詳しくは、UEFIシステムユーティリティのユーザーガイドを参照してください。
2. ナビゲーションツリーで情報をクリックし、診断タブをクリックします。
3. システム診断を表示をクリックします。
4. システムデフォルト設定のリストアをクリックします。

   iLOにより、要求の確認を求められ、以前に構成した設定がデフォルト値にリセットされることが警告されます。
5. はい、続行しますをクリックします。

   BIOS構成設定がデフォルト値にリセットされ、サーバーが再起動します。

ステータスを監視するには、サーバーのPOST画面を確認します。

このアクションの結果はIMLに記録されます。

POST中のUEFIシリアルデバッグメッセージのActive Health Systemログへの保存

前提条件

- サーバーが、電源投入時セルフテスト（POST）状態にある。

このタスクについて

通常のサーバー操作中、UEFIシリアルログメッセージは自動的にActive Health Systemログに保存されます。これらのメッセージは、Active Health Systemログをトラブルシューティングに使用する場合に役立ちます。サーバーが停止するか起動に失敗した場合、UEFIシリアルデバッグメッセージは自動的に送信されません。この手順を使用して、UEFIシリアルデバッグメッセージをActive Health Systemログに1回手動で保存します。UEFIシリアルデバッグメッセージを再度保存するには、この手順を繰り返します。

この機能は、サーバーのPOST中にのみ使用できます。POSTが完了すると、キャプチャーボタンは使用できなくなります。

手順

1. ナビゲーションツリーで情報をクリックし、診断タブをクリックします。
2. キャプチャーをクリックします。

   UEFIシリアルデバッグメッセージがActive Health Systemログに保存されたことをiLOが通知します。

全般的なシステム情報の表示

サブトピック

ヘルスサマリー情報の表示

プロセッサー情報の表示

メモリ情報の表示

ネットワーク情報の表示

デバイスインベントリの表示

ストレージ情報の表示

ヘルスサマリー情報の表示

このタスクについて

ヘルスサマリーページには、監視対象サブシステムおよびデバイスのステータスが表示されます。このページの情報は、サーバー構成によって異なります。

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、最後の電源オフ時のものです。ヘルス情報は、サーバーの電源が入っており、POSTが完了している場合にのみアップデートされます。

手順

1. ナビゲーションツリーでシステム情報をクリックします。

2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

3. （オプション）サポートされるサブシステムとデバイスタイプの関連ページに移動するには、サブシステムおよびデバイスリストで値の名前をクリックします。

   液冷モジュールを備えたシステムでファンまたは液冷モジュールの値をクリックすると、電力 & 温度ページが開き、ファン&冷却モジュールタブが表示されます。液冷モジュールが存在しないかサポートされていない場合、タブ名はファンになります。

   Agentless Management Serviceなどの一部のサブシステムおよびデバイスタイプには、関連ページがありません。

サブトピック

冗長ステータス

サブシステムおよびデバイスのステータス

サブシステムおよびデバイスステータスの値

冗長ステータス

以下の項目に関する冗長ステータスが表示されます。

- ファンの冗長化
- 電源

  システムで使用可能なパワードメインに基づいて、冗長ステータスが表示されます。システムに複数のパワードメインがある場合、システムの冗長性とGPUの冗長性のステータスが表示されます。（このオプションは、サポートされているサーバーでのみ使用できます）。
- 冗長液冷（サポート対象サーバーのみ）

サブシステムおよびデバイスのステータス

以下の項目に関するステータス情報が表示されます。

- Agentless Management Service
- BIOS/ハードウェアヘルス
- ファン
- 液冷（サポート対象サーバーのみ）
- メモリ
- ネットワーク
- 電源装置（非ブレードサーバーのみ）

  システムで使用可能な電源装置ドメインに基づいて、システムドメインとGPUドメインが表示されます（このオプションは、サポートされているサーバーでのみ使用できます）。
- プロセッサー
- ストレージ

- 温度
- Smart Storage Energy Pack（サポート対象のサーバーのみ）

サブシステムおよびデバイスステータスの値

- 冗長化–デバイスまたはサブシステム用のバックアップコンポーネントがあります。
- OK–デバイスまたはサブシステムは正常に動作しています。
- 非冗長化–デバイスまたはサブシステム用のバックアップコンポーネントがありません。
- 利用不可能–コンポーネントは利用できないか、インストールされていません。
- 劣化–デバイスまたはサブシステムの機能が低下しています。

  iLOでは、一致しない電源装置が取り付けられている場合、電源装置のステータスは劣化となります。

  非冗長ファンまたは電源装置を備えたサーバーを起動する場合、システムヘルスステータスはOKと表示されます。システムの起動時に冗長ファンまたは電源装置で障害が発生すると、ファンまたは電源装置を交換するまでシステムヘルスステータスは劣化になります。
- 冗長化障害–デバイスまたはサブシステムは動作していません。
- 障害–デバイスまたはサブシステムの1つまたは複数のコンポーネントが動作していません。
- クリティカル – デバイスまたはサブシステムの1つまたは複数のコンポーネントが動作していません。
- その他 – 詳しくは、このステータスを報告するコンポーネントのシステム情報ページに移動してください。
- 不明 – iLOファームウェアがデバイスステータス情報を受信していません。サーバーの電源がオフになっているときにiLOをリセットした後、一部のサブシステムでステータスが不明と表示されます。サーバーの電源がオフになっているとき、iLOはこれらのサブシステムのステータスをアップデートできません。
- 未インストール–サブシステムまたはデバイスがインストールされていません。

プロセッサー情報の表示

このタスクについて

プロセッサー情報ページは、空いているプロセッサースロット、各スロットに装着されたプロセッサーの種類、プロセッサーサブシステムの概要を表示します。

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、最後の電源オフ時のものです。ヘルス情報は、サーバーの電源が入っており、POSTが完了している場合にのみアップデートされます。

手順

ナビゲーションツリーでシステム情報をクリックし、プロセッサータブをクリックします。

サブトピック

プロセッサーの詳細

プロセッサーの詳細

プロセッサーごとに、次の情報が表示されます。

- プロセッサー名 – プロセッサーの名前。
- プロセッサーステータス – プロセッサーのヘルスステータス。
- プロセッサー速度 – プロセッサーの速度。
- 実行テクノロジー – プロセッサーのコアおよびスレッドに関する情報。
- メモリテクノロジー – プロセッサーのメモリ機能。
- 内部L1キャッシュ – L1キャッシュサイズ。
- 内部L2キャッシュ – L2キャッシュサイズ。
- 内部L3キャッシュ – L3キャッシュサイズ。

メモリ情報の表示

このタスクについて

メモリ情報ページには、システムメモリの概要が表示されます。サーバーの電源が入っていない場合は、AMPデータが使用できないため、POST実行時に存在するメモリモジュールのみが表示されます。

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、最後の電源オフ時のものです。ヘルス情報は、サーバーの電源が入っており、POSTが完了している場合にのアップデートされます。

手順

1. ナビゲーションツリーでシステム情報をクリックし、メモリタブをクリックします。

   メモリページには、以下の詳細が表示されます。

   - アドバンストメモリプロテクション（AMP）
   - メモリの概要
   - 物理メモリ

2. （オプション）デフォルトでは、物理メモリテーブルに空のメモリソケットは表示されません。空のメモリスロットを表示するには、空きのメモリスロットを表示をクリックします。空のメモリスロットが表示されているときにそれらを非表示にするには、空きのメモリスロットを隠すをクリックします。

   このオプションは、空のスロットがない場合は表示されません。

3. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

4. （オプション）追加のメモリ詳細を表示するには、メモリモジュールを選択します。

   メモリ詳細ペインが表示されます。

サブトピック

アドバンストメモリプロテクションの詳細

メモリの概要

物理メモリ詳細

メモリ詳細ペイン（物理メモリ）

アドバンストメモリプロテクションの詳細

アドバンストメモリプロテクションは、サポートされているプラットフォームでのみ使用できます。

AMPモードステータス

AMPサブシステムのステータスです。

- 不明/その他 – システムがAMPをサポートしていない、またはマネジメントソフトウェアがステータスを判定できません。
- 非保護 – システムはAMPをサポートしていますが、機能が無効になっています。
- プロテクト済み – システムはAMPをサポートしています。機能は有効ですが、動作してはいません。
- 劣化 – システムは保護されていましたが、AMPが保留中です。したがって、AMPはもう使用できません。
- DIMM ECC – システムは、DIMM ECCのみによって保護されます。
- ミラーリング – システムはミラーモードのAMPで保護されています。DIMMの不具合は検出されていません。
- ミラーリング劣化 – システムはミラーモードのAMPで保護されています。1つまたは複数のDIMMの不具合が検出されています。
- オンラインスペア – システムはホットスペアモードのAMPで保護されています。DIMMの不具合は検出されていません。
- オンラインスペア劣化 – システムはホットスペアモードのAMPで保護されています。1つまたは複数のDIMMの不具合が検出されています。
- RAID-XOR – システムはXORメモリモードのAMPで保護されています。DIMMの不具合は検出されていません。
- RAID-XOR劣化 – システムはXORメモリモードのAMPで保護されています。1つまたは複数のDIMMの不具合が検出されています。
- アドバンストECC – システムはアドバンストECCモードのAMPで保護されています。
- アドバンストECC劣化 – システムはアドバンストECCモードのAMPで保護されています。1つまたは複数のDIMMの不具合が検出されています。
- ロックステップ – システムはロックステップモードのAMPで保護されています。
- ロックステップ劣化 – システムはロックステップモードのAMPで保護されています。1つまたは複数のDIMMの不具合が検出されています。
- A3DC – システムはA3DCモードのAMPで保護されています。
- A3DC劣化 – システムはA3DCモードのAMPで保護されています。1つまたは複数のDIMMの不具合が検出されています。

構成済みAMPモード

アクティブなAMPモード。以下のモードがサポートされます。

- なし/不明 – マネジメントソフトウェアがAMPフォールトトレランスを判定できない、またはシステムがAMP用に構成されていません。
- オンラインスペア – 起動時にメモリの単一のスペアバンクが確保されています。多数のECCエラーが発生すると、スペアメモリがアクティブになり、エラーが発生したメモリは無効になります。
- ミラーリング – システムはミラーメモリ用に構成されています。オンラインスペアメモリの場合の1つのメモリバンクとは異なり、ミラー化されたメモリではすべてのメモリバンクが二重化されています。多数のECCエラーが発生すると、スペアメモリがアクティブになり、エラーが発生したメモリは無効になります。
- RAID-XOR – システムは、XORエンジンを使用してAMP用に構成されています。
- アドバンストECC – システムはアドバンストECCエンジンを使用してAMP用に構成されています。
- ロックステップ – システムは、ロックステップエンジンを使用してAMP用に構成されています。

- オンラインスペア（ランクスペアリング） - システムはオンラインスペアランクAMP用に構成されています。
- オンラインスペア（チャネルスペアリング） - システムはオンラインスペアランクAMP用に構成されています。
- インターソケットミラーリング - システムは2つのプロセッサーまたはボードのメモリの間でミラー化されたIntersocket AMP用に構成されています。
- イントラソケットミラーリング - システムは1つのプロセッサーまたはボードのメモリの間でミラー化されたIntrasocket AMP用に構成されています。
- A3DC - システムは、A3DCエンジンを使用してAMP用に構成されています。

サポートされるAMPモード

- RAID-XOR - システムは、XORエンジンを使用してAMP用に構成することができます。
- デュアルボードミラーリング - システムは、デュアルメモリボード構成で、ミラー化されたアドバンストメモリ保護用に構成することができます。ミラーメモリは、同じメモリボード上のメモリまたは2番目のメモリボード上のメモリと交換することができます。
- シングルボードミラーリング - システムは、単一のメモリボードで、ミラー化されたアドバンストメモリ保護用に構成することができます。
- アドバンストECC - システムは、アドバンストECC用に構成することができます。
- ミラーリング - システムは、ミラー化されたAMP用に構成することができます。
- オンラインスペア - システムは、オンラインスペアAMP用に構成することができます。
- ロックステップ - システムは、ロックステップAMP用に構成することができます。
- オンラインスペア（ランクスペアリング） - システムはOnline Spare Rank AMP用に構成できます。
- オンラインスペア（チャネルスペアリング） - システムはOnline Spare Channel AMP用に構成できます。
- インターソケットミラーリング - システムは2つのプロセッサーまたはボードのメモリの間でミラー化されたIntersocket AMP用に構成できます。
- イントラソケットミラーリング - システムは1つのプロセッサーまたはボードのメモリの間でミラー化されたIntrasocket AMP用に構成できます。
- A3DC - このシステムはA3DC AMP用に構成できます。
- なし - このシステムは、AMP用に構成することができません。

メモリの概要

メモリの概要セクションには、搭載され、POST実行時に正常に動作したメモリの概要が表示されます。

位置

メモリボード、カートリッジ、またはライザーが搭載されているスロットまたはプロセッサー。表示される可能性がある値は、以下のとおりです。

- システムボード - 個別のメモリボードスロットはありません。すべてのDIMMがマザーボードに取り付けられています。
- ボード<番号> - 使用できるメモリボードスロットがあります。すべてのDIMMがメモリボードに取り付けられています。
- プロセッサー<番号> - メモリDIMMが搭載されているプロセッサー。
- ライザー<番号> - メモリDIMMが搭載されているライザー。

合計メモリスロット

メモリモジュールスロットの数。

トータルメモリ

メモリの容量。これには、オペレーティングシステムが認識するメモリ、およびスペア、ミラー、またはXOR構成に使用されるメモリが含まれます。

動作周波数

メモリが動作する周波数。

物理メモリ詳細

物理メモリセクションには、ホストに搭載され、POST実行時に正常に動作していた、ホスト上の物理メモリモジュールが表示されます。メモリモジュールが取り付けられていない位置も示されます。各種の耐障害メモリ構成により、実際のメモリインベントリが、POSTの実行時に検出されたものから変化する場合があります。システムに多数のメモリモジュールが搭載されている場合は、一部のモジュール位置しか表示されない場合があります。

ソケットロケーター

メモリモジュールが搭載されているスロットまたはプロセッサー。

ステータス

メモリモジュールのステータスおよびモジュールが使用中かどうか。表示される可能性がある値は、以下のとおりです。

- 追加済 未使用 – DIMMが追加されましたが、未使用です。
- 構成エラー – DIMMに構成エラーがあります。
- 劣化 – DIMMステータスが低下しています。
- 不一致 – DIMMタイプが一致していません。
- 予想されたが不明 – DIMMは予想されていますが、欠落しています。
- 良好、使用中 – DIMMは正しく機能しており、使用中です。
- 良好、一部使用 – DIMMは正しく機能しており、一部使用中です。
- マップアウトエラー – トレーニングに失敗したため、DIMMはマップから解除されています。
- マップアウト構成 – 構成エラーのため、DIMMがマップから解除されています。
- 未装着 – DIMMが存在しません。
- 未サポート – DIMMはサポートされていません。
- その他 – DIMMステータスは、標準のステータス定義のいずれにも当てはまりません。
- 装着、スペア – DIMMが存在し、スペアとして使用されています。
- 装着、未使用 – DIMMが存在し、使用されていません。
- 不明 – DIMMステータスは不明です。
- 更新済 未使用 – DIMMはアップグレードされましたが、使用されていません。

サイズ

メモリモジュールのサイズ。

サポートされる最大周波数

メモリモジュールでサポートされる最大周波数。

テクノロジー

メモリモジュールのテクノロジー。表示される可能性がある値は、以下のとおりです。

- 不明 - メモリのテクノロジーを判定できません。
- N/A - メモリモジュールはありません。
- SDRAM（シンクロナスダイナミックRAM）
- RDIMM（レジスタ付きメモリモジュール）
- UDIMM（レジスタなしメモリモジュール）
- LRDIMM（負荷低減メモリモジュール）

メモリ詳細ペイン（物理メモリ）

製造者

メモリモジュールの製造者。

部品番号

メモリモジュールの部品番号。

この値は、HPEメモリモジュールについてのみ表示されます。

シリアル番号

メモリモジュールのシリアル番号。

この値は、空のメモリスロットについては表示されません。

タイプ

搭載されたメモリのタイプ。表示される可能性がある値は、以下のとおりです。

- その他 - メモリタイプを判定できません。
- ボード - メモリモジュールは（モジュール式でなく）システムボードまたはメモリ拡張ボードに固定されています。
- DDR5
- N/A - メモリモジュールはありません。

ランク

メモリモジュール内のランクの数。

エラー訂正

メモリモジュールが使用するエラー訂正のタイプ。

データ幅ビット

メモリモジュールのデータ幅（ビット単位）。

バス幅ビット

メモリモジュールのバス幅（ビット単位）。

チャネル

メモリモジュールが接続されているチャネル番号。

メモリコントローラー

メモリコントローラー番号。

CPUソケット

メモリモジュールのソケット番号。

メモリスロット

メモリモジュールのスロット番号。

状態

メモリの状態。

ベンダー

メモリベンダー名。ベンダー名が不明な場合、値N/Aが表示されます。

ベンダーID

メモリベンダーID。

Armed

NVDIMM-Nの現在のバックアップ準備状態（使用できる場合）。

最後の操作

最後の操作のステータス（NVDIMMのみ）。

メディア寿命

メディアの残りの寿命の割合（NVDIMMのみ）。

ネットワーク情報の表示

このタスクについて

サーバーの電源が切れている場合、NIC情報ページのヘルスステータス情報は、最後に電源が切れた時点の情報になります。ヘルス情報は、サーバーの電源が入っており、POSTが完了している場合にのみアップデートされます。

このページのすべてのデータセットを表示するには、AMSがインストールされていて実行中であることを確認します。AMSがインストールされ、サーバー上で実行されている場合にのみ、サーバーのIPアドレス、アドインのネットワークアダプター、サーバーのNICステータスが表示されます。

このページの情報は、iLOにログインしたときにアップデートされます。データを更新するには、iLOからログアウトしてログインし直します。

手順

1. ナビゲーションツリーでシステム情報をクリックし、ネットワークタブをクリックします。
2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。
3. （オプション）このページで情報を展開するにはすべてを展開をクリックし、情報を折りたたむにはすべて閉じるをクリックします。

サブトピック

物理ネットワークアダプター

論理ネットワークアダプター

物理ネットワークアダプター

内蔵と追加のNICおよびファイバーチャネルアダプター

このセクションには、サーバー内の内蔵と追加のNICおよびファイバーチャネルアダプターに関する次の情報が表示されます。

アダプター番号

アダプター番号。例えば、アダプター1、アダプター2など。

位置

システムボード上のアダプターの位置。

ファームウェア

インストールされているアダプターのファームウェアのバージョン（該当する場合）。この値は、システムNIC（内蔵および直立型）の場合にのみ表示されます。

ステータス

NICステータス。

- Windowsサーバー：
  - NICがネットワークに接続され、正しく機能している場合、iLOにはステータスOKが表示されます。
  - NICがネットワークに接続されていなかった場合、iLOはステータスを不明と表示します。
  - NICがネットワークに接続されていた場合、iLOはステータスをリンクダウンと表示します。
  - 複数のNICによる構成で、コンポーネントが故障しているがシステムはまだ機能している場合、iLOはステータスを劣化と表示します。
  - NICが障害を報告した場合、iLOによってステータスクリティカルが表示されます。
- Linuxサーバー：
  - システムが起動したときにイーサーネットケーブルがネットワークスイッチに接続されている場合、デフォルトのステータスはOKであり、リンクステータスがiLOに表示されます。
  - システムが起動したときにイーサーネットケーブルがネットワークスイッチに接続されていない場合、iLOはステータスを不明と表示します。システムが起動した後にイーサーネットケーブルが接続されると、ステータスが表示されます。
  - 複数のNICによる構成で、コンポーネントが故障しているがシステムはまだ機能している場合、iLOはステータスを劣化と表示します。
  - NICが障害を報告した場合、iLOによってステータスクリティカルが表示されます。
- VMwareサーバー：
  - iLOがNICポートと通信できない場合、ステータスを不明と表示します。
  - NICドライバーが`link_down`のステータスを報告する場合、iLOはステータスをダウンと表示します。
  - NICドライバーが`link_up`のステータスを報告する場合、iLOはステータスをOKと表示します。
  - 複数のNICによる構成で、コンポーネントが故障しているがシステムはまだ機能している場合、iLOはステータスを劣化と表示します。
  - NICが障害を報告した場合、iLOによってステータスクリティカルが表示されます。

注記: 複雑なNIC（イーサーネット、FCoE、iSCSIなどの複数のポート機能を備えたNIC）の場合、アダプターのステータスは、物理ポートのステータスとそのポートで実行されている機能のステータスを示します。いずれかのポートで実行されている機能がスイッチによって構成されていない場合、またはファイバーチャネルファブリックがダウンしている場合、個々の物理ポートのステータスが OKの場合でも、アダプターのステータスは 劣化を示している可能性があります。

ポート

構成されているネットワークポート。この値は、システムNIC（内蔵および直立型）の場合にのみ表示されます。

MACアドレス

ポートのMACアドレス。

ステータス

ポートのステータス。

表示される可能性がある値は、OK、障害、不明、およびリンクダウンです。

チーム/ブリッジ

ポートがNICチーミング用に構成されている場合、論理ネットワークアダプターを形成する物理ポートの間で構成されているリンクの名前。この値は、システムNIC（内蔵および直立型）の場合にのみ表示されます。

ファイバーチャネルホストバスアダプターまたはコンバージドネットワークアダプター

ファイバーチャネルのホストバスアダプターまたはコンバージドネットワークアダプターに関する、次の情報が表示されます。

- 物理ポート - 物理ネットワークのポート番号。
- WWNN - ポートのワールドワイドノード名。
- WWPN - ワールドワイドポート名。
- ステータス - ポートのステータス。

ブートの進行状況とブートターゲット

DCI接続が使用可能な場合は、以下の情報が表示されます。

- ポート - 構成済み仮想ポート番号。
- ブート進行中 - ブートの現在のステータス。
- **ブートターゲット**
  - WWPN - ワールドワイドポート名。
  - LUN ID - 論理ユニット番号ID。

論理ネットワークアダプター

このセクションには、NICチーミングを使用して1つの論理ネットワーク接続に2つ以上のポートを搭載しているネットワークアダプターに関する以下の情報が表示されます。

- アダプター名 - 論理ネットワークアダプターを形成する物理ポートの間で設定されているリンクの名前。
- MACアドレス - 論理ネットワークアダプターのMACアドレス。
- IPアドレス - 論理ネットワークアダプターのIPアドレス。
- ステータス - 論理ネットワークアダプターのステータス。

各論理ネットワークアダプターを形成するポートに関する、次の情報が表示されます。

- メンバー - 論理ネットワークアダプターを形成する各ポートに割り当てられた一連の番号。
- MACアドレス - 物理アダプターポートのMACアドレス。
- ステータス - 物理アダプターポートのステータス。

デバイスインベントリの表示

このタスクについて

デバイスインベントリページには、サーバーにインストールされたデバイスに関する情報が表示されます。このページに表示されるデバイスには、たとえば、取り付けられているアダプター、PCIデバイス、SATAコントローラー、Smartストレージバッテリなどがあります。

サーバーの電源が切れている場合、このページのヘルスステータス情報は、最後に電源が入った時点の情報になります。へ

ルス情報は、サーバーの電源が入っており、POSTが完了している場合にのみアップデートされます。

業界標準の管理仕様に準拠していない古いアダプターでは、アダプターのファームウェアバージョン、部品番号、シリアル番号、およびステータスを取得するために、Agentless Management Service（AMS）が必要です。

フィールド交換可能ユニット（FRU）EEPROMをサポートしているアダプターでは、iLOが製品名や部品番号などの静的アダプターの詳細を取得します。これらの値は、IPMIプラットフォーム管理FRU情報ストレージ定義の仕様に従ってフォーマットされます。

手順

1. ナビゲーションツリーでシステム情報をクリックし、デバイスインベントリタブをクリックします。
2. （オプション）デフォルトでは、空のスロットがデバイスインベントリテーブルで非表示になっています。空のスロットを表示するには、空きのスロットを表示をクリックします。空のスロットが表示されているときにそれらを非表示にするには、空きのスロットを隠すをクリックします。

   このオプションは、空のスロットがない場合は表示されません。
3. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。
4. （オプション）追加のスロット詳細を表示するには、テーブル内のデバイスをクリックします。

   スロット詳細ペインが表示されます。

サブトピック

デバイスインベントリの詳細

スロットの詳細ペイン

デバイスステータスの値

MCTP検出の構成

MCTP工場出荷時リセットの開始

詳しくは

Agentless ManagementとAMS

デバイスインベントリの詳細

- MCTP検出 - サーバーについて、この機能が有効になっているか無効になっているか。
- 位置 - デバイスの取り付け位置。
- 製品名 - デバイスの製品名。

  通常、iLOは、FRU EEPROMからこの値を取得します（製品情報領域フォーマット地域、製品名の値）。

  一部のアダプターでは、この値は専用アダプターのインターフェイスを通じて取得されます。
- 製品のバージョン - デバイスの製品のバージョン。

  通常、iLOは、FRU EEPROMからこの値を取得します（製品情報地域フォーマット地域、製品のバージョンの値）。

  一部のアダプターでは、この値は専用アダプターのインターフェイスを通じて取得されます。
- ファームウェアバージョン - インストールされているアダプターのファームウェアバージョン。

  iLOでは、複数の方法を使用してこのアダプター固有情報を取得できます。

  UEFIデバイスドライバーインターフェイスをサポートしているアダプターの場合、この値を取得するための基本的な方

法はUEFIです。

- コンポーネントの完全性ステータス - デバイスのSPDM認証ステータス。
- ステータス - デバイスステータスの値。

  不明という値が表示された場合は、次を意味します。

  - iLOが、デバイスの初期化を完了していない。
  - デバイスでステータスを提供できない（レガシーチップセットSAS/SATAコントローラーなど）。
  - Agentless ManagementとAgentless Management Serviceが、このデバイスに関する情報を提供できない。

  ネットワークアダプターの不明なステータスの値について詳しくは、ネットワーク情報ページのドキュメントを参照してください。

  ストレージデバイスの不明なステータスの値について詳しくは、ストレージ情報ページのドキュメントを参照してください。

詳しくは

MCTP検出の構成
ネットワーク情報の表示
ストレージ情報の表示

スロットの詳細ペイン

デバイスインベントリテーブルの行をクリックすると、スロットの詳細ペインに詳細情報が表示されます。

表示される値は、選択したデバイスタイプによって異なります。リストされた値をすべて表示しないデバイスタイプもあります。

- 製品部品番号 - アダプターベンダーのプライマリ部品番号。

  通常、iLOは、FRU EEPROMからこの値を取得します（製品情報領域フォーマット地域、製品部品/モデル番号の値）。

  部品番号がサーバーモデルごとに異なる内蔵グラフィックスデバイスに依存している場合は、各種ありが表示されます。

  ストレージコントローラーに接続されたバックプレーンについては、N/Aが表示されます。

- アセンブリ番号 - アダプターベンダーのスペア部品番号（存在する場合）。

  アダプターベンダーのスペア部品番号が存在しない場合、iLOは、FRU EEPROMからこの値を取得します（ボード情報領域フォーマット地域、ボード部品番号の値）。

  ストレージコントローラーに接続されたバックプレーンについては、N/Aが表示されます。

- シリアル番号 - アダプターのシリアル番号。

  通常、iLOは、FRU EEPROMからこの値を取得します（製品情報領域フォーマット地域、製品シリアル番号の値）。

  内蔵デバイスに対しては、通常、N/Aが表示されます。

- MCTPステータス - MCTP検出が有効または無効かどうかを示します。
- スロットの詳細
  - タイプ - スロットタイプ（PCIe、MXM、SATAなど）、または別の業界標準のスロットタイプ。
  - バス幅 - スロットのバス幅。
  - 長さ - スロットの長さ。
  - 特性 - スロットに関する情報。例えば、電圧やその他のサポートに関する情報です。

スロットの詳細の値について詳しくは、System Management BIOS（SMBIOS）参照仕様のシステムスロット（タイプ9）を参照してください。

- セグメント（PCIeデバイスのみ） – PCI構成中にBIOSによって割り当てられたPCIセグメント。その他すべてのデバイスタイプに対しては、FFhまたはN/Aが表示されます。
- バス（PCIeデバイスのみ） – PCI構成中にBIOSによって割り当てられたPCIバス。その他すべてのデバイスタイプに対しては、FFhまたはN/Aが表示されます。
- デバイス（PCIeデバイスのみ） – PCI構成中にBIOSによって割り当てられたPCIデバイス。その他すべてのデバイスタイプに対しては、FFhまたはN/Aが表示されます。
- 機能（PCIeデバイスのみ） – PCI構成中にBIOSによって割り当てられたPCI機能。その他すべてのデバイスタイプに対しては、FFhまたはN/Aが表示されます。
- 分岐されたデバイスピアのインスタンス – 分岐をサポートするデバイスの分岐の詳細。分岐されたデバイスピアにインスタンスは、デバイスが分岐されているかどうかと分岐のインスタンスを示します。

詳しくは

MCTP検出の構成

デバイスステータスの値

デバイスインベントリページでは、次のステータスの値を使用します。

- 有効 – デバイスが有効であり、ヘルスステータスはOKです。
- 未サポートCPU – デバイスのスロットをサポートするCPUが取り付けられていません。
- N/A – デバイスが取り付けられていません。
- 有効 – デバイスが有効であり、ヘルスステータスはクリティカルです。
- 有効 – デバイスが有効であり、ヘルスステータスは警告です。
- 不明 – iLOファームウェアがデバイスステータスに関するデータを受信していません。
- 無効 – デバイスが無効になっています。
- 未サポート – デバイスはSPDM（Security Protocol and Data Model）認証をサポートしていません。
- 成功 – デバイスのSPDM認証が成功しました。
- 障害 – デバイスのSPDM認証が失敗しました。

MCTP検出の構成

前提条件

iLOの設定を構成する権限

このタスクについて

MCTPは、サーバーにインストールされているオプションに直接通信するためにiLOが使用する業界標準テクノロジーです。MCTP検出は、デフォルトで有効です。サーバーまたは個々のアダプターに対してMCTP検出を無効にすると、問題のあるオプションをトラブルシューティングできます。例えば、アダプターが動作しない場合は、MCTP検出を一時的に無効にすると、サーバーを操作しながら問題を調査できます。無効にしたMCTP検出を再び有効にする唯一の方法は、MCTP工場出荷時リセットを実行することです。MCTP工場出荷時リセットを実行すると、サーバースロットおよびすべてのアダプタースロットに対するMCTP検出が有効になります。

サーバーのMCTP検出を無効にすると、すべてのアダプタースロットについて自動的に無効になります。

Hewlett Packard Enterpriseでは、サポート担当者が推奨しない限り、MCTP検出を無効にしないことをお勧めします。

警告:

- HPE OneViewによって管理されているサーバーのMCTP検出を無効にすると、無効にしたデバイスからHPE OneViewにアクセスできなくなります。
- サーバーのMCTP検出を無効にすると、iLOは、内蔵NIC、Smartアレイ、メモリ、CPU、およびオプションアダプターなどのコンポーネントのステータス情報の監視や表示を行いません。
- MCTP検出が無効になっている場合は、パフォーマンス設定、パフォーマンス監視、ワークロードパフォーマンスアドバイザーの各ページは使用できません。

手順

1. ナビゲーションツリーでシステム情報をクリックし、デバイスインベントリタブをクリックします。
2. 検出をクリックします。

   検出設定ページが開きます。
3. サーバースロットおよびすべてのアダプタースロットのMCTP検出を無効にするには、MCTP検出を無効に設定します。
4. 選択したアダプタースロットのMCTP検出を無効にするには、デバイステーブルの1つまたは複数のMCTPオプションを無効に設定します。
5. 適用をクリックします。

   iLOによって、MCTP検出を再度有効にするにはMCTPの出荷時リセットが必要であることが通知されます。
6. OKをクリックします。

MCTP工場出荷時リセットの開始

前提条件

iLO設定の構成権限

このタスクについて

MCTP検出がサーバーまたはサーバーのアダプタースロットに対して無効になっている場合、これを再度有効にする唯一の方法は、MCTP工場出荷時リセットを実行することです。この手順を実行しても、iLOまたはサーバーはリセットされません。

手順

1. ナビゲーションツリーでシステム情報をクリックし、デバイスインベントリタブをクリックします。
2. 検出をクリックします。

   検出設定ページが開きます。
3. MCTP工場出荷時リセットをクリックします。

   iLOによって、MCTP工場出荷時リセットを行うとすべてのデバイスでMCTPが有効になるという警告が表示され、要求を確認するように求められます。
4. はいをクリックします。

   MCTP工場出荷時リセットが開始されます。

   プロセスが完了すると、MCTP検出がすべてのデバイスで有効になります。

ストレージ情報の表示

このタスクについて

サーバーの電源がオフの場合、ストレージ情報ページのシステムのステータス情報は、最後の電源オフ時のものです。ステータス情報は、サーバーの電源が入っており、POSTが完了している場合にのみアップデートされます。

ストレージ情報ページのすべてのデータセットを表示するには、AMSがインストールされていて実行中であることを確認します。AMSがインストールされ、サーバー上で実行されている場合にのみ、SAS/SATAコントローラーの情報が表示されます。

このページに表示される情報は、ご使用のストレージ構成によって異なります。一部のストレージ構成では、各カテゴリの情報は表示されません。

このページには、ファイバーチャネルアダプターの一覧は表示されません。ファイバーチャネルアダプターに関する情報を表示するには、ナビゲーションツリーでシステム情報をクリックし、ネットワークタブをクリックします。

手順

1. ナビゲーションツリーでシステム情報をクリックし、ストレージタブをクリックします。
2. （オプション）すべてのデータを展開するにはすべてを展開 ↙↗ をクリックし、すべてのデータを折りたたむにはすべて閉じる ↗↙ をクリックします。
3. （オプション）コンポーネントの詳細を展開または折りたたむには、次のアイコン、› または⌄ をクリックします。
4. （オプション）コンポーネントの詳細を表示するには、リストされているコンポーネントをクリックします。

   詳細ペインが開き、追加情報が表示されます。
5. （オプション）NVMeまたはSATAドライブの物理ドライブインジケーターLEDステータスを変更するには、物理ドライブインジケーターLEDアイコン⊙ をクリックします。

   この機能は、サポート対象のサーバーでのみ使用できます。

   この機能を使用するには、iLOの設定を構成する権限が必要です。

   LEDステータスをオンまたはオフに変更できます。
6. （オプション）NVMeまたはSATAドライブの電源をオンまたはオフにするには、ドライブ電源ボタン機能を使用します。

   この機能は、サポート対象のサーバーでのみ使用できます。

   この機能を使用するには、iLOの設定を構成する権限が必要です。

サブトピック

サポート対象のストレージコンポーネント

サポートされるストレージ製品

ストレージ詳細

ステータスの値と定義

ドライブの電源の管理

詳しくは

ネットワーク情報の表示

サポート対象のストレージコンポーネント

ストレージ情報ページには、以下のストレージコンポーネントに関する次の情報が表示されます。

- Smartアレイコントローラー、ドライブエンクロージャー、接続されているボリューム、およびそれらのボリュームを構

成する物理ドライブ。

iLOでは、合計256の物理ドライブと合計256のボリュームを監視できます。

- 直接接続ストレージを管理するHewlett Packard Enterpriseおよびサードパーティ製のストレージコントローラー、および接続された物理ドライブ。

  直接接続ストレージのタイプ、SATA、NVMe、およびRDE対応デバイスがサポートされています。表示される情報は、ストレージタイプによって異なります。

サポートされるストレージ製品

- HPE ML/DLサーバーM.2 SSD対応キット
- HPEデュアル8 GB MicroSD EM USBキット（Windowsのみ）
- NVMeドライブ
- HPE NS204i-t Gen10 Plusブートコントローラー
- HPE SR932i-p Gen11コントローラー
- HPE SR416ie-m Gen11コントローラー
- HPE E208e-p SR Gen10コントローラー
- HPE MR416i-p Gen10 Plusコントローラー
- HPE MR216i-p Gen10 Plusコントローラー
- HPE MR416i-p Gen11コントローラー
- HPE MR416i-o Gen11コントローラー
- HPE MR408i-o Gen11コントローラー
- HPE MR216i-p Gen11コントローラー
- HPE MR216i-o Gen11コントローラー
- AHCI SATAコントローラー
- Intel VROC 8.0

ストレージ詳細

ストレージ情報ページには、Smartアレイおよび直接接続ストレージに関する以下の詳細が表示されます。

注記:
表示される情報は、ストレージタイプによって異なります。一部のストレージタイプでは、リストされている一部プロパティが含まれないことがあります。

サブトピック

コントローラー

ボリューム

ドライブ

コントローラー

コントローラーセクションには、各コントローラーに関する次の詳細が表示されます。

- 位置 – サーバー内のコントローラーの位置。
- ステータス – コントローラーのハードウェアヘルスとコントローラーの現在の状態の組み合わせ。表示される値は、ステータスアイコン（OK、クリティカル、または警告）と、詳細情報を提供するテキストを示します。

  ヘルスと現在の状態の値と定義について詳しくは、ステータスの値と定義を参照してください。
- モデル
- 合計ボリューム数 – コントローラーによって管理されるドライブ内のボリュームの数。
- 合計ドライブ数 – コントローラーによって管理されるドライブの数。

コントローラーを選択すると、コントローラー詳細ペインが開き、詳細情報が表示されます。

コントローラー詳細ペイン

コントローラー詳細ペインには、選択したコントローラーに関する詳細が表示されます。

（オプション）コントローラー詳細ペインにすべてのデータまたは一部のデータを表示するには、すべて表示または一部を表示をクリックします。

ボリューム

ボリュームセクションには、ボリュームごとに次の詳細が表示されます。

- 名前
- ステータス – ヘルスと現在の状態の値と定義について詳しくは、ステータスの値と定義を参照してください。
- 容量
- フォールトトレランス

ボリュームは、Smart Storage Administratorソフトウェアで構成しないと、このページに表示されません。

ボリュームを選択すると、ボリューム詳細ペインが開き、詳細情報が表示されます。

ボリューム詳細ペイン

ボリューム詳細ペインには、選択したボリュームに関する詳細が表示されます。

（オプション）ボリューム詳細ペインにすべてのデータまたは一部のデータを表示するには、すべて表示または一部を表示をクリックします。

ドライブ

ドライブセクションには、各ドライブについて次の詳細が表示されます。

- 位置 – ドライブのポート、ボックス、およびベイ番号
- ステータス – ヘルスと現在の状態の値と定義について詳しくは、ステータスの値と定義を参照してください。
- 容量

- メディアタイプ

ドライブを選択すると、ドライブ詳細ペインが開き、詳細情報が表示されます。

ドライブ詳細ペイン

ドライブ詳細ペインには、選択したドライブに関する次の詳細が表示されます。

- インジケーターLED – LEDステータス（オンまたはオフ）。 をクリックして、LEDステータスを変更できます。この機能は、NVMeとSATAドライブでのみ使用できます。

  この機能を使用するには、iLOの設定を構成する権限が必要です。

- ドライブ電源 – 現在のドライブの電源の状態（オン、オフ、または開始中）。

  電源オンまたは電源オフボタンを使用して、NVMeおよびSATAドライブのドライブ電源を制御できます。

  （オプション）ドライブ詳細ペインにすべてのデータまたは一部のデータを表示するには、すべて表示または一部を表示をクリックします。

ドライブエンクロージャー（Smartアレイのみ）

ドライブエンクロージャーセクションには、各エンクロージャーに関する次の詳細が表示されます。

- 位置 – エンクロージャーのポート番号とボックス番号。
- ステータス – ヘルスと現在の状態の値と定義について詳しくは、ステータスの値と定義を参照してください。
- ドライブベイ – ドライブベイの数。

一部のエンクロージャーでは表示されるプロパティの一部しか含まれておらず、一部のストレージ構成ではドライブエンクロージャーが含まれていません。

エンクロージャーを選択すると、ドライブエンクロージャー詳細ペインが開き、詳細情報が表示されます。

ドライブエンクロージャー詳細ペイン

ドライブエンクロージャー詳細ペインには、ドライブエンクロージャーに関する詳細が表示されます。

（オプション）ドライブエンクロージャー詳細ペインにすべてのデータまたは一部のデータを表示するには、すべて表示または一部を表示をクリックします。

注記: 言語翻訳機能は、詳細ペインには適用されません。

ステータスの値と定義

可能性のあるヘルス値は次のとおりです。

- OK – 正常を示します
- クリティカル – ただちに注意を要するクリティカルな状態が存在します。
- 警告 – 注意を必要とする状態が存在します。

指定可能な状態値は、以下のとおりです。

- 有効 – デバイスが有効になっています。
- 無効 – デバイスが無効になっています。

- テスト中 – デバイスはテスト中です。
- 静止中 – デバイスは有効になっていますが、制限されたコマンドセットのみを処理します。
- スタンバイオフライン – デバイスは有効になっていますが、アクティブ化するための外部アクションを待機しています。
- スタンバイスペア – デバイスは冗長セットの一部であり、アクティブ化するためのフェイルオーバーまたはその他の外部アクションを待機しています。
- 起動中 – デバイスは起動中です。
- オフラインで使用不可 – デバイスは存在しますが、使用できません。
- アップデート中 – デバイスはアップデート中であり、使用できないか、劣化している可能性があります。
- 存在しない – デバイスが存在しないか、検出されません。
- 遅延中 – デバイスはコマンドを処理しませんが、新しい要求をキューに入れます。

ドライブの電源の管理

前提条件

- iLOの設定を構成する権限
- このサーバー構成では、ドライブの電源の管理をサポートします。

このタスクについて

サポート対象ドライブを選択すると、物理ドライブ詳細ペインのドライブ電源ボタンセクションに、現在のドライブの電源状態が表示されます。表示される可能性のある値はオン、オフ、および開始中です。

ドライブ電源ボタンオプションを使用して、ドライブの電源をオンまたはオフにすることができます。

電源オフオプションは、サポートされているドライブファームウェアでのみ機能します。

互換性のあるドライブのリストについては、https://ssd.hpe.com/recommendationを参照してください。

電源オンオプション（ホットプラグ）は、標準のIDEコントローラーではサポートされていません。システムをコールドブートして、ドライブを復旧してください。ドライブでこれらの電源リセット機能がサポートされているかどうかを確認するには、ドライブの仕様を参照してください。

手順

1. ナビゲーションツリーでシステム情報をクリックし、ストレージタブをクリックします。
2. ドライブを選択します。

   物理ドライブ詳細ペインが表示されます。
3. 電源オンまたは電源オフボタンをクリックします。
4. 要求を確認するメッセージが表示されたら、OKをクリックします。

サブトピック

ドライブの電源ボタンオプション

ドライブの電源ボタンオプション

- 電源オン – すぐにドライブの電源を入れます。

- 電源オフ – すぐにドライブの電源を切ります。このオプションを使用すると、強制的にシャットダウンされます。

ファームウェアおよびソフトウェアの表示および管理

サブトピック

ファームウェアのアップデート

iLOファームウェアとソフトウェアの管理

インストール済みファームウェア情報の表示

冗長化システムROMでアクティブシステムROMを交換

フラッシュファームウェア機能を使用したiLOまたはサーバーのファームウェアのアップデート

ソフトウェア情報の表示

メンテナンスウィンドウ

iLOレポジトリ

インストールセット

インストールキュー

ファームウェアのアップデート

ファームウェアのアップデートでは、新機能、改良、およびセキュリティアップデートによりサーバーとiLO機能が向上します。

オンライン方式またはオフライン方式によりファームウェアをアップデートすることができます。

サブトピック

オンラインでのファームウェアアップデート

オフラインでのファームウェアアップデート

オンラインでのファームウェアアップデート

オンライン方式を使用してファームウェアをアップデートする場合、サーバーオペレーティングシステムをシャットダウンせずにアップデートを実行できます。オンラインでのファームウェアアップデートは、インバンドまたはアウトオブバンドで実行できます。

インバンド

ファームウェアは、サーバーホストオペレーティングシステムからiLOに送信されます。

インバンドのファームウェアアップデートにはiLOドライバーが必要です。

iLOが製品セキュリティ状態に設定されている場合、ホストベースのファームウェアアップデートでは、ユーザーの認証情報または権限は確認されません。ホストベースのユーティリティでは、ルート（LinuxおよびVMware）または管理者（Windows）ログインが必要です。

iLOが、高セキュリティ、FIPS、またはCNSAのセキュリティ状態を使用するように構成されている場合、ユーザー認証情報が必要になります。

アウトオブバンド

ファームウェアは、ネットワーク接続経由でiLOに送信されます。iLO設定の構成権限を持つユーザーは、アウトオブバンド方式を使用してファームウェアをアップデートできます。

製品セキュリティ状態を使用するシステムのiLOのセキュリティが無効になるように、システムメンテナンススイッチが設定されている場合、すべてのユーザーは、アウトオブバンド方式でファームウェアをアップデートできます。システムが、高度なセキュリティ状態を使用するように構成されている場合、ユーザー認証情報が必要になります。

サブトピック

インバンドのファームウェアアップデート方法

アウトオブバンドのファームウェアアップデート方法

インバンドのファームウェアアップデート方法

オンラインROMフラッシュコンポーネント

サーバーの稼動中に実行可能ファイルを使用してファームウェアをアップデートします。実行可能ファイルには、インストーラーとファームウェアパッケージが含まれています。

このオプションは、iLOが本番環境セキュリティ状態を使用して構成されている場合にサポートされます。

HPONCFG

このユーティリティを使用し、XMLスクリプトを使用してファームウェアをアップデートします。iLOまたはサーバーのファームウェアイメージと`Update_Firmware.xml`サンプルスクリプトをダウンロードします。セットアップの詳細でサンプルスクリプトを編集し、スクリプトを実行します。

iLO6 1.10以降と共にHPONCFG 6.0.0以降を使用する場合、必要なユーザー権限を持っていないと、エラーメッセージが表示されます。

アウトオブバンドのファームウェアアップデート方法

iLO Webインターフェイス

iLO Webインターフェイスを使用してサポートされるファームウェアファイルをダウンロードし、インストールします。単一のサーバーまたはiLO連携グループのファームウェアをアップデートできます。

iLO RESTful API

iLO RESTful APIおよびRESTfulインターフェイスツールなどのRESTクライアントを使用して、ファームウェアをアップデートします。

HPQLOCFG

このユーティリティを使用し、XMLスクリプトを使用してファームウェアをアップデートします。iLOまたはサーバーのファームウェアイメージと`Update_Firmware.xml`サンプルスクリプトをダウンロードします。セットアップの詳細でサンプルスクリプトを編集し、スクリプトを実行します。

HPLOMIG（ProLiant管理プロセッサー用のディレクトリサポートとも呼ばれる）

HPLOMIGのファームウェアアップデート機能を使用するためにディレクトリ統合を使用する必要はありません。HPLOMIGを使用すると、複数のiLOプロセッサーを検出し、そのファームウェアを一度にアップデートすることができます。

SMASH CLP

SSHポートを通じてSMASH CLPにアクセスし、標準のコマンドを使用してファームウェア情報を表示し、ファームウェアをアップデートします。

LOCFG.PL

Perlサンプルを使用してRIBCLスクリプトをiLOにネットワーク経由で送信してください。

オフラインでのファームウェアアップデート

ファームウェアのアップデートにオフラインの方法を使用する場合は、オフラインユーティリティを使用してサーバーを再起動する必要があります。

サブトピック

オフラインでのファームウェアアップデート方法

オフラインでのファームウェアアップデート方法

SPP

ファームウェアアップデートをダウンロードし、インストールする

SUM

SUMを使用してサポートされるサーバーおよびその他のノードのファームウェア、ドライバー、およびソフトウェアメンテナンスを実行してください。

iLOと一緒にSUMを使用して、iLOレポジトリにアクセスし、インストールセットとインストールキューを管理できます。

Scripting Toolkit

Scripting Toolkitを使用して、サーバー内で複数の設定を構成したり、ファームウェアをアップデートしたりします。この方法は、複数のサーバーを展開する場合に便利です。

iLOファームウェアとソフトウェアの管理

iLO Webインターフェイスでは、以下のファームウェアおよびソフトウェア管理機能がサポートされています。

- インストールされているファームウェアを表示する。
- 冗長なシステムROMでアクティブなシステムROMを交換する
- ファームウェアのアップデート制御を使用して、ローカルの管理対象サーバーにファームウェアをインストールする。

  ファームウェアのアップデート制御を使用して、iLO言語パックをインストールすることもできます。
- インストールされているソフトウェアを表示する。
- メンテナンスウィンドウを管理する。インストールキューに追加するタスクにメンテナンスウィンドウを適用できます。
- グループファームウェアアップデート機能を使用して、iLO連携グループ内の複数のサーバーにファームウェアをインストールする。
- Smart Update機能が統合されているiLOにアクセスする。このバージョンのiLOでは、次の操作がサポートされます。
  - iLOレポジトリでコンポーネントを表示および管理する。
  - iLOレポジトリからインストールキューにコンポーネントを追加する。
  - インストールセットの表示と削除、およびインストールキューへの追加を行う。

    インストールセットを構成するには、SUMを使用します。詳しくは、SUMドキュメントを参照してください。
  - システムリカバリセットを表示するか、iLO RESTful APIを使用してシステムリカバリセットを作成する。

- インストールキューでタスクを表示および管理する。

  インストールキューの管理にはSUMを使用することをお勧めします。詳しくは、SUMドキュメントを参照してください。

ファームウェアのアップデート、iLOレポジトリへのアップロード、キューに追加制御には、ファームウェア & OSソフトウェアページのすべてのタブからアクセスできます。

詳しくは、**ファームウェアのアップデート**のビデオを参照してください。

インストール済みファームウェア情報の表示

手順

1. ナビゲーションツリーでファームウェア& OSソフトウェアをクリックします。

   インストールされたファームウェアページには、さまざまなサーバーコンポーネントのファームウェア情報が表示されます。サーバーの電源が切れている場合、このページの情報は、最後に電源が切れた時点の情報になります。ファームウェア情報は、サーバーの電源が入っており、POSTが完了している場合にのみアップデートされます。

   注記: スマートコンポーネントを使用してホストシステムを介してコンポーネントをアップデートした場合、アップデートされたファームウェアを表示するには、 iLOまたはホストをリセットすることが必要になる場合もあります。

2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

サブトピック

ファームウェアタイプ

ファームウェアの詳細

ファームウェアタイプ

インストールされたファームウェアページに表示されるファームウェアタイプは、サーバーの構成によって変化します。

ほとんどのサーバーでは、システムROMおよびiLOファームウェアが表示されます。他の可能なファームウェアオプションは、次のとおりです。

- Power Management Controller
- Server Platform Services Firmware
- Smart Array
- Intelligent Platform Abstraction Data
- Smart Storage Energy Pack
- TPM or TM firmware
- SAS Programmable Logic Device
- System Programmable Logic Device
- Intelligent Provisioning

- Networking adapters
- NVMe Backplane firmware
- Drive firmware
- Power Supply firmware
- Embedded Video Controller
- Language packs
- CPUメザニンプログラマブルロジックデバイス（このファームウェアタイプは、サポートされているプラットフォームでのみ表示されます）
- Secondary System Programmable Logic Device（このファームウェアタイプは、サポートされているプラットフォームでのみ表示されます）

ファームウェアの詳細

インストールされたファームウェアページでは、リストされているファームウェアのタイプごとに以下の情報が表示されます。

- ファームウェア名 - ファームウェアの名前。
- ファームウェアバージョン - ファームウェアのバージョン。
- 位置 - 表示されたファームウェアを使用するコンポーネントの位置。

冗長化システムROMでアクティブシステムROMを交換

前提条件

- ホストBIOS構成権限
- サーバーは冗長化システムROMをサポートしています。

手順

1. ナビゲーションツリーでファームウェア& OSソフトウェアをクリックします。
2. インストール済みファームウェアページで、 （冗長化システムROMの詳細の横）をクリックします。

   iLOが要求を確認するように求めます。
3. OKをクリックします。

   変更は、次のサーバー再起動後に有効になります。

   iLOから開始されるサーバーの再起動には、仮想電源およびリセットの権限が必要です。

フラッシュファームウェア機能を使用したiLOまたはサーバーのファームウェアのアップデート

前提条件

- iLOレポジトリにファームウェアをフラッシュし、コンポーネントを格納するには、iLO設定の構成権限が必要です。

- 正常なファームウェアアップデート後、システムリカバリセットの任意のアップデートを実行するには、リカバリセット権限が必要です。
- リカバリセットをアップデート機能を使用する場合、システムリカバリセットが存在し、アップデートするコンポーネントがこれに含まれている必要があります。

このタスクについて

iLO Webインターフェイスを使用して、任意のネットワーククライアントからファームウェアをアップデートできます。署名済みファイルが必要です。

重要:

ファームウェアのアップデートオプションは、UEFIまたはRuntime Agentを使用してアップデートする必要があるファームウェアパッケージでは機能しません。

iLOを使用してそのようなパッケージをアップデートするには、iLOレポジトリにアップロードオプションを使用してiLOレポジトリにパッケージを追加する必要があります。パッケージは、POST実行中にインストール対象として自動的に選択されます。

手順

1. サーバーファームウェアまたはiLOファームウェアのファイルを入手します。
2. サーバープラットフォームサービス（SPS）のファームウェアをアップデートする場合は、サーバーの電源を切ってから30秒待ちます。

   サーバーOSの実行中は、SPSファームウェアをアップデートできません。
3. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、ファームウェアアップデートをクリックします。

   ファームウェアアップデートオプションが表示されない場合は、iLO Webインターフェイスの右上隅にある省略記号アイコンをクリックし、ファームウェアアップデートをクリックします。
4. ローカルファイルまたはリモートファイルオプションを選択します。
5. 選択したオプションに応じて、以下のいずれかを実行します。
   - 使用するブラウザーに応じて、ローカルファイルボックスで参照またはファイルを選択をクリックして、ファームウェアコンポーネントの場所を指定します。
   - リモートファイルURLボックスに、アクセス可能なWebサーバー上のファームウェアコンポーネントのURLを入力します。

   a. （オプション）拡張されたダウンロードパフォーマンスを構成するには、拡張されたダウンロードパフォーマンスリンクをクリックします。

   アクセス設定ページが表示されます。これらの設定は、 アクセス設定ページで構成できます。

   オプションについて詳しくは、 アクセス設定ページのヘルプを参照してください。

   注記: すでに有効になっている場合、拡張されたダウンロードパフォーマンスリンクは表示されません。
6. （オプション）コンポーネントのコピーをiLOレポジトリに保存するには、同様に、iLOレポジトリに保存チェックボックスを選択します。
7. （オプション）手順5で選択したコンポーネントのバージョンがシステムリカバリセットに存在する場合は、リカバリセットをアップデートチェックボックスを選択して、選択したコンポーネントに既存のコンポーネントを置き換えます。

   このオプションを選択すると、システムリカバリセット内のコンポーネントのバージョンの方が新しい場合でも、コンポーネントが置き換えられます。

   システムリカバリセットが存在しない場合やこの操作に必要な権限が与えられていない場合、このオプションは表示されません。

このオプションを選択すると、システムリカバリセットがiLOレポジトリに保存されるため、iLOレポジトリに保存オプションが自動的に選択されます。

8. TPMまたはTMがサーバーにインストールされているサーバーでは、TPMまたはTMの情報を保存するソフトウェアを一時停止またはバックアップしてから、TPMの無効を確認してくださいチェックボックスを選択します。

   ドライブ暗号化ソフトウェアは、TPMまたはTMの情報を保存するソフトウェアの例です。

   > △ **注意**: ドライブ暗号化ソフトウェアを使用している場合は、ファームウェアのアップデートを開始する前に停止してください。この指示に従わない場合、ご使用のデータにアクセスできなくなる可能性があります。

9. フラッシュをクリックして、アップデートプロセスを開始します。

   サーバーの構成に応じて、iLOによって次のことが通知されます。

   - iLOファームウェアをアップデートすると、iLOは自動的に再起動します。
   - 一部のサーバーファームウェアタイプではサーバーの再起動が必要になりますが、サーバーは自動的には再起動しません。

10. OKをクリックします。

    > ⓘ **重要**:
    >
    > PLDMファームウェアのアップデート中は、サーバーを起動または再起動しないでください。この操作により、サーバーが起動するまでに約20分間のスタンバイモードに入ってしまう可能性があるためです。

    iLOファームウェアは、ファームウェアイメージを受信、検証、フラッシュします。

    iLOファームウェアをアップデートすると、iLOが再起動し、ブラウザー接続が終了します。接続が再確立されるまでに、数分かかることがあります。

11. iLOファームウェアのアップデートのみ：新しいファームウェアを使用するには、ブラウザーのキャッシュをクリアし、iLOにログインします。

12. サーバーファームウェアのアップデートのみ：ファームウェアのタイプによって、サーバーの電源オンや再起動、あるいはシステムリセットの開始が必要になる場合は、適切なアクションを実行します。

13. （オプション）新しいファームウェアがアクティブであることを確認するには、インストールされたファームウェアページでファームウェアバージョンを確認します。

    概要ページでiLOファームウェアバージョンを確認することもできます。

サブトピック

iLOファームウェアイメージファイルの入手

サポートされるサーバーファームウェアイメージファイルの入手

ファームウェアアップデートを有効にするための要件

サポートされるファームウェアタイプ

日次のファームウェアフラッシュ制限

詳しくは

iLOファームウェアイメージファイルの入手
サポートされるサーバーファームウェアイメージファイルの入手
ファームウェアアップデートを有効にするための要件
フラッシュファームウェア機能で言語パックをインストール
システムリカバリセット

iLOファームウェアイメージファイルの入手

このタスクについて

iLOファームウェアイメージファイルをダウンロードし、それを使用してグループ内の1つのサーバーまたは複数のサーバーをアップデートできます。

ファームウェア書き換えアップデート機能またはグループファームウェアアップデート機能を使用してiLOファームウェアをアップデートするには、iLOオンラインフラッシュコンポーネントからのBINファイルが必要です。

手順

1. 次のWebサイトに移動します。https://www.hpe.com/support/hpesc
2. 画面の指示に従ってiLOオンラインフラッシュコンポーネントファイルを探し、ダウンロードします。

   ユニバーサル（FWPKG）、Windows(EXE) またはLinux(RPM) のコンポーネントをダウンロードします。
3. BINファイルを抽出します。
   - Windowsコンポーネントの場合：ダウンロードしたファイルをダブルクリックし、解凍ボタンをクリックします。ファイルを抽出する位置を選択して、OKをクリックします。
   - Linuxコンポーネントの場合：ファイル形式によって異なりますが、次のいずれかのコマンドを入力します。
     - `#rpm2cpio <firmware_file_name>.rpm | cpio -id`

   iLOファームウェアイメージファイルの名前は、`iLO6_<yyy>.bin`です。ここで、`<yyy>`はファームウェアバージョンを表します。

サポートされるサーバーファームウェアイメージファイルの入手

手順

1. 次のWebサイトに移動します。https://www.hpe.com/support/hpesc
2. 画面の指示に従ってオンラインフラッシュコンポーネントファイルを探し、ダウンロードします。
3. Windowsコンポーネントをダウンロードした場合：
   a. ダウンロードしたファイルをダブルクリックし、解凍ボタンをクリックします。
   b. ファイルを抽出する位置を選択して、OKをクリックします。
4. Linuxコンポーネントをダウンロードした場合：
   a. Linuxコンポーネントの場合は、ファイルの形式に応じて、次のコマンドのいずれかを入力します。
      - `#rpm2cpio <firmware_file_name>.rpm | cpio -id`
   b. （オプション）サーバープラットフォームサービス（SPS）のファームウェアコンポーネントを使用する場合は、`<firmware_file_name>.zip`ファイルを見つけて、バイナリファイルを抽出します。

サブトピック

サーバーファームウェアのファイルタイプの詳細

サーバーファームウェアのファイルタイプの詳細

- システムROMをアップデートする場合、署名付きのイメージまたは署名付きのROMPAQイメージを使用する必要がありま

す。

- 署名付きイメージの例：

  http://<server.example.com:8080>/<wwwroot>/P79_1.00_10_25_2013.signed.flash

- 署名付きROMPAQイメージの例：

  http://<server.example.com>/<wwwroot>/CPQPJ0612.A48

- Power Management ControllerおよびNVMeバックプレーンファイルは、ファイル拡張子`.hex`を使用します。例えば、ファイル名は`ABCD5S95.hex`のようになります。
- システムプログラマブルロジックデバイス（CPLD）のファームウェアファイルは、ファイル拡張子`.vme`を使用します。
- サーバープラットフォームサービス（SPS）ファームウェアファイルは、ファイル拡張子`.bin`を使用します。
- 言語パックファイルは拡張子`.lpk`を使用します。

ファームウェアアップデートを有効にするための要件

アップデートを有効にするには、ファームウェアタイプに応じて、追加のアクションが必要になる場合があります。

- iLOのファームウェアまたは言語パック - これらの種類のファームウェアは、自動起動されるiLOリセットの後に有効になります。
- システムROM（BIOS） - サーバーの再起動が必要です。
- システムプログラマブルロジックデバイス（CPLD） - サーバーの再起動が必要です。

> **注記:**
> CPLDファームウェアアップデート後のサーバーの再起動は、サーバーのAC電源サイクルに変換されます。AC電源サイクルの一環として、iLOはリセットされます。

- Power Management ControllerおよびNVMeバックプレーンファームウェア - サーバーの再起動やシステムのリセットは必要ありません。

  NVMeファームウェアバージョンは、次のサーバー再起動後にiLO Webインターフェイスに表示されます。

- サーバープラットフォームサービス（SPS） - これらのファームウェアタイプでは、インストールする前にサーバーの電源を切る必要があります。サーバーに電源を入れると、変更が有効になります。

サポートされるファームウェアタイプ

サーバーのプラットフォームに応じて、さまざまなファームウェアアップデートのタイプがサポートされます。一般的な例には、以下のものがあります。

- iLO
- システムROM/BIOS
- Power Management Controller
- システムプログラマブルロジックデバイス（CPLD）
- バックプレーン
- サーバープラットフォームサービス（SPS）

- 言語パック
- サードパーティのファームウェアパッケージ

  プラットフォームレベルのデータモデル（PLDM）ファームウェアパッケージがサポートされるのは、アクセス設定ページでサードパーティーのファームウェアアップデートパッケージの受け入れオプションが有効の場合です。

一部のファームウェアタイプは、組み合わせたアップデートとして提供されます。以下に例を示します。

- SASプログラマブルロジックデバイスのアップデートは、多くの場合、SASコントローラーのファームウェアアップデートとの組み合わせになります。
- Intelligent Platform Abstraction Dataのファームウェアは、多くの場合、システムROM/BIOSのアップデートとの組み合わせになります。

日次のファームウェアフラッシュ制限

iLOおよびサーバーハードウェアを執拗なフラッシュ攻撃から保護するために、iLOでは、サポートされている各ファームウェアタイプをフラッシュできる1日あたりの回数を制限しています。制限は20回です。これには、ファームウェアフラッシュアクティビティの成功と失敗の両方が含まれます。ファームウェアフラッシュカウントは24時間ごとに、またはファームウェアのアップデートに成功してから24時間後にリセットされます。ファームウェアフラッシュ制限は、どのアプリケーションまたはインターフェイスから開始されたファームウェアアップデートにも適用されます。

ファームウェアフラッシュカウントは不揮発性メモリに保存されます。フラッシュ制限を超えた場合、ファームウェアをフラッシュできず、後で再試行する必要があることがソフトウェアから通知されます。

ファームウェアアップデートが失敗すると、イベントがiLOイベントログに記録されます。

フラッシュ制限プロセスの例

1. 月曜日の午前10時に、前の金曜日以降では初めて、BIOSファームウェアがフラッシュされます。
2. ファームウェアのフラッシュ中、BIOSファームウェアフラッシュ制限のタイムスタンプがiLOによりチェックされます。

   この例では、最後のファームウェアフラッシュは24時間以上前であり、ファームウェアフラッシュカウントは1にリセットされます。
3. 月曜日のそれ以降に、BIOSファームウェアがさらに19回フラッシュされます。

   フラッシュアクティビティごとにフラッシュカウントが1ずつ増加し、合計20になります。
4. 月曜日の終業前にBIOSファームウェアがもう一度フラッシュされますが、フラッシュ制限のためアップデートは失敗します。

   この失敗は、翌朝10時にフラッシュカウントがリセットされるまで続きます。

ソフトウェア情報の表示

前提条件

このページのすべてのデータのセットを表示するには、AMSがインストールされている必要があります。

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、ソフトウェアタブをクリックします。
2. （オプション）ソフトウェア情報のデータをアップデートするには、 をクリックします。

   このページの情報はブラウザーにキャッシュされ、iLOでは最終アップデートの日時が表示されます。ページをアップデートしてから5分以上経過した場合は、 をクリックし、ページを最新情報にアップデートします。

3. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

HPEソフトウェアの詳細

このセクションでは、管理対象サーバー上のすべてのHPEソフトウェアを一覧表示します。このリストには、手動で、またはSPPを使用して追加された、Hewlett Packard Enterpriseのソフトウェアおよび Hewlett Packard Enterprise推奨の他社製ソフトウェアが含まれます。

- 名前 – ソフトウェアの名前。
- バージョン – ソフトウェアのバージョン。

  表示されているファームウェアコンポーネントのバージョンは、ローカルのオペレーティングシステムに保存されているファームウェアフラッシュコンポーネントで利用可能なファームウェアバージョンを示しています。表示されるバージョンが、サーバーで実行されているファームウェアと一致しない可能性があります。
- 説明 – ソフトウェアの説明。

実行中のソフトウェアの詳細

このセクションには、管理対象サーバー上で実行されているか、実行可能であるすべてのソフトウェアが表示されます。

- 名前 – ソフトウェアの名前。
- パス – ソフトウェアのファイルパス。

インストールされたソフトウェアの詳細

インストールされたソフトウェア – インストールされた各ソフトウェアプログラムの名前が表示されます。

メンテナンスウィンドウ

メンテナンスウィンドウとは、インストールタスクに適用される構成済みの期間のことです。

メンテナンスウィンドウは次のいずれかの方法で作成できます。

- メンテナンスウィンドウタブ上
- タスクをインストールキューに追加するとき

メンテナンスウィンドウの追加

前提条件

iLOの設定を構成する権限

このタスクについて

iLOは、最大8つのメンテナンスウィンドウをサポートします。

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、メンテナンスウィンドウをクリックします。
2. ＋ をクリックします。

   iLOは、メンテナンスウィンドウ情報を入力するよう求めるメッセージを表示します。
3. 名前ボックスに名前を入力します。

4. 説明ボックスに説明を入力します。
5. メンテナンスウィンドウの開始時刻と終了時刻を開始および終了ボックスに入力します。
   a. 開始ボックスにある をクリックします。

      カレンダーが表示されます。
   b. 開始日時を選択し、完了をクリックします。
   c. 終了ボックスにある をクリックします。

      カレンダーが表示されます。
   d. 終了日時を選択し、完了をクリックします。

   iLOを管理するために使用しているクライアントの現時時間に基づいて日時を入力します。

   入力した日時に相当するUTCが日時の上に表示されます。

   既存のタスクの開始時刻よりも前の終了の値を入力した場合、iLOから、別の値を入力するよう求められます。インストールキューは、タスクの先入れ先出しリストです。既存のタスクの実行前に有効期限が切れるメンテナンスウィンドウを作成することはできません。
6. 追加をクリックします。

   メンテナンスウィンドウが追加されます。

メンテナンスウィンドウの編集

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、メンテナンスウィンドウをクリックします。
2. をクリックします。

   iLOに、メンテナンスウィンドウ情報をアップデートするよう求められます。
3. 名前ボックスでメンテナンスウィンドウ名をアップデートします。
4. 説明ボックスで説明をアップデートします。
5. 開始および終了ボックスでメンテナンスウィンドウの開始時刻と終了時刻をアップデートします。
   a. 開始ボックスにある をクリックします。

      カレンダーが表示されます。
   b. 開始日時を選択し、完了をクリックします。
   c. 終了ボックスにある をクリックします。

      カレンダーが表示されます。
   d. 終了日時を選択し、完了をクリックします。

   iLOを管理するために使用しているクライアントの現時時間に基づいて日時を入力します。

   入力した日時に相当するUTCが日時の上に表示されます。

   既存のタスクの開始時刻よりも前の終了の値を入力した場合、iLOから、別の値を入力するよう求められます。インストールキューは、タスクの先入れ先出しリストです。既存のタスクの実行前に有効期限が切れるメンテナンスウィンドウを作成することはできません。

6. OKをクリックします。

   メンテナンスウィンドウがアップデートされます。

メンテナンスウィンドウの削除

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、メンテナンスウィンドウをクリックします。
2. 🗑 （削除するメンテナンスウィンドウの横）をクリックします。

   iLOに、メンテナンスウィンドウの削除を確認するプロンプトが表示されます。
3. はい、削除をクリックします。

   メンテナンスウィンドウが削除されます。

   削除されたメンテナンスウィンドウに関連付けられているすべてのタスクが取り消されます。

すべてのメンテナンスウィンドウを削除

前提条件

iLO設定の構成権限

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、メンテナンスウィンドウをクリックします。
2. すべて削除をクリックします。

   iLOに、すべてのメンテナンスウィンドウの削除を確認するプロンプトが表示されます。
3. はい、すべて削除しますをクリックします。

   メンテナンスウィンドウが削除されます。

   削除されたメンテナンス ウィンドウに関連付けられているすべてのタスクが取り消されます。

メンテナンスウィンドウの表示

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、メンテナンスウィンドウをクリックします。
2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。
3. （オプション）詳細情報を表示するには、個々のメンテナンスウィンドウをクリックします。

メンテナンスウィンドウのサマリーの詳細

メンテナンスウィンドウタブにiLOの日時および構成された各メンテナンスウィンドウに関する次の詳細が表示されます。

- 名前 - メンテナンスウィンドウのユーザー定義名。
- 開始時間 - メンテナンスウィンドウの開始時刻（UTC）。

- 終了時刻 – メンテナンスウィンドウの終了時刻（UTC）。

メンテナンスウィンドウは期限を過ぎてから24時間以内に自動的に削除されます。

各メンテナンスウィンドウの詳細

各メンテナンスウィンドウをクリックすると、以下の詳細が表示されます。

- 名前 – メンテナンスウィンドウのユーザー定義名。
- 開始 – メンテナンスウィンドウの開始時刻（UTC）。
- 終了 – メンテナンスウィンドウの終了時刻（UTC）。
- 説明 – メンテナンスウィンドウの説明。

iLOレポジトリ

iLOレポジトリは、システムボードに埋め込まれた不揮発性フラッシュメモリ内の安全なストレージ領域です。不揮発性フラッシュメモリはサイズが1ギガバイトで、iLO NANDと呼ばれます。SUMまたはiLOを使用して、iLOレポジトリ内の署名済みソフトウェアおよびファームウェアコンポーネントを管理します。

iLO、UEFI BIOS、SUM、および他のクライアントソフトウェアは、これらのコンポーネントを取得し、サポートされているサーバーに適用できます。SUMを使用して、インストールセットに保存するコンポーネントを整理し、SUMまたはiLOを使用してインストールキューを管理します。

iLO、SUM、およびBIOSソフトウェアがどのように連携してソフトウェアとファームウェアを管理するかについて詳しくは、**SUMのドキュメント**を参照してください。

iLOレポジトリへのコンポーネントの追加

前提条件

- iLOレポジトリにファイルをアップロードするには、iLO設定の構成権限が必要です。
- iLOレポジトリへのファイルのアップロード後、システムリカバリセットの任意のアップデートを実行するには、リカバリセット権限が必要です。
- リカバリセットをアップデート機能を使用する場合、システムリカバリセットが存在し、アップデートするコンポーネントがこれに含まれている必要があります。

このタスクについて

iLOレポジトリにアップロードペインを使用して、iLOレポジトリにコンポーネントを追加します。iLOレポジトリにアップロードペインは、ファームウェア & OSソフトウェアページのタブからアクセスできます。

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックして、iLOレポジトリにアップロードをクリックします。

   ブラウザーウィンドウのサイズが小さいために、iLOレポジトリにアップロードオプションが表示されない場合は、iLO Webインターフェイスの右上隅の省略符号アイコンをクリックしてから、iLOレポジトリにアップロードをクリックします。

2. ローカルファイルまたはリモートファイルオプションを選択します。
3. 選択したオプションに応じて、以下のいずれかを実行します。
   - ローカルファイルボックスで、（使用するブラウザーに応じて）参照またはファイルを選択をクリックして、ファームウェアコンポーネントの場所を指定します。
   - リモートファイルURLボックスに、アクセス可能なWebサーバー上のファームウェアコンポーネントのURLを入力します。

a. （オプション）拡張されたダウンロードパフォーマンスを構成するには、拡張されたダウンロードパフォーマンスリンクをクリックします。

アクセス設定ページが表示されます。これらの設定は、 アクセス設定ページで構成できます。

オプションについて詳しくは、 アクセス設定ページのヘルプを参照してください。

> **注記**: すでに有効になっている場合、拡張されたダウンロードパフォーマンスリンクは表示されません。

4. 複数ファイルのみで指定されたファームウェアコンポーネントの場合：コンポーネントの署名ファイルを持っていますチェックボックスを選択します。
5. 手順4でチェックボックスを選択した場合は、以下のいずれかを実行します。
   - ローカル署名ファイルボックスで、（使用するブラウザーに応じて）参照またはファイルを選択をクリックしてから、コンポーネント署名ファイルの場所を指定します。
   - リモート署名ファイルURLボックスに、アクセス可能なWebサーバー上のコンポーネント署名ファイルのURLを入力します。
6. （オプション）手順3で選択したコンポーネントのバージョンがシステムリカバリセットに存在する場合は、リカバリセットをアップデートチェックボックスを選択して、選択したコンポーネントに既存のコンポーネントを置き換えます。

   このオプションを選択すると、システムリカバリセット内のコンポーネントのバージョンの方が新しい場合でも、コンポーネントが置き換えられます。

   システムリカバリセットが存在しない場合やこの操作に必要な権限が与えられていない場合、このオプションは表示されません。
7. アップロードをクリックします。

   iLOにより、既存のコンポーネントと同じ名前を持つコンポーネントをアップロードすると既存のコンポーネントが置換されることが通知されます。
8. OKをクリックします。

   アップロードが開始されます。アップロードステータスはiLO Webインターフェイスの上部に表示されます。

詳しくは

iLOファームウェアイメージファイルの入手
サポートされるサーバーファームウェアイメージファイルの入手
システムリカバリセット

iLOレポジトリからコンポーネントをインストールする

前提条件

iLOの設定を構成する権限

このタスクについて

iLOレポジトリページからインストールキューにコンポーネントを追加できます。

コンポーネントをインストールキューに追加すると、タスクがキューの末尾に追加されます。キューに入れられた他のタスクが完了した後、コンポーネントタイプのアップデートを開始するソフトウェアがインストール要求を検出したときに、追加されたコンポーネントがインストールされます。アップデートを開始できるソフトウェアについては、iLOレポジトリページとインストールキューページでコンポーネントの詳細を確認してください。

前にキューに入れられたタスクが開始または終了を待機している場合、新しいタスクは無期限に遅延する場合があります。例えば、キューに入れられたコンポーネントがUEFI BIOSによってインストール可能な場合、インストールを開始する前にサーバーの再起動が必要です。サーバーが再起動されない場合、これよりも後のキュー内のタスクは無期限に遅延します。

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、iLOレポジトリをクリックします。

2. （インストールするコンポーネントの横）をクリックします。

   インストールコンポーネントペインが開き、要求の確認を求められます。

   ファームウェアパッケージ2.0をレポジトリから
   インストールキュー
   にiLO Webインターフェイスを介して追加するとき、iLOはパッケージの
   UpdatableBy
   フィールドの値（BMC、UEFIなど）に基づいて複数のタスクを作成します。次に、iLOはBMCとUEFIのタスクを作成します。BMCまたはUEFIの
   UpdatableBy
   デバイスがない場合、いずれかのタスクが例外状態になります。キュー内の残りのタスクを実行するには、タスクを手動でクリアする必要があります。

3. （オプション）インストールのスケジュールを指定するには、スケジュールウィンドウをセットチェックボックスを選択します。

   a. スケジュールを定義する方法を選択します。

      - メンテナンスウィンドウを使用（デフォルト）を選択し、メンテナンスウィンドウページで構成したメンテナンスウィンドウを選択します。

        メンテナンスウィンドウを追加するには、新規をクリックしてメンテナンスウィンドウページに移動します。メンテナンスウィンドウを作成してから、この手順を再開します。

      - 時間枠を指定してくださいを選択し、スケジュールをその場で入力します。

   b. 選択した方法によって、以下のいずれかを実行します。

      - メンテナンスウィンドウを使用を選択した場合は、メンテナンスウィンドウリストで値を選択します。
      - 時間枠を指定してくださいを選択した場合は、スケジュールの詳細を入力します。

4. はい、キューの最後に追加をクリックします。

   インストールキューが空で、iLOがコンポーネントのインストールを開始できる場合、ボタンに、はい、今インストールというラベルが付けられます。

   キューに入れられた既存のタスクが終了し、選択されたコンポーネントタイプのインストールを開始するソフトウェアが保留中のインストールを検出すると、アップデートが開始されます。

   インストールキューが空で、iLOがアップデートを開始できる場合、すぐにアップデートが開始されます。

詳しくは

iLOレポジトリへのコンポーネントの追加
iLOレポジトリの概要とコンポーネントの詳細の表示
インストールキューの表示
日次のファームウェアフラッシュ制限
iLOファームウェアイメージファイルの入手
サポートされるサーバーファームウェアイメージファイルの入手

コンポーネントのインストール時に時間枠の詳細を入力する

前提条件
iLOの設定を構成する権限

このタスクについて
時間枠を指定してくださいが選択されているときは、以下の手順を使用してスケジュールを入力します。

手順

1. 開始ボックスにある をクリックします。

カレンダーが表示されます。

2. 開始日時を選択し、完了をクリックします。

   選択した日時は開始ボックスに表示されます。

3. 終了ボックスにある をクリックします。

   カレンダーが表示されます。

4. 終了日時を選択し、完了をクリックします。

   この値によって、インストールセット内のタスクの有効期限（日付時刻）が設定されます。

   選択した日時は終了ボックスに表示されます。

iLOレポジトリからのコンポーネントの削除

前提条件

- iLOの設定を構成する権限
- コンポーネントがインストールセットに含まれていない。
- コンポーネントがキューに入れられたタスクの一部ではない。

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、iLOレポジトリタブをクリックします。
2. をクリックします。

   iLOが要求を確認するように求めます。

3. はい、削除をクリックします。

   コンポーネントが削除されます。

iLOレポジトリからすべてのコンポーネントを削除する

前提条件

- iLO設定の構成権限
- コンポーネントがインストールセットに含まれていない。
- コンポーネントがキューに入れられたタスクの一部ではない。

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、iLOレポジトリタブをクリックします。
2. すべて削除をクリックします。

   iLOが要求を確認するように求めます。

3. はい、すべて削除しますをクリックします。

   コンポーネントが削除されます。

iLOレポジトリの概要とコンポーネントの詳細の表示

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、iLOレポジトリタブをクリックします。
2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンを

クリックします。

3. （オプション）コンポーネントの詳細な情報を表示するには、個々のコンポーネントをクリックします。

iLOレポジトリのストレージの詳細

iLOレポジトリページの概要セクションには、iLOレポジトリのストレージの使用状況に関する以下の詳細が表示されます。

- 容量 – iLOレポジトリの総ストレージ容量
- 使用中 – 使用されているストレージ
- 空き容量 – iLOレポジトリの使用可能なストレージ
- コンポーネント – iLOレポジトリに保存されているコンポーネントの数

iLOレポジトリの内容

iLOレポジトリページのコンテンツセクションには、ソフトウェアコンポーネントまたは各ファームウェアに関する以下の詳細が表示されます。

- 名前
- バージョン

iLOレポジトリの個々のコンポーネントの詳細

個々のコンポーネントをクリックすると、以下の詳細が表示されます。

- 名前 – コンポーネント名
- バージョン – コンポーネントのバージョン
- ファイル名 – コンポーネントのファイル名
- サイズ – コンポーネントのサイズ
- アップロード – アップロードの日時
- インストール元 – コンポーネントのアップデートを開始できるソフトウェア
- インストールセットまたはタスクで使用中ですか? – コンポーネントがインストールセットまたはキューに入れられたタスクの一部かどうか

  コンポーネントがインストールセットまたはキューに入れられたタスクの一部である場合、インストールセットまたはタスク名のリンクをクリックして、インストールセットの詳細またはキューに入れられたタスクの詳細を表示できます。

インストールセット

インストールセットは、1つのコマンドでサポートされるサーバーに適用できるコンポーネントのグループです。SUMは、サーバーに何をインストールするかを決定し、iLOにコピーするインストールセットを作成します。既存のインストールセットは、iLO Webインターフェイスのインストールセットページで確認できます。

SUMから展開するときにインストールセットを保存すると、iLOシステム上のすべてのコンポーネントが後で使用できるように保持されます。例えば、元のSPPが見つからなくても、保存したコンポーネントを使用してコンポーネントバージョンをリストアまたはロールバックすることができます。

iLO、SUM、およびBIOSソフトウェアがどのように連携してソフトウェアとファームウェアを管理するかについて詳しくは、**SUMのドキュメント**を参照してください。

インストールセットのインストール

前提条件

- iLOの設定を構成する権限
- インストールセット内のコンポーネントが別のインストールタスクの一部としてキューに入れられることはありません。

このタスクについて

インストールセットページからインストールセットをインストールキューに追加できます。

インストールセットをインストールキューに追加すると、iLOは、インストールセット内のコンポーネントまたはコマンドごとにタスクを追加します。新しいタスクはキューの末尾に追加されます。

キュー内のコンポーネントは、キューに入れられた他のタスクが完了した後、コンポーネントタイプのアップデートを開始するソフトウェアがインストール要求を検出したときにインストールされます。アップデートを開始できるソフトウェアについては、iLOレポジトリページとインストールキューページでコンポーネントの詳細を確認してください。

前にキューに入れられたコンポーネントが開始または終了を待機している場合、新しいタスクは無期限に遅延する場合があります。たとえば、キューに入れられたコンポーネントがUEFI BIOSによってインストール可能な場合、インストールを開始する前にサーバーの再起動が必要です。サーバーが再起動されない場合、これよりも後のキュー内のタスクは無期限に遅延します。

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、インストールセットタブをクリックします。
2. （インストールするインストールセットの横）をクリックします。

   インストールコンポーネントペインが開き、要求の確認を求められます。
3. （オプション）インストールのスケジュールを指定する場合は、スケジュールウィンドウをセットチェックボックスを選択します。
   a. スケジュールを定義する方法を選択します。
      - メンテナンスウィンドウを使用（デフォルト）を選択し、メンテナンスウィンドウページで構成したメンテナンスウィンドウを選択します。

        メンテナンスウィンドウを追加するには、新規をクリックしてメンテナンスウィンドウページに移動します。メンテナンスウィンドウを作成してから、この手順を再開します。
      - 時間枠を指定してくださいを選択し、スケジュールをその場で入力します。
   b. 選択した方法によって、以下のいずれかを実行します。
      - メンテナンスウィンドウを使用を選択した場合は、メンテナンスウィンドウリストで値を選択します。
      - 時間枠を指定してくださいを選択した場合は、スケジュールの詳細を入力します。
4. （オプション）キューに入れられた既存のタスクがあり、それらを削除する場合は、 インストールキューをクリアチェックボックスを選択します。

   既存のタスクがある場合、iLOは、キューに入っているタスクの数を表示し、インストールセットの内容がキューの末尾に追加されることを通知します。

   キューが空で、iLOがインストールセットでアップデートを開始できる場合、このチェックボックスは表示されません。

   キューが空で、iLOがインストールセットでアップデートを開始できない場合、このチェックボックスは無効になっています。
5. はい、キューの最後に追加をクリックします。

   手順4でチェックボックスを選択しているか、キューがすでに空のときに、iLOがインストールセットでアップデートを開始できる場合は、ボタンラベルがはい、今インストールになります。

   キューに入れられた既存のタスクが終了し、選択されたコンポーネントタイプのインストールを開始するソフトウェアが保留中のインストールを検出すると、アップデートが開始されます。

インストールキューが空で、iLOが要求されたアップデートを開始できる場合、すぐにアップデートが開始されます。

詳しくは

インストールキューの表示

インストールセットのインストール時に時間枠の詳細を入力する

前提条件

iLOの設定を構成する権限

このタスクについて

時間枠を指定してくださいが選択されているときは、以下の手順を使用してスケジュールを入力します。

手順

1. 開始ボックスにある をクリックします。

   カレンダーが表示されます。
2. 開始日時を選択し、完了をクリックします。

   選択した日時は開始ボックスに表示されます。
3. 終了ボックスにある をクリックします。

   カレンダーが表示されます。
4. 終了日時を選択し、完了をクリックします。

   この値によって、インストールセット内のタスクの有効期限（日付時刻）が設定されます。

   選択した日時は終了ボックスに表示されます。

インストールセットを削除する

前提条件

- 保護されていないインストールセットのiLO設定の構成権限。
- 保護されたインストールセットを削除するためのiLO設定の構成権限とリカバリセット権限。

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、インストールセットタブをクリックします。
2. 削除するインストールセットの横にある をクリックします。

   iLOが要求を確認するように求めます。
3. はい、削除をクリックします。

   インストールセットが削除されます。

すべてのインストールセットを削除する

前提条件

- iLOの設定を構成する権限
- すべてのインストールセットを削除する要求にシステムリカバリセットを含めるには、リカバリセット権限が必要です。

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、インストールセットタブをクリックします。

2. すべて削除をクリックします。

   iLOが要求を確認するように求めます。

3. （オプション）システムリカバリセットが存在する場合、リカバリセットを削除するには、保護されたリカバリセットも削除チェックボックスを選択します。

   ユーザーアカウントにリカバリセット権限が割り当てられていない場合、このオプションは表示されません。

4. はい、すべて削除をクリックします。

   インストールセットが削除されます。

インストールセットを表示する

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、インストールセットタブをクリックします。
2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

3. （オプション）インストールセットをクリックして詳細情報を表示します。

インストールセットの概要の詳細

インストールセットタブには、各インストールセットに関する以下の詳細が表示されます。

- 名前 – インストールセットの名前。
- コンポーネント/コマンド – インストールセット内のコンポーネントとコマンド。バージョン情報はすべてのコンポーネントに含まれます。

インストールセットアイコンを使用して、インストールセットをインストールキューに追加したり、インストールセットを削除したりできます。保護されたインストールセットは、ロックアイコン付きで表示されます。

詳しくは

インストールセットのインストール
インストールセットを削除する

個々のインストールセットの詳細

個々のインストールセットをクリックすると、以下の詳細が表示されます。

- 名前 – インストールセットの名前。
- 作成済み – 作成日時。
- 説明 – インストールセットの説明。
- コンポーネント/コマンド – インストールセット内のコンポーネントとコマンド。バージョン情報はすべてのコンポーネントに含まれます。

  インストールセットにコンポーネントが含まれている場合、コンポーネント名のリンクをクリックすると、コンポーネントの詳細をiLOレポジトリに表示することができます。

- システムリカバリセット–インストールセットがシステムリカバリセットとして指定されているかどうかを示します。

  システムリカバリセットは、ランタイムのファームウェアリカバリ操作で使用されます。システムリカバリセットは同時に1つのみ存在できます。

システムリカバリセット

デフォルトでは、システムリカバリセットがすべてのサーバーに付属します。**リカバリセット**権限を持つユーザーアカウントは、このインストールセットを構成できます。システムリカバリセットは同時に1つのみ存在できます。

インテルサーバー用のデフォルトのシステムリカバリセットには、以下のファームウェアコンポーネントが含まれます。

- システムROM（BIOS）
- iLOファームウェア
- システムプログラマブルロジックデバイス（CPLD）
- サーバープラットフォームサービス（SPS）ファームウェア
- サーバープラットフォームサービスのフルリカバリイメージ

AMDサーバー用のデフォルトのシステムリカバリセットには、以下のファームウェアコンポーネントが含まれます。

- システムROM（BIOS）
- iLOファームウェア
- システムプログラマブルロジックデバイス（CPLD）

デフォルトのシステムリカバリセットが削除されている場合

- リカバリセット権限を所有しているユーザーは、iLO RESTful APIおよびRESTfulインターフェイスツールを使用してiLOレポジトリに保存されているコンポーネントからシステムリカバリセットを作成することができます。
- リカバリセット権限を持つユーザーは、SUMを使用してインストールセットを作成し、iLO RESTful APIを使用してそれをシステムリカバリセットとして指定できます。

詳しくは

システムリカバリセットの作成

システムリカバリセットの作成

前提条件

- リカバリセット権限
- システムのリカバリのセットは、サーバー上に存在しません。
- RESTfulインターフェイスツールがインストールされている。

  詳しくは、https://www.hpe.com/info/redfishを参照してください。

このタスクについて

システムリカバリセットが削除された場合、iLO RESTful APIおよびRESTfulインターフェイスツールを使用して、iLOレポジトリに保存されているコンポーネントから新しいセットを作成できます。

> **注記:** 既存のシステムリカバリセットにある個々のコンポーネントを交換するには、 iLOレポジトリにコンポーネントを追加して、 リカバリセットをアップデートチェックボックスを選択します。

手順

1. システムリカバリセットに含めるファームウェアコンポーネントをダウンロードします。

   通常、システムリカバリセットには、以下のコンポーネントが含まれます。

   - iLOファームウェア
   - システムROM/BIOS
   - システムプログラマブルロジックデバイス（CPLD）
   - サーバープラットフォームサービス（SPS）
2. ダウンロードされたコンポーネントから必要なファイルを抽出します。

3. iLOレポジトリにファームウェアコンポーネントを追加します。
4. テキストエディターを開き、システムリカバリセットを定義するファイルを作成します。

   このファイルには、名前と説明が含まれ、`IsRecovery`プロパティを割り当て、追加するコンポーネントを一覧表示します。インストールセットを使用する際に、インストールされる順番でコンポーネントを追加します。

   テンプレートとして、次の例を使用します。内容は、ダウンロードしたコンポーネントのバージョンによって異なる場合があります。

```
{
    "Description": "Essential system firmware components",
    "IsRecovery": true,
    "Name": "System Recovery Set",
    "Sequence": [
        {
            "Command": "ApplyUpdate",
            "Filename": "ilo6_110.bin",
            "Name": "System Recovery Set item (iLO 6)",
            "UpdatableBy": [
                "Bmc"
             ]
        },
        {
            "Command": "ApplyUpdate",
            "Filename": "A55_1.10_10_14_2022.signed.flash",
            "Name": "System Recovery Set item (System ROM)",
            "UpdatableBy": [
                "Bmc"
             ]
        },
        {
            "Command": "ApplyUpdate",
            "Filename": "CPLD_DL385_DL365_gen11_v0A0A_full_signed.vme",
            "Name": "System Recovery Set item (System Programmable Logic Device)",
            "UpdatableBy": [
                "Bmc"
             ]
        }

    ]
}
```

5. ファイルをJSONファイルとして保存します。例えば、 system_recovery_set.jsonと名付けます。
6. RESTfulインターフェイスツールを起動します。

   インストール設定の作業に関するヘルプを表示するには、`ilorest installset -help`と入力します。

   詳しくは、次のWebサイトを参照してください。**https://www.hpe.com/support/restfulinterface/docs**
7. システムリカバリセットを作成するためのコマンドを入力します。

```
C:\WINDOWS\system32 > ilorest installset add < JSONファイルの場所 > \ < JSONファイル名 >
-u < iLOのログイン名 >-p < iLOパスワード > --url = < iLOホスト名またはIPアドレス >
```

8. （オプション）インストール設定を表示するには、次のコマンドを入力します。

```
ilorest installset-u < iLOのログイン名 >-p < iLOパスワード > - url = < iLOホスト名またはIPアドレス >
```

   サーバー上のインストールセットは、含まれるコンポーネントと一緒に表示されます。

詳しくは

iLOファームウェアイメージファイルの入手
サポートされるサーバーファームウェアイメージファイルの入手
iLOレポジトリへのコンポーネントの追加

インストールキュー

インストールキューは、キューに個別に、またはインストールセットの一部として追加されたコンポーネントおよびコマンドの順序付けされたリストです。タスクは、次の方法を使用してキューに追加できます。

- iLOのキューに追加ペインを使用する。
- ＋（インストールキューページ）をクリックします。
- （iLOレポジトリページ）をクリックします。
- SUMを使用する。

サブトピック

インストールキューへのタスクの追加

インストールキューのタスクの編集

インストールキューからのタスクの削除

インストールキューからのすべてのタスクの削除

インストールキューの表示

詳しくは

インストールキューへのタスクの追加
iLOレポジトリからコンポーネントをインストールする

インストールキューへのタスクの追加

前提条件

- インストールキューにタスクを追加するには、iLO設定の構成権限が必要です。
- キューに入れられたアップデートが正常に完了した後に、システムリカバリセットの任意のアップデートを実行するには、リカバリセット権限が必要です。
- リカバリセットをアップデート機能を使用する場合、システムリカバリセットが存在し、アップデートするコンポーネントがこれに含まれている必要があります。

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、インストールキュータブをクリックします。
2. ＋ をクリックするか、キューに追加をクリックします。

   キューに追加ペインは、ファームウェア & OSソフトウェアページのタブで使用できます。ブラウザーウィンドウのサイズが小さいために、キューに追加オプションが表示されない場合は、iLO Webインターフェイスの右上隅にある省略記号アイコンをクリックして、キューに追加をクリックします。

   ファームウェアパッケージ2.0をレポジトリから
   `インストールキュー`
   にiLO Webインターフェイスを介して追加するとき、iLOはパッケージの

`UpdatableBy`
フィールドの値（BMC、UEFIなど）に基づいて複数のタスクを作成します。次に、iLOはBMCとUEFIのタスクを作成します。
`UpdatableBy`
フィールドの値（BMCまたはUEFI）のデバイスがない場合、いずれかのタスクが例外状態になります。キュー内の残りのタスクを実行するには、タスクを手動でクリアする必要があります。

iLOは、タスク情報を追加するよう求めるメッセージを表示します。

3. タスク名ボックスにタスク名（最大64文字）を入力します。
4. コンポーネント/コマンドボックスで値を選択します。

   このリストには、以下のものが含まれます。

   - iLOレポジトリに保存されているコンポーネント。
   - 待機およびiLOをリセットコマンド。
5. 待機コマンドを選択した場合、待機時間を待機時間（秒）ボックスに入力します。

   有効な値は1～3600秒です。
6. （オプション）インストールのスケジュールを指定するには、スケジュールウィンドウをセットチェックボックスを選択します。
   a. スケジュールを定義する方法を選択します。
      - メンテナンスウィンドウを使用（デフォルト）を選択し、メンテナンスウィンドウページで構成したメンテナンスウィンドウを選択します。

        メンテナンスウィンドウを追加するには、新規をクリックしてメンテナンスウィンドウページに移動します。メンテナンスウィンドウを作成してから、この手順を再開します。
      - 時間枠を指定してくださいを選択し、スケジュールをその場で入力します。

   b. 選択した方法によって、以下のいずれかを実行します。
      - メンテナンスウィンドウを使用を選択した場合は、メンテナンスウィンドウリストで値を選択します。
      - 時間枠を指定してくださいを選択した場合は、スケジュールの詳細を入力します。
7. （オプション）手順4でコンポーネントを選択し、そのコンポーネントがシステムリカバリセットに存在する場合は、リカバリセットをアップデートチェックボックスを選択して、選択したコンポーネントに既存のコンポーネントを置き換えます。

   このオプションを選択すると、システムリカバリセット内のコンポーネントのバージョンの方が新しい場合でも、コンポーネントが置き換えられます。

   次の場合、このオプションは表示されません。

   - コマンドが選択されている。
   - システムリカバリセットがない。
   - 必要な権限がユーザーアカウントに割り当てられていない。
8. サーバーにTPMまたはTMが存在する場合は、TPMまたはTMの情報を保存するソフトウェアを一時停止またはバックアップしてから、TPMの上書きを確認してくださいチェックボックスを選択します。

   ドライブ暗号化ソフトウェアは、TPMまたはTMの情報を保存するソフトウェアの例です。

   > △ **注意**: ドライブ暗号化ソフトウェアを使用している場合は、ファームウェアのアップデートを開始する前に停止してください。この指示に従わない場合、ご使用のデータにアクセスできなくなる可能性があります。
9. キューに追加をクリックします。

iLOによって、タスクがインストールキューの最後に追加されたことが通知されます。このイベントはiLOイベントログに記録されます。

タスクの有効期限が、キューでそのタスクに先行する既存のタスクの開始時刻より前に切れる場合、iLOはタスクを保存できないことを通知します。インストールキューは、タスクの先入れ先出しリストです。既存のタスクの実行前に有効期限が切れるタスクを作成することはできません。

リカバリセットをアップデートチェックボックスを選択した場合は、タスクが開始され、正常に完了した後に、コンポーネントがアップデートされます。

サブトピック

インストールキューに追加できるコマンド

タスクをキューに入れるときに時間枠の詳細を入力する

インストールキュー内のタスクの処理方法

詳しくは

メンテナンスウィンドウの追加
タスクをキューに入れるときに時間枠の詳細を入力する
インストールキューに追加できるコマンド
システムリカバリセット
インストールキュー内のタスクの処理方法

インストールキューに追加できるコマンド

待機

インストールキューを停止し、構成された時間（秒）待機します。有効な値は1～3600秒です。

iLOをリセット

iLOをリセット（再起動）します。

このコマンドを実行しても構成が変更されることはありませんが、iLOファームウェアへのアクティブな接続がすべて終了します。

タスクをキューに入れるときに時間枠の詳細を入力する

前提条件

iLOの設定を構成する権限

このタスクについて

時間枠を指定してくださいが選択されているときは、以下の手順を使用してスケジュールを入力します。

手順

1. 開始ボックスにある をクリックします。

   カレンダーが表示されます。

2. 開始日時を選択し、完了をクリックします。

   選択した日時は開始ボックスに表示されます。

3. 終了ボックスにある をクリックします。

   カレンダーが表示されます。

4. 終了日時を選択し、完了をクリックします。

   この値によってタスクの有効期限（日付時刻）が設定されます。

   選択した日時は終了ボックスに表示されます。

インストールキュー内のタスクの処理方法

タスクをインストールキューに追加するとき：

- キューの最後に追加されます。
- コマンドを追加した場合、キューに入れられた既存のタスクが終了した後、タスクが開始されます。
- コンポーネントを追加した場合、タスクは以下の後に開始されます。
  - キューに入れられた既存のタスクが終了した。
  - 選択されたコンポーネントタイプのインストールを開始するソフトウェアが保留中のインストールを検出した。

  インストールキューが空で、iLOがアップデートを開始できる場合、すぐにアップデートが開始されます。

  アップデートを開始できるソフトウェアについては、iLOレポジトリページとインストールキューページでコンポーネントの詳細を確認してください。
- 前にキューに入れられたタスクが開始または終了を待機している場合、新しいタスクは無期限に遅延する場合があります。たとえば、サーバーPOST中にUEFI BIOSが検出するまで待機している、キューに入れられたコンポーネントがあるとします。サーバーが再起動されない場合、キュー内のこのタスクに続くタスクは、無期限に保留されたままになります。
- タスクが、インストールキュー内で先行しているタスクの開始時刻より前に期限切れになった場合、iLOはタスクを保存しません。
- 指定された時間枠内にアップデートが開始されない場合、アップデートは有効期限切れになります。アップデートの有効期限が切れた場合は、タスクを削除して再作成するか、タスクを編集します。

詳しくは

iLOレポジトリの概要とコンポーネントの詳細の表示
インストールキューの表示

インストールキューのタスクの編集

前提条件

- インストールキューのタスクを編集するには、iLO設定の構成権限が必要です。
- キューに入れられたアップデートが正常に完了した後に、システムリカバリセットの任意のアップデートを実行するには、リカバリセット権限が必要です。
- リカバリセットをアップデート機能を使用する場合、システムリカバリセットが存在し、アップデートするコンポーネントがこれに含まれている必要があります。
- 編集対象のタスクは保留ステータスです。

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、インストールキュータブをクリックします。
2. 編集対象のタスクの横にある をクリックします。

iLOから、タスク情報をアップデートするよう求められます。

3. タスク名をアップデートするには、タスク名ボックスに新しい名前（最大64文字）を入力します。
4. コンポーネントボックスまたはコマンドボックスで値を選択します。
   - 元のタスクがコンポーネントのアップデートの場合、選択できるのは別のコンポーネントだけです。
   - 元のタスクがコマンドの場合、選択できるのは別のコマンドだけです。
5. 待機コマンドを選択した場合、待機時間を待機時間（秒）ボックスに入力するか、アップデートします。

   有効な値は1～3600秒です。
6. （オプション）インストールのスケジュールを指定または編集するには、スケジュールウィンドウをセットチェックボックスを選択またはクリアします。
   a. スケジュールウィンドウをセットチェックボックスが選択されている場合は、スケジュールの定義に使用する方法を選択またはアップデートします。
      - メンテナンスウィンドウを使用（デフォルト）を選択し、メンテナンスウィンドウページで構成したメンテナンスウィンドウを選択します。

        メンテナンスウィンドウを追加するには、新規をクリックしてメンテナンスウィンドウページに移動します。メンテナンスウィンドウを作成してから、この手順を再開します。
      - 時間枠を指定してくださいを選択し、スケジュールをその場で入力します。
   b. 選択した方法によって、以下のいずれかを実行します。
      - メンテナンスウィンドウを使用が選択されている場合は、メンテナンスウィンドウリストで値を選択または変更します。
      - 時間枠を指定してくださいが選択されている場合は、スケジュールの詳細を追加またはアップデートします。
7. （オプション）手順4で選択したコンポーネントのバージョンがシステムリカバリセットに存在する場合は、リカバリセットをアップデートチェックボックスを選択または選択解除します。

   このオプションが有効になっている場合、システムリカバリセットの既存のコンポーネントは、タスクが完了すると、選択したコンポーネントに置き換えられます。

   このオプションを選択すると、システムリカバリセット内のコンポーネントのバージョンの方が新しい場合でも、コンポーネントが置き換えられます。

   次の場合、このオプションは表示されません。
   - コマンドが選択されている。
   - システムリカバリセットがない。
   - 必要な権限がユーザーアカウントに割り当てられていない。
8. サーバーにTPMまたはTMが存在する場合は、TPMまたはTMの情報を保存するソフトウェアを一時停止またはバックアップしてから、TPMの無効を確認してくださいチェックボックスを選択します。

   ドライブ暗号化ソフトウェアは、TPMまたはTMの情報を保存するソフトウェアの例です。

   > △ **注意**: ドライブ暗号化ソフトウェアを使用している場合は、ファームウェアのアップデートを開始する前に停止してください。この指示に従わない場合、ご使用のデータにアクセスできなくなる可能性があります。
9. OKをクリックします。

   iLOは、タスクがアップデートされたことを通知します。

   タスクの有効期限が、キューでそのタスクに先行するタスクの開始時刻より前に切れる場合、iLOはタスクを保存できないことを通知します。インストールキューは、タスクの先入れ先出しリストです。既存のタスクの実行前に有効期限

が切れるタスクを作成することはできません。

リカバリセットをアップデートチェックボックスを選択した場合は、タスクが開始され、正常に完了した後に、コンポーネントがアップデートされます。

詳しくは

メンテナンスウィンドウの追加
タスクをキューに入れるときに時間枠の詳細を入力する
インストールキューに追加できるコマンド
システムリカバリセット
インストールキュー内のタスクの処理方法

インストールキューからのタスクの削除

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、インストールキュータブをクリックします。
2. コンポーネントの削除アイコン をクリックします。

   iLOが要求を確認するように求めます。
3. はい、削除をクリックします。

   コンポーネントが削除されます。

インストールキューからのすべてのタスクの削除

前提条件

- iLOの設定を構成する権限
- コンポーネントがインストールセットに含まれていない。
- コンポーネントがキューに入れられたタスクの一部ではない。

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、インストールキュータブをクリックします。
2. すべて削除をクリックします。

   iLOが要求を確認するように求めます。
3. はい、削除をクリックします。

   タスクが削除されます。

インストールキューの表示

このタスクについて

インストールキューページにはキューに入っている各タスクの概要情報が表示されます。個々のタスクをクリックすると、詳細情報が表示されます。現在のiLO 日付/時間の値は、ページの上部に表示されます。

手順

1. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、インストールキュータブをクリックします。
2. （オプション）詳細な情報を表示するには、個々のタスクをクリックします。

サブトピック

キューに入れられたタスクサマリーの詳細

個々のタスクの詳細

キューに入れられたタスクサマリーの詳細

状態

タスクのステータス。値には、以下のものがあります。

- 待機中 – コンポーネントタイプのアップデートを開始するソフトウェアがインストール要求を検出したときにタスクは実行されます。
- 進行中 – タスクは処理されています。
- 完了 – タスクが正常に完了しました。
- キャンセル – タスクがキャンセルされた、または期限切れのメンテナンスウィンドウに関連付けられています。
- 失効 – タスクの期限が切れています。このタスクがキューから削除されるまで、その後のタスクは実行されません。
- 例外 – タスクを完了できませんでした。このタスクがキューから削除されるまで、その後のタスクは実行されません。

名前

タスク名。

開始

タスクの開始日時（UTC）。タスクが他のタスクの完了を待機している場合、値は前のタスクの実行後になります。

完了、期限切れ、例外の状態のタスクには、N/Aという値が表示されます。

期限切れ

タスクの有効期限（日付と時刻）（UTC）。有効期限の日付を設定しない場合、なしという値が表示されます。

個々のタスクの詳細

名前

タスク名。

コマンド

コマンドが選択されている場合、この値はコマンド名です。例：待機、iLOリセット。

コンポーネントが選択されている場合、アップデートを適用の値が表示されます。

コンポーネント名

iLOレポジトリのコンポーネントが選択されている場合は、コンポーネント名。

コンポーネント名のリンクをクリックすると、コンポーネントの詳細をiLOレポジトリに表示することができます。

ファイル名

iLOレポジトリのコンポーネントが選択されている場合は、コンポーネントのファイル名。

状態

タスクのステータス。表示される値は保留中、進行中、完了、キャンセル、失効、または例外です。

待機時間（秒）

タスクが待機コマンドの場合は、待機時間（秒）。

結果

タスクの結果（ある場合）。例：タスクは正常に完了しました、アップデートはコンポーネント固有のエラーのために失敗しました。コンポーネントエラーを修正した後にアップデートを再試行してください。

インストール元

選択したコンポーネントのアップデートを開始できるソフトウェア。例：iLO、**Smart Update Manager**、**Smart Update Tool**、UEFI BIOS。

メンテナンスウィンドウ

タスクがメンテナンスウィンドウ中に実行されるように構成されている場合のメンテナンスウィンドウ名。

開始時刻

タスクの開始日時（UTC）。

- 時間枠が指定されている場合は、開始時刻がリストされます。
- メンテナンスウィンドウが選択されている場合は、メンテナンスウィンドウの開始時刻がリストされます。
- 開始時刻が指定されておらず、タスクの状態が完了、失効、または例外の場合は、N/Aの値が表示されます。
- 開始時刻が指定されておらず、タスクの状態が進行中または保留中の場合は、次のようになります。
  - タスクがキューの最初にある場合は、関連するアップデータの確認の後、ただちにの値が表示されます。
  - タスクがキューの最初にない場合は、前のタスクの実行後の値が表示されます。

失効

タスクの有効期限（日付と時刻）（UTC）。

メンテナンスウィンドウが選択されている場合は、メンテナンスウィンドウの終了時刻がリストされます。

リカバリセットをアップデートしますか?

この値が表示されるのは、コンポーネントが選択されている場合だけです。値がはいの場合、キューに入れられたコンポーネントは、タスクが開始され、正常に完了した後にシステムリカバリセット内のコンポーネントを置き換えます。

リカバリセット権限を持つユーザーによって作成されましたか?

この値が表示されるのは、コンポーネントが選択されている場合だけです。値がはいの場合、タスクはリカバリセット権限を持つユーザーによって作成されました。

キューに入れられたアップデートが正常に完了した後に、システムリカバリセットの任意のアップデートを実行するには、この権限が必要です。

ダウングレードポリシーがダウングレードには、’リカバリセット’の権限が必要です。オプションに設定されている場合、この権限はファームウェアのダウングレードにも必要です。

iLO連携の構成と使用

サブトピック

iLO連携

iLO連携の構成

iLO連携機能の使用

iLO連携

iLO連携では、iLO Webインターフェイスを使用して、1つのシステムから複数のサーバーを管理できます。

iLO連携が構成されている場合、iLOはマルチキャスト検出およびピアツーピア通信を使用して、iLO連携グループ内のシステム間の通信を可能にします。

iLO連携ページの1つに移動すると、Webインターフェイスを実行するiLOシステムからそのピアへ、そしてそれらのピアから他のピアへ、選択したiLO連携グループのすべてのデータが取得されるまでデータリクエストが送信されます。

iLOは次の機能をサポートします。

- グループのヘルスステータス - サーバーのヘルス情報とモデル情報を表示します。
- グループ仮想メディア - サーバーのグループからアクセスできるURLベースのメディアに接続します。
- グループ電源制御 - サーバーのグループの電源ステータスを管理します。
- グループファームウェアアップデート - サーバーのグループのファームウェアをアップデートします。
- グループライセンスのインストール - ライセンスキーを入力して、サーバーのグループでライセンス済みのiLO機能を有効にします。
- グループ構成 - 複数のiLOシステムに対するiLO連携グループメンバーシップを追加します。

どのユーザーもiLO連携ページの情報を表示できますが、次の機能を使用するにはライセンスが必要です。グループ仮想メディア、グループ電源制御、グループ消費電力上限、グループ構成、およびグループファームウェアアップデート。

iLO連携の構成

サブトピック

iLO連携機能を使用するための前提条件

iLO連携のネットワーク要件

iLO連携マルチキャストオプションの構成

iLO連携グループ

iLO連携グループメンバーシップを管理する（ローカルiLOシステム）

iLO連携グループメンバーシップの追加（複数のiLOシステム）

エンクロージャーiLO連携サポートの設定

iLO連携機能を使用するための前提条件

手順

- ネットワーク構成が、iLO連携の要件を満たしている。

- iLO連携グループに追加される各iLOシステムで、マルチキャストオプションが構成されている。

  デフォルトのマルチキャストオプションの値を使用する場合、構成は不要です。

- iLO連携のグループメンバーシップが構成されている。

  すべてのiLOシステムが、自動的にDEFAULTグループに追加されます。

- iLO連携のエンクロージャーサポートがOnboard Administratorソフトウェア（ProLiantサーバーブレードのみ）で構成されている。

  この設定は、デフォルトで有効になっています。

iLO連携のネットワーク要件

- （オプション）iLO連携は、IPv4とIPv6の両方をサポートしています。有効な構成が両方のオプションにある場合、IPv6ではなくIPv4を使用するようにiLOを構成できます。この設定を構成するには、IPv6設定ページのiLOクライアントアプリケーションはIPv6を最初に使用オプションを無効にします。
- 複数の場所にあるiLOシステムを管理する場合は、マルチキャストトラフィックを転送するようにネットワークを設定します。
- ネットワーク内のスイッチにマルチキャストトラフィックを有効または無効にするためのオプションが含まれている場合は、有効になっていることを確認します。この構成は、iLO連携と他のHewlett Packard Enterprise製品が、ネットワーク上でiLOシステムを検出するために必要です。
- レイヤー3スイッチで分断されているiLOシステムの場合は、ネットワーク間でSSDPマルチキャストトラフィックを転送するようにスイッチを構成する必要があります。
- iLOシステム間のマルチキャストトラフィック（UDPポート1900）と直接HTTP（TCPのデフォルトポート80）通信を許可するようにネットワークを構成します。
- 複数のVLANを持つネットワークの場合、VLAN間でマルチキャストトラフィックを許可するようにスイッチを構成します。
- レイヤー3スイッチを使用したネットワーク：
  - IPv4ネットワークの場合：スイッチのPIMを有効にし、PIMデンスモードに設定します。
  - IPv6ネットワークの場合：スイッチをMLDスヌーピングに設定します。

詳しくは

IPv6設定の構成
エンクロージャーiLO連携サポートの設定

iLO連携マルチキャストオプションの構成

前提条件

iLOの設定を構成する権限

このタスクについて

以下の手順を実行して、iLO連携グループに追加するシステムのマルチキャストオプションを構成します。デフォルト値を使用する場合は、構成の必要はありません。

手順

1. ナビゲーションツリーでiLO連携をクリックします。

セットアップタブが表示されます。

2. iLO連携管理オプションを有効または無効にします。
3. マルチキャスト検出オプションを有効または無効にします。
4. マルチキャストアナウンスメント間隔（秒/分）の値を入力します。
5. IPv6マルチキャストスコープの値を選択します。

   マルチキャスト検出が正しく機能するようにするため、IPv6マルチキャストスコープに、同じグループ内のすべてのiLOシステムで同じ値を使用していることを確認してください。
6. マルチキャストTime To Live（TTL）の値を入力します。

   マルチキャスト検出が正しく機能するようにするため、マルチキャストTime To Live （TTL）に、同じグループ内のすべてのiLOシステムで同じ値を使用していることを確認してください。
7. 適用をクリックします。

   ネットワークが変更され、このページで行った変更は、次のマルチキャスト通知後に有効となります。

サブトピック

マルチキャストオプション

マルチキャストオプション

iLO連携管理

iLO連携機能を有効または無効にします。デフォルト設定は、有効です。無効を選択すると、ローカルiLOシステムに対するiLO連携機能が無効になります。

マルチキャスト検出

マルチキャスト検出を有効または無効にします。デフォルト設定は、有効です。無効を選択すると、ローカルiLOシステムに対するiLO連携機能が無効になります。

Synergyコンピュートモジュールでは、マルチキャスト検出を無効にすることはできません。Synergyコンピュートモジュールで、ネットワーク上のマルチキャストトラフィックの影響を制限するには、IPv6マルチキャストスコープおよびマルチキャストTime To Live（TTL）の設定を調整します。

マルチキャストアナウンスメント間隔（秒/分）

この値は、iLOシステムがネットワーク上で通知する頻度を設定します。各マルチキャスト通知は約300バイトです。30秒から30分の値を選択します。デフォルト値は10分です。無効を選択すると、ローカルiLOシステムに対するiLO連携機能が無効になります。

表示される値は、以下のとおりです。

- 30、60、120秒
- 5、10、15、30分
- 無効

IPv6マルチキャストスコープ

マルチキャストトラフィックを送受信するネットワークの規模です。有効な値は、リンク、サイト、および組織です。デフォルト値はサイトです。

マルチキャストTime To Live（TTL）

マルチキャスト検出が停止する前に通過できるスイッチの数を指定します。有効な値は1～255です。デフォルト値は5です。

iLO連携グループ

サブトピック

iLO連携グループの特性

- すべてのiLOシステムはDEFAULTグループに自動的に追加され、このグループにはそれぞれのグループメンバーのログイン権限が認められています。DEFAULTグループメンバーシップは編集することも削除することもできます。
- iLO連携グループは、一部共通することも、複数のラックおよびデータセンターにまたがることもできます。また、管理ドメインの作成に使用することもできます。
- 各iLOシステムは最大で10のiLO連携グループのメンバーになることができます。
- グループに指定できるiLOシステムの数に制限はありません。
- グループメンバーシップを構成するには、iLO設定権限が必要です。
- iLO Webインターフェイスを使用して、ローカルiLOシステムまたはiLOシステムのグループのグループメンバーシップを構成することができます。
- RIBCL XMLスクリプトを使用してグループメンバーシップを表示および構成できます。

  詳しくは、iLO連携ユーザーガイドを参照してください。
- iLO RESTful APIを使用してグループメンバーシップを構成できます。

  詳しくは、iLO連携ユーザーガイドを参照してください。
- Hewlett Packard Enterpriseは、同じiLO連携グループ内のiLOシステムには、同じバージョンのiLOファームウェアをインストールすることをお勧めします。

ローカルiLOシステムに対するiLO連携グループメンバーシップ

ローカルiLOシステムにグループメンバーシップを構成する場合、グループのメンバーがローカルの管理対象サーバーを構成するために所有する権限を指定する必要があります。

例えば、ローカルiLOシステムを**group1**に追加し、仮想電源およびリセット権限を割り当てた場合、**group1**の他のiLOシステムのユーザーは管理対象サーバーの電力状態を変更できます。

ローカルiLOシステムが仮想電源およびリセット権限を**group1**に認めていない場合は、**group1**の他のiLOシステムのユーザーはグループの電力制御機能を使用して管理対象サーバーの電力状態を変更することはできません。

ローカルiLOシステム上でiLOセキュリティを無効にするようシステムメンテナンススイッチが設定されている場合、**group1**の他のiLOシステムのユーザーは、割り当てられたグループ権限とは無関係に、管理対象サーバーの状態を変更できます。

ローカルiLOシステムに対するグループメンバーシップは、iLO連携ページのセットアップタブで構成します。

ローカルiLOシステムに対して、以下のタスクを実行できます。

- グループメンバーシップの表示。
- グループメンバーシップの追加と編集。

- グループメンバーシップの削除。

詳しくは

iLO連携グループメンバーシップを管理する（ローカルiLOシステム）

iLOシステムのセットに対するiLO連携グループメンバーシップ

複数のiLOシステムに対するグループメンバーシップを一度に追加する場合、グループのメンバーがグループの他のメンバーを構成するために所有する権限を指定する必要があります。

たとえば、**DEFAULT**グループに基づいて**group2**を構成し、仮想電源およびリセット権限を割り当てた場合、**group2**のiLOシステムのユーザーはグループ内のすべてのサーバーの電力状態を変更できます。

グループ構成ページで、複数のiLOシステムに対してグループメンバーシップを追加できます。

iLOシステムのグループに対して、以下のタスクを実行できます。

- 既存のグループとメンバーは同じだが、権限が異なるグループを作成します。
- iLO連携フィルターを使用して選択したメンバーを含むグループを作成します。

詳しくは

iLO連携グループメンバーシップの追加（複数のiLOシステム）

iLO連携グループの権限

システムがグループに追加されると、グループに以下の権限を付与することができます。

- ログイン - グループのメンバーは、iLOにログインできます。
- 仮想電源およびリセット - グループメンバーは、ホストシステムの電源再投入やリセットを実行できます。これらの操作はシステムの可用性を中断します。
- 仮想メディア - グループメンバーは、管理対象サーバーでURLベースの仮想メディアを使用できます。
- iLOの設定を構成 - グループのメンバーは、iLOの設定を構成し、リモートでファームウェアをアップデートすることができます。

さらに、グループには以下の権限も付与できます。ただし、現在のiLO連携機能セットでは、それらを必要とするアクションをサポートしていません。

- ユーザーアカウント管理 - ユーザーアカウント管理権限を必要とするアクションをサポートします。
- リモートコンソール - リモートコンソール権限を必要とするアクションをサポートします。
- ホストBIOS - ホストBIOS権限を必要とするアクションをサポートします。
- ホストNIC - ホストNIC権限を必要とするアクションをサポートします。
- ホストストレージ - ホストストレージ権限を必要とするアクションをサポートします。
- リカバリセット - リカバリセット権限を必要とするアクションをサポートします。

iLO連携グループメンバーシップを管理する（ローカルiLOシステム）

サブトピック

iLO連携グループメンバーシップの追加

iLO連携グループメンバーシップの編集

ローカルiLOシステムからのグループメンバーシップの削除

iLO連携グループメンバーシップの表示（ローカルiLOシステム）

iLO連携グループメンバーシップの追加

前提条件

- iLOの設定を構成する権限
- アクセス設定ページの最小パスワード長設定が31文字以下に設定されている。

手順

1. ナビゲーションツリーでiLO連携をクリックします。

   セットアップタブが表示されます。
2. グループへの参加をクリックします。
3. グループ名を入力します。

   この値は1～31文字の長さです。
4. グループキーおよびグループキーの確認の値を入力します。

   グループキー（パスワード）は、設定されている最小パスワード長～31文字で指定できます。

   ローカルiLOシステムでパスワードの複雑さが有効になっている場合、グループキーがパスワードの複雑さの要件を満たしている必要があります。
5. グループに割り当てる権限を選択します。

   ローカルiLOシステムによりグループに付与される権限は、管理対象サーバーで、グループ内の他のiLOシステムのユーザーが実行できるタスクを制御します。
6. グループへの参加をクリックします。

   既存のグループの名前とキーを入力した場合、ローカルiLOシステムがそのグループに追加されます。

   存在しないグループの名前とキーを入力した場合、グループが作成され、ローカルiLOシステムがそのグループに追加されます。

詳しくは

ローカルiLOシステムに対するiLO連携グループメンバーシップ
iLO連携グループの権限
iLO連携グループの特性

iLO連携グループメンバーシップの編集

前提条件

- iLOの設定を構成する権限
- グループキーを編集する場合、アクセス設定ページの最小パスワード長設定が31文字以下に設定されている。

手順

1. ナビゲーションツリーでiLO連携をクリックします。

   セットアップタブに、ローカルiLOシステムの既存のグループメンバーシップが表示されます。

2. グループメンバーシップを選択して、編集をクリックします。
3. グループ名を変更するには、グループ名ボックスに新しい名前を入力します。

   グループ名は、1～31文字で指定できます。

4. グループキーを変更するには、グループキーの変更チェックボックスを選択して、グループキーおよびグループキーの確認ボックスに新しい値を入力します。

   グループキーは、設定されている最小パスワード長～31文字で指定できます。

   ローカルiLOシステムでパスワードの複雑さが有効になっている場合、グループキーがパスワードの複雑さの要件を満たしている必要があります。

5. アップデートする権限のチェックボックスをオンまたはオフにします。

   ローカルiLOシステムによりグループに付与される権限は、管理対象サーバーで、グループ内の他のiLOシステムのユーザーが実行できるタスクを制御します。

6. グループのアップデートをクリックします。
7. グループ名またはグループキーをアップデートした場合は、それらを他のシステムの影響を受けるグループでアップデートします。

詳しくは

ローカルiLOシステムに対するiLO連携グループメンバーシップ
iLO連携グループの権限
iLO連携グループの特性

ローカルiLOシステムからのグループメンバーシップの削除

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーでiLO連携をクリックします。

   セットアップタブに、ローカルiLOシステムのグループメンバーシップが表示されます。

2. 削除するグループメンバーシップの横にあるチェックボックスを選択します。
3. 削除をクリックします。
4. 要求を確認するメッセージが表示されたら、はい、削除しますをクリックします。

iLO連携グループメンバーシップの表示（ローカルiLOシステム）

手順

ナビゲーションツリーでiLO連携をクリックします。

このiLOのグループメンバーシップテーブルには、ローカルiLOシステムを含む各グループの名前と、ローカルiLOシステムによってそのグループに与えられている権限が示されます。割り当てられた権限がチェックマークのアイコンで表示され、割り当てられていない権限がXアイコンで表示されます。

詳しくは

iLO連携グループの権限

iLO連携グループメンバーシップの追加（複数のiLOシステム）

サブトピック

既存のグループに基づくグループの追加

サーバーのフィルターされたリストからのグループの作成

グループメンバーシップの変更によって影響を受けるサーバー

既存のグループに基づくグループの追加

前提条件

- iLOの設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- 少なくとも1つのiLO連携グループが存在する。

このタスクについて

この手順を使用して、既存のグループと同じメンバーで構成されるグループを作成します。例えば、DEFAULTグループとシステムは同じだが権限が異なるグループを作成できます。

手順

1. ナビゲーションツリーでiLO連携をクリックして、グループ構成タブをクリックします。
2. 選択されたグループメニューからグループを選択します。

   選択したグループ内のすべてのシステムが、作成したグループに追加されます。
3. 影響を受けるシステム上にグループを作成をクリックします。

   グループの作成インターフェイスが開きます。
4. グループ名を入力します。

   この値は1～31文字の長さです。

   存在するグループ名を入力すると、iLOから一意のグループ名の入力が求められます。
5. グループキーおよびグループキーの確認の値を入力します。

   グループキー（パスワード）は、設定されている最小パスワード長～31文字で指定できます。

   既存のグループ内のシステムでパスワードの複雑さが有効になっており、グループキーがパスワードの複雑さの要件を満たしていない場合、それらのシステムは新しいグループに追加できません。

   グループキーがパスワードの複雑さの要件を満たしていない場合、それらのシステムは新しいグループに追加できません。
6. （オプション）管理するリモートシステム上で、ユーザーアカウントのログイン名およびパスワードを入力します。

   選択したグループに、管理するリモートシステム上のiLOの設定を構成する権限が割り当てられていない場合は、この情報が必要です。

複数のリモートシステムの認証情報を入力するには、ログイン名とパスワードが同じユーザーアカウントを各システムで作成します。

7. グループに割り当てる権限を選択します。

   使用できるすべての権限を選択するには、すべてを選択チェックボックスをクリックします。

8. グループの作成をクリックします。

   グループの作成プロセスには、数分かかります。グループは、マルチキャストアナウンスメント間隔に構成された時間内に、完全に実装されます。

詳しくは

iLO連携グループの権限
iLO連携グループの特性
iLOシステムのセットに対するiLO連携グループメンバーシップ
選択されたグループのリスト

サーバーのフィルターされたリストからのグループの作成

前提条件

- iLOの設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- 少なくとも1つのiLO連携グループが存在する。

このタスクについて

この手順を使用して、サーバーのフィルターされたリストからグループを作成します。例えば、特定バージョンのiLOファームウェアを備えているすべてのサーバーを含むグループを作成する場合があります。

サーバーのフィルターされたリストからグループを作成すると、グループ作成プロセスの間、影響するシステムリスト内のサーバーのみがグループに含まれます。グループが作成された後にフィルターの条件に適合するサーバーは、グループに追加されません。

手順

1. iLO連携ページでフィルターを使用して、システムのセットを作成します。
2. ナビゲーションツリーでiLO連携をクリックして、グループ構成タブをクリックします。

   アクティブなフィルターは影響するシステムリストの上に一覧表示されます。

3. 選択されたグループメニューからグループを選択します。

   選択したグループ内の、選択したフィルター条件に適合するすべてのシステムが、新しいグループに追加されます。

4. 影響を受けるシステム上にグループを作成をクリックします。
5. グループ名を入力します。

   この値は1～31文字の長さです。

   存在するグループ名を入力すると、iLOから一意のグループ名の入力が求められます。

6. グループキーおよびグループキーの確認の値を入力します。

   グループキー（パスワード）は、設定されている最小パスワード長～31文字で指定できます。

   フィルターされたリスト内に、パスワードの複雑さが有効になっているシステムがあり、グループキーがパスワードの複雑さの要件を満たしていない場合、それらのシステムは新しいグループに追加できません。

7. （オプション）管理するリモートシステム上で、ユーザーアカウントのログイン名およびパスワードを入力します。

   選択したグループに、管理するリモートシステム上のiLOの設定を構成する権限が割り当てられていない場合は、この情報が必要です。

   複数のリモートシステムの認証情報を入力するには、ログイン名とパスワードが同じユーザーアカウントを各システムで作成します。

8. グループに割り当てる権限を選択します。

   使用できるすべての権限を選択するには、すべてを選択チェックボックスをクリックします。

9. グループの作成をクリックして設定を保存します。

   グループの作成プロセスには、数分かかります。グループは、マルチキャストアナウンスメント間隔に構成された時間内に、完全に実装されます。

詳しくは

iLO連携グループの権限
iLOシステムのセットに対するiLO連携グループメンバーシップ
iLO連携グループの特性
選択されたグループのリスト

グループメンバーシップの変更によって影響を受けるサーバー

グループ構成ページの影響するシステムセクションには、グループメンバーシップの変更によって影響を受けるサーバーについて、次の詳細が表示されます。

- サーバー名 - ホストオペレーティングシステムで定義されたサーバー名。
- サーバー電源 - サーバー電源の状態（オンまたはオフ）。
- UIDインジケーター - UID LEDの状態。UID LEDを使用すると、特に高密度ラック環境でサーバーを特定し、その位置を見つけることができます。状態には、UIDオン、UIDオフ、およびUID点滅があります。
- iLOホスト名 - iLOサブシステムに割り当てられた完全修飾ネットワーク名。サーバーのiLO Webインターフェイスを開くには、iLOホスト名列のリンクをクリックします。
- IPアドレス - iLOサブシステムのネットワークIPアドレス。サーバーのiLO Webインターフェイスを開くには、IPアドレス列のリンクをクリックします。

次へまたは前へ（使用可能な場合）をクリックして、リストのサーバーをさらに表示します。

詳しくは

iLO連携情報をCSVファイルにエクスポートする方法

エンクロージャーiLO連携サポートの設定

このタスクについて

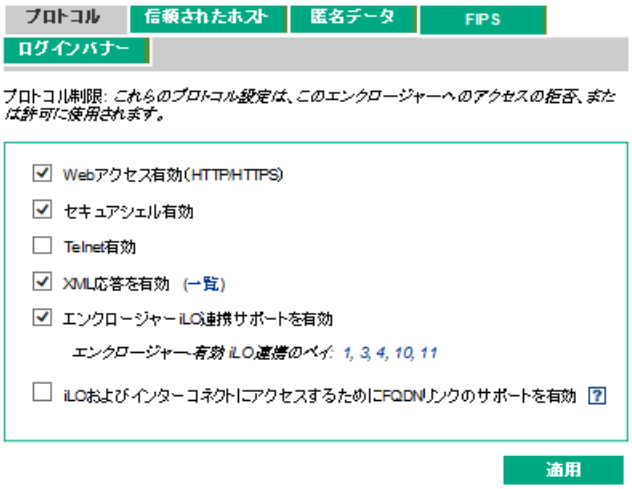
iLO連携でBladeSystem c-Classエンクロージャー内のサーバーブレードを使用する場合、Onboard Administratorソフトウェアで、エンクロージャーiLO連携サポートオプションを有効にする必要があります。この設定は、エンクロージャー内のサーバーブレード間でピアツーピアの通信を可能にするために必要です。エンクロージャーiLO連携サポートを有効オプションは、デフォルトで有効です。

手順

1. Onboard AdministratorのWebインターフェイス（https://<OAのホスト名またはIPアドレス>）にログインします。
2. ナビゲーションツリーで、エンクロージャー情報 > エンクロージャー設定 > ネットワークアクセスを選択します。

プロトコルタブが表示されます。

3. エンクロージャーのiLO連携サポートを有効チェックボックスを選択し、適用をクリックします。



CLIを使用して、エンクロージャーiLO連携サポートを有効オプションを有効または無効にすることもできます。オプションを有効にするには、`ENABLE ENCLOSURE_ILO_FEDERATION_SUPPORT`を入力します。オプションを無効にするには、`DISABLE ENCLOSURE_ILO_FEDERATION_SUPPORT`を入力します。詳しくは、Onboard Administrator CLIユーザーガイドを参照してください。

サブトピック

[iLO連携に関するサーバーブレードサポートの確認]

iLO連携に関するサーバーブレードサポートの確認

手順

1. Onboard AdministratorのWebインターフェイス（https://<OAのホスト名またはIPアドレス>）にログインします。
2. ナビゲーションツリーでデバイスベイ ＞<デバイス名>＞ iLOを選択します。
3. iLO連携機能設定がはいの値に設定されていることを確認します。

iLO連携機能の使用

サブトピック

[選択されたグループのリスト]

[iLO連携情報をCSVファイルにエクスポートする方法]

[iLO連携マルチシステムビュー]

[iLO連携マルチシステムマップの表示]

[iLO連携グループ仮想メディア]

[iLO連携グループ電源]

[グループ消費電力上限の構成]

iLO連携グループファームウェアアップデート

ライセンスキーのインストール（iLO連携グループ）

選択されたグループのリスト

セットアップを除くすべてのiLO連携のページには、選択されたグループのリストがあります。

選択されたグループリストからグループを選択する場合：

- グループ仮想メディア、グループ電源、グループファームウェアアップデート、グループライセンス、およびグループ構成ページでの変更の影響を受けるサーバーは、影響するシステムの表に表示されます。
- iLO連携ページに表示される情報は、選択したグループ内のすべてのサーバーに適用されます。
- iLO連携ページで加えた変更は、選択したグループ内のすべてのサーバーに適用されます。
- 選択されたグループはcookieに保存され、iLOからログアウトする場合でも、維持されます。

グループを選択した後、サーバーの情報を表示するため、またはグループ内のサーバーのサブセットに対して操作を実行するために、リスト内のサーバーをフィルター処理できます。

サブトピック

選択されたグループのリストのフィルター

選択されたグループのリストのフィルター条件

選択されたグループのリストのフィルター

サーバーのリストを選別する場合：

- iLO連携ページに表示される情報は、フィルター条件に適合する、選択したグループ内のすべてのサーバーに適用されます。
- iLO連携ページで加えた変更は、フィルター条件に適合する、選択したグループ内のすべてのサーバーに適用されます。
- フィルターの設定はcookieに保存され、iLOからログアウトする場合でも、維持されます。
- Xアイコンまたはフィルター名をクリックすることで、フィルターを削除できます。

選択されたグループのリストのフィルター条件

次の条件を使用して、グループ内のサーバーをフィルタリングすることができます。

- ヘルスステータス - ヘルスステータスのリンクをクリックして、特定のヘルスステータスを持つサーバーを選択します。
- モデル - サーバーのモデル番号リンクをクリックして、選択したモデルと一致するサーバーを選択します。
- サーバー名 - 個々のサーバーによってフィルタリングするには、サーバー名をクリックします。
- ファームウェア情報 - ファームウェアのバージョンまたはフラッシュステータスをクリックし、選択したファームウェアのバージョンまたはステータスに一致するサーバーを選択します。
- TPMまたはTMオプションROM計測 - オプションROM計測ステータスをクリックして、選択したオプションROM計測のステータスに一致するサーバーを含めるか、除外します。

- ライセンスの使用 – ライセンスキーに関連するエラーメッセージが表示される場合は、ライセンスキーをクリックして、そのライセンスキーを使用しているサーバーを選択します。
- ライセンスタイプ – ライセンスタイプをクリックして、選択したライセンスタイプがインストールされているサーバーを選択します。
- **ライセンスステータス** – ライセンスステータスをクリックして、選択したステータスに一致するライセンスがインストールされているサーバーを選択します。

iLO連携情報をCSVファイルにエクスポートする方法

前提条件

iLOの構成とネットワーク構成が、iLO連携機能を使用するための前提条件を満たしている。

このタスクについて

以下のiLO連携ページで、情報をCSVファイルにエクスポートできます。

- マルチシステムビュー – クリティカルまたは劣化のステータスのシステムリストをエクスポートします。
- マルチシステムマップ – iLOピアリストをエクスポートします。
- グループ仮想メディア – 影響を受けるシステムリストをエクスポートします。
- グループ電源 – 影響を受けるシステムリストをエクスポートします。
- グループファームウェアアップデート – 影響を受けるシステムリストをエクスポートします。
- グループライセンス – 影響を受けるシステムリストをエクスポートします。
- グループの構成 – 影響を受けるシステムリストをエクスポートします。

手順

1. ファイルエクスポート機能をサポートするページに移動します。
2. 表をCSV形式で表示をクリックします。
3. CSVアウトプットウィンドウで、保存をクリックしてから、ブラウザーのプロンプトに従ってファイルを保存または開きます。

   サーバーが複数のページにまたがってリストされている場合、CSVファイルにはiLOのWebインターフェイスページに現在表示されているサーバーだけが含まれます。

   クエリのエラーが発生した場合、クエリに応答しなかったシステムは、iLOのWebインターフェイスページおよびCSVファイルから除外されます。

詳しくは

iLO連携機能を使用するための前提条件

iLO連携マルチシステムビュー

マルチシステムビューページは、iLO連携グループ内のサーバーモデル、サーバーのヘルス、およびクリティカルおよび劣化したサーバーに関する概要を提供します。

サブトピック

サーバーヘルスおよびモデル情報の表示

クリティカルおよび劣化のステータスを持つサーバーの表示

サーバーヘルスおよびモデル情報の表示

前提条件

iLOの構成とネットワーク構成が、iLO連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーでiLO連携をクリックして、マルチシステムビュータブをクリックします。
2. 選択されたグループメニューからグループを選択します。
3. （オプション）サーバーのリストをフィルタリングするには、ヘルスステータス、サーバーモデル、またはサーバー名のリンクをクリックします。

サブトピック

サーバーヘルスおよびモデルの詳細

詳しくは

iLO連携機能を使用するための前提条件

サーバーヘルスおよびモデルの詳細

- ヘルス – 表示された各ヘルスステータスにあるサーバーの数。一覧表示された各ヘルスステータス内のサーバーの総数の%も表示されます。
- モデル – モデル番号でグループ化したサーバーのリスト。各モデル番号に対するサーバー総数の割合（%）も表示されます。
- クリティカルおよび劣化システム – ステータスがクリティカルまたは劣化であるサーバーのリスト。

詳しくは

サブシステムおよびデバイスステータスの値

クリティカルおよび劣化のステータスを持つサーバーの表示

前提条件

iLOの構成とネットワーク構成が、iLO連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーでiLO連携をクリックして、マルチシステムビュータブをクリックします。
2. 選択されたグループメニューからグループを選択します。
3. （オプション）サーバーのリストをフィルタリングするには、ヘルスステータス、サーバーモデル、またはサーバー名のリンクをクリックします。
4. 次へまたは前へ（使用できる場合）をクリックして、クリティカルおよび劣化システムリストのサーバーをさらに表示します。

サブトピック

クリティカルおよび劣化のサーバーステータスの詳細

詳しくは

iLO連携機能を使用するための前提条件

クリティカルおよび劣化のサーバーステータスの詳細

- サーバー名 - ホストオペレーティングシステムで定義されたサーバー名。
- システムヘルス - サーバーのヘルスステータス。
- サーバーの電源 - サーバーの電源ステータス（オンまたはオフ）。
- UIDインジケーター - サーバーUID LEDの状態。UID LEDを使用すると、特に高密度ラック環境でサーバーを特定し、その位置を見つけることができます。状態には、UIDオン、UIDオフ、およびUID点滅があります。
- システムROM - インストールされているシステムROMバージョン。
- iLOホスト名 - iLOサブシステムに割り当てられた完全修飾ネットワーク名。サーバーのiLO Webインターフェイスを開くには、iLOホスト名列のリンクをクリックします。
- IPアドレス - iLOサブシステムのネットワークIPアドレス。サーバーのiLO Webインターフェイスを開くには、IPアドレス列のリンクをクリックします。

詳しくは

サブシステムおよびデバイスステータスの値
iLO連携情報をCSVファイルにエクスポートする方法

iLO連携マルチシステムマップの表示

前提条件

iLOの構成とネットワーク構成が、iLO連携機能を使用するための前提条件を満たしている。

このタスクについて

マルチシステムマップページには、ローカルiLOシステムのピアに関する情報が表示されます。ローカルiLOシステムはマルチキャスト検出を使用してそのピアを識別します。

iLO連携ページの1つに移動すると、Webインターフェイスを実行するiLOシステムからそのピアへ、そしてそれらのピアから他のピアへ、選択したグループのすべてのデータが取得されるまでデータリクエストが送信されます。

手順

1. ナビゲーションツリーでiLO連携をクリックして、マルチシステムマップタブをクリックします。
2. 選択されたグループメニューからグループを選択します。

サブトピック

iLOピアの詳細

詳しくは

iLO連携機能を使用するための前提条件

iLOピアの詳細

- # - ピア番号。

- iLO UUID - iLOシステムのUPnP UUID。
- 最後の参照 - サーバーからの前回の通信のタイムスタンプ。
- 最後のエラー - 表示されているピアとローカルのiLOシステムの間での最新の通信エラーの説明。
- 問い合わせ時間（秒）- タイムアウトが発生した場合、この値を使用して、迅速に応答していないシステムを識別できます。この値は、最新のクエリに適用されます。
- ノードカウント - エラーが発生した場合、この値は、不足している可能性があるデータの量を示していることがあります。値がゼロであることは、直前のクエリがタイムアウトしたことを示します。この値は、最新のクエリに適用されます。
- URL - 表示されているピアのiLO Webインターフェイスを起動するためのURL。
- IP - ピアのIPアドレス。

詳しくは

iLO連携情報をCSVファイルにエクスポートする方法

iLO連携グループ仮想メディア

グループ仮想メディアを使用すると、サーバーのグループからアクセスできるURLベースのメディアに接続できます。

- URLベースの仮想メディアは、1.44 MBのフロッピーディスクイメージ（IMG）およびCD/DVD-ROMイメージ（ISO）のみをサポートします。イメージは、グループ化されたiLOシステムと同じネットワーク上のWebサーバーに存在する必要があります。
- 同時に1種類のメディアしかグループに接続できません。
- URLベースのメディアの表示、接続、取り出しや、CD/DVD-ROMディスクイメージからの起動ができます。URLベースのメディアを使用する場合は、フロッピーディスクやCD/DVD-ROMのディスクイメージをWebサーバーに保存し、URLを使用してそのディスクイメージに接続します。iLOではHTTPまたはHTTPS形式のURLを使用できます。iLOはFTPをサポートしていません。
- 仮想メディア機能を使用する前に、仮想メディアオペレーティングシステムに関する注意事項を確認してください。

サブトピック

グループのURLベースの仮想メディアの接続

グループのURLベースの仮想メディアのステータス表示

URLベースの仮想メディアデバイスの取り出し

グループ仮想メディアの操作の影響を受けるサーバー

詳しくは

仮想メディアを使用するためのオペレーティングシステム要件

グループのURLベースの仮想メディアの接続

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- 選択したiLO連携グループの各メンバーが、仮想メディア権限をグループに認めている。

- iLOの構成とネットワーク構成が、iLO連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーでiLO連携をクリックして、グループ仮想メディアタブをクリックします。
2. 選択されたグループメニューからグループを選択します。

   接続するURLベースのメディアは、選択したグループ内のすべてのシステムで利用可能になります。
3. 仮想フロッピーに接続セクション（IMGファイル）またはCD/DVD-ROMを接続セクション（ISOファイル）の仮想メディアURLボックスにディスクイメージのURLを入力します。
4. 次のサーバー再起動時にのみこのディスクイメージからグループ内のサーバーを起動する場合は、次回リセット時に起動チェックボックスを選択します。

   イメージは2番目のサーバー再起動時に自動的に取り出されるので、サーバーは一度しかこのイメージから起動しません。

   このチェックボックスを選択しない場合、イメージは手動で取り出すまで接続されたまま残ります。また、サーバーは、システムブートオプションがそのように設定されている場合、以後のすべてのサーバーリセットでイメージから起動します。

   次回のリセット時に起動チェックボックスを有効にしているときにグループ内のサーバーがPOSTを実行していると、エラーが発生します。POST中はサーバーブート順序を変更できません。POSTが終了するのを待ってから、再試行してください。
5. 仮想フロッピーデバイスのみ：読み取り専用パーミッションを持つ仮想メディアデバイスを接続する場合、読み取り専用チェックボックスを選択します。

   読み取り専用チェックボックスはデフォルトで有効になっています。
6. メディアの挿入をクリックします。

   iLOはコマンドの結果を表示します。

詳しくは

iLO連携機能を使用するための前提条件

グループのURLベースの仮想メディアのステータス表示

前提条件

iLOの構成とネットワーク構成が、iLO連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーでiLO連携をクリックして、グループ仮想メディアタブをクリックします。
2. （オプション）表示される情報をフィルタリングするには、読み取り専用ステータスあるいはイメージURLいずれかのリンクをクリックします。

サブトピック

URLベースの仮想メディアの詳細

詳しくは

iLO連携機能を使用するための前提条件

URLベースの仮想メディアの詳細

URLベースの仮想メディアを接続すると、以下のセクションに詳細が表示されます。

仮想フロッピー/USBキー/仮想フォルダーステータス

- 挿入されたメディア - 接続されている仮想メディアの種類。URLベースのメディアが接続されている場合、スクリプトメディアと表示されます。
- イメージが接続されました - 仮想メディアデバイスが接続されているかどうかを示します。
- 読み取り専用ステータス - 仮想メディアデバイスが読み取り専用と読み取り/書き込みのどちらのアクセス許可で接続されているかを示します。
- イメージURL - 接続されているURLベースのメディアをポイントするURL。

仮想CD/DVD-ROMステータス

- 挿入されたメディア - 接続されている仮想メディアの種類。URLベースのメディアが接続されている場合、スクリプトメディアと表示されます。
- イメージが接続されました - 仮想メディアデバイスが接続されているかどうかを示します。
- イメージURL - 接続されているURLベースのメディアをポイントするURL。

URLベースの仮想メディアデバイスの取り出し

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- 選択したiLO連携グループの各メンバーが、仮想メディア権限をグループに認めている。
- iLOの構成とネットワーク構成が、iLO連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーでiLO連携をクリックして、グループ仮想メディアタブをクリックします。
2. 選択されたグループメニューからグループを選択します。

   取り出すURLベースの仮想メディアデバイスは、選択したグループ内のすべてのシステムから切断されます。
3. 仮想フロッピーステータスセクションまたは仮想CD/DVD-ROMステータスセクションのメディアの取り出しをクリックします。

詳しくは

iLO連携機能を使用するための前提条件

グループ仮想メディアの操作の影響を受けるサーバー

影響するシステムセクションには、グループ仮想メディアの操作を開始すると影響を受けるサーバーについて、次の詳細が表示されます。

- サーバー名 - ホストオペレーティングシステムで定義されたサーバー名。
- サーバー電源 - サーバー電源の状態（オンまたはオフ）。
- UIDインジケーター - UID LEDの状態。UID LEDを使用すると、特に高密度ラック環境でサーバーを特定し、その位置を見つけることができます。状態には、UIDオン、UIDオフ、およびUID点滅があります。

- iLOホスト名 – iLOサブシステムに割り当てられた完全修飾ネットワーク名。サーバーのiLO Webインターフェイスを開くには、iLOホスト名列のリンクをクリックします。
- IPアドレス – iLOサブシステムのネットワークIPアドレス。サーバーのiLO Webインターフェイスを開くには、IPアドレス列のリンクをクリックします。

次へまたは前へ（使用可能な場合）をクリックして、リストのサーバーをさらに表示します。

詳しくは

iLO連携情報をCSVファイルにエクスポートする方法

iLO連携グループ電源

グループ電源機能を使用すると、iLO Webインターフェイスを実行しているシステムから複数のサーバーの電源を管理できます。この機能を使用して、以下を行います。

- オンまたはリセット状態にあるサーバーのグループに対して、電源を切る、リセットする、または電源再投入を行う。
- オフ状態にあるサーバーのグループに対して電源を入れる。
- グループ電源ページの仮想電源ボタンセクションでボタンをクリックすると影響を受けるサーバーのリストを表示する。

サーバーグループの電源状態の変更

前提条件

- 仮想電源およびリセット権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- 選択したiLO連携グループの各メンバーが、仮想電源およびリセット権限をグループに認めている。
- iLOの構成とネットワーク構成が、iLO連携機能を使用するための前提条件を満たしている。

このタスクについて

グループ電源ページの仮想電源ボタンセクションには、グループ内のサーバーの現在の電源状態をまとめています。概要情報として、オン、オフ、またはリセット状態のサーバーの合計数が含まれます。 システム電源概要は、ページが初めて開かれるときのサーバー電源の状態を示します。システム電源情報をアップデートするには、ブラウザーの更新機能を使用します。

手順

1. ナビゲーションツリーでiLO連携をクリックして、グループ電源タブをクリックします。
2. 選択されたグループメニューからグループを選択します。

   iLOは電源状態別にグループ化されたサーバーを表示し、各状態のサーバーの合計数を示すカウンターも表示します。
3. サーバーのグループの電源状態を変更するには、次のいずれかを実行します。
   - オンまたはリセット状態にあるサーバーの場合は、次のいずれかのボタンをクリックします。
     - 瞬間的に押す
     - 押し続ける
     - リセット
     - コールドブート
   - オフ状態にあるサーバーの場合は、瞬間的に押すボタンをクリックします。

オフ状態にあるサーバーでは、押し続ける、リセット、およびコールドブートオプションは使用できません。

iLOが要求を確認するように求めます。

4. はい、<アクション>をクリックします。

   例えば、リセットをクリックすると、ボタンのラベルがはい、リセットしますになります。クリックするボタンの名前は、開始したグループ電源オプションによって異なります。

   仮想電源ボタンの作動に対してグループ化されたサーバーが応答する間、iLOには進行状況バーが表示されます。進行状況バーには、コマンドの実行に成功したサーバーの数が示されます。

   コマンド結果セクションには、電源状態の変更に関連したエラーメッセージなど、コマンドのステータスおよび結果が表示されます。

詳しくは

iLO連携機能を使用するための前提条件

グループの電源状態オプション

- 瞬間的に押す - 物理的な電源ボタンを押す場合と同じです。

  一部のオペレーティングシステムは、瞬間的に押した後で適切なシャットダウンを開始するか、またはこのイベントを無視するように構成されている場合があります。Hewlett Packard Enterpriseでは、仮想電源ボタンを使用してシャットダウンを実行する前に、システムコマンドを使用して正常なオペレーティングシステムのシャットダウンを完了することをお勧めします。

- 押し続ける - 物理的な電源ボタンを5秒間押し続け、離すことと同じです。

  この操作の結果、選択したグループ内のサーバー電源がオフになります。このオプションを使用すると、適切なオペレーティングシステムの終了に影響する場合があります。

  このオプションは、一部のオペレーティングシステムが実装しているACPI機能を提供します。これらのオペレーティングシステムは、瞬間的に押すと押し続けるによって動作が異なります。

- コールドブート - 選択したグループ内のサーバー電源をただちに切ります。プロセッサー、メモリ、およびI/Oリソースは、メインの電源が失われます。サーバーは、約6秒後再起動します。このオプションを使用すると、適切なオペレーティングシステムの終了に影響します。

- リセット - 選択したグループ内のサーバーを強制的にウォームブートします。CPUとI/Oリソースがリセットされます。このオプションを使用すると、適切なオペレーティングシステムの終了に影響します。

グループの電源状態の変更によって影響を受けるサーバー

影響するシステムリストには、仮想電源ボタンの動作を開始すると影響を受けるサーバーについて、次の詳細が示されます。

- サーバー名 - ホストオペレーティングシステムで定義されたサーバー名。
- サーバー電源 - サーバー電源の状態（オンまたはオフ）。
- UIDインジケーター - UID LEDの状態。UID LEDを使用すると、特に高密度ラック環境でサーバーを特定し、その位置を見つけることができます。状態には、UIDオン、UIDオフ、およびUID点滅があります。
- iLOホスト名 - iLOサブシステムに割り当てられた完全修飾ネットワーク名。サーバーのiLO Webインターフェイスを開くには、iLOホスト名列のリンクをクリックします。
- IPアドレス - iLOサブシステムのネットワークIPアドレス。サーバーのiLO Webインターフェイスを開くには、IPアドレス列のリンクをクリックします。

次へまたは前へ（使用可能な場合）をクリックして、リストのサーバーをさらに表示します。

詳しくは

グループ消費電力上限の構成

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- 選択したiLO連携グループの各メンバーが、iLO設定権限をグループに認めている。
- iLOの構成とネットワーク構成が、iLO連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーでiLO連携をクリックして、グループ電力設定タブをクリックします。
2. 選択されたグループメニューからグループを選択します。

   このページで行った変更は、選択したグループ内のすべてのシステムに影響します。
3. 手動の電力消費上限を有効オプションを有効に設定します。
4. 消費電力上限値をワット数、BTU/時、または割合（%）で入力します。

   %は、最大電力値と最小電力値の差です。消費電力上限値は、サーバー最小電力値より下には設定できません。
5. （オプション）値がワット単位で表示されている場合、BTU/時単位での表示に変更するには電力単位メニューのBTU/時を選択します。値がBTU/時で表示されている場合、ワット単位での表示に変更するにはワットを選択します。
6. 適用をクリックします。

詳しくは

iLO連携機能を使用するための前提条件

グループ消費電力上限の注意事項

グループ消費電力上限機能では、iLO Webインターフェイスを実行するシステムから、複数のサーバーの消費電力上限を動的に設定することができます。

- グループ消費電力上限を設定している場合、グループ化されたサーバーは、消費電力上限を超えないように電力を共有します。電力はビジー状態のサーバーにより多く割り当てられ、アイドル状態のサーバーにはより少ない電力が割り当てられます。
- グループに対して設定した消費電力上限は、個々のサーバーの電力設定ページで設定できる消費電力上限とともに動作します。
- エンクロージャーまたは個々のサーバーレベルで構成されている消費電力上限や、別のiLO連携グループによって構成されている消費電力上限がサーバーに影響を与える場合は、他のグループの消費電力上限によりそのサーバーに割り当てられる電力が少なくなる可能性があります。
- 消費電力上限が設定されている場合、グループ化されたサーバーの平均電力測定値は、消費電力上限値以下である必要があります。
- POST実行中、ROMは最大電力測定値と最小電力測定値を決定する2つの電力テストを実行します。

  消費電力上限の設定を決定するときは、HPE自動グループ消費電力上限の設定の表の値を考慮してください。
  - 最大利用可能電力 - グループ内のすべてのサーバーの総電源容量。この値は、最大消費電力上限値のしきい値でもあります。設定できる最高の消費電力上限です。
  - サーバー最大電力 - グループ内のすべてのサーバーの最大電力測定値。この値は、最小ハイパフォーマンス上限のしきい値でもあります。グループ内のサーバーのパフォーマンスに影響を与えずに設定できる最小の消費電力上限

値です。

- サーバー最小電力 - グループ内のすべてのサーバーの最小電力測定値。この値は、最小消費電力上限のしきい値でもあります。グループ内のサーバーが使用する最小電力を表します。この値に設定されている消費電力上限は、サーバーの電力使用量を最小化するため、その結果サーバーのパフォーマンスが低下します。

- 消費電力上限は、一部のサーバーではサポートされていません。詳しくは、サーバーの仕様書を参照してください。
- 一部のサーバーでは、iLO Webインターフェイスの外部で消費電力上限設定を管理する必要があります。次のようなツールを使用できます。
  - HPE Advanced Power Manager

  サーバーでサポートされる電力管理機能について詳しくは、https://www.hpe.com/info/qsでサーバーの仕様書を参照してください。

グループ消費電力上限情報の表示

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- iLOの構成とネットワーク構成が、iLO連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーでiLO連携をクリックして、グループ電源設定タブをクリックします。
2. 選択されたグループメニューからグループを選択します。
3. （オプション）値がワット単位で表示されている場合、BTU/時単位での表示に変更するには値をBTU/時で表示をクリックします。値がBTU/時で表示されている場合、表示をWに変更するには値をワットで表示をクリックします。

詳しくは

iLO連携機能を使用するための前提条件

消費電力上限の詳細

HPE自動グループ消費電力上限の設定

このセクションの内容は、次のとおりです。

- 計測された電力値 - 最大利用可能電力、サーバー最大電力、およびサーバー最小電力。
- 電力消費上限値 - 電力消費上限値（設定されている場合）。

現在の状態

このセクションでは、以下の内容について説明します。

- 現在の電力測定値 - 選択されたグループの現在の電力測定値。
- 現在の消費電力上限値 - 選択したグループに割り当てられている電力の合計量。消費電力上限が設定されていない場合、この値はゼロです。

このシステムへのグループの電力割り当て

ローカルiLOシステムに影響を及ぼすグループ消費電力上限と、各グループ消費電力上限によってローカルiLOシステムに割り当てられる電力の量。消費電力上限が設定されていない場合、割り当て電力値はゼロです。

iLO連携グループファームウェアアップデート

グループファームウェアアップデート機能では、iLO Webインターフェイスを実行している1つのシステムから、複数のサーバーのファームウェア情報を表示し、ファームウェアをアップデートすることができます。

グループのファームウェアアップデート機能は、次のファームウェアタイプをサポートします。これらのファームウェアタイプは、サーバーと環境がサポートしている場合にのみアップデートできます。

- iLOファームウェア
- システムROM（BIOS）
- Power Management Controller
- システムプログラマブルロジックデバイス（CPLD）
- NVMeバックプレーンファームウェア
- サーバープラットフォームサービス（SPS）
- 言語パック
- サードパーティのファームウェアパッケージ

  プラットフォームレベルのデータモデル（PLDM）ファームウェアパッケージがサポートされるのは、アクセス設定ページでサードパーティーのファームウェアアップデートパッケージの受け入れオプションが有効の場合です。
- GPU

  次のGPUがサポートされます。
  - NVIDIA A100 x4/x8 SXM4
  - AMD MI100 GPU

一部のファームウェアタイプは、組み合わせたアップデートとして提供されます。以下に例を示します。

- SASプログラマブルロジックデバイスのアップデートは、多くの場合、SASコントローラーのファームウェアアップデートとの組み合わせになります。
- Intelligent Platform Abstraction Dataのファームウェアは、多くの場合、システムROM/BIOSのアップデートとの組み合わせになります。

サブトピック

複数のサーバーのファームウェアのアップデート

グループのファームウェアアップデートの影響を受けるサーバー

グループファームウェア情報の表示

複数のサーバーのファームウェアのアップデート

前提条件

- iLOの設定を構成する権限
- 選択したiLO連携グループの各メンバーが、iLO設定権限をグループに認めている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- iLOの構成とネットワーク構成が、iLO連携機能を使用するための前提条件を満たしている。

手順

1. サポートされているファームウェアを、Hewlett Packard Enterpriseサポートセンター

（https://www.hpe.com/support/hpesc）からダウンロードしてください。

2. Webサーバーにファームウェアファイルを保存します。
3. ナビゲーションツリーでiLO連携をクリックして、グループファームウェアアップデートタブをクリックします。
4. 選択されたグループメニューからグループを選択します。

   このページでファームウェアアップデートを開始すると、選択したグループ内のすべてのシステムが影響を受けます。
5. （オプション）ファームウェアのバージョン、フラッシュステータス、またはTPMまたはTMオプションROM計測ステータスリンクをクリックして、影響を受けたシステムのリストをフィルタリングします。

   △ 注意:

   TPMまたはTMがインストールされているサーバーでシステムROMまたはiLOファームウェアのアップデートを実行しようとすると、iLOは、TPMまたはTMに情報を保存しているソフトウェアを一時停止またはバックアップするように求めます。例えば、ドライブ暗号化ソフトウェアを使用している場合は、ファームウェアのアップデートを開始する前に停止してください。この指示に従わない場合、ご使用のデータにアクセスできなくなる可能性があります。
6. サーバープラットフォームサービス（SPS）のファームウェアをアップデートする場合は、アップデートしたいサーバーの電源を切ってから30秒待ちます。

   サーバーOSの実行中は、SPSファームウェアをアップデートできません。
7. ファームウェアアップデートセクションで、Webサーバーのファームウェアファイルへのurlを入力し、ファームウェアのアップデートをクリックします。

   入力するURLは、`http://<server.example.com>/<subdir>/iLO6_<yyy>.bin`です。ここで、`<yyy>`はファームウェアバージョンを表します。

   iLOが要求を確認するように求めます。
8. はい、アップデートしますをクリックします。

   選択した各システムがファームウェアイメージをダウンロードし、それをフラッシュしようと試みます。

   フラッシュステータスセクションがアップデートされ、iLOはアップデートが進行中であることを通知します。アップデートが完了すると、ファームウェア情報セクションがアップデートされます。

   ファームウェアイメージがシステムに対して無効か、署名が不適切またはない場合、iLOはイメージを拒否し、フラッシュステータスセクションに、影響を受けるシステムのエラーが表示されます。

   ファームウェアアップデートの種類によっては、新しいファームウェアを有効にするために、システムのリセット、iLOのリセット、またはサーバーの再起動が必要になる場合があります。

詳しくは

iLOファームウェアイメージファイルの入手
サポートされるサーバーファームウェアイメージファイルの入手
iLO連携機能を使用するための前提条件
選択されたグループのリスト

グループのファームウェアアップデートの影響を受けるサーバー

影響するシステムリストには、グループのファームウェアアップデートによって影響を受けるサーバーについて、次の詳細が示されます。

- サーバー名 - ホストオペレーティングシステムで定義されたサーバー名。
- システムROM - インストールされているシステムROM（BIOS）。

- iLOファームウェアバージョン – インストールされているiLOファームウェアバージョン。
- iLOホスト名 – iLOサブシステムに割り当てられた完全修飾ネットワーク名。サーバーのiLO Webインターフェイスを開くには、iLOホスト名列のリンクをクリックします。
- IPアドレス – iLOサブシステムのネットワークIPアドレス。サーバーのiLO Webインターフェイスを開くには、IPアドレス列のリンクをクリックします。

次へまたは前へ（使用可能な場合）をクリックして、リストのサーバーをさらに表示します。

詳しくは

iLO連携情報をCSVファイルにエクスポートする方法

グループファームウェア情報の表示

前提条件

iLOの構成とネットワーク構成が、iLO連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーでiLO連携をクリックして、グループファームウェアアップデートタブをクリックします。
2. 選択されたグループメニューからグループを選択します。
3. （オプション）ファームウェアのバージョン、フラッシュステータス、またはTPMまたはTMオプションROM計測ステータスリンクをクリックして、表示されるシステムのリストをフィルタリングします。

サブトピック

ファームウェアの詳細

詳しくは

iLO連携機能を使用するための前提条件
選択されたグループのリスト

ファームウェアの詳細

ファームウェア情報セクションには、以下の情報が表示されます。

- サポート対象のiLOファームウェアバージョンのサーバー数。リストされているファームウェアのバージョンを搭載するサーバーの総数の割合（%）も表示されます。
- グループ化されたサーバーのフラッシュステータス。一覧表示されたステータスのサーバーの総数の%も表示されます。
- グループ化されたサーバーのTPMまたはTMオプションROM計測ステータス。一覧表示されたステータスのサーバーの総数の%も表示されます。
- システムROMのバージョンごとのサーバーの数。一覧表示されたシステムROMバージョンを搭載するサーバーの総数の%も表示されます。

ライセンスキーのインストール（iLO連携グループ）

前提条件

- iLOの設定を構成する権限

- iLO連携グループの各メンバーが、iLO設定の構成権限をグループに認めている。
- iLOライセンスが、選択したサーバーでサポートされている。
- 選択したサーバーの数に対して認証されているiLOライセンスアクティベーションキーを取得している。
- iLOの構成とネットワーク構成が、iLO連携機能を使用するための前提条件を満たしている。

このタスクについて

グループライセンスページには、選択したiLO連携グループのメンバーのライセンスステータスが表示されます。以下の手順を使用して、キーを入力して、ライセンス済みのiLO機能を有効にします。

手順

1. ナビゲーションツリーでiLO連携をクリックして、グループライセンスタブをクリックします。
2. （オプション）影響を受けたシステムのリストをフィルタリングするには、ライセンスのタイプまたはステータスリンクをクリックします。

   以下に例を示します。すでにキーがインストールされているサーバー上でライセンスキーをインストールした場合、現在のキーは新しいキーに置き換えられます。既存のライセンスを置き換えたくない場合は、ステータスセクションのUnlicensedをクリックして、ライセンスが適用されていないサーバーにのみラインセンスをインストールします。
3. アクティベーションキーボックスにライセンスキーを入力します。

   アクティベーションキーボックスで、セグメント間でカーソルを移動するには、Tabキーを押す、またはボックスのセグメントの内側をクリックします。 アクティベーションキーボックスのセグメントにデータを入力すると、カーソルは自動的に次に進みます。

   ライセンスキーをインストールすると、iLOに最後の5桁のみが表示されます。Hewlett Packard Enterpriseでは、後で必要になる場合に備えて、ライセンスキー情報を記録して保存することをお勧めします。
4. インストールをクリックします。

   エンドユーザー使用許諾契約を読み、合意したことを確認するプロンプトがiLOで表示されます。

   エンドユーザー使用許諾契約の詳細は、ライセンスパックオプションキットに記載されています。
5. 同意するをクリックします。

   ライセンスがインストールされた後、ライセンス情報セクションがアップデートされ、選択したグループ用の新しいライセンスの詳細を表示します。

詳しくは

iLOライセンス
iLO連携機能を使用するための前提条件
選択されたグループのリスト

ライセンスインストールの影響を受けるサーバー

影響するシステムセクションには、ライセンスキーをインストールする場合に影響を受けるサーバーに関する、次の詳細が表示されます。

- サーバー名 - ホストオペレーティングシステムで定義されたサーバー名。
- ライセンス - インストールされているライセンスタイプ。
- iLOファームウェアバージョン - インストールされているiLOファームウェアバージョン。
- iLOホスト名 - iLOサブシステムに割り当てられた完全修飾ネットワーク名。サーバーのiLO Webインターフェイスを開くには、iLOホスト名列のリンクをクリックします。
- IPアドレス - iLOサブシステムのネットワークIPアドレス。サーバーのiLO Webインターフェイスを開くには、IPアドレス列のリンクをクリックします。

次へまたは前へ（使用可能な場合）をクリックして、リストのサーバーをさらに表示します。

詳しくは

iLO連携情報をCSVファイルにエクスポートする方法

iLO連携グループライセンス情報の表示

前提条件

iLOの構成とネットワーク構成が、iLO連携機能を使用するための前提条件を満たしている。

手順

1. ナビゲーションツリーでiLO連携をクリックして、グループライセンスタブをクリックします。
2. 選択されたグループメニューからグループを選択します。
3. （オプション）サーバーのリストをフィルタリングするには、ライセンス情報セクションのライセンスタイプまたはステータスリンクをクリックします。

詳しくは

iLO連携機能を使用するための前提条件
選択されたグループのリストのフィルター
選択されたグループのリストのフィルター条件

iLO連携グループのライセンスの詳細

- タイプ - 一覧表示されている各ライセンスタイプのあるサーバーの数。一覧表示されている各ライセンスタイプを持つサーバーの総数の%も表示されます。
- ステータス - 一覧表示されている各ライセンスステータスのあるサーバーの数。各ライセンスステータスのあるサーバーの総数の%も表示されます。以下のステータス値が表示されます。
  - Evaluation - 有効な評価ライセンスをインストールします。
  - Expired - 期限切れの評価ライセンスがインストールされています。
  - Perpetual - 有効なiLOライセンスがインストールされています。このライセンスに有効期限はありません。
  - Unlicensed - 工場出荷時のデフォルト（iLO Standard）機能が有効になっています。

iLOリモートコンソール

iLOリモートコンソールを使用すると、ホストサーバーのグラフィックディスプレイ、キーボード、およびマウスにリモートにアクセスできます。リモートコンソールを使用すると、リモートファイルシステムやネットワークドライブにアクセスできます。

リモートコンソールでアクセスすれば、サーバーが起動するときのPOSTメッセージを確認することができ、ROMベースのセットアップアクティビティを開始してサーバーハードウェアを構成することができます。OSをリモートでインストールする場合、リモートコンソールにより、インストールプロセス全体をホストサーバーのモニターに表示して、制御することができます。

統合リモートコンソール（IRC）のアクセスオプション

iLO Webインターフェイスから、以下の統合リモートコンソールオプションにアクセスできます。

- **HTML5統合リモートコンソール** - サポートされているブラウザーを使用しているクライアント用。
- **.NET統合リモートコンソール** - サポートされているバージョンのWindows .NET Frameworkを使用しているWindowsクライアント用。このコンソールを使用するには、使用しているブラウザーで、ClickOnceを使用した.NETアプリケーションの起動をサポートしている必要があります。

ブレードサーバーでは、統合リモートコンソールは常に有効です。

ブレード以外のサーバーで、OSの起動後に統合リモートコンソールを使用するには、ライセンスをインストールする必要があります。

その他のリモートコンソールのアクセスオプション

iLO Webインターフェイスの外部から、以下のリモートコンソールオプションを使用できます。

- **HTML5スタンドアロンリモートコンソール** - iLO Webインターフェイスを使用せずに、サポートされているブラウザーからHTML5リモートコンソールにアクセスできます。
- **スタンドアロンのリモートコンソール（HPLOCONS）** - iLOのWebインターフェイスを経由せずに、Windowsデスクトップからリモートコンソールに直接アクセスできます。

  HPLOCONSの機能と要件は、.NET統合リモートコンソールと同じです。HPLOCONSは、Webサイト**https://www.hpe.com/support/ilo6**からダウンロードしてください。

リモートコンソールの使用に関する留意事項

- 統合リモートコンソールは、遅延が大きい（モデム）接続に適しています。
- 同じサーバー上のホストオペレーティングシステムから統合リモートコンソールを実行しないでください。
- リモートコンソールを通じてサーバーにログインするとき、Hewlett Packard Enterpriseでは、コンソールを閉じる前にログアウトすることを推奨します。
- リモートコンソールの使用が完了したら、ウィンドウを閉じるか、ブラウザーの閉じるボタン（X）をクリックして終了します。
- リモートコンソールセッションがアクティブの場合、UID LEDが点滅します。
- アイドル接続タイムアウトでは、ユーザーの操作がないまま経過し、リモートコンソールセッションが自動的に終了するまでの時間を指定します。仮想メディアデバイスが接続されている場合、この値はリモートコンソールセッションに影響を与えません。
- リモートコンソールウィンドウ上にマウスが置かれている場合、コンソールウィンドウにフォーカスがあるかどうかに関係なく、コンソールはすべてのキーストロークをキャプチャーします。
- アクセス設定ページでリモートコンソール機能を有効および無効にできます。
- HTML5リモートコンソールをスタンドアロンモードまたは新規ウィンドウモードで使用すると、リモートコンソールは最初にiLO Web UIセッションで稼動します。リモートコンソールビデオが開始すると、専用のリモートコンソールセッションが開始します。Web UIセッションが終了すると、HTML5コンソールへの接続が終了するため、リモートコンソールに再接続する必要があります。

注記: 共有ネットワークポートを使用している場合は、リモートコンソールと仮想メディアが切断される可能性があります。詳しくは、 共有ネットワークポートに関する考慮事項を参照してください。

サブトピック

リモートコンソールのアクセス設定の表示

統合リモートコンソールの起動

統合リモートコンソールの機能

リモートコンソールのホットキー

リモートコンソールセキュリティの設定

詳しくは

iLOアクセス設定の構成

リモートコンソールのアクセス設定の表示

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブでは、リモートコンソールのアクセス設定が一般情報セクションに表示されます。

2. （オプション）これらの設定を構成できるアクセス設定ページに移動するには、リモートコンソールステータスリンクまたはリモートコンソールポートリンクをクリックします。

サブトピック

リモートコンソールのアクセス設定の詳細

リモートコンソールのアクセス設定の詳細

リモートコンソールステータス

現在のリモートコンソールのアクセス設定（有効または無効）。

リモートコンソールが無効になっている場合：

- グラフィカルリモートコンソールまたはテキストベースのリモートコンソールにアクセスできません。
- ポートスキャナーを使用して、セキュリティの脆弱性をスキャンするセキュリティ監査で、設定されているリモートコンソールポートが検出されません。

アクセス設定ページでこの設定を表示するには、リモートコンソールステータスリンクをクリックします。

リモートコンソールポート

設定されているリモートコンソールポート。デフォルト値は17990です。

アクセス設定ページでこの設定を表示するには、リモートコンソールポートリンクをクリックします。

統合リモートコンソールの起動

サブトピック

HTML5 IRCの起動

概要ページからのHTML5 IRCの起動

HTML5スタンドアロンリモートコンソールの起動

HTML5リモートコンソールモード

HTML5リモートコンソールのコントロール

.NET IRCの起動

概要ページからの.NET IRCの起動

.NET IRC要件

リモートコンソールの取得

共有リモートコンソールセッションへの参加（.NET IRC専用）

リモートコンソールのステータスバーの表示

HTML5 IRCの起動

前提条件

- リモートコンソール権限
- リモートコンソール機能がアクセス設定ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

このタスクについて

サポートされているブラウザーでリモートコンソールにアクセスするには、以下の手順を使用します。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. 次のいずれかを実行して、HTML5 IRCを開始します。
   - HTML5コンソールボタンをクリックします。

     このオプションにより、コンソールがiLO Webインターフェイスと同じブラウザーウィンドウで開かれます。コンソールをブラウザーウィンドウから移動することはできません。

   - 新規ウィンドウボタンをクリックします。

     このオプションにより、コンソールが新しいウィンドウで開かれます。ウィンドウを別の位置またはモニターに移動したり、最小化したりすることができます。

   HTML5 IRCが起動します。

3. リモートコンソール機能を使用します。
4. （オプション）HTML5リモートコンソールのオンラインヘルプを表示するには、メニューアイコン、ヘルプの順に選択します。

詳しくは

iLOアクセス設定の構成
HTML5リモートコンソールのコントロール

概要ページからのHTML5 IRCの起動

前提条件

- リモートコンソール権限
- リモートコンソール機能がアクセス設定ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

このタスクについて

サポートされているブラウザーでリモートコンソールにアクセスするには、以下の手順を使用します。

手順

1. ナビゲーションツリーで情報をクリックし、概要タブをクリックします。
2. 次のいずれかを実行して、HTML5 IRCを開始します。

- HTML5リンクをクリックします。

  このオプションにより、コンソールがiLO Webインターフェイスと同じブラウザーウィンドウで開かれます。コンソールをブラウザーウィンドウから移動することはできません。

- をクリックします。

  このオプションにより、コンソールが新しいウィンドウで開かれます。ウィンドウを別の位置またはモニターに移動したり、最小化したりすることができます。

HTML5 IRCが起動します。

3. リモートコンソール機能を使用します。
4. （オプション）HTML5リモートコンソールのオンラインヘルプを表示するには、メニューアイコン、ヘルプの順に選択します。

詳しくは

iLOアクセス設定の構成
HTML5リモートコンソールのコントロール

HTML5スタンドアロンリモートコンソールの起動

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- リモートコンソール機能がアクセス設定ページで有効になっている。

このタスクについて

最初にiLO Webインターフェイスにログインせずに、HTML5リモートコンソールにアクセスするには、この手順を使用します。

手順

1. ブラウザーウィンドウを開き、次のWebページに移動します。
   `https://<iLOホスト名またはIPアドレス>/irc.html`

   iLO HTML5リモートコンソールのログインページが開きます。

   - ログインセキュリティバナーが構成されている場合は、バナーテキストが通知セクションに表示されます。
   - iLOヘルスステータスが劣化で匿名データアクセスオプションが有効な場合は、ヘルスステータスと問題の説明がiLOのログインページに表示されます。セキュリティ侵害の可能性があるセルフテスト障害は、説明には表示されません。

2. ディレクトリまたはローカルアカウントログイン名とパスワードを入力して、ログインをクリックします。

   iLOがKerberosネットワーク認証用に設定されている場合は、ログインボタンの下に Zeroサインインボタンが表示されます。Zeroサインインボタンを使用して、ユーザー名とパスワードを入力せずにログインできます。

   iLOがCAC Smartcard認証用に設定されている場合は、ログインボタンの下にSmartcardでログインボタンが表示されます。スマートカードを接続して、Smartcardでログインボタンをクリックすることができます。CAC Smartcard認証を使用する場合、ログイン名とパスワードを入力しないでください。

3. リモートコンソール機能を使用します。
4. （オプション）HTML5リモートコンソールのオンラインヘルプを表示するには、メニューアイコン、ヘルプの順に選

択します。

HTML5リモートコンソールモード

HTML5リモートコンソールには、利用可能ないくつかの表示モードがあります。コンソールを使用しているときに、ある表示モードからサポートされている別のモードに切り替えることができます。サポートされている表示モードは、コンソールの起動に使用する方法によって異なります。

ウィンドウモード

リモートコンソールは、iLO Webインターフェイスと同じブラウザーウィンドウのセカンダリウィンドウに表示されます。コンソールをブラウザーウィンドウから移動することはできません。

このモードは、次の方法を使用してコンソールを起動するときに使用できます。

- iLO概要ページのHTML5をクリックします。
- iLO統合リモートコンソールページのHTML5コンソールをクリックします。
- iLOナビゲーションペインのリモートコンソールサムネイルをクリックし、次にHTML5コンソールを選択します。

このモードからドッキングモードまたはフルスクリーンモードに切り替えることができます。

新規ウィンドウモード

リモートコンソールは、別の位置やモニターに移動できるウィンドウに表示されます。ブラウザーのタブとして追加したり、ウィンドウを最小化したりすることもできます。

このモードは、次の方法を使用してコンソールを起動するときに使用できます。

-  （iLO概要ページ）をクリックします。
- iLO統合リモートコンソールページの新規ウィンドウをクリックします。

このモードからフルスクリーンモードに切り替えることができます。

ドッキングモード

リモートコンソールは、ナビゲーションペインサムネイルに表示されます。

このモードは、次の方法を使用してコンソールを起動するときに使用できます。

- iLO概要ページのHTML5をクリックします。
- iLO統合リモートコンソールページのHTML5コンソールをクリックします。
- iLOナビゲーションペインのリモートコンソールサムネイルをクリックし、次にHTML5コンソールを選択します。

このモードからウィンドウモードまたはフルスクリーンモードに切り替えることができます。

フルスクリーンモード

リモートコンソールはモニターのフルサイズで表示されます。リモートコンソールメニューを表示するには、カーソルを画面の一番上に移動します。メニューのデフォルト位置は左上です。クリックしてドラッグすると、メニューを別の位置に移動できます。メニューの位置を変更すると、変更は現在のリモートコンソールセッションに対して維持されます。

このモードは、すべてのコンソールモードで使用できます。

スタンドアロンモード

スタンドアロンモードの使用時は、リモートコンソールがブラウザータブに表示されます。

このモードは、次の方法を使用してコンソールを起動するときに使用できます。

- 次のWebページに移動して、ログインします。
  https://<iLOホスト名またはIPアドレス>/irc.html

このモードからフルスクリーンモードに切り替えることができます。

HTML5リモートコンソールのコントロール

リモートコンソールウィンドウの上には、以下のコントロールがあります（左から右の順）。コントロールアイコンの上にカーソルを移動すると、ツールヒントの説明が表示されます。

メニュー

このアイコンでは、以下を行うことができます。

- iLO仮想電源ボタン機能にアクセスします。
- 環境設定メニューを使用して、リモートコンソールのステータスバーを表示または非表示にします。
- iLOホスト名とサーバー名を表示するには、情報メニューを使用します。
- HTML5コンソールのオンラインヘルプを表示するには、ヘルプメニューを使用します。

このアイコンは、ドッキングモードでは使用できません。

仮想キーボード

このアイコンでは、以下を行うことができます。

- リモートサーバーに送信できる次のキーボードショートカットにアクセスする：CTRL+ALT+DEL
- リモートコンソールの以下の仮想キーにアクセスする：
  - CTRL-コントロール
  - ESC-エスケープ
  - CAPS-CapsLock
  - NUM-NumLock
  - L OS-左OS固有のキー
  - L ALT-左ALTキー
  - R ALT-右ALTキー
  - R OS-右OS固有のキー
- HTML5リモートコンソールキーボードレイアウトを表示または変更します。

仮想メディア

このアイコンから、仮想メディア機能にアクセスできます。

リモートコンソールを閉じる

リモートコンソールセッションを閉じるには、このアイコンを使用します。

リモートコンソールディスプレイおよびモードコントロール

次のコントロールを使用して、リモートコンソールの表示を変更したり、別の表示モードに切り替えたりします。

利用可能なコントロールは、アクティブなコンソールモードによって異なります。アクティブなコンソールモードでコントロールがサポートされていない場合、そのコントロールは表示されません。

最大化 およびリストア

最大化アイコンは、リモートコンソールウィンドウをブラウザーウィンドウ内で最大化します。

リストアアイコンは、ウィンドウを元のサイズにリセットします。

これらの機能はウィンドウモードで使用できます。

全画面に切り替え

この機能はすべてのモードで使用できます。

ドッキングモード

このアイコンを使用して、ウィンドウモードからドッキングモードに変更できます。

この機能はウィンドウモードでは使用できません

全画面を終了

フルスクリーンモードを終了し、以前に選択したモードに戻るには、このアイコンを使用します。

Escキーを押してフルスクリーンモードを終了することもできます。

ウィンドウモード

このアイコンを使用して、ドッキングモードからセカンダリウィンドウに変更できます。

この機能はドッキングモードでは使用できません。

ピンアイコン

画面の上部にあるツールバーを固定または固定解除するには、このアイコンを使用します。この設定は現在のリモートコンソールセッションに対して維持されます。

この機能はフルスクリーンモードで使用できます。

.NET IRCの起動

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- リモートコンソール機能がアクセス設定ページで有効になっている。
- サポート対象のバージョンのMicrosoft .NET Frameworkがインストールされている。
- 使用しているブラウザーで、ClickOnceを使用した.NETアプリケーションの起動をサポートしている。

  Microsoft Edgeで.NET IRCを使用する方法については、iLO6トラブルシューティングガイドを参照してください。
- ポップアップブロッカーが無効になっている。

  場合によっては、.NETコンソールボタンをCtrlを押したままクリックすることでポップアップブロッカーをバイパスできることがあります。

このタスクについて

Windowsクライアント上のサポートされているブラウザーでリモートコンソールにアクセスするには、以下の手順を使用します。

詳しくは

iLOアクセス設定の構成
.NET IRC要件

概要ページからの.NET IRCの起動

前提条件

- リモートコンソール権限

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- リモートコンソール機能がアクセス設定ページで有効になっている。
- サポート対象のバージョンのMicrosoft .NET Frameworkがインストールされている。
- 使用しているブラウザーで、ClickOnceを使用した.NETアプリケーションの起動をサポートしている。

  Microsoft Edgeで.NET IRCを使用する方法については、HPE iLO 6トラブルシューティングガイドを参照してください。
- ポップアップブロッカーが無効になっている。

  場合によっては、.NETコンソールボタンをCtrlを押したままクリックすることでポップアップブロッカーをバイパスできることがあります。

このタスクについて

Windowsクライアント上のサポートされているブラウザーでリモートコンソールにアクセスするには、以下の手順を使用します。

手順

1. ナビゲーションツリーで情報をクリックし、概要タブをクリックします。
2. .NETリンクをクリックします。
3. リモートコンソール機能を使用します。

詳しくは

iLOアクセス設定の構成
.NET IRC要件

.NET IRC要件

Microsoft .NET Framework

.NET IRCには、Microsoft .NET Frameworkバージョン4.5.1以降が必要です。

Windows 7、8、8.1、および10では、サポートされる.NET Frameworkバージョンは、オペレーティングシステムに含まれています。.NET Frameworkは、Microsoftダウンロードセンター（http://www.microsoft.com/download）でも入手できます。

Microsoft Edgeブラウザーでは、インストールされている.NET Frameworkのバージョンに関する情報は表示されません。

Microsoft ClickOnce

.NET IRCは、.NET Frameworkの一部であるMicrosoft ClickOnceを使用して起動します。ClickOnceでは、SSL接続からインストールされるすべてのアプリケーションが信頼できるソースからのものでなければなりません。ブラウザーがiLOシステムを信頼するように設定されていないときにIRCはiLO内の信頼された証明書を要求しますの設定が有効に設定されている場合、ClickOnceに次のエラーメッセージが表示されます。

```
アプリケーションを起動できません。アプリケーションのダウンロードは成功しませんでした。
```

.NETアプリケーションを起動するためのClickOnce拡張機能をサポートしていないため、.NET IRCはGoogle ChromeまたはMozilla Firefoxではサポートされていません。回避策として、別のリモートコンソールを選択するか、別のブラウザーを使用します。

リモートコンソールの取得

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- リモートコンソール機能がアクセス設定ページで有効になっている。

このタスクについて

別のユーザーがリモートコンソールで作業している場合、そのユーザーからリモートコンソールを取得することができます。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. 使用するリモートコンソールのボタンをクリックします。

   別のユーザーがリモートコンソールで作業していることがiLOから通知されます。
3. リモートコンソールを取得する要求を送信するには、画面の指示に従います。

   他のユーザーは、要求を承認するか拒否するように求められます。

   他のユーザーが承認するか、10秒以内に応答しない場合、許可が与えられます。リモートコンソールが起動します。

詳しくは

iLOアクセス設定の構成

共有リモートコンソールセッションへの参加（.NET IRC専用）

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- リモートコンソール機能がアクセス設定ページで有効になっている。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. .NETコンソールボタンをクリックします。

   .NETリモートコンソールが使用中であることを通知するメッセージが表示されます。
3. Share（共有）をクリックします。

   セッションリーダーは、共有リモートコンソールセッションへの参加要求を受信します。

   セッションリーダーがはいをクリックすると、ユーザーはセッションへのアクセスを許可され、キーボードやマウスを使えるようになります。

サブトピック

共有リモートコンソール（.NET IRC専用）

詳しくは

iLOアクセス設定の構成

共有リモートコンソール（.NET IRC専用）

共有リモートコンソール機能を使用すると、複数のユーザーが同じリモートコンソールセッションに接続できます。この機能は、トレーニングやトラブルシューティングのような活動に使用できます。

通常、リモートコンソールセッションを開始する最初のユーザーがサーバーに接続し、セッションリーダーに指名されます。リモートコンソールアクセスを要求する以後のユーザーは、サテライトクライアント接続のアクセス要求を開始します。セッションリーダーのデスクトップで、各アクセス要求のダイアログボックスが開きます。要求には、要求元のユーザー名とDNS名またはIPアドレスが含まれています。セッションリーダーは、アクセスを許可または拒否するよう求められます。応答がない場合、アクセスは拒否されます。

セッションリーダーの指名を別のユーザーに譲渡することはサポートされていません。

接続障害が発生した場合、再接続はサポートされていません。接続障害後にユーザーアクセスを許可するには、リモートコンソールセッションを再起動する必要があります。

共有リモートコンソールセッション中、セッションリーダーはすべてのリモートコンソール機能にアクセスできます。他のユーザーはキーボードとマウスにアクセスできるだけです。

iLOは、最初にクライアントを認証し、セッションリーダーが新しい接続を許可するかどうかを決定して共有リモートコンソールセッションを暗号化します。

リモートコンソールのステータスバーの表示

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- リモートコンソール機能がアクセス設定ページで有効になっている。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. リモートコンソールを起動します。

   リモートコンソールウィンドウが開き、ステータスバーが表示されます。

3. （オプション）ステータスバーのオンとオフを切り替えるには、メニューアイコンをクリックして、環境設定 > ステータスバーを表示を選択します。

   HTML5 IRCのみがこの機能をサポートしています。

4. （オプション）ステータスバーのオンとオフを切り替えるには、メニューアイコン をクリックして、環境設定 > ステータスバーを表示を選択します。

   HTML5 IRCのみがこの機能をサポートしています。

サブトピック

リモートコンソールのステータスバーの詳細

詳しくは

リモートコンソールのステータスバーの詳細

解像度

リモートコンソールウィンドウの解像度。

POSTコード

POST実行中のPOSTコードは、ステータスバーの中央に表示されます。

コンソールの取得（.NET IRC専用）

これらのコントロールを使用して、コンソールウィンドウに表示されるアクティビティを記録および再生できます。

スクリーンキャプチャー

HTML5 IRCでカメラアイコンをクリックして、コンソールウィンドウに表示されるアクティビティのスクリーンキャプチャーを作成できます。

.NET IRCのステータスバーをダブルクリックして、画面をキャプチャーし、スクリーンキャプチャーを画像エディターに貼り付けることができます。

暗号化

リモートコンソールとiLOの間の接続のステータスおよび暗号化タイプ。

ヘルスステータス

サーバーヘルスインジケーター。この値は、全体的なステータスや冗長性（障害処理能力）など、監視対象サブシステムの状態を要約します。起動時にいずれかのサブシステムが冗長でなくても、システムヘルスステータスは劣化しません。表示される値は、OK、劣化、およびクリティカルです。

アクティビティLED

リモートコンソールを介して接続されているローカルの仮想メディアデバイスのためのアクティビティインジケーター。この機能はURLベースの仮想メディアデバイスについてはアクティブではありません。

電源ステータス

電源 - サーバーの電源状態（ オンまたは オフ）。

統合リモートコンソールの機能

統合リモートコンソール（IRC）は、以下の機能をサポートします。

- IRCを使用したキーボード操作
- 仮想電源IRCの機能
- 仮想メディアIRCの機能
- コンソールのキャプチャー（.NET IRC）
- IRCを使用したスクリーンキャプチャー

サブトピック

IRCを使用したキーボード操作

仮想電源IRCの機能

仮想メディアIRCの機能

コンソールのキャプチャー（.NET IRC）

IRCを使用したスクリーンキャプチャー

IRCを使用したキーボード操作

サブトピック

HTML5 IRCを使用したキーボード操作の送信

.NET IRCを使用したキーボード操作の送信

リモートコンソールのホットキーの送信

HTML5 IRCのキーボードレイアウトを変更する

HTML5 IRCを使用したキーボード操作の送信

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- リモートコンソール機能がアクセス設定ページで有効になっている。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. HTML5 IRCを起動します。
3. 次のいずれかを実行します。
   - クライアントのキーボードを使用して、目的のキーを押します。
   - Ctrl+Alt+Del操作を送信するには、仮想キーボードアイコン⌨ をクリックして、CTRL+ALT+DELキーボードショートカットをクリックします。
   - Caps LockまたはNum Lock設定を無効にするには、次のいずれかの操作を行います。
     - クライアントキーボードのNumLockまたはCapsLockキーを押します。
     - 仮想キーボードアイコン⌨ をクリックして、CAPSまたはNUMキーボードショートカットをクリックします。

詳しくは

iLOアクセス設定の構成

.NET IRCを使用したキーボード操作の送信

前提条件

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

い。

- リモートコンソール機能がアクセス設定ページで有効になっている。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. リモートコンソールを起動します。
3. 次のいずれかを実行します。
   - クライアントのキーボードを使用して、目的のキーを押します。
   - Ctrl+Alt+Del操作を送信するには、キーボード > CTRL-ALT-DELを選択します。
   - Caps LockまたはNum Lock設定を無効にするには、次のいずれかの操作を行います。
     - クライアントキーボードのNumLockまたはCapsLockキーを押します。
     - キーボード > Caps Lockまたはキーボード > Num Lockを選択します。

リモートコンソールのホットキーの送信

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- リモートコンソール機能がアクセス設定ページで有効になっている。
- ホットキーページでリモートコンソールのホットキーが設定されている。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. リモートコンソールを起動します。
3. ご使用のクライアントのキーボードで、構成されているリモートコンソールホットキーのキーの組み合わせを押します。

詳しくは

iLOアクセス設定の構成
リモートコンソールのホットキー
リモートコンソールのホットキーの作成

HTML5 IRCのキーボードレイアウトを変更する

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされて

いる機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

- リモートコンソール機能がアクセス設定ページで有効になっている。
- サーバーOSは、使用するキーボードレイアウトをサポートするように構成されています。
- iLOへのブラウズに使用するクライアントは、使用するキーボードレイアウトをサポートするように構成されています。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. HTML5 IRCを起動します。
3. 仮想キーボードアイコン をクリックします。
4. キーボードレイアウト > *キーボードレイアウト名*を選択します。

   iLOでは、EN 101およびJP 106/109のキーボードレイアウトをサポートします。

   この設定はcookieに保存され、同じブラウザーでリモートコンソールを使用する際に永続的に残ります。

詳しくは

iLOアクセス設定の構成

仮想電源IRCの機能

サブトピック

HTML5 IRCでリモートコンソールの仮想電源スイッチを使用する

.NET IRCでリモートコンソールの仮想電源スイッチを使用する

仮想電源ボタンのオプション

HTML5 IRCでリモートコンソールの仮想電源スイッチを使用する

前提条件

- リモートコンソール権限
- 仮想電源およびリセット権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- リモートコンソール機能がアクセス設定ページで有効になっている。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. HTML5 IRCを起動します。
3. メニューアイコンをクリックして、電源メニューからオプションを選択します。

サーバーの電源が入っていない場合、押し続ける、リセット、およびコールドブートオプションは使用できません。

iLOが要求を確認するように求めます。

4. メニューアイコン をクリックして、電源メニューからオプションを選択します。

   サーバーの電源が入っていない場合、押し続ける、リセット、およびコールドブートオプションは使用できません。

   iLOが要求を確認するように求めます。

5. OKをクリックします。

詳しくは

iLOアクセス設定の構成

.NET IRCでリモートコンソールの仮想電源スイッチを使用する

前提条件

- リモートコンソール権限
- 仮想電源およびリセット権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- リモートコンソール機能がアクセス設定ページで有効になっている。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. .NET IRCを起動します。
3. リモートコンソールの電源スイッチメニューからオプションを選択します。

   サーバーの電源が入っていない場合、押し続ける、リセット、およびコールドブートオプションは使用できません。

   iLOが要求を確認するように求めます。

4. OKをクリックします。

仮想電源ボタンのオプション

- 瞬間的に押す – 物理的な電源ボタンを押す場合と同じです。サーバーの電源が切れている場合は、瞬間的に押すを押すとサーバーに電源が投入されます。

  一部のオペレーティングシステムは、瞬間的に押した後で適切なシャットダウンを開始するか、またはこのイベントを無視するように構成されている場合があります。Hewlett Packard Enterpriseでは、仮想電源ボタンを使用してシャットダウンを実行する前に、システムコマンドを使用して正常なオペレーティングシステムのシャットダウンを完了することをお勧めします。

- 押し続ける – 物理的な電源ボタンを5秒間押し続け、離すことと同じです。

  サーバーはこの操作の結果、電源がオフになります。このオプションは、オペレーティングシステムの正常なシャットダウン機能に影響する場合があります。

このオプションは、一部のオペレーティングシステムが実装しているACPI機能を提供します。これらのオペレーティングシステムは、瞬間的に押すと押し続けるによって動作が異なります。

- リセット - サーバーを強制的にウォームブートします。CPUとI/Oリソースがリセットされます。このオプションは、オペレーティングシステムの正常なシャットダウン機能に影響する場合があります。
- コールドブート - サーバーからただちに電源を切断します。プロセッサー、メモリ、およびI/Oリソースは、メインの電力が失われます。サーバーは、約8秒後に再起動します。このオプションは、オペレーティングシステムの正常なシャットダウン機能に影響する場合があります。

仮想メディアIRCの機能

統合リモートコンソール（IRC）を使用すると、次の作業を実行できます。

- 以下を含む仮想ドライブの接続と切断：
  - クライアントPCの物理ドライブ（フロッピーディスク、CD/DVD-ROM、USBキー）
  - ローカルのIMGまたはISOファイル
  - URLベースのメディア（IMGまたはISO）
  - 仮想フォルダー

  使用するコンソールが仮想メディアタイプをサポートしていることを確認するには、そのメディアタイプの使用に関する説明を確認してください。

サブトピック

仮想ドライブ（クライアントPC上の物理ドライブ）の使用

HTML5 IRCでのローカルIMGまたはISOファイルの使用

.NET IRCでのローカルIMGまたはISOファイルの使用

仮想ドライブを使用してOSのインストールと必要なドライバーの指定を行う（.NET IRC）

仮想ドライブを使用してOSのインストールと必要なドライバーの指定を行う（HTML5 IRC）

HTML5 IRCでURLベースのイメージファイルを使用する

.NET IRCでURLベースのイメージファイルを使用する

仮想フォルダーの使用（HTML5 IRC）

仮想フォルダーの使用（.NET IRC）

詳しくは

iLO Webインターフェイスの仮想メディアオプション

仮想ドライブ（クライアントPC上の物理ドライブ）の使用

前提条件

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

- リモートコンソール機能がアクセス設定ページで有効になっている。
- 仮想メディア機能がアクセス設定ページで有効になっている。
- Windowsでリモートコンソールを使用する場合は、物理ドライブをマウントするために必要なWindows管理者権限を有している。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. この機能をサポートしているリモートコンソールを起動します。

   このリリースでは、.NET IRCがこの機能をサポートしています。

3. 仮想ドライブメニューをクリックし、クライアントシステムに接続されているフロッピーディスク、CD-ROM/DVD、またはUSBキードライブを選択します。

   アクティビティLEDが点滅して、仮想ドライブ動作中を示します。

4. 仮想ドライブの使用が終了したら、サーバーOSを介してファイルの接続を解除します。

   また、仮想ドライブメニューから仮想ドライブの接続を解除することもできます。仮想ドライブをクリックし、それぞれのチェックボックスをオフにします。

詳しくは

iLOアクセス設定の構成
仮想メディアに関する留意事項

HTML5 IRCでのローカルIMGまたはISOファイルの使用

前提条件

- リモートコンソール権限
- リモートコンソール機能がアクセス設定ページで有効になっている。
- 仮想メディア機能がアクセス設定ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. HTML5 IRCを起動します。

3. 仮想メディアアイコン ⊙ をクリックして、フロッピー > ローカル*.imgファイル、またはCD/DVD > ローカル*.isoファイルを選択します。

   リモートコンソールによってファイルを選択するよう求められます。

4. ファイル名テキストボックスに、イメージファイルのパスまたはファイル名を入力します。

   ファイルの場所を参照して、開くをクリックすることもできます。

   仮想ドライブのアクティビティLEDは、仮想ドライブのアクティビティを示します。OSがシステム通知をサポートしている場合は、通知が表示されます。

5. ローカルのIMGまたはISOファイルの使用が終了したら、サーバーOSを介してファイルの接続を解除します。

   また、⊙ をクリックしてから、*メディアタイプ* > メディアの強制取り出しを選択して、ローカルのIMGまたはISOファイルの接続を解除することもできます。

詳しくは

iLOアクセス設定の構成
仮想メディアに関する留意事項

.NET IRCでのローカルIMGまたはISOファイルの使用

前提条件

- リモートコンソール権限
- リモートコンソール機能がアクセス設定ページで有効になっている。
- 仮想メディア機能がアクセス設定ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. .NET IRCを起動します。
3. 仮想メディアメニューをクリックし、イメージファイルリムーバルメディア（IMG）またはイメージファイルCD-ROM/DVD（ISO）を選択します。

   IRCによってファイルを選択するよう求められます。

4. ファイル名テキストボックスに、イメージファイルのパスまたはファイル名を入力します。

   ファイルの場所を参照して、開くをクリックすることもできます。

   仮想ドライブのアクティビティLEDは、仮想ドライブのアクティビティを示します。

5. ローカルのIMGまたはISOファイルの使用が終了したら、サーバーOSを介してファイルの接続を解除します。

   また、仮想ドライブ > *接続されたメディア*を選択して、ローカルのIMGまたはISOファイルの接続を解除することもできます。

詳しくは

iLOアクセス設定の構成
仮想メディアに関する留意事項

仮想ドライブを使用してOSのインストールと必要なドライバーの指定を行う（.NET IRC）

前提条件

- リモートコンソール権限
- リモートコンソール機能がアクセス設定ページで有効になっている。

- 仮想メディア機能がアクセス設定ページで有効になっている。
- オペレーティングシステムのISOファイルは、リモートコンソールを実行するのに使用するクライアント上で利用可能です。
- オペレーティングシステムをNVMeドライブにインストールする場合は、ブートモードがUnified Extensible Firmware Interface (UEFI)に設定されます。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

このタスクについて

リモートコンソールの仮想ドライブ機能を使用して、オペレーティングシステムをインストールできます。インストール中に、ストレージコントローラードライバーなどの必要なドライバーへのアクセスを提供するようにプロンプトが表示されることがあります。

手順

1. 必要なドライバーをダウンロードして展開してください。

   SPPからドライバーを入手するか、Webサイト（https://www.hpe.com/support/hpesc）からダウンロードできます。
2. ドライバーをUSBキーまたはクライアント上のフォルダーにコピーし、そこからリモートコンソールにアクセスします。
3. リモートコンソールを起動します。
   - USBキーを使用して必要なドライバーを提供する場合は、.NET IRCを選択します。
   - 仮想フォルダーを使用して必要なドライバーを提供する場合は、.NET IRCを選択します。
4. オペレーティングシステムのISOをマウントします。
   a. 仮想ドライブ > イメージファイルCD-ROM/DVDを選択します。

      リモートコンソールによってファイルを選択するよう求められます。

   b. ファイル名テキストボックスに、イメージファイルのパスまたはファイル名を入力します。

      ファイルの場所を参照して、開くをクリックすることもできます。
5. USBキー上で必要なドライバーを指定する場合、以下の操作を実行します。
   a. USBキーをiLOの管理に使用しているクライアントに接続します。
   b. リモートコンソールで、仮想ドライブメニューをクリックし、クライアントPC上のUSBキーのドライブ文字を選択します。
6. iLOの管理に使用しているクライアント上のフォルダーで必要なドライバーを指定する場合、以下の操作を実行します。
   a. 仮想ドライブ > フォルダーの順に選択します。
   b. フォルダーの参照ウィンドウで、ドライバーファイルを格納しているフォルダーを選択します。
7. オペレーティングシステムのISOを起動します。
8. オペレーティングシステムのインストーラーによってドライバーのパスを入力するプロンプトが表示されるまで、画面の指示に従います。
9. ドライバーの場所を指定するプロンプトが表示されたら、ドライバーを格納したUSBキーまたは仮想フォルダーのパスを入力します。
10. 画面の説明に従って、オペレーティングシステムのインストールを完了します。
11. 必要なデバイスドライバーがほかにある場合は、それをインストールします。

デバイスドライバーはSPPから入手できます。

詳しくは

iLOアクセス設定の構成
仮想メディアに関する留意事項
サーバーブートモードの設定
.NET IRCでのローカルIMGまたはISOファイルの使用
仮想フォルダーの使用（.NET IRC）

仮想ドライブを使用してOSのインストールと必要なドライバーの指定を行う（HTML5 IRC）

前提条件

- リモートコンソール権限
- リモートコンソール機能がアクセス設定ページで有効になっている。
- 仮想メディア機能がアクセス設定ページで有効になっている。
- オペレーティングシステムのISOファイルは、リモートコンソールを実行するのに使用するクライアント上で利用可能です。
- オペレーティングシステムをNVMeドライブにインストールする場合は、ブートモードがUnified Extensible Firmware Interface (UEFI)に設定されます。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（**https://www.hpe.com/support/ilo-docs**）にあるライセンス文書を参照してください。

このタスクについて

リモートコンソールの仮想ドライブ機能を使用して、オペレーティングシステムをインストールできます。インストール中に、ストレージコントローラードライバーなどの必要なドライバーへのアクセスを提供するようにプロンプトが表示されることがあります。

手順

1. 必要なドライバーをダウンロードして展開してください。

   SPPからドライバーを入手するか、Webサイト（**https://www.hpe.com/support/hpesc**）からダウンロードできます。

2. ドライバーをクライアント上のフォルダーにコピーし、そこからリモートコンソールにアクセスします。
3. HTML5リモートコンソールを起動します。
4. オペレーティングシステムのISOをマウントします。

   a. 仮想メディアアイコン をクリックして、CD/DVD > ローカル*.isoファイルを選択します。

      リモートコンソールによってファイルを選択するよう求められます。

   b. ファイル名テキストボックスに、イメージファイルのパスまたはファイル名を入力します。

      ファイルの場所を参照して、開くをクリックすることもできます。

      アクティビティLEDが点滅して、仮想ドライブ動作中を示します。OSがシステム通知をサポートしている場合は、通知が表示されます。

5. 必要なドライバーが含まれているフォルダーをクライアントコンピューターからHTML5 IRCウィンドウにドラッグアンドドロップします。

   仮想フォルダーが、iLOフォルダーという名前でサーバーにマウントされます。

アクティビティLEDが点滅して、仮想ドライブ動作中を示します。OSがシステム通知をサポートしている場合は、通知が表示されます。

6. オペレーティングシステムのISOを起動します。
7. オペレーティングシステムのインストーラーによってドライバーのパスを入力するプロンプトが表示されるまで、画面の指示に従います。
8. ドライバーの場所を指定するプロンプトが表示されたら、ドライバーを格納した仮想フォルダーのパスを入力します。
9. 画面の説明に従って、オペレーティングシステムのインストールを完了します。
10. 必要なデバイスドライバーがほかにある場合は、それをインストールします。

    デバイスドライバーはSPPから入手できます。

HTML5 IRCでURLベースのイメージファイルを使用する

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- リモートコンソール機能がアクセス設定ページで有効になっている。
- 仮想メディア機能がアクセス設定ページで有効になっている。
- 使用するイメージファイルが、iLOと同じネットワーク上のWebサーバーにある。

このタスクについて

以下の種類のURLベースのメディアを接続できます。1.44 MBのフロッピーディスクイメージ（IMG）およびCD/DVD-ROMイメージ（ISO）。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. HTML5 IRCを起動します。
3. 仮想メディアアイコン⊙ をクリックして、フロッピー > 仮想メディアURL、またはCD/DVD > 仮想メディアURLを選択します。

   リモートコンソールで、イメージファイルURLの入力を求められます。

4. 仮想ドライブとしてマウントしたいイメージファイルのURLを入力して、適用をクリックします。

   仮想ドライブのアクティビティLEDは、URLでマウントされた仮想メディアのドライブのアクティビティを表示しません。

5. イメージファイルの使用が終了したら、サーバーOSを介してファイルの接続を解除します。

   また、⊙ をクリックしてから、*メディアタイプ* > メディアの強制取り出しを選択して、イメージファイルの接続を解除することもできます。

詳しくは

iLOアクセス設定の構成
スクリプト仮想メディア用IISのセットアップ

.NET IRCでURLベースのイメージファイルを使用する

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- リモートコンソール機能がアクセス設定ページで有効になっている。
- 仮想メディア機能がアクセス設定ページで有効になっている。
- 使用するイメージファイルが、iLOと同じネットワーク上のWebサーバーにある。

このタスクについて

以下の種類のURLベースのメディアを接続できます。1.44 MBのフロッピーディスクイメージ（IMG）およびCD/DVD-ROMイメージ（ISO）。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. .NET IRCを起動します。
3. 仮想ドライブ > URLリムーバブルメディア（IMGファイル）または仮想ドライブ > URL CD-ROM/DVD（ISOファイル）を選択します。

   iLOがイメージファイルのURLを入力するように求めます。

4. 仮想ドライブとしてマウントしたいイメージファイルのURLを入力して、接続をクリックします。

   仮想ドライブのアクティビティLEDは、URLでマウントされた仮想メディアのドライブのアクティビティを表示しません。

5. イメージファイルの使用が終了したら、サーバーOSを介してファイルの接続を解除します。

   また、仮想ドライブ > *接続されたメディア*を選択して、イメージファイルの接続を解除することもできます。

詳しくは

iLOアクセス設定の構成
スクリプト仮想メディア用IISのセットアップ

仮想フォルダーの使用（HTML5 IRC）

前提条件

- リモートコンソール権限
- 仮想メディア権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- リモートコンソール機能がアクセス設定ページで有効になっている。
- 仮想メディア機能がアクセス設定ページで有効になっている。

- 仮想フォルダーとしてマウントするフォルダーのサイズは2 GB以下である。
- この機能をサポートするブラウザーを使用している。

このタスクについて

HTML5 IRCでは、仮想フォルダー機能はドラッグアンドドロップを使用して仮想フォルダーをマウントします。仮想メディアアイコン をクリックしたときの仮想フォルダーオプションがあります。仮想フォルダーオプションは、機能に関する情報を提供します。仮想フォルダーがマウントされると、仮想フォルダーメニューオプションは、仮想フォルダーをアンマウントするためのオプションを提供します。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. HTML5リモートコンソールを起動します。
3. 1つ以上のフォルダーまたは1つ以上の選択したファイルを、リモートコンソールを実行しているシステムからコンソールウィンドウにドラッグアンドドロップします。

   仮想フォルダーが、iLOフォルダーという名前でサーバーにマウントされます。

   アクティビティLEDが点滅して、仮想ドライブ動作中を示します。OSがシステム通知をサポートしている場合は、通知が表示されます。

4. 仮想フォルダーの使用が終了したら、サーバーOSを介してファイルの接続を解除します。

   また、 をクリックしてから、仮想フォルダー > メディアの強制取り出しを選択して、仮想フォルダーの接続を解除することもできます。

仮想フォルダーの使用（.NET IRC）

前提条件

- リモートコンソール権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- リモートコンソール機能がアクセス設定ページで有効になっている。
- 仮想メディア機能がアクセス設定ページで有効になっている。
- 仮想フォルダーとしてマウントするフォルダーのサイズは2 GB以下である。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. .NET IRCを起動します。
3. 仮想メディア > フォルダーの順に選択します。
4. フォルダーの参照ウィンドウで、使用するフォルダーを選択し、OKをクリックします。

   仮想フォルダーが、iLOフォルダーという名前でサーバーにマウントされます。

   アクティビティLEDが点滅して、仮想ドライブ動作中を示します。

5. 仮想フォルダーの使用が終了したら、サーバーOSを介してファイルの接続を解除します。

また、仮想ドライブメニューから仮想ドライブの接続を解除することもできます。仮想ドライブをクリックし、それぞれのチェックボックスをオフにします。

サブトピック

仮想フォルダー

詳しくは

iLOアクセス設定の構成
仮想メディアに関する留意事項

仮想フォルダー

仮想フォルダーを使用すると、ファイルにアクセスし、ファイルを参照し、クライアントから管理対象サーバーにファイルを転送できます。ローカルディレクトリまたはクライアント経由でアクセスできるネットワーク接続されたディレクトリのマウントとアンマウントを行うことができます。フォルダーまたはディレクトリの仮想イメージが作成された後、サーバーはそのイメージにUSBストレージデバイスとして接続します。ユーザーはサーバーにアクセスし、仮想イメージからサーバーにファイルを転送できます。

仮想フォルダーは読み取り専用であり、ここからは起動できません。マウントされたフォルダーは静的です。クライアントフォルダーに行った変更は、マウントされたフォルダーに複製されません。クライアントフォルダーを変更した後で仮想フォルダーの表示をアップデートしたければ、仮想フォルダーを切り離して再接続するだけで十分です。

コンソールのキャプチャー（.NET IRC）

コンソールのキャプチャーを使用すると、起動、ASRイベント、および検出されたオペレーティングシステムの不具合のようなイベントのビデオストリームを記録し、再生することができます。iLOが、サーバー起動シーケンスとサーバー事前障害シーケンスを自動的にキャプチャーします。コンソールビデオの録画を手動で開始および停止することもできます。

- サーバー起動シーケンスとサーバー事前障害シーケンスは、ファームウェアのアップデート中またはリモートコンソールの使用中には自動的にキャプチャーされません。
- サーバー起動シーケンスとサーバー事前障害シーケンスは、自動的にiLOメモリに保存されます。ファームウェアのアップデート中、iLOのリセット時、および電源の消失時には失われます。.NET IRCを使用すると、キャプチャーしたビデオをローカルドライブに保存できます。
- サーバー起動ファイルは、サーバーの起動が検出されると、情報のキャプチャーを開始します。ファイルの領域がなくなると停止します。このファイルは、サーバーが起動するたびに上書きされます。
- サーバー事前障害ファイルは、サーバー起動ファイルがいっぱいになると、情報のキャプチャーを開始します。iLOがASRイベントを検出すると停止します。サーバー事前障害ファイルは、iLOがASRイベントを検出したときにロックされます。ファイルのロックが解除され、.NET IRCを介してダウンロードした後でファイルが上書き可能になります。
- コンソールのキャプチャーのコントロールボタンは、.NET IRCセッションウィンドウの下部にあります。

サブトピック

コンソールキャプチャーコントロール

サーバー起動シーケンスとサーバー事前障害シーケンスの表示

サーバー起動ビデオファイルとサーバー事前障害ビデオファイルの保存

リモートコンソールを使用したビデオファイルのキャプチャー

リモートコンソールを使用した保存済みビデオファイルの表示

コンソールキャプチャーコントロール

左から右に、以下のコンソールキャプチャーコントロールがあります。

- スタートにスキップ – ファイルの最初から再生を再開します。
- 一時停止 – 再生を一時停止します。
- 再生 – 現在選択されているファイルが再生されていなかったり一時停止されている場合は、再生を開始します。
- 録画 – .NET IRCセッションを記録します。
- 進行状況バー – ビデオセッションの進行状況が示されます。

サーバー起動シーケンスとサーバー事前障害シーケンスの表示

前提条件

- リモートコンソール権限
- リモートコンソール機能がアクセス設定ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. .NET IRCを起動します。
3. 再生ボタンをクリックします。

   再生ボタンは緑色の三角形のアイコンで示され、リモートコンソールウィンドウの下部にあるツールバーにあります。

   再生ソースダイアログボックスが表示されます。
4. サーバースタートアップまたはサーバー事前障害を選択します。
5. 開始をクリックします。

詳しくは

iLOアクセス設定の構成
コンソールのキャプチャー（.NET IRC）

サーバー起動ビデオファイルとサーバー事前障害ビデオファイルの保存

前提条件

- リモートコンソール権限
- リモートコンソール機能がアクセス設定ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. .NET IRCを起動します。
3. 再生ボタンをクリックします。

   再生ボタンは緑色の三角形のアイコンで示され、リモートコンソールウィンドウの下部にあるツールバーにあります。

4. サーバースタートアップまたはサーバー事前障害を選択します。
5. 開始をクリックします。
6. 再生ボタンを再びクリックして、再生を停止します。

   iLOによって、記録が書き込み保護されなくなったことが通知され、保存するように求められます。

7. はいをクリックします。
8. 保存場所を選択し、ファイル名を入力して、保存をクリックします。
9. （オプション）ビデオファイルを再生します。

詳しくは

iLOアクセス設定の構成
コンソールのキャプチャー（.NET IRC）

リモートコンソールを使用したビデオファイルのキャプチャー

前提条件

- リモートコンソール権限
- リモートコンソール機能がアクセス設定ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

このタスクについて

この手順を使用して、サーバー起動およびサーバー事前障害以外のシーケンスのビデオファイルを手動でキャプチャーします。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。

2. .NET IRCを起動します。
3. 録画ボタンをクリックします。

   録画ボタンは赤い円のアイコンで示され、リモートコンソールウィンドウの下部にあるツールバーにあります。

   ビデオの保存ダイアログボックスが開きます。

4. ファイル名と保存位置を入力し、保存をクリックします。
5. 録画が終了したら、もう一度録画ボタンを押して録画を停止します。
6. （オプション）ビデオファイルを再生します。

詳しくは

iLOアクセス設定の構成
コンソールのキャプチャー（.NET IRC）

リモートコンソールを使用した保存済みビデオファイルの表示

前提条件

- リモートコンソール権限
- リモートコンソール機能がアクセス設定ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. .NET IRCを起動します。
3. 再生ボタンをクリックします。

   再生ボタンは緑色の三角形のアイコンで示され、リモートコンソールウィンドウの下部にあるツールバーにあります。

   再生ソースダイアログボックスが表示されます。
4. ファイルからボックスの横にある虫眼鏡アイコンをクリックします。
5. ビデオファイルに移動し、開くをクリックします。

   リモートコンソールでキャプチャーしたビデオファイルは、iLOファイルタイプを使用します。
6. 開始をクリックします。

詳しくは

iLOアクセス設定の構成
コンソールのキャプチャー（.NET IRC）

IRCを使用したスクリーンキャプチャー

サーバーアクティビティのスクリーンキャプチャーを保存する必要がある場合は、リモートコンソールのスクリーンキャプチャー機能を使用します。たとえば、リモートコンソール画面に表示されたPOSTコードのキャプチャーが必要な場合があります。

IRCスクリーンキャプチャー機能を使用する場合、キャプチャーイメージにリモートコンソールのステータスバーは含まれません。ステータスバーを含むスクリーンキャプチャーが必要な場合、別のスクリーンキャプチャー方法を使用してください。

サブトピック

HTML5リモートコンソール画面のキャプチャー

.NET IRC画面のキャプチャー

HTML5リモートコンソール画面のキャプチャー

前提条件

- リモートコンソール権限
- リモートコンソール機能がアクセス設定ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. HTML5リモートコンソールを起動します。
3. ステータスバーのカメラアイコン をクリックします。

   新しいブラウザータブでスクリーンキャプチャーが開きます。
4. （オプション）スクリーンキャプチャーを保存します。

詳しくは

iLOアクセス設定の構成

.NET IRC画面のキャプチャー

前提条件

- リモートコンソール権限
- リモートコンソール機能がアクセス設定ページで有効になっている。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックします。

   起動タブにリモートコンソールの起動オプションが表示されます。
2. .NET IRCを起動します。
3. ステータスバーをダブルクリックします。

   スクリーンキャプチャーはクリップボードに保存されます。
4. （オプション）スクリーンキャプチャーをイメージエディターに貼り付けます。

詳しくは

iLOアクセス設定の構成

リモートコンソールのホットキー

ホットキーページを使用すると、リモートコンソールセッション中に使用する最大6つのホットキーを定義できます。各ホットキーは、最大5つのキーの組み合わせを表します。ホットキーが押されると、キーの組み合わせがホストサーバーに

送信されます。ホットキーは、統合リモートコンソールおよびテキストベースのリモートコンソールを使用するリモートコンソールセッション中アクティブです。

ホットキーが設定されていない場合、たとえば、Ctrl+VはNONE、NONE、NONE、NONE、NONEに設定され、このホットキーは無効になります。サーバーオペレーティングシステムは、Ctrl+Vを通常のように解釈します（この例では「貼り付け」）。別のキーの組み合わせを使用するようにCtrl+Vを設定すると、サーバーオペレーティングシステムはiLOに設定されたキーの組み合わせを使用します（貼り付け機能がなくなります）。

例1: Alt+F4をリモートサーバーに送信したいが、このキーの組み合わせを押すとブラウザーが閉じる場合は、Alt+F4のキーの組み合わせをリモートサーバーに送信するようにホットキーCtrl+Xを構成することができます。ホットキーの設定後は、リモートサーバーにAlt+F4を送信したいとき、リモートコンソールウィンドウでCtrl+Xを押します。

例2：国際キーボードのAltGRキーをリモートサーバーに送信してホットキーを作成したい場合は、キーリストのR_ALTを使用します。

注記:

リモートコンソールセッションでの入力が多いと、場合によっては、Ctrl + XおよびCtrl + Vショートカットを使用するホットキーの割当てを避ける必要があります。これらのショートカットは、通常、カットアンドペースト機能に割り当てられます。

サブトピック

リモートコンソールのホットキーの作成

リモートコンソールコンピューターのロックキーおよびホットキーを構成するキー

ホットキーのリセット

リモートコンソールのホットキーの作成

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックして、ホットキータブをクリックします。
2. 作成するホットキーごとに、リモートサーバーに送信するキーの組み合わせを選択します。

   ホットキーを構成して国際キーボードからのキーシーケンスを生成するには、国際キーボード上のキーと同じ位置にあるUSキーボードのキーを選択します。リモートコンソールコンピューターのロックキーおよびホットキーを構成するキーはホットキーを設定するときに使用できるキーを示します。
3. ホットキーを保存をクリックします。

   iLOは、ホットキーの設定が正常にアップデートされたことを確認します。

詳しくは

リモートコンソールのホットキーの送信
リモートコンソールコンピューターのロックキーおよびホットキーを構成するキー

リモートコンソールコンピューターのロックキーおよびホットキーを構成するキー

ESC	SCRL LCK	0	f
L_ALT	SYS RQ	1	g
R_ALT	PRINT SCREEN	2	h
L_SHIFT	F1	3	I
R_SHIFT	F2	4	j
L_CTRL	F3	5	k
R_CTRL	F4	6	l
L_GUI	F5	7	m
R_GUI	F6	8	n
INS	F7	9	o
DEL	F8	;	p
HOME	F9	=	q
END	F10	[	r
PG UP	F11	¥	s
PG DN	F12	]	t
ENTER	SPACE	`	u
TAB	'	a	v
BREAK	,	b	w
BACKSPACE	-	c	x
NUM PLUS	.	d	y
NUM MINUS	/	e	z

ホットキーのリセット

前提条件

iLOの設定を構成する権限

このタスクについて

ホットキーをリセットすると、現在のすべてのホットキー割り当てがクリアされます。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックして、ホットキータブをクリックします。
2. ホットキーをリセットをクリックします。

   iLOが要求を確認するように求めます。
3. 要求を確認するメッセージが表示されたら、はい、ホットキーをリセットしますをクリックします。

ホットキーがリセットされたことがiLOによって通知されます。

リモートコンソールセキュリティの設定

サブトピック

リモートコンソールのコンピューターロック設定を構成する

リモートコンソールの信頼設定の構成（.NET IRC）

リモートコンソールのコンピューターロック設定を構成する

前提条件

iLOの設定を構成する権限

このタスクについて

この機能により、リモートコンソールセッションが終了したりiLOへのネットワークリンクが失われると、OSがロックされるかユーザーがログアウトされます。この機能が有効になっているときにリモートコンソールウィンドウを開いた場合、ウィンドウを閉じるときにOSがロックされます。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックして、セキュリティタブをクリックします。
2. 以下のリモートコンソールコンピューターロック設定から選択します。Windows、カスタム、および無効。
3. カスタムを選択した場合は、コンピューターのロックキーシーケンスを選択します。
4. 変更を保存するには、適用をクリックします。

サブトピック

リモートコンソールのコンピューターロックオプション

詳しくは

リモートコンソールのコンピューターロックオプション
リモートコンソールコンピューターのロックキーおよびホットキーを構成するキー

リモートコンソールのコンピューターロックオプション

- Windows - Windowsオペレーティングシステムを実行している管理対象サーバーをロックするようにiLOを構成します。リモートコンソールセッションが終了した場合やiLOネットワークリンクが失われた場合は、サーバーにコンピューターロックダイアログボックスが自動的に表示されます。
- カスタム - カスタムキーシーケンスを使用して管理対象サーバーをロックしたりサーバーにログインしているユーザーをログアウトさせたりするようにiLOを構成します。最大で5つのキーをリストから選択できます。リモートコンソールセッションが終了した場合やiLOネットワークリンクが失われた場合は、選択されたキーシーケンスがサーバーのOSに自動的に送信されます。
- 無効（デフォルト） - リモートコンソールのコンピューターロック機能を無効にします。リモートコンソールセッションが終了したり、iLOネットワークリンクが失われた場合でも、管理対象サーバー上のOSはロックされません。

詳しくは

リモートコンソールのコンピューターロックオプション
リモートコンソールコンピューターのロックキーおよびホットキーを構成するキー

リモートコンソールの信頼設定の構成（.NET IRC）

前提条件

iLOの設定を構成する権限

このタスクについて

.NET IRCは、Microsoft .NET Frameworkの一部であるMicrosoft ClickOnceを介して起動します。ClickOnceでは、SSL接続からインストールされるすべてのアプリケーションが信頼できるソースからのものでなければなりません。ブラウザーがiLOプロセッサーを信頼するように設定されていないときにこの設定が有効に設定されている場合、ClickOnceは、アプリケーションを起動できないことを通知します。

Hewlett Packard Enterpriseでは、信頼済みのSSL証明書をインストールして、IRCはiLO内の信頼された証明書を要求します設定を有効にすることをおすすめします。この構成では、.NET IRCはHTTPS接続を使用することにより起動します。

IRCはiLO内の信頼された証明書を要求します設定が無効の場合、.NET IRCはSSL以外の接続を使用することで起動するため、安全ではありません。この構成では、.NET IRCが暗号キーの交換を開始すると、SSLが使用されます。信頼済みのSSL証明書をインストールできず、SSL以外の接続を使用したくない場合は、スタンドアロンリモートコンソール（HPLOCONS）またはHTML 5統合リモートコンソールを使用できます。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックして、セキュリティタブをクリックします。
2. IRCはiLO内の信頼された証明書を要求します設定の有効と無効を切り替えるには、切り替えスイッチをクリックします。
3. 変更を保存するには、適用をクリックします。

詳しくは

SSL証明書の管理
.NET IRC要件

テキストベースのリモートコンソールの使用

iLOは、テキストベースのリモートコンソールをサポートします。サーバーからビデオ情報が取得され、ビデオメモリの内容がiLOマネジメントプロセッサーへ送信され、圧縮され、暗号化され、管理クライアントアプリケーションに転送されます。iLOは画面フレームバッファーを使用して、テキストベースのクライアントアプリケーションに（画面上の位置情報とともに）文字を送信します。この方法により、標準的なテキストベースクライアントとの互換性、良好な性能、および単純さが確保されます。ただし、ASCII以外の文字やグラフィカル情報は表示できず、表示される文字の画面上の位置の送信順序が前後にずれる場合があります。

iLOは、ビデオアダプターのDVOポートを使用して、ビデオメモリに直接アクセスします。この方法により、iLOの性能が大幅に向上します。ただし、デジタルビデオストリームには有用なテキストデータが含まれず、テキストベースのクライアントアプリケーション（SSHなど）では、このデータを表示できません。

テキストベースのコンソールオプションについては、次の項で説明します。

- iLO仮想シリアルポート

サブトピック

iLO仮想シリアルポート

iLO仮想シリアルポート

標準ライセンスと仮想シリアルポートを使用すると、iLOからテキストベースのコンソールにアクセスできます。

仮想シリアルポートにより、サーバーのシリアルポートと双方向データフローが提供されます。リモートコンソールを使用すると、リモートサーバーシリアルポート上に物理シリアル接続が存在するかのように操作できます。

仮想シリアルポートはテキストベースのコンソールとして表示されますが、その情報はグラフィカルビデオデータを通じて描画されます。iLOでは、サーバーがプレオペレーティングシステム状態であるときに、この情報がSSHクライアント経由で表示されます。この機能を使用すると、iLO標準システムでPOST中のサーバーを監視および操作できます。

仮想シリアルポートを使用すると、リモートユーザーは以下の操作を実行できます。

- サーバーのPOSTシーケンスおよびオペレーティングシステムの起動シーケンスの操作

  UEFIシステムユーティリティを起動するには、仮想シリアルポートセッション中に、ESC + Shift 9キーまたはEsc + (キーの組み合わせを入力します。

- オペレーティングシステムとのログインセッションの確立、オペレーティングシステムの操作、およびオペレーティングシステム上のアプリケーションの実行と操作
- グラフィックフォーマットでLinuxを実行するiLOシステムの場合は、サーバーのシリアルポートで`getty`を構成し、仮想シリアルポートを使用してLinux OSへのログインセッションを表示できます。
- 仮想シリアルポートからのEMSコンソールの使用。EMSは、Windowsの起動の問題とカーネルレベルの問題をデバッグする場合に便利です。

サブトピック

iLO仮想シリアルポートの使用

手順

1. UEFIシステムユーティリティでiLO仮想シリアルポートを構成します。
2. iLO仮想シリアルポートを使用するようにオペレーティングシステムを設定します。
   - サポートされるLinuxオペレーティングシステムについては、iLO仮想シリアルポートを使用するためのLinuxの設定を参照してください。
   - サポートされるWindowsオペレーティングシステムについては、iLO仮想シリアルポート搭載のWindows EMSコンソールを参照してください。
3. iLO仮想シリアルポートセッションを開始します。
4. （オプション）iLO仮想シリアルポートログを表示します。
5. （オプション）iLO Webインターフェイスを介したiLO仮想シリアルポートログをダウンロードします。

UEFIシステムユーティリティでのiLO仮想シリアルポートの構成

このタスクについて

次の手順は、iLO仮想シリアルポートを使用する前に必要な設定です。この手順はWindowsシステムとLinuxシステムの両方で必要です。

手順

1. UEFIシステムユーティリティにアクセスします。
   a. （オプション）サーバーにリモートアクセスする場合、iLOリモートコンソールセッションを開始します。
   b. サーバーを再起動するかまたは電源を入れます。
   c. サーバーのPOST画面でF9キーを押します。

      UEFIシステムユーティリティが起動します。
2. 仮想シリアルポートのCOMポートを設定します。
   a. システム構成をクリックし、BIOS/プラットフォーム構成（RBSU）をクリックします。
   b. システムオプションをクリックし、シリアルポートオプションをクリックします。
   c. 仮想シリアルポートメニューで、使用するCOMポートを選択します。
3. BIOSシリアルコンソールおよびEMSプロパティを設定します。
   a. シリアルポートオプションページの上部で、BIOSシリアルコンソールおよびEMSを選択します。
   b. BIOSシリアルコンソールポートメニューで、使用するCOMポートを選択します。
   c. BIOSシリアルコンソールボーレートメニューで、115200を選択します。

      注記:
      iLO仮想シリアルポートは物理UARTを使用しません。BIOSシリアルコンソールボーレートの値は、iLO仮想シリアルポートがデータを送受信するのに使用する速度には影響しません。
   d. Windowsユーザーの場合のみ：EMSコンソールメニューで、仮想シリアルポートで選択したCOMポートに一致するCOMポートを選択します。
4. 変更を保存して終了するには、F12キーを押します。
5. 要求を確認するメッセージが表示されたら、はい - 変更を保存しますをクリックします。

   UEFIシステムユーティリティによって、システムの再起動が必要であることが通知されます。
6. 再起動をクリックします。

iLO仮想シリアルポートを使用するためのLinuxの設定

このタスクについて

コンソールリダイレクションを使用して、Linuxサーバーをリモートから管理できます。コンソールリダイレクションを使用するようにLinuxを設定するには、Linuxブートローダー（GRUB）を設定する必要があります。サーバーのシステムROMがPOSTを完了すると、ブート可能デバイスからブートローダーアプリケーションがロードされます。シリアルインターフェイスをデフォルトのインターフェイスに定義して、10秒（デフォルトタイムアウト値）以内にローカルキーボードから入力がなければ、システムは出力先をシリアルインターフェイス（iLO仮想シリアルポート）に変更します。

サブトピック

iLO仮想シリアルポートを使用するためのRed Hat Enterprise Linux 9の構成

iLO仮想シリアルポートを使用するためのRed Hat Enterprise Linux 8の構成

iLO仮想シリアルポートを使用するためのRed Hat Enterprise Linux 9の構成

手順

1. テキストエディターで`/etc/sysconfig/grub`を開きます。

   この設定例では、`ttys0`を使用します。

   - `GRUB_CMDLINE_LINUX`行の最後に、
     `console=ttys0`
     を入力します。
   - `rhgb quiet`を削除します。
   - 次のパラメーターを入力します。

     ```
     GRUB_TIMEOUT=5
     GRUB_DEFAULT=saved
     GRUB_DISABLE_SUBMENU=true
     GRUB_TERMINAL_OUTPUT="console"
     GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap
     console=ttyS0,115200n8"
     GRUB_DISABLE_RECOVERY="true"
     ```

2. 次のコマンドを入力して`grub.cfg`ファイルを作成します。

   ```
   grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
   ```

3. シリアルポートに対して`getty`ログインサービスを有効にします。

   以下に例を示します。

   ```
   systemctl enable serial-getty@ttyS0.service
   ```

4. シリアルポートで`getty`をリッスンします。

   以下に例を示します。

   ```
   systemctl start getty@ttyS0.service
   ```

5. 構成したシリアルポートでシェルセッションを開始するには、システムブート中に自動的にログインプロセスを開始するように`/etc/inittab`ファイルに次の行を追加します。

   次の例は、`/dev/ttyS0`でログインコンソールを開始します。

   ```
   S0:2345:respawn:/sbin/agetty 115200 ttyS0 vt100
   ```

6. SSHを使用してiLOに接続し、CLPコマンド`start /system1/oemhpe_vsp1`を使用して、Linuxオペレーティングシステムへのログインセッションを表示します。

iLO仮想シリアルポートを使用するためのRed Hat Enterprise Linux 8の構成

手順

1. `grub2-env`コマンドを使用して、`kernelopts`パラメーターを確認します。

   以下に例を示します。

```
# grub2-editenv - list | grep kernelopts
kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhel-swap
rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap
```

2. listコマンドの結果をコピーします。

   以下に例を示します。

```
kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhel-swap
rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap
```

3. カーネルオプションを設定します。

   手順2でコピーした既存のカーネルオプションを含め、最後にシリアルコンソールオプションを追加します。

   以下に例を示します。

```
# grub2-editenv - set
"kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhel-swap
rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap console=ttyS0,115200 console=tty0"
```

4. （オプション）パラメーターが正しく設定されたことを確認するには、listコマンドを再度実行します。

   以下に例を示します。

```
# grub2-editenv - list | grep kernelopts
kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhel-swap
rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap console=ttyS0,115200 console=tty0
```

5. サーバーを再起動します。

サブトピック

シリアルコンソールを使用するためのGRUBの構成（Red Hat Enterprise Linux 8）

シリアルコンソールを使用するためのGRUBの構成（Red Hat Enterprise Linux 8）

このタスクについて

VGAコンソールの代わりにシリアルコンソールを使用するようにGRUBを構成できます。この機能を使用すると、別のカーネルを選択するために起動プロセスを中断するタスクや、シングルユーザーモードでの起動タスク用のカーネルパラメーターを追加するタスクなどを実行できます。

手順

シリアルコンソールを使用するようにGRUBを構成するには、スプラッシュイメージをコメントアウトして、`grub.conf`ファイルに`serial`オプションと`terminal`オプションを追加します。

以下に例を示します。

```
[root@localhost ~]# cat /boot/grub/grub.conf
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
```

```
timeout=10
#splashimage=(hd0,0)/grub/splash.xpm.gz
serial --unit=0 --speed=115200
terminal --timeout=5 serial console
title Red Hat Enterprise Linux AS (2.4.21-27.0.2.ELsmp)
root (hd0,0)
        kernel /vmlinuz-2.4.21-27.0.2.ELsmp ro root=LABEL=/ console=ttyS0,115200 console=tty0
        initrd /initrd-2.4.21-27.0.2.ELsmp.img
```

変更は、次のシステム再起動後に有効になります。

iLO仮想シリアルポートを使用するためのSUSE Linux Enterprise Serverの構成

手順

1. テキストエディターで`/etc/default/grub`を開きます。

   この設定例では、`ttys0`を使用します。

   `GRUB_CMDLINE_LINUX_DEFAULT`行の最後に、
   `"console=tty0 console=ttyS0,115200n8"`
   を入力します。

2. `grub.cfg`ファイルをアップデートするには、次のいずれかのコマンドを入力します。

   UEFIブートモードを使用しているサーバーの場合：

   ```
   grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

   レガシーBIOSブートモードを使用しているサーバーの場合：

   ```
   grub-mkconfig -o /boot/efi/EFI/sles/grub.cfg
   ```

3. `systemctl`を使用して、`getty`を`/dev/ttyS0`上でリッスンするように構成します。

   ```
   systemctl start getty@ttyS0.service
   ```

4. `getty`をすべてのブートで`/dev/ttyS0`をリッスンするように構成するには、その特定のポートに対してサービスを有効にします。

   以下に例を示します。

   ```
   systemctl enable serial-getty@ttyS0.service
   ```

5. 構成したシリアルポートでシェルセッションを開始するには、システムブート中に自動的にログインプロセスを開始するように`/etc/inittab`ファイルに次の行を追加します。

   次の例は、`/dev/ttyS0`でログインコンソールを開始します。

   ```
   S0:2345:respawn:/sbin/agetty 115200 ttyS0 vt100
   ```

6. SSHを使用してiLOに接続し、iLOのCLPコマンド`start /system1/oemhpe_vsp1`を使用して、Linuxオペレーティングシステムへのログインセッションを表示します。

iLO仮想シリアルポート搭載のWindows EMSコンソール

iLOを使用すると、Windows EMSコンソールをネットワーク経由でWebブラウザーを介して使用できます。EMSを使用すると、ビデオ、デバイスドライバーなどOS機能が原因で通常の動作や通常の修正処置が実行できない場合に、Emergency Management Services（EMS）を実行できます。

iLOでWindows EMSコンソールを使用する場合：

- 仮想シリアルポートを使用する前に、OSにWindows EMSコンソールを構成する必要があります。EMSコンソールを有効化する方法については、OSのドキュメントを参照してください。EMSコンソールがOSで有効になっていない場合は、仮想シリアルポートにアクセスしようとしたときに、iLOがエラーメッセージを表示します。
- Windows EMSシリアルポートは、UEFIシステムユーティリティから有効にする必要があります。構成オプションでは、EMSポートを有効または無効にすることやCOMポートを選択することができます。iLOは、EMSポートの有効/無効を自動的に検出し、COMポートの選択を検出します。
- Windows EMSコンソールは、リモートコンソールと同時に使用できます。
- `SAC>`プロンプトを表示するには、仮想シリアルポートコンソールを介して接続した後で、Enterを押す必要があります。

サブトピック

iLO仮想シリアルポートを使用するためのWindowsの構成

iLO仮想シリアルポートを使用するためのWindowsの構成

このタスクについて

これらの手順を実行するときの構文ヘルプについては、
```
bcdedit /?
```
を入力します。

手順

1. コマンドウィンドウを開きます。
2. 起動構成データを編集するには、次のコマンドを入力します。

   ```
   bcdedit /ems on
   ```

3. 次のコマンドを入力して、EMSPORTおよびEMSBAUDRATEの値を構成します。

   ```
   bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
   ```

   注記:
   EMSPORT:1がCOM1で、EMSPORT:2がCOM2です。

4. ブートアプリケーションに対して緊急管理サービスを有効または無効にするには、次のコマンドを入力します。

   ```
   bcdedit /bootems on
   ```

5. オペレーティングシステムを再起動します。

iLO仮想シリアルポートセッションの開始

前提条件

- 仮想シリアルポート設定は、UEFIシステムユーティリティで構成されます。
- WindowsまたはLinuxオペレーティングシステムは、仮想シリアルポートを使用するように構成されます。

手順

1. SSHセッションを開始します。

   例えば、
   ```
   ssh Administrator@<iLO IPアドレス>
   ```
   を入力するか、または `putty.exe` をポート22で接続します。

2. プロンプトが表示されたら、iLOアカウントの認証情報を入力します。

3. `</>hpiLO->` プロンプトで、
   ```
   VSP
   ```
   と入力し、Enterキーを押します。

4. （Windowsシステムの場合のみ） `<SAC>` プロンプトで
   ```
   cmd
   ```
   と入力して、コマンドプロンプトチャネルを作成します。

5. （Windowsシステムの場合のみ）チャネル番号で指定されたチャネルに切り替えるには、
   ```
   ch - si <#>
   ```
   と入力します。

6. プロンプトが表示されたら、OSのログイン認証情報を入力します。

詳しくは

iLO仮想シリアルポートの使用

iLO仮想シリアルポートログの表示

前提条件

- セキュリティ – アクセス設定ページのセキュアシェル（SSH）および仮想シリアルポートログover CLIを有効にします。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

このタスクについて

仮想シリアルポートの動作がiLOメモリにある150ページの循環バッファーに記録され、CLIコマンド `vsp log` を使用して表示できます。仮想シリアルポートのバッファーサイズは、128 KBです。

`vsp log` コマンドを使用して仮想シリアルポートアクティビティを表示できます。

手順

1. SSH経由でCLIに接続します。

   ```
   vsp
   ```
   コマンドを使用して、仮想シリアルポートの動作を表示します。

   ```
   ESC
   ```
   を入力して、終了します。

4. 仮想シリアルポートログを表示するには、
   ```
   vsp log
   ```
   を入力します。

詳しくは

iLOアクセス設定の構成

iLO Webインターフェイスを介した仮想シリアルポートログのダウンロード

前提条件

- iLOの設定を構成する権限
- ダウンロード可能な仮想シリアルポートログオプションは、アクセス設定ページで有効になっています。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

手順

1. ナビゲーションツリーでセキュリティをクリックします。

   アクセス設定ページが表示されます。

2. iLOアクセス設定カテゴリの横にある をクリックします。

   iLO設定の編集ページが表示されます。

3. ダウンロード可能な仮想シリアルポートログオプションの横にあるダウンロードリンクをクリックします。

   ダウンロードが終了すると、iLOから通知されます。

ホスト上でのiLOの使用

仮想NIC機能により、ホストオペレーティングシステムから直接iLOに安全に接続できます。この機能をホストサーバーで直接使用するか、リモートコンソール接続経由で使用します。iLOとの対話は、Webインターフェイス、SSH、またはiLORESTful APIを使用して行うことができます。

仮想NIC機能は、以下を行う場合に役立ちます。

- ネットワーク構成により管理ネットワーク経由で接続できない場合にiLOにアクセスするとき。たとえば、本番環境ネットワークにアクセスできるがiLO専用管理ネットワークにアクセスできない場合、仮想NICの接続を使用します。
- ホストまたはiLOにNICケーブルが接続されていない場合にiLOにアクセスするとき。

工場出荷時のデフォルトの仮想NIC設定は、iLOのほとんどのバージョンで無効になっています。iLO6 v2.10では、この設定はデフォルトで有効になっています。iLOを工場出荷時のデフォルト設定にリセットすると、仮想NIC設定は、iLOのインストールされているバージョンのデフォルト設定に戻ります。ファームウェアのアップグレードまたはダウングレードでは、この設定は変更されません。

サブトピック

仮想NICを使用するための前提条件

仮想NICについてのオペレーティングシステムのサポート

仮想NIC機能の構成

iLO Webインターフェイスにアクセスするための仮想NICの使用

ホスト上でのiLORESTの使用

仮想NICでのSSH接続の使用

仮想NICを使用するための前提条件

- USB CDC-EEM用のインボックスドライバーモジュールを備えたホストサーバーオペレーティングシステムは、仮想NICをサポートします。

  サポートされているWindowsおよびLinuxオペレーティングシステムのほとんどは、iLOで仮想NICが有効になっている場合、ドライバーモジュールを自動的にロードします。

  Windowsホストでは、`C:\Windows\System32`で`usbnet.sys`を探すことで、サポートを確認できます。

  Linuxホストでは、次の方法を使用して、仮想NIC機能がiLOで無効になっている場合のサポートを確認できます。

  - 次のコマンドを入力して、 `/lib/modules`で `cdc_eem.ko`を探します。

    ```
    find /lib/modules/$(uname -r)  *.ko* | grep cdc_eem
    ```

  - 次のコマンドを入力して、`cdc_eem`がロードされているかどうか確認します。

    ```
    lsmod | grep cdc_eem
    ```

    `cdc_eem`がロードされていない場合は、次のコマンドを入力してロードできます。

    ```
    sudo modprobe cdc_eem
    ```

    `cdc_eem`を手動でロードした後、`lsmod | grep cdc_eem`を再度実行し、正常にロードされたことを確認します。

- ホストサーバーOSが仮想NICをサポートしている。
- Linuxホストでは、USB CDC-EEMドライバーがホストサーバーOSにインストールされ構成されています。

  このドライバーは、この機能をサポートするオペレーティングシステムのOSインストールの一部です。

- 仮想NIC機能がアクセス設定ページで有効になっている。
- iLOへの接続に使用するインターフェイスがアクセス設定ページで有効になっている。

  例えば、iLO Webインターフェイスに接続する場合、iLO Webインターフェイスオプションが有効になっている。

- ホストサーバーが、iLOへの接続に使用するインターフェイス用のポートをブロックするように構成されていない。

  例えば、デフォルトのiLO構成でiLO Webインターフェイスを使用するとき、ホストサーバーがポート443をブロックしないようにしてください。

- 仮想NICインターフェイスが、いずれのホストNICともチーミングまたはブリッジされていない。この構成では、仮想NICが使用できなくなったり安全でなくなる可能性があります。
- iLOのホスト名と仮想NIC IPアドレスは、仮想NICへのアクセスに使用するクライアントシステム上の`hosts`ファイル内にあります。iLOのホスト名を使用して仮想NICでiLOに接続するには、この構成で名前解決が機能し、SSL接続が正しく検証される必要があります。

詳しくは

iLOアクセス設定の構成
仮想NICについてのオペレーティングシステムのサポート

仮想NICについてのオペレーティングシステムのサポート

仮想NIC機能は、iLO6および次のオペレーティングシステムを有するサーバーが要件を満たします。

- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- SUSE Linux Enterprise Server 12
- SUSE Linux Enterprise Server 15

- Red Hat Enterprise Linux 9
- Red Hat Enterprise Linux 8

この機能は、必要なドライバーが含まれている、要件を満たさない他のオペレーティングシステムで動作することが予想されます。

仮想NIC機能の構成

前提条件

iLOの設定を構成する権限

手順

1. 仮想NIC機能が有効になっていることを確認します。
   a. ナビゲーションツリーでセキュリティをクリックします。

      アクセス設定ページが表示されます。

   b. iLOセクションで仮想NICが有効に設定されていることを確認します。
2. 仮想NICが有効に設定されていない場合は、有効にします。
   a. （iLOカテゴリの隣にある）をクリックします。

      iLO設定の編集ページが表示されます。

   b. 仮想NICチェックボックスを選択して、OKをクリックします。

      iLOが、保留中の変更を有効にするにはリセットを必要であることを通知します。

   c. アクセス設定のアップデートが完了している場合は、iLOのリセットをクリックします。

      iLOが要求を確認するように求めます。

   d. はい、iLOをリセットしますをクリックします。

      接続が再確立されるまでに、数分かかることがあります。

      リセットが完了したら、仮想NIC機能が有効になり、ホストサーバーのOSによって検出されます。
3. （オプション）DHCP用の新しいネットワークインターフェイスを自動的に構成しないLinuxディストリビューションの場合：仮想NICインターフェイスのネットワーク構成を静的からDHCPに変更します。

   詳しくは、以下を参照してください。

   - 仮想NICインターフェイスを静的からDHCPに変更する（ネットワークマネージャー）
   - 仮想NICインターフェイスを静的からDHCPに変更する（CLI）
4. ホストオペレーティングシステムで仮想NICが使用できることを確認します。
   a. リモートコンソールセッションを開始するか、物理ホストシステムにアクセスします。
   b. ホストサーバーのオペレーティングシステムにログインします。
   c. 次のいずれかを実行します。
      - Windowsシステムの場合：`ipconfig`を実行し、IPアドレスが16.1.15.2、サブネットマスクが255.255.255.252のEthernet adapter Ethernetという名前のアダプターを探します。
      - Linuxシステムの場合：ネットワークインターフェイス名を特定し、`ifconfig`を実行します。アダプターのIPアドレスは16.1.15.2、サブネットマスクは255.255.255.252です。

> **警告:**
> ホストのアダプターIPアドレスは変更しないでください。IPアドレスを16.1.15.2から他の値に変更すると、仮想NICにアクセスできなくなります。

サブトピック

仮想NICインターフェイスを静的からDHCPに変更する（ネットワークマネージャー）

仮想NICインターフェイスを静的からDHCPに変更する（CLI）

詳しくは

iLOアクセス設定の構成

仮想NICインターフェイスを静的からDHCPに変更する（ネットワークマネージャー）

このタスクについて

LinuxディストリビューションがDHCPの新しいネットワークインターフェイスを自動的に構成しない場合、仮想NICインターフェイスのネットワーク構成を静的からDHCPに変更します。

手順

1. ネットワークマネージャーを開きます。
2. 仮想NICインターフェイスを探します。
3. DHCPを使用するように仮想NICインターフェイスを構成します。

仮想NICインターフェイスを静的からDHCPに変更する（CLI）

このタスクについて

LinuxディストリビューションがDHCPの新しいネットワークインターフェイスを自動的に構成しない場合、仮想NICインターフェイスのネットワーク構成を静的からDHCPに変更します。

手順

1. `/sys/bus/usb/devices`内のデバイスを特定します。

   以下に例を示します。

   - `cat /sys/bus/usb/devices/1-4/idVendor`は値`03f0`を表示します。
   - `cat /sys/bus/usb/devices/1-4/idProduct`は値`2927`を表示します。
2. 仮想NICネットワークインターフェイス名を特定します。

   以下に例を示します。

   `/sys/bus/usb/devices/1-4/1-4:1.0/net/usb0`
3. DHCPを使用するよう仮想NICインターフェイスを構成するネットワーク構成スクリプトを記述します。

   たとえば、構成スクリプトに次のエントリーを含む`/etc/sysconfig/network/ifcfg-usb0`を作成します。`BOOTPROTO='dhcp'`
4. 仮想NICインターフェイスにアクセスするか、ネットワークサービスを再起動します。

iLO Webインターフェイスにアクセスするための仮想NICの使用

前提条件

- ご使用の環境が仮想NIC機能を使用するための一般的な前提条件を満たしていること。
- プロキシサーバーを使用するようにブラウザーが構成されていないこと。

手順

1. リモートコンソールセッションを開始するか、物理ホストシステムにアクセスします。
2. ホストサーバーのオペレーティングシステムにログインします。
3. サポートされているブラウザーを開きます。
4. 次のURLを入力します。

   ```
   https://16.1.15.1
   ```

   iLOのホスト名と仮想NICのIPアドレスがクライアントシステムのhostsファイルにある場合は、iLOホスト名を使用して接続することもできます。

   ```
   https://iLO hostname
   ```

   Webサイト証明書に関連するセキュリティ警告が表示されます。
5. ブラウザーに応じて、以下のいずれかを行います。
   - **Microsoft Edge** – 詳細をクリックしてから、Webページへ移動をクリックします。
   - **Google Chrome** – 詳細をクリックしてから、<iLOホスト名またはIPアドレス>にアクセスする（安全ではありません）をクリックします。
   - Mozilla Firefox – 詳細をクリックしてから、危険性を承知で続行をクリックします。

   ローカルシステムのiLOログイン画面が表示されます。
6. iLOにログインします。

   IPアドレスが16.1.15.2のセッションがセッションリストページに表示されます。
7. iLO Webインターフェイスを使用してサーバーまたはiLO構成を表示またはアップデートします。

詳しくは

iLO Webインターフェイスへのログイン
仮想NICを使用するための前提条件
サポートされているブラウザー

ホスト上でのiLORESTの使用

前提条件

- ご使用の環境が仮想NIC機能を使用するための一般的な前提条件を満たしていること。
- ホストサーバーオペレーティングシステムにRESTfulインターフェイスツールがインストールされていること。

手順

1. リモートコンソールセッションを開始するか、物理ホストシステムにアクセスします。
2. ホストサーバーOSにログインします。

3. iLORESTを開始します。
4. iLOシステムにログインします。

   ```
   iLOrest > login 16.1.15.1 -u iLO user name -p iLO password
   ```

   iLOのホスト名と仮想NICのIPアドレスがクライアントシステムのhostsファイルにある場合は、iLOホスト名を使用して接続することもできます。

   ```
   iLOrest > login iLO hostname -u iLO user name -p iLO password
   ```

5. iLORESTコマンドを使用してサーバーまたはiLO構成を表示またはアップデートします。

詳しくは

仮想NICを使用するための前提条件

仮想NICでのSSH接続の使用

前提条件

- ご使用の環境が仮想NIC機能を使用するための一般的な前提条件を満たしていること。
- Windowsオペレーティングシステムの場合のみ：PuTTyまたはOpenSSHがインストールされていること。

手順

1. リモートコンソールセッションを開始するか、物理ホストシステムにアクセスします。
2. ホストサーバーのオペレーティングシステムにログインします。
3. インストールされているオペレーティングシステムに応じて、コマンドプロンプトまたはPuTTYターミナルプロンプトを開きます。
4. iLOシステムにログインします。

   ```
   ssh iLO user name@16.1.15.1
   ```

   iLOのホスト名と仮想NICのIPアドレスがクライアントシステムのhostsファイルにある場合は、iLOホスト名を使用して接続することもできます。

   ```
   ssh iLO user name@iLO hostname
   ```

5. SSHクライアントを使用してサーバーまたはiLO構成を表示またはアップデートします。

詳しくは

仮想NICを使用するための前提条件

iLO仮想メディアの使用

サブトピック

仮想メディアに関する留意事項

仮想メディアを使用するためのオペレーティングシステム要件

iLO Webインターフェイスの仮想メディアオプション

スクリプト仮想メディア用IISのセットアップ

仮想メディアに関する留意事項

iLO仮想メディアは、ネットワークウェブの任意の位置で標準のメディアからリモートホストサーバーを起動するために使用できる仮想デバイスを提供します。仮想メディアデバイスは、ホストシステムの起動時に使用できます。仮想メディアデバイスは、USBテクノロジーを使用してホストサーバーに接続します。

仮想メディアを使用する場合、以下の点に注意してください。

- 同時に1種類の仮想メディアしか接続できません。

  この制限により、仮想フロッピー/USBキーと仮想フォルダーが同じタイプの仮想メディアとして分類されます。

- 仮想メディア機能は、最大8 TBのISOイメージをサポートしています。ISOイメージの最大ファイルサイズは、ISOイメージが保存されているファイルシステムの1つのファイルサイズの制限や、サーバーのOSがサポートするSCSIコマンドなどの要因に依存します。
- 2ギガバイトまでのサイズの仮想フォルダーがサポートされます。
- OSでは、仮想フロッピー/USBキーまたは仮想CD/DVD-ROMは、通常のドライブのように見えます。仮想メディアを初めて使用する場合、ホストOSが、新しいハードウェアの検出ウィザードを実行するよう指示する場合があります。
- 仮想デバイスが接続されてから接続を切断するまで、ホストサーバーは仮想デバイスを使用できます。仮想メディアデバイスの使用を終了して仮想メディアを切断するときに、ホストOSから「unsafe device removal」という警告メッセージを受け取る場合があります。デバイスを切断する前に、デバイスを停止するためのOS機能を使用することにより、この警告を避けることができます。
- iLO仮想CD/DVD-ROMは、サポートされるオペレーティングシステムで、サーバーの起動時に使用できます。仮想CD/DVD-ROMから起動することにより、ネットワークドライブからのOSの展開、障害の発生したオペレーティングシステムのディザスタリカバリなどの作業を実行できます。
- ホストサーバーのOSがUSBの大容量記憶装置またはSDデバイスをサポートする場合、ホストサーバーのOSをロードした後で、iLO仮想フロッピー/USBキーを使用できます。
  - ホストサーバーのOSの実行中に、仮想フロッピー/USBキーは、ドライバーのアップグレード、緊急時修復ディスクの作成などの作業に使用できます。
  - サーバーの実行時に仮想フロッピー/USBキーを使用できるようにしておくと、NICドライバーを診断し、修復する必要がある場合に役立てることができます。
  - 仮想フロッピー/USBキーは、Webブラウザーが動作している物理フロッピーディスク、USBキー、またはSDドライブである場合があります。または、ローカルのハードディスクドライブまたはネットワークドライブに保存されているイメージファイルの場合もあります。
  - 最適な性能を得るために、Hewlett Packard Enterpriseはクライアントpcのハードディスクドライブまたは高速ネットワークリンクを介してアクセスできるネットワークドライブに格納されているイメージファイルを使用することを推奨します。
- ホストサーバーのOSがUSBの大容量記憶装置をサポートする場合、ホストサーバーのOSをロードした後にも、iLO仮想CD/DVD-ROMを使用できます。
  - ホストサーバーのOSの実行中に、仮想CD/DVD-ROMを使用して、デバイスドライバーのアップグレード、ソフトウェアのインストールなどの作業を行うことができます。
  - サーバーの実行時に仮想CD/DVD-ROMを使用できるようにしておくと、NICドライバーを診断し、修復する必要がある場合に役立てることができます。
  - 仮想CD/DVD-ROMは、Webブラウザーを実行しているマシン上の物理CD/DVD-ROMドライブである場合があります。また、仮想CD/DVD-ROMは、ローカルのハードディスクドライブまたはネットワークドライブに保存されているイメージファイルの場合もあります。
  - 最適な性能を得るために、Hewlett Packard Enterpriseはクライアントpcのハードディスクドライブまたは高速ネットワークリンクを介してアクセスできるネットワークドライブに格納されているイメージファイルを使用することを推奨します。

- 仮想フロッピー/USBキーまたは仮想CD/DVD-ROM機能が使用されている場合、通常、クライアントOSからはフロッピードライブまたはCD/DVD-ROMドライブにアクセスできません。

  注意:

  ファイルやデータが壊れることを防止するために、ローカルメディアを仮想メディアデバイスとして使用しているときは、ローカルメディアへのアクセスを試行しないでください。

- HTML5 IRCの場合：iLOのWebインターフェイスウィンドウを更新するか閉じると、リモートコンソール接続は終了します。

  リモートコンソール接続が終了すると、URLベースの仮想メディアを使用して接続されていたデバイスを除き、リモートコンソールを通じて接続されていた仮想メディアデバイスにアクセスできなくなります。

- ローカルIMG、ISOファイル、または仮想フォルダーを使用して仮想メディアをマウントした場合、Redfishを介してアンマウントすることはできません。

注記: 共有ネットワークポートを使用している場合は、リモートコンソールと仮想メディアが切断される可能性があります。詳しくは、 共有ネットワークポートに関する考慮事項を参照してください。

仮想メディアを使用するためのオペレーティングシステム要件

ここでは、iLO仮想メディア機能を使用する場合に注意する必要があるオペレーティングシステム要件について説明します。

サブトピック

オペレーティングシステムのUSB要件

オペレーティングシステムに関する注意事項：仮想フロッピー/USBキー

オペレーティングシステムに関する注意事項：仮想CD/DVD-ROM

オペレーティングシステムに関する注意事項：仮想フォルダー

オペレーティングシステムのUSB要件

仮想メディアデバイスを使用するには、オペレーティングシステムがUSB大容量記憶装置を含むUSBデバイスをサポートする必要があります。詳しくは、オペレーティングシステムのドキュメントを参照してください。

システムのブート中に、ROM BIOSがUSBサポートを適用し、オペレーティングシステムがロードされます。MS-DOSは、BIOSを使用してストレージデバイスと通信しているので、DOSを起動するユーティリティフロッピーも仮想メディアとして機能します。

オペレーティングシステムに関する注意事項：仮想フロッピー/USBキー

Windows Server 2008以降

仮想フロッピー/USBキードライブは、WindowsがUSBデバイスを認識した後に自動的に表示されます。仮想デバイスを、ローカル接続されたデバイスと同じように使用してください。

Windowsのインストール中に仮想フロッピーをドライバーディスクとして使用するには、ホストRBSUの内蔵ディスクドライブを無効にします。この操作により、仮想フロッピーが強制的にドライブAとして表示されます。

Windowsのインストール中にドライバーフロッピーとして仮想USBキーを使用するには、USBキードライブのブート順序

を変更します。Hewlett Packard Enterpriseでは、USBキードライブのブート順序を最初にすることをお勧めします。

Red Hat Enterprise LinuxおよびSUSE Linux Enterprise Server

Linuxは、USBフロッピーとキードライブの使用をサポートしています。

サブトピック

フロッピーの交換

フロッピーの交換

物理USBディスクドライブがあるクライアントマシンで、仮想フロッピー/USBキーを使用する場合、ディスク交換操作は認識されません。たとえば、フロッピーディスクからディレクトリリストを取得した後、ディスクを交換すると、次のディレクトリリストには、最初のフロッピーのディレクトリリストが表示されます。仮想フロッピー/USBキーの使用中にディスクを交換する必要がある場合は、必ず、非USBのディスクドライブを搭載するクライアントマシンを使用してください。

オペレーティングシステムに関する注意事項：仮想CD/DVD-ROM

MS-DOS

仮想CD/DVD-ROMは、MS-DOSではサポートされていません。

Windows

仮想CD/DVD-ROMは、Windowsがデバイスのマウントを認識した後に自動的に表示されます。これを、ローカル接続されたCD/DVD-ROMドライブと同じように使用してください。

Linux

仮想CD/DVD-ROMは、Linux GUIでは自動的にマウントされます。

Linuxコマンドラインで仮想CD/DVD-ROMをマウントする方法については、USB仮想メディアCD/DVD-ROMをマウントする（Linuxコマンドライン）を参照してください。

Linuxディストリビューションによっては、仮想CD/DVD-ROMは次のいずれかデバイスファイルでアクセスできます。

- `/dev/cdrom`
- `/dev/scd0`
- `/dev/sr0`

ローカルのCD/DVD-ROMデバイスが存在するサーバーでは、仮想CD/DVD-ROMデバイスは、ローカルDVDデバイスに続くデバイス番号（たとえば、`/dev/cdrom1`）でアクセスできます。

サブトピック

USB仮想メディアCD/DVD-ROMをマウントする（Linuxコマンドライン）

USB仮想メディアCD/DVD-ROMをマウントする（Linuxコマンドライン）

手順

1. iLO Webインターフェイスにログインします。
2. .NET IRCを起動します。
3. 仮想ドライブメニューを選択します。

4. CD/DVD-ROMまたはISOファイルを選択します。
5. Linuxシステム上のiLO仮想メディアデバイスエントリーを見つけます。

   デバイスエントリーはシステムメッセージログファイルで確認できます。例えば、次のイメージはデバイスエントリー`/dev/sr0`を示しています。

6. マウントポイントを作成します。

   以下に例を示します。

   - Red Hat Enterprise Linux：`mkdir/mnt/cdrom`*`X`*、ここでXは選択した数字です。
   - SUSE Linux Enterprise Server：`mkdir /media/cdrom`*`X`*、ここでXは選択した数字です。

7. `mount` *`device file mount point`*のようにコマンドを入力して、デバイスをマウントします。

   以下に例を示します。

   - Red Hat Enterprise Linux：`mount /dev/cdrom1 /mnt/cdrom1`
   - SUSE Linux Enterprise Server：`mount /dev/scd0 /media/cdrom1`

オペレーティングシステムに関する注意事項：仮想フォルダー

- **起動プロセスおよびDOSセッション** – 仮想フォルダーデバイスは、標準BIOSフロッピードライブ（ドライブA）として表示されます。このとき、物理的に接続されたフロッピードライブがあっても使用できません。ローカル物理フロッピードライブと仮想フォルダーを同時に使用することはできません。
- **Windows** – Windowsが仮想USBデバイスのマウントを認識すると、仮想フォルダーは自動的に表示されます。フォルダーは、ローカル接続されたデバイスと同じように使用できます。仮想フォルダーからは起動できません。仮想フォルダーから起動しようとすると、サーバーが起動できない場合があります。
- **Red Hat Enterprise LinuxおよびSuSE Linux Enterprise Server** – Linuxは、FAT 16ファイルシステムフォーマットを使用する仮想フォルダー機能の使用をサポートします。

iLO Webインターフェイスの仮想メディアオプション

アクセス設定ページで仮想メディア機能が有効になっている場合、仮想メディアページで次の作業を実行できます。

- 物理ドライブ、ローカルイメージファイル、仮想フォルダーなどのローカルメディアを表示または取り出す。
- URLベースのメディアから表示、接続、イジェクト、または起動を実行する。URLベースのメディアとは、URLを使用してWebサーバーに保存されているイメージを接続することを示します。iLOでは、HTTPまたはHTTPS形式のURLを使用できます。FTPはサポートされません。

サブトピック

仮想メディアのステータスおよびポート構成の表示

接続されているローカルメディアの表示

ローカル仮想メディアデバイスの取り出し

URLベースのメディアの接続

接続されているURLベースのメディアの表示

URLベースの仮想メディアデバイスの取り出し

詳しくは

仮想メディアIRCの機能

仮想メディアのステータスおよびポート構成の表示

このタスクについて

仮想メディア機能の構成を表示するには、仮想メディアページを使用します。これらの設定は、アクセス設定ページで構成できます。

手順

1. リモートコンソール & メディアページに移動し、仮想メディアタブをクリックします。

   仮想メディアステータス、仮想メディアポート、および拡張されたダウンロードパフォーマンスが表示されます。

   注記: すでに有効になっている場合、拡張されたダウンロードパフォーマンスリンクは表示されません。

2. （オプション）仮想メディア機能のステータスを構成するには、仮想メディアステータスリンクをクリックします。

   アクセス設定ページが表示されます。

3. （オプション）仮想メディアポートを構成するには、仮想メディアポートリンクをクリックします。

   アクセス設定ページが表示されます。

4. （オプション）拡張されたダウンロードパフォーマンスを構成するには、拡張されたダウンロードパフォーマンスリンクをクリックします。

   アクセス設定ページが表示されます。これらの設定は、アクセス設定ページで構成できます。

   オプションについて詳しくは、 アクセス設定ページのヘルプを参照してください。

詳しくは

iLOアクセス設定の構成

接続されているローカルメディアの表示

前提条件

- 仮想メディア権限
- 仮想メディア機能がアクセス設定ページで有効になっている。

手順

接続されたローカルメディアデバイスを表示するには、ナビゲーションツリーでリモートコンソール&メディアをクリックして、仮想メディアタブをクリックします。

サブトピック

ローカルメディアの詳細

詳しくは

iLOアクセス設定の構成

ローカルメディアの詳細

ローカル仮想メディアを接続すると、以下のセクションに詳細が表示されます。

仮想フロッピー/USBキー/仮想フォルダーステータス

- 挿入されたメディア – 接続されている仮想メディアの種類。

  ローカルメディアが接続されている場合、ローカルメディアと表示されます。
- 接続ステータス – 仮想メディアデバイスが接続されているかどうかを示します。
- 読み取り専用 – 仮想メディアデバイスが読み取り専用パーミッションで接続されているかどうか。

仮想CD/DVD-ROMステータス

- 挿入されたメディア – 接続されている仮想メディアの種類。

  ローカルメディアが接続されている場合、ローカルメディアと表示されます。
- 接続ステータス – 仮想メディアデバイスが接続されているかどうかを示します。

ローカル仮想メディアデバイスの取り出し

前提条件

- 仮想メディア権限
- 仮想メディア機能がアクセス設定ページで有効になっている。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックして、仮想メディアタブをクリックします。
2. 仮想フロッピー/USBキー/仮想フォルダーステータスセクションまたは仮想CD/DVD-ROMステータスセクションにあるメディアの強制取り出しボタンをクリックします。

詳しくは

iLOアクセス設定の構成

URLベースのメディアの接続

前提条件

- 仮想メディア権限
- 仮想メディア機能がアクセス設定ページで有効になっている。

このタスクについて

仮想メディアページからURLベースのメディアを接続できます。 仮想メディアページは、1.44 MBのフロッピーイメージ（IMG）およびCD/DVD-ROMイメージ（ISO）の接続をサポートします。イメージは、iLOと同じネットワーク上のWebサーバー

に存在している必要があります。

手順

1. ナビゲーションツリーでリモートコンソール&メディアをクリックして、仮想メディアタブをクリックします。
2. 仮想フロッピーに接続セクション（IMGファイル）またはCD/DVD-ROMを接続セクション（ISOファイル）の仮想メディアURLボックスにURLベースのメディアのURLを入力します。
3. CD/DVD-ROMのみ：次のサーバー再起動時にサーバーをこのイメージだけから起動したい場合は、次回のリセット時に起動チェックボックスを選択します。

   イメージは2番目のサーバー再起動時に自動的に取り出されるので、サーバーは一度しかこのイメージから起動しません。

   このチェックボックスを選択しない場合、イメージは手動でイジェクトするまで接続されたまま残ります。サーバーは、システムブートオプションがそのように構成されている場合、以後すべてのサーバーリセット時にイメージに対して起動します。

   サーバーがPOSTを実行している場合に、次回のリセット時に起動チェックボックスを有効にしようとすると、エラーが発生します。POST中はブート順序を変更できません。POSTが終了するのを待ってから、再試行してください。
4. 仮想フロッピーのみ：読み取り専用パーミッションを持つ仮想メディアデバイスを接続する場合、読み取り専用チェックボックスを選択します。

   読み取り専用チェックボックスはデフォルトで有効になっています。
5. メディアの挿入をクリックします。
6. （オプション）接続されたイメージからいますぐ起動するには、サーバーを再起動します。

詳しくは

iLOアクセス設定の構成
スクリプト仮想メディア用IISのセットアップ

接続されているURLベースのメディアの表示

前提条件

- 仮想メディア権限
- 仮想メディア機能がアクセス設定ページで有効になっている。

手順

ナビゲーションツリーでリモートコンソール&メディアをクリックして、仮想メディアタブをクリックします。

サブトピック

URLベースのメディアの詳細

詳しくは

iLOアクセス設定の構成

URLベースのメディアの詳細

URLベースの仮想メディアを接続すると、以下のセクションに詳細が表示されます。

仮想フロッピー/USBキー/仮想フォルダーステータス

- 挿入されたメディア – 接続されている仮想メディアの種類。

  URLベースのメディアが接続されている場合、スクリプトメディアと表示されます。
- 接続ステータス – 仮想メディアデバイスが接続されているかどうかを示します。
- イメージURL – 接続されているURLベースのメディアをポイントするURL。
- 読み取り専用 – 仮想メディアデバイスが読み取り専用パーミッションで接続されているかどうか。

仮想CD/DVD-ROMステータス

- 挿入されたメディア – 接続されている仮想メディアの種類。

  URLベースのメディアが接続されている場合、スクリプトメディアと表示されます。
- 接続ステータス – 仮想メディアデバイスが接続されているかどうかを示します。
- イメージURL – 接続されているURLベースのメディアをポイントするURL。

URLベースの仮想メディアデバイスの取り出し

前提条件

- 仮想メディア権限
- 仮想メディア機能がアクセス設定ページで有効になっている。

手順

1. ナビゲーションツリーでリモートコンソール & メディアをクリックして、仮想メディアをクリックします。
2. URLベースのメディアデバイスを取り出すには、仮想フロッピー/仮想フォルダーステータスセクションまたは仮想CD/DVD-ROMステータスセクションにあるメディアの強制取り出しボタンをクリックします。

詳しくは

iLOアクセス設定の構成

スクリプト仮想メディア用IISのセットアップ

前提条件

スクリプト仮想メディア用にIISをセットアップする前に、IISが動作状態であることを確認してください。IISを使用して、簡単なWebサイトをセットアップし、そのサイトにアクセスして正しく動作していることを確認します。

サブトピック

IISの設定

読み出し/書き込みアクセス用のIISの設定

ヘルパーアプリケーションによる仮想メディアの挿入

仮想メディアヘルパーアプリケーションのサンプル

IISの設定

このタスクについて

以下の手順に従って、フロッピーまたはISO-9660 CDイメージの読み取り専用アクセス用にIISを設定します。

手順

1. ディレクトリをWebサイトに追加し、イメージをディレクトリに置きます。
2. IISが使用しているMIMEタイプにアクセスできることを確認します。

   たとえば、フロッピーイメージファイルが拡張子`.img`を使用している場合は、その拡張子に対してMIMEタイプを追加する必要があります。IIS Managerを使用して、自分のWebサイトのプロパティダイアログボックスにアクセスします。HTTPヘッダータブで、**MIMEの種類**をクリックしてMIMEタイプを追加します。

   Hewlett Packard Enterpriseは、次のタイプを追加することをおすすめします。

   - `.img application/octet-stream`
   - `.iso application/octet-stream`
3. 読み取り専用ディスクイメージを処理するようにWebサーバーが構成されていることを確認します。
   a. Webブラウザーを使用して、ディスクイメージの位置に移動します。
   b. ディスクイメージをクライアントにダウンロードします。

   以下の手順が正常に完了した場合、Webサーバーは正しく設定されます。

読み出し/書き込みアクセス用のIISの設定

手順

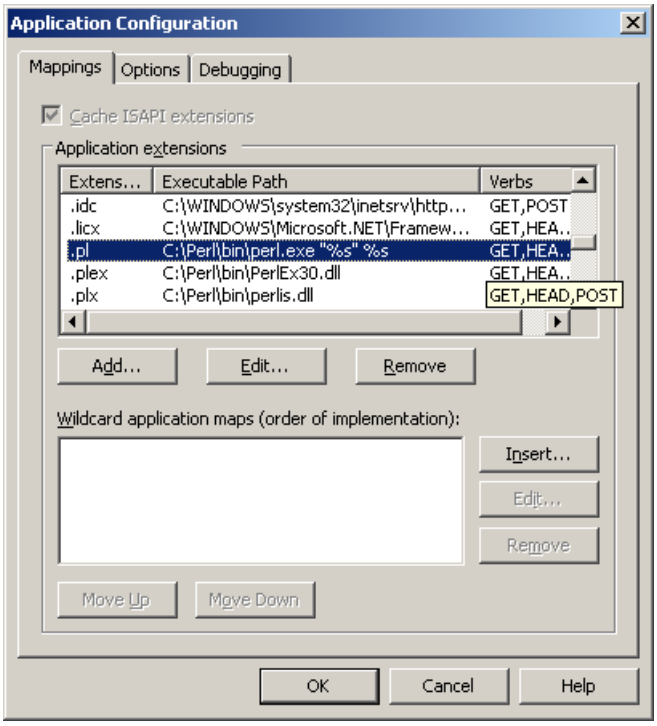
1. Perl（たとえば、ActivePerl）をインストールします。
2. 必要に応じて、仮想メディアヘルパーアプリケーションをカスタマイズします。
3. 仮想メディアヘルパースクリプトのWebサイトにディレクトリを作成し、そのディレクトリにスクリプトをコピーします。

   スクリプト例ではディレクトリ名`cgi-bin`を使用していますが、任意の名前を使用できます。
4. ディレクトリのプロパティページのアプリケーションの設定で作成をクリックしてアプリケーションディレクトリを作成します。

   IIS Managerのディレクトリのアイコンがフォルダーアイコンからギアアイコンに変わります。
5. 実行アクセス許可をスクリプトのみに設定します。
6. Perlがスクリプトインタープリターとしてセットアップされていることを確認します。

   アプリケーションの関連を確認するには、プロパティページの構成をクリックします。Perlが次の例に示すように構成されていることを確認します。

図 1. Perl設定の例



7. Web Service ExtensionsがPerlスクリプトの実行を許可していることを確認します。そうでない場合は、Web Service ExtensionsをクリックしてPerl CGI ExtensionをAllowedに設定します。
8. ヘルパーアプリケーションのプレフィックス変数が正しく設定されていることを確認します。

詳しくは

ヘルパーアプリケーションによる仮想メディアの挿入
仮想メディアヘルパーアプリケーションのサンプル

ヘルパーアプリケーションによる仮想メディアの挿入

`INSERT_VIRTUAL_MEDIA`コマンドでヘルパーアプリケーションを使用する場合、URLの基本形式は次のようになります。

```
protocol://user:password@servername:port/path,helper-script
```

変数は次のとおりです。

- `protocol` – 必須です。HTTPまたはHTTPSです。
- `user:password` – オプションです。指定された場合は、HTTP基本認証が使用されます。
- `servername` – 必須です。Webサーバーのホスト名またはIPアドレスです。
- `port` – オプションです。Webサーバーの標準でないポートです。
- `path` – 必須です。アクセスしているイメージファイルです。
- `helper-script` – オプションです。IIS Webサーバー上のヘルパースクリプトの位置です。

`INSERT_VIRTUAL_MEDIA`コマンドについて詳しくは、HPE iLO 6スクリプティング/コマンドラインガイドを参照してください。

仮想メディアヘルパーアプリケーションのサンプル

以下のPerlスクリプトは、部分書き込みの不可能なWebサーバー上でフロッピーへの書き込みを可能にするCGIヘルパーアプリケーションの例です。ヘルパーアプリケーションと`INSERT_VIRTUAL_MEDIA`コマンドを組み合わせて使用すると、書き込み可能なディスクをマウントできます。

ヘルパーアプリケーションを使用する場合、iLOファームウェアは、以下のパラメーターを使用して、このアプリケーションに要求を提示します。

- `file`パラメーターは、元のURLで提供されるファイルの名前を含みます。
- `range`パラメーターは、データの書き込み先を指定する16進数の包含範囲を含みます。
- `data`パラメーターは、書き込まれるデータを示す16進数の文字列を含みます。

ヘルパースクリプトは、`file`パラメーターをその作業ディレクトリに対する相対パスに変換する必要があります。この手順では、パラメーターの前に"../,"というプレフィックスを配置するか、またはエイリアス化されたURLパスをファイルシステム上の真のパスに変換する必要があります。ヘルパースクリプトは、ターゲットファイルに対する書き込みアクセスを必要とします。フロッピーイメージファイルは、適切なパーミッションを備える必要があります。

例：

```
#!/usr/bin/perl

use CGI;
use Fcntl;

#
# The prefix is used to get from the current working directory to the
# location of the image file that you are trying to write
#
my ($prefix) = "c:/inetpub/wwwroot";
my ($start, $end, $len, $decode);

my $q = new CGI();          # Get CGI data

my $file =  $q->param('file'); # File to be written
my $range = $q->param('range'); # Byte range to be written
my $data =  $q->param('data'); # Data to be written

#
# Change the file name appropriately
#
$file = $prefix . "/" . $file;

#
# Decode the range
#
if ($range =~ m/([0-9A-Fa-f]+)-([0-9A-Fa-f]+)/) {
$start = hex($1);
$end = hex($2);
$len = $end - $start + 1;
}

#
# Decode the data (a big hexadecimal string)
#
$decode = pack("H*", $data);

#
# Write it to the target file
#
sysopen(F, $file, O_RDWR);
binmode(F);
```

```
sysseek(F, $start, SEEK_SET);
syswrite(F, $decode, $len);
close(F);

print "Content-Length:0\r\n";
print "\r\n";
```

電力および温度機能の使用

サブトピック

サーバーの電源オン

セキュアリカバリ

電源がシステムに供給されると、iLOによって独自のファームウェアが検証および起動されます。iLOファームウェアで検証に失敗すると、リカバリイメージが使用可能な場合は自動的にiLOファームウェアがフラッシュされます。この機能は、iLO Standardライセンスでサポートされています。

サーバーの起動時に、システムROMが検証されます。アクティブなシステムROMの検証に失敗し、冗長化システムROMが有効である場合は、冗長化システムROMがアクティブになります。アクティブシステムROMと冗長化システムROMの両方が無効であり、iLO Advancedライセンスがインストールされている場合は、ファームウェア検証スキャンが開始されます。構成されているファームウェア検証の設定に応じて、システムリカバリセット内のコンポーネントを使用した修復が開始されるか、または障害のログが記録され、手動で修復を完了する必要があります。システムROMが検証されない場合、サーバーは起動しません。

ファームウェアの検証アクティビティおよびリカバリアクションについてIMLをチェックします。

ブレード以外のサーバー

iLO6を搭載したGen11サーバーでAC電源が失われた場合は、再びサーバーの電源を入れる前に約30秒待つ必要があります。この間に電源ボタンを押すと、電源ボタンが点滅し、要求が保留状態であることを示します。

この遅延は、iLOファームウェアのロード、認証、およびブートが行われているためです。iLOは、初期化の完了時に保留中の電源ボタン要求を処理します。サーバー電源が切断されていない場合、遅延はありません。30秒の遅延は、iLOのリセット中のみ発生します。iLOが電源を管理できるようになるまで、電源ボタンは無効になります。

iLOファームウェアは管理対象電源システムをサポートするために、（例えば、Hewlett Packard Enterprise消費電力上限テクノロジーを使用して）電力しきい値を監視し、構成します。iLOが電源を管理できる前にシステムの起動を許可すると、複数のシステムで電圧低下、電圧消失、および温度過負荷が発生する場合があります。AC電源が失われると電源管理状態が失われるので、電源管理状態を復元し、電源を投入できるように、最初にiLOを起動する必要があります。

電圧低下からの復旧

電圧低下条件は、動作中のサーバーへの電源が瞬間的に失われるとが発生します。電圧低下の期間およびサーバーハードウェアの構成によっては、電圧低下によりオペレーティングシステムが中断することがありますが、iLOファームウェアは中断しません。

iLOは、電圧低下を検出し、電圧低下から復旧します。iLOが電圧低下の発生を検出すると、常に電源オンが常に電源をオフのままに設定されていない場合、電源オン遅延の後でサーバー電源が復元されます。電圧低下の復旧後、iLOファームウェアは、iLOイベントログに`Brown-out recovery`イベントを記録します。

詳しくは

自動電源オン

正常なシャットダウン

iLOのプロセッサーで正常なシャットダウンを実行するには、オペレーティングシステムの協調動作が必要です。正常なシャットダウンを実行するには、Agentless Management Service（AMS）をロードする必要があります。iLOはAMSと通信し、オペレーティングシステムを安全にシャットダウンするための適切な方法を実行して、データの完全性を確保します。

AMSがロードされていない場合、iLOプロセッサーはオペレーティングシステムを使用して、電源ボタンにより正常なシャットダウンを行います。iLOは、オペレーティングシステムを正常にシャットダウンするために、電源ボタンを押す操作（iLO瞬間的に押す）をエミュレートします。オペレーティングシステムの動作は、オペレーティングシステムの設定と電源ボタンを押す設定によって異なります。

UEFIシステムユーティリティのサーマルシャットダウンオプションを使用して、自動シャットダウン機能を無効にできます。この構成では、物理的な損傷が発生する可能性がある極端な条件下の場合を除き、自動シャットダウンを無効にすることができます。

詳しくは

Agentless Management Service

電力効率

iLOを使用すると、高効率モード（HEM）を使用して電力消費を改善できます。HEMは、セカンダリパワーサプライを省電力モードに入れてシステムの電力効率を改善します。セカンダリパワーサプライが省電力モードにある場合は、プライマリパワーサプライがシステムにすべてのDC電力を供給します。各AC入力ワット数あたりのDC出力ワット数が増えるため、パワーサプライがより効率的です。

HEMは、ブレードサーバー以外でのみ使用できます。

システムがプライマリパワーサプライの最大電力出力の70%を超える電力を使用すると、セカンダリパワーサプライが正常動作に戻ります（省電力モードを終了する）。消費電力がプライマリパワーサプライの60%未満の容量に低下すると、セカンダリパワーサプライが省電力モードに戻ります。HEMを使用すると、プライマリパワーサプライとセカンダリパワーサプライの最大電力出力に等しい消費電力を実現し、低い消費電力レベルで改善された効率を維持することができます。

HEMは、電源の冗長性に影響しません。プライマリパワーサプライに障害が発生した場合は、セカンダリパワーサプライがただちにシステムへのDC電力の供給を開始し、停止時間を防止します。

HEMを設定するには、UEFIシステムユーティリティを使用します。これらの設定をiLOから行うことはできません。詳しくは、UEFIシステムユーティリティユーザーガイドを参照してください。

構成済みのHEM設定は、電力情報ページに表示されます。

詳しくは

電力情報の表示

電源投入時の保護

電源投入時の保護は、自動電源投入および仮想電源ボタンの瞬間的に押す機能と連携して動作します。サーバーの電源がリストアされるか、または瞬間的に押すが要求されたときに、サーバーハードウェアを識別できない場合、サーバーの電源がオンになりません。

電源投入時の保護機能により、サーバーの電源投入が妨げられる場合：

- イベントがIMLに記録されます。
- サーバーのヘルスステータスがクリティカルに設定されます。
- HPE OneViewがサーバーを管理する場合、SNMPトラップがHPE OneViewに送信されます。

詳しくは

自動電源オン
仮想電源ボタンのオプション

電力割り当て（ブレードサーバーおよびコンピュートモジュール）

ブレードサーバーは、エンクロージャーと電力を共有する環境で動作します。サーバーの電源を入れる前に、そのエンクロージャーから電力の割り当てを取得する必要があります。

電源投入が妨げられた場合、エラーがIMLに記録され、サーバーヘルスLEDが変更されます。次のエラーは、電源投入を妨げる場合があります。

- **Electronic KeyingまたはI/O設定エラー** - サーバーのメザニンデバイスとエンクロージャーの背面のスイッチが一致していません。
- **電力が十分でない** - サーバーに電源を投入するために十分な電力がエンクロージャーで利用できません。
- **冷却が十分でない** - サーバーを冷却するために十分な冷却がエンクロージャーで利用できません。
- **エンクロージャーがビジー状態である** - エンクロージャーがブレードに関する情報を収集中でビジー状態です。サーバーの挿入後にこのエラーが発生し、自動電源投入が有効になっている場合、iLOは許可されるまで電力を要求し続けます。それ以外の場合は、瞬間的に押すボタンをもう一度押してください。

トラブルシューティングについては、ご使用のサーバーのエラーメッセージガイドを参照してください。

サーバー電源の管理

前提条件

仮想電源およびリセット権限

このタスクについて

サーバー電源ページの仮想電源ボタンセクションは、サーバーの現在の電源状態およびリモートサーバー電源制御オプションを表示します。システム電源は、ページが初めて開かれるときのサーバー電源の状態を示します。サーバー電源の状態は、オン、オフ、またはリセットのいずれかです。サーバー電源の現在の状態を表示するには、ブラウザーの更新機能を使用します。サーバーは、まれにリセット状態に入ることがあります。

手順

1. ナビゲーションツリーで電力 & 温度をクリックします。

   サーバー電源タブが選択されたページが開きます。

2. 次のいずれかのボタンをクリックします。

   - 瞬間的に押す
   - 押し続ける
   - リセット
   - コールドブート

   サーバーの電源が入っていない場合、押し続ける、リセット、およびコールドブートオプションは使用できません。

3. 要求を確認するメッセージが表示されたら、OKをクリックします。

サブトピック

仮想電源ボタンのオプション

仮想電源ボタンのオプション

- 瞬間的に押す - 物理的な電源ボタンを押す場合と同じです。サーバーの電源が切れている場合は、瞬間的に押すを押すとサーバーに電源が投入されます。

  一部のオペレーティングシステムは、瞬間的に押した後で適切なシャットダウンを開始するか、またはこのイベントを無視するように構成されている場合があります。Hewlett Packard Enterpriseでは、仮想電源ボタンを使用してシャットダウンを実行する前に、システムコマンドを使用して正常なオペレーティングシステムのシャットダウンを完了することをお勧めします。

- 押し続ける - 物理的な電源ボタンを5秒間押し続け、離すことと同じです。

  この動作の結果、サーバーの電源が切れます。このオプションは、オペレーティングシステムの正常なシャットダウン機能に影響する場合があります。

  このオプションは、一部のオペレーティングシステムが実装しているACPI機能を提供します。これらのオペレーティングシステムは、瞬間的に押すと押し続けるによって動作が異なります。

- リセット - サーバーを強制的にウォームブートします。CPUとI/Oリソースがリセットされます。このオプションは、オペレーティングシステムの正常なシャットダウン機能に影響する場合があります。
- コールドブート - サーバーからただちに電源を切断します。プロセッサー、メモリ、およびI/Oリソースの主電力が失われます。サーバーは、約8秒後に再起動します。このオプションは、オペレーティングシステムの正常なシャットダウン機能に影響する場合があります。

システム電源リストア設定の構成

前提条件

iLOの設定を構成する権限

このタスクについて

システム電源リストア設定セクションでは、電源が喪失した後のシステムの動作を制御できます。

手順

1. ナビゲーションツリーで電力 & 温度をクリックします。

サーバー電源タブが選択されたページが開きます。

2. サーバーの自動電源オンの値を選択します。

   サーバーの自動電源オンの値の変更は次回のサーバーの再起動後まで有効にならない場合があります。

3. 電源オン遅延の値を選択します。

   サーバーの自動電源オンオプションが常に電源をオフのままに設定されている場合、この設定は選択できません。

4. 適用をクリックします。

サブトピック

自動電源オン

電源オン遅延

自動電源オン

自動電源オン設定は、例えば、サーバーの電源を接続した場合や、電源障害の後でUPSがアクティブになった場合など、電源のリストア後のiLOの動作を制御します。この設定は、Micro UPSシステムではサポートされていません。

次の自動電源オン設定の中から選択します。

- 常に電源オン - 電源投入の遅延の後でサーバーの電源を入れます。

  このオプションは、すべてのProLiantサーバーのデフォルト設定です。

- 常に電源をオフのまま - サーバーは、オンにされるまでオフのまま残ります。
- 最新の電源状態をリストア - サーバーを、電源が失われたときの電源状態に戻します。サーバーがオン状態だった場合、電源がオンになります。サーバーがオフ状態だった場合、オフのままとなります。

  このオプションは、すべてのProLiantサーバーのデフォルト設定です。

  電力不足や冷却不足などの問題が発生した場合、またはHPE OneViewの電力保持が発生すると、電源状態を戻せない可能性があります。詳しくは、HPE OneViewまたはIMLをチェックしてください。

  Synergyコンピュートモジュールがこの設定を使用するように構成されている場合、電源が復旧すると、iLOは以前の電源状態に戻すように試みます。電力不足や冷却不足などの問題が発生した場合、またはHPE OneViewの電力保持が発生すると、電源状態を戻せない可能性があります。詳しくは、HPE OneViewまたはIMLをチェックしてください。

電源オン遅延

電源オン遅延設定は、データセンター内のサーバーの自動電源投入を遅らせます。これは、iLOの起動が完了してからサーバーの電源をオンにするまでのiLOの待機時間を決定します。この設定は、Micro UPSシステムではサポートされていません。

サポートされているサーバーで、次の電源オン遅延設定のいずれかを選択します。

- 最小遅延 - iLOの起動が完了した後に電源オンします。
- 15秒遅延 - 電源投入を15秒遅らせます。
- 30秒遅延 - 電源投入を30秒遅らせます。
- 45秒遅延 - 電源投入を45秒遅らせます。
- 60秒遅延 - 電源投入を60秒遅らせます。
- 120秒までランダム - 電源投入遅延は変化し、最大120秒まで可能です。

サーバー電力使用量の表示

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- サーバー電源装置とシステムBIOSは、電力読み取りをサポートしています。電力読み取りがサポートされていない場合、このページには次のメッセージが表示されます。`Power Metering is unavailable for this configuration.`（電力メーターは、この構成では利用することができません。）

このタスクについて

電力メーターグラフは、最新のサーバー電力使用量を表示します。サーバーの電源が切断されているときは、電力履歴情報は収集されません。サーバーの電源が切断されていた期間を含むグラフを表示する場合、グラフには、データが収集されていないことを示すギャップが表示されます。

iLOがリセットされるかサーバーの電源が再投入されると、グラフのデータはクリアされます。例えば、仮想電源ボタンのリセットまたはコールドブート操作を使用すると、データが消去されます。瞬間的に押したり押し続けたりした場合、データは消去されません。

手順

1. ナビゲーションツリーで電力 & 温度をクリックして、電力メータータブをクリックします。
2. 20分、24時間、または1週間をクリックして、グラフタイプを選択します。

   直近20分間、直近24時間、または直近1週間のグラフを表示できます。
3. （オプション）グラフ表示をカスタマイズするには、以下のチェックボックスを選択またはクリアします。
   - 消費電力上限
   - 最大
   - 平均値
   - 合計CPU
   - 合計GPU
   - 合計DIMM

   サーバーが機能をサポートしていない場合、関連するチェックボックスは表示されません。
4. （オプション）このページでデータを更新する方法を選択します。

   デフォルトでは、ページを開いた後はページのデータは自動的には更新されません。
   - 選択したグラフタイプのページデータを更新するには、↻ をクリックします。
   - ページデータの自動更新を開始するには、▷ をクリックします。選択したグラフのタイプに応じて、□ をクリックするか、別のページに移動するまで、ページは自動的に更新されます。
5. （オプション）ワットまたはBTU/時をクリックし、iLO電源単位の優先設定を構成します。

   この値を設定すると、一貫したWebインターフェイス体験が提供されるよう値がcookieに保存されます。電源単位を表示するその他のページにも、これと同じ設定が使用されます。
6. （オプション）グラフ上で特定のポイントのデータを表示するには、グラフの下にあるスライダー○ を目的のポイントに移動します。

   次の方法でスライダーを移動することもできます。
   - スライダートラックをクリックします。

- スライダーアイコンをクリックし、キーボードの矢印キーを押します。

電力メーターグラフ表示オプション

グラフタイプ

20分、24時間、または1週間オプションをクリックし、グラフタイプを選択します。

- 20分 – 過去20分間にわたるサーバーの電力使用量を示します。iLOファームウェアは、このグラフの電力使用量情報をサーバーから10秒ごとに収集します。
- 24時間 – 過去24時間にわたるサーバーの電力使用量を示します。iLOファームウェアは、このグラフの電力使用量情報を5分ごとにアップデートします。
- 1週間 – 過去1週間にわたるサーバーの電力使用量を示します。iLOファームウェアは、このグラフの電力使用量情報を1時間に一度アップデートします。

グラフデータ

以下のチェックボックスを使用して、電力メーターグラフに含まれるデータをカスタマイズします。

サーバーが機能をサポートしていない場合、関連するチェックボックスは表示されません。

- 消費電力上限 – サンプル中に設定されている消費電力上限。
  - 消費電力上限は、長期間の平均消費電力を制限します。
  - 消費電力上限は、サーバーの再起動時に維持されないため、起動時に一時的なスパイクが発生します。
  - 消費電力上限を、最大電力とアイドル電力間の指定されたパーセンテージしきい値未満に設定すると、サーバー内の変化によりサーバーにアクセスできなくなることがあります。Hewlett Packard Enterpriseは、このしきい値より低い消費電力上限を設定することはお勧めしません。システム構成に対して低すぎる消費電力上限値を構成すると、システムパフォーマンスが低下する可能性があります。
- 最大 – サンプル中の瞬間最高電力。iLOは、秒未満の単位でこの値を記録します。
- 平均 – サンプル中の電力測定値の平均。
- 合計CPU – サーバー内のすべてのCPUを対象とした電力測定値の合計。
- 合計GPU – サーバー内のすべてのGPUを対象とした電力測定値の合計。

  この値は次の場合に表示されます。
  - サーバーに1つ以上のGPUがインストールされている。
  - OSが実行されている（POSTは終了済み）。
  - GPUドライバーがOSにインストールされている。

    LinuxおよびVMwareの場合：NVIDIAオプションカードにはベンダーのドライバーがインストールされ、持続モードが有効になっている必要があります。詳しくは、ベンダーのオプションカードドキュメントを参照してください。
  - GPUが電力レポートをサポートしている。
  - 電力履歴データを利用できる。
- 合計DIMM – サーバー内のすべてのDIMMを対象とした電力測定値の合計。

> **注記**: Intelプラットフォームで合計DIMM電力レポートを作成するには、ROMベースシステムユーティリティでDRAM RAPLレポートサポートオプションを有効にする必要があります。ROMベースシステムユーティリティのRAM RAPLレポートサポートオプションのデフォルト値は 有効です。

電力メーターデータの更新

能力メーターページに移動すると、デフォルトの20分のグラフが表示されます。

- 選択したグラフタイプのページデータを更新するには、 をクリックします。この方法を使用すると、カスタムグラ

フ設定が保持されます。

- ページデータの自動更新を開始するには、▷ をクリックします。選択したグラフのタイプに応じて、□ をクリックするか、別のページに移動するまで、ページは自動的に更新されます。

電力単位の表示

ワットまたはBTU/時をクリックし、電力読み取り表示をワットまたはBTU/時に変更します。

グラフ上に特定のデータポイントを表示

- グラフ上で特定のポイントのデータを表示するには、グラフの下にあるスライダー○ を目的のポイントに移動します。

  次の方法でスライダーを移動することもできます。
  - スライダートラックをクリックします。
  - スライダーアイコンをクリックし、キーボードの矢印キーを押します。

- 自動更新の実行時に、グラフの下にあるスライダー○ を動かすと、x軸方向の特定の履歴ポイントに該当するデータポイントに焦点が当たります。例えば、20分のグラフでは、スライダーを-10分の位置に配置できます。チャートを更新しても、スライダーの位置は10分前に設定された値の位置のままになります。

現在の電源状態の表示

前提条件

サーバー電源装置とシステムBIOSは、電力読み取りをサポートしています。電力読み取りがサポートされていない場合、このページには次のメッセージが表示されます。`Power Metering is unavailable for this configuration.`（電力メーターは、この構成では利用することができません。）

手順

ナビゲーションツリーで電力 & 温度をクリックして、電力メータータブをクリックします。

電源ステータスセクションに、現在の電源状態の詳細が表示されます。

現在の電源状態の詳細

電力ステータスセクションに表示される情報は、サーバータイプによって変化します。表示される可能性のある値は次のとおりです。

- 現在の電力読み取り値 – サーバーからの現在の電力読み取り値。

  この値は、すべてのサーバーについて表示されます。

- 現在の消費電力上限値 – サーバーに対して設定されている消費電力上限。消費電力上限が設定されていない場合、この値は0です。

  この値は、MLサーバーおよびDLサーバーについて表示されます。消費電力上限をサポートしないサーバーでは表示されません。

- 入力電圧 – サーバーに指定された入力電圧。

  この値は、MLサーバーおよびDLサーバーについて表示されます。

- パワーレギュレーターモード – 設定されているモード。設定できる内容については、電力設定を参照してください。

  この値は、すべてのサーバーについて表示されます。

- パワーサプライ容量 – サーバーの電力容量。

  この値は、サポートされているサーバーについて表示されます。

- ピーク電力測定値 – 最大電力測定値。

  この値は、サポートされているサーバーについて表示されます。

サーバー電力履歴の表示

前提条件

サーバー電源装置とシステムBIOSは、電力読み取りをサポートしています。電力読み取りがサポートされていない場合、このページには次のメッセージが表示されます。`Power Metering is unavailable for this configuration.`（電力メーターは、この構成では利用することができません。）

手順

ナビゲーションツリーで電力 & 温度をクリックして、電力メータータブをクリックします。

電力履歴セクションには、サーバーの電力履歴の詳細が表示されます。

電力履歴の詳細

電力の履歴テーブルには、5分、20分、24時間、および1週間の4つの期間で電力読み取り値を表示します。

- 最大電力 – 指定された期限でのサーバーからの最大電力測定値。サーバーが指定された期限にわたり稼動していない場合は、サーバーの起動時からのすべての測定値の最大値になります。
- 平均電力 – 指定された期限での電力測定値の平均。サーバーが指定された期限にわたり稼動していない場合は、サーバーの起動時からのすべての測定値の平均になります。
- 最小電力 – 指定された期限でのサーバーからの最小電力測定値。サーバーが指定された期限にわたり稼動していない場合は、サーバーの起動時からのすべての測定値の最小値になります。

複数の電源装置がサーバーから同時に削除されると、iLOが電力履歴セクションまたは電源メーターグラフに情報を表示しない短い期間が発生します。この情報は、搭載されている残りの電源装置に関する情報をiLOが収集した後、再度表示されます。

電力設定

電力設定ページを使用すると、サーバーの電力管理機能を表示および制御することができます。このページに表示される電力管理機能は、サーバーの構成によって変化します。

サブトピック

パワーレギュレーターの設定

消費電力上限の構成

バッテリバックアップユニット設定の構成

電力しきい値設定超過のSNMPアラートの構成

マウスとキーボードの持続接続の設定

パワーレギュレーターの設定

前提条件

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

このタスクについて

パワーレギュレーター機能を使用すると、iLOは動作条件に基づいてプロセッサーの周波数レベルと電圧レベルを変更でき

ます。これにより、パフォーマンスへの影響を最小限に抑えながら電力を節約することができます。

手順

1. ナビゲーションツリーで電力 & 温度をクリックして、電力設定タブをクリックします。
2. パワーレギュレーターモードを設定します。

   サポートされているモードのみがリストされます。以下から選択します。

   - ダイナミックパワーセービングモード - Intelシステムのみ
   - スタティックローパワーモード - Intelシステムのみ
   - スタティックハイパフォーマンスモード - IntelおよびAMDシステム
   - OS制御モード - IntelおよびAMDシステム
3. 適用をクリックします。

   Intelシステムでは、サーバーがオフまたはPOST状態の場合、この変更はPOSTが完了するまで有効になりません。

   AMDシステムでは、システムがPOST状態の場合、モードの変更内容は適用できません。

   > **注記**: パワーレギュレーターモードは、ROMベースのシステムユーティリティで設定されたワークロードプロファイルに関係なく変更できます。

   - Intelシステムで適用をクリックすると、以下のようになります。
     - ダイナミックパワーセービングモード、スタティックローパワーモード、およびスタティックハイパフォーマンスモードに変更した場合、iLOは、パワーレギュレーターの設定が変更されたことを通知します。
     - OS制御モードに変更した場合、またはOS制御モードから他のモードに変更した場合は、iLOは、変更を完了するにはサーバーを再起動する必要があることを通知します。
   - AMDシステムでは、適用をクリックすると、iLOは、変更を完了するにはサーバーを再起動する必要があることを通知します。
4. 再起動が必要である場合は、サーバーを再起動します。

サブトピック

パワーレギュレーターモード

パワーレギュレーターモード

パワーレギュレーターを設定するときに、以下のモードから選択します。

- ダイナミックパワーセービングモード - プロセッサーの利用率に基づいてプロセッサー速度と電力使用量を自動的に変化させます。このオプションにより、パフォーマンスに影響を与えずに全体的な消費電力を減らすことができます。このオプションは、OSのサポートを必要としません。
- スタティックローパワーモード - プロセッサー速度を下げ、電力使用量を減らします。このオプションは、システムの最大電力量の値を低く抑えます。パフォーマンスへの影響は、プロセッサーの使用率が高い環境では増大します。
- スタティックハイパフォーマンスモード - OSの電力管理ポリシーに関係なく、プロセッサーは常に最大電力および最大パフォーマンスで動作します。
- OSコントロールモード - OSが電力管理ポリシーを有効にしない場合、プロセッサーは常に最大電力および最大パフォーマンスで動作します。

消費電力上限の構成

前提条件

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

  サポート情報については、サーバーの仕様書を参照してください。

  消費電力上限は、Synergyコンピュートモジュールではサポートされません。
- 消費電力上限値管理機能は、ROMベースのシステムユーティリティでは有効になっています。

  BIOS設定をデフォルト値にリセットすると、ROMベースシステムユーティリティの消費電力上限が無効になります。機能を使用するには、機能を有効にする必要があります。
- サーバーには、一致しない電源装置の構成はありません。

手順

1. ナビゲーションツリーで電力管理をクリックして、電力設定タブをクリックします。
2. 手動の消費電力上限を有効チェックボックスを選択します。
3. 消費電力上限値をワット数、BTU/時、または割合（%）で入力します。

   %は、最大電力値と最小電力値の差です。

   消費電力上限値は、サーバー最小電力値より下には設定できません。
4. （オプション）値がワット単位で表示されている場合、BTU/時単位での表示に変更するには値をBTU/時で表示をクリックします。値がBTU/時で表示されている場合、表示をWに変更するには値をワットで表示をクリックします。
5. 適用をクリックします。

   変更が正常に終了したことがiLOによって通知されます。

サブトピック

消費電力上限の注意事項

消費電力上限の注意事項

- POST実行中、ROMは最大電力測定値と最小電力測定値を決定する2つの電力テストを実行します。

  消費電力上限の構成を決定するときは、消費電力上限値設定の表の値を検討してください。

  - 電源定格–最大電力上限のしきい値（設定可能な最大消費電力上限）。

    サーバーブレードの場合、この値は初期パワーオンリクエスト値です。

    ブレード以外のサーバーの場合、この値は電源装置容量です。
  - サーバー最大電力 – サーバーの最大電力測定値。この値は、最小ハイパフォーマンス上限のしきい値でもあります。サーバーのパフォーマンスに影響を与えずに設定できる最小の消費電力上限値です。
  - サーバー最小電力 – サーバーの最小電力測定値。この値は、最小電力上限のしきい値でもあります。サーバーが使用する最小電力を表します。この値に設定されている消費電力上限は、サーバーの電力使用量を最小化するため、

その結果サーバーのパフォーマンスが低下します。

- 消費電力上限を設定した場合は、サーバーの平均電力測定値が、消費電力上限以下にならなければなりません。
- サーバーがエンクロージャー動的消費電力上限に含まれる場合、消費電力上限値設定は無効になっています。

  これらの値は、Onboard AdministratorまたはInsight Control電力管理を使用して設定と変更を行います。
- 消費電力上限は、一部のサーバーではサポートされていません。詳しくは、サーバーの仕様書を参照してください。
- 一部のサーバーの消費電力上限値設定は、iLO Webインターフェイスの外部で次のようなツールを使用して管理する必要があります。
  - HPE Advanced Power Manager

  サーバーでサポートされる電力管理機能について詳しくは、https://www.hpe.com/info/qsでサーバーの仕様書を参照してください。
- 消費電力上限機能は、一致しない電源装置があるサーバーでは無効になります。

バッテリバックアップユニット設定の構成

前提条件

iLOの設定を構成する権限

このタスクについて

バッテリバックアップユニットを備えているサーバーに対して電源装置が電源を供給できない場合、サーバーはバッテリバックアップユニットから供給される電源で実行されます。

以下の手順を使用して、サーバーがバッテリバックアップユニットで実行中である場合にiLOが実行する操作を選択します。

手順

1. ナビゲーションツリーで電力 & 温度をクリックして、電力設定タブをクリックします。
2. バッテリバックアップユニット設定セクションで、サーバーがバッテリバックアップユニットで動作している場合にiLOが実行する操作を選択します。
3. 適用をクリックします。

   変更が正常に終了したことがiLOによって通知されます。

サブトピック

バッテリバックアップユニットのオプション

バッテリバックアップユニットのオプション

サーバーがバッテリ電源で動作している場合に、以下のいずれかの操作を実行するようにiLOを設定できます。

- アクションなし（デフォルト） - サーバーがバッテリ電源で動作しているときは何もしません。電源が回復しない場合、バッテリが消耗するとサーバーの電源は失われます。
- 電源ボタンを一瞬押す - サーバーがバッテリ電源で10秒以上動作していることをiLOが検出した場合、電源ボタンを一瞬押す指示をサーバーに送信します。オペレーティングシステムが電源ボタンの押下に対応するように構成されている場合、オペレーティングシステムはシャットダウンを開始します。

  シャットダウンメッセージをOSに送信 - サーバーがバッテリ電源で10秒以上動作していることをiLOが検出した場合、

ホストのオペレーティングシステムにシャットダウンメッセージを送信します。必要なサーバー管理ソフトウェアがインストールされている場合、オペレーティングシステムはシャットダウンを開始します。

サーバーがバッテリバックアップユニットをサポートしているかどうかを確認するには、Webサイト（https://www.hpe.com/info/qs）でサーバー仕様をご覧ください。

電力しきい値設定超過のSNMPアラートの構成

前提条件

iLOの設定を構成する権限

このタスクについて

電力しきい値超過によるSNMPアラート機能を使用すると、定義されたしきい値を消費電力が超えたときにSNMPアラートを送信できます。

手順

1. ナビゲーションツリーで電力 & 温度をクリックして、電力設定タブをクリックします。
2. 警告トリガーリストで値を選択します。
3. ピーク時消費電力または平均消費電力を選択した場合は、次を入力します。
   - 警告しきい値
   - 期間
4. （オプション）警告しきい値のワット表示とBTU/時表示を切り替えるには、値をワットで表示と値をBTU/時で表示のいずれかをクリックします。
5. 適用をクリックします。

サブトピック

電力しきい値超過によるSNMPアラートのオプション

電力しきい値超過によるSNMPアラートのオプション

- 警告トリガー – 警告が、ピーク電力消費量に基づくか、平均電力消費量に基づくか、または無効かを決定します。
- 警告しきい値–消費電力しきい値を設定します。指定期間にわたって消費電力がこの値を超える場合、SNMPアラートがトリガーされます。
- 持続時間–SNMPアラートがトリガーされるまでに消費電力が警告しきい値を超えていなければならない時間を分単位で設定します。生成されるSNMPアラートは、iLOがサンプリングした電力使用量のデータに基づいています。持続時間の値が変更された正確な日時には基づいていません。5～240分の値を入力します。この値は5の倍数でなければなりません。

マウスとキーボードの持続接続の設定

前提条件

iLOの設定を構成する権限

このタスクについて

電力設定ページのその他の設定セクションを使用すると、キーボードとマウスの持続接続の機能を有効または無効にすることができます。

手順

1. ナビゲーションツリーで電力管理をクリックして、電力設定タブをクリックします。
2. マウス、キーボードの持続接続設定を構成します。

   設定が変更されたことがiLOによって通知されます。

サブトピック

その他の設定オプション

その他の設定オプション

マウス、キーボードの持続接続

- **有効** – iLO仮想キーボードおよびマウスは、iLO UHCI USBコントローラーに常時接続されます。
- **無効**（デフォルト） – iLO仮想キーボードおよびマウスは、リモートコンソールアプリケーションが開いてiLOに接続したときにのみ、iLO UHCIコントローラーに動的に接続されます。

  この機能を無効にすると、一部のサーバーでは次の場合に15ワットの消費電力をさらに節約できます。
  - サーバーOSがアイドル状態である。
  - 仮想USBキーボードおよびマウスが接続されていない。

  たとえば、24時間当たりの電力節約は15ワット×24時間、つまり360ワット時間（0.36キロワット時）になります。

電力情報の表示

手順

ナビゲーションツリーで電力管理をクリックして、電力タブをクリックします。

電力情報ページに表示される情報は、サーバータイプによって変化します。表示される可能性のあるセクションは次のとおりです。

- 電源装置の概要
- 電源装置
- HPE Power Discovery Services
- バッテリバックアップユニット
- Smart Storage Energy Pack
- 電力測定値
- パワーマイクロコントローラー

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、最後の電源オフ時のものです。ヘルス情報は、サーバーの電源が入っており、POSTが完了している場合にのみアップデートされます。

電源装置概要の詳細

このセクションは、ブレード以外のサーバーに対して表示されます。

現在の電力測定値

共有スロット電源装置が取り付けられている場合、サーバーからの最新の電力測定値が表示されます。他の電源装置では、このデータは表示されません。

この値は、通常、すべてのアクティブな電源装置の出力の合計に等しくなりますが、個々の電源装置を読み取るため、変動する場合があります。この値はあくまで参考であり、電力メーターページに表示される値ほど正確ではありません。

Power Management Controllerのファームウェアバージョン

Power Management Controllerのファームウェアバージョン番号。iLOファームウェアがこの値を決定するには、サーバーの電源が入っている必要があります。この機能は、一部のサーバーではサポートされません。

電源ステータス

サーバーに供給されている電源の全体的なステータス。

- サーバーの電源装置がインテリジェントタイプではない電源に接続されている場合、このセクションにはサーバー内部の電源装置のステータスが表示されます。
- サーバーの電源装置がiPDUを介してPower Discovery Serviceに接続されている場合、このセクションにはサーバー内部の電源装置に供給されている電源のステータスが表示されます。
- デュアルパワードメインシステムの場合、電源装置冗長化ルールはドメインごとに独立しています。

以下の電源ステータス値が表示されます。

- 冗長化 - 電源装置に冗長性があることを示します。

  インフラストラクチャにPower Discovery Serviceが統合されている場合、この値は、内部電源装置に外部から供給されている電源に冗長性があるどうかを示します。

- 非冗長化 - 電源装置またはiPDU（Power Discovery Serviceを使用している場合）の少なくとも1つがサーバーに電力を提供していないことを示します。このステータスの最も一般的な原因は、電源装置への入力電力の喪失です。また、同じiPDUに複数の電源装置が接続されている構成でも、このステータスが発生する場合があります。その場合、個々の電源装置のステータスは良好、使用中ですが、電源ステータスの値は非冗長化です。これは、そのiPDUへの入力電源が喪失するとサーバーの電源がすべて喪失するからです。

- 冗長化の障害 - 4つの電源装置をサポートするサーバーでは、このステータスは、サーバーに電力を提供している電源装置の数がサーバーの動作に必要な数よりも少ないことを示します。サーバーは引き続き動作する場合がありますが、この状態では電源問題のリスクが高くなります。電源装置冗長化設定が正しいことをROMベースのシステムユーティリティで確認してください。

- OK - 共有スロット電源装置は取り付けられていません。インストールされている電源装置は正常に動作しています。

- N/A - 電源装置が1つのみ搭載されています。この構成では冗長化を適用できません。

Power Discovery Servicesステータス

次の値が表示される可能性があります。

- 冗長化 - サーバーは冗長化iPDU構成用に設定されています。
- 非冗長化 - 冗長性をサポートするのに十分なiPDUがないか、またはサーバーの電源装置が同じiPDUに接続されています。
- N/A - iPDUは検出されませんでした。

iLOプロセッサーまたはサーバーがリセットされると、iPDUの検出プロセスの完了に数分間かかる場合があります。

高効率モード

冗長電源装置が構成されている場合に使用される冗長電源装置モード。

デュアルパワードメインシステムの場合、高効率モード設定はドメインごとに独立しています。

次の値が表示される可能性があります。

- N/A - 該当なし。

- バランスモード – 取り付けられているすべての電源装置に均一に電力が供給されます。
- 高効率モード（自動） – 片方の電源装置には完全に電力を供給し、もう一方の電源装置は低い消費電力レベルでスタンバイ状態にします。自動オプションではサーバーのシリアル番号に基づいて奇数の電源装置か偶数の電源装置が選ばれるため、ほぼランダムに電力が供給されます。
- 高効率モード（偶数サプライがスタンバイ） – 奇数番号の電源装置には完全に電力を供給し、偶数番号の電源装置は低い消費電力レベルでスタンバイ状態にします。
- 高効率モード（奇数サプライがスタンバイ） – 偶数番号の電源装置には完全に電力を供給し、奇数番号の電源装置は低い消費電力レベルでスタンバイ状態にします。
- サポートされていません – 取り付けられている電源装置は高性能モードをサポートしていません。

詳しくは

サーバー電力使用量の表示

システムドメイン

システムの冗長性に関する概要情報がシステムドメインの下に表示されます。詳しくは、電源装置のリストを参照してください（このオプションは、サポートされているサーバーでのみ使用できます）。

GPUドメイン

GPUの冗長性に関する概要情報がGPUドメインの下に表示されます。詳しくは、電源装置のリストを参照してください（このオプションは、サポートされているサーバーでのみ使用できます）。

電源装置のリスト

このリストの一部の値について情報を提供しない電源装置もあります。ある値について電源装置からの情報がない場合は、N/Aが表示されます。

このセクションは、ブレード以外のサーバー（DL、ML）に対して表示されます。

- ベイ – 電源装置のベイ番号。
- 設置 – 電源装置が搭載されているかどうかを示します。指定できる値は、OKおよび未インストールです。
- ステータス – 電源装置のステータス。表示される値は、ステータスアイコン（OK、劣化、障害、またはその他）、および詳細情報を提供するテキストを示します。値には、以下のものがあります。
  - 不明
  - 良好、使用中
  - 良好、スタンバイ
  - 一般障害
  - 過電圧障害
  - 過電流障害
  - 過熱障害
  - 入力電圧消失
  - ファン障害
  - 高入力A/C警告
  - 低入力A/C警告
  - 高出力警告
  - 低出力警告
  - 入口温度警告

- 内部温度警告
- 高Vaux警告
- 低Vaux警告
- 電源装置の不一致

- PDS - 搭載された電源装置がPower Discovery Service（電力情報検出機能）用に有効になっているかどうか。
- ホットプラグ - 電源装置ベイがサーバーの電源が入った状態での電源装置の交換をサポートするかどうか。この値がはいで、電源装置が冗長化の場合は、サーバーの電源がオンのときに電源装置を取り外したり、交換したりすることができます。
- モデル - 電源装置のモデル番号。
- スペア - スペア電源装置の部品番号。
- シリアル番号 - 電源装置のシリアル番号。
- 容量 - 電源装置の容量（W）。
- ファームウェア - 搭載された電源装置のファームウェアバージョン。

Power Discovery Services iPDU概要

このセクションは、ブレード以外のサーバーでサーバーの電源装置がiPDUに接続されている場合に表示されます。

iLOをリセットしてから、またはiPDUを接続してから、iLO Webインターフェイスに iPDU概要データが表示されるまで約2分かかります。この遅延は、iPDU検出プロセスによるものです。

ベイ

電源装置のベイ番号。

ステータス

iPDUによって決定される全体的な通信リンクステータスおよびラック入力電源の冗長。表示される可能性がある値は、以下のとおりです。

- iPDU冗長化 - この良好ステータスは、サーバーが2台以上の異なるiPDUに接続されていることを示します。
- iPDU非冗長化 - この警告ステータスは、サーバーが2台以上の異なるiPDUに接続されていないことを示します。このステータスは、次のいずれかの条件が発生すると表示されます。
  - iPDUリンクが、一部の電源装置で確立されていない。
  - 同じiPDUに2台以上の電源装置が接続されている。

    入力電力が同じiPDUから供給される電源装置について、iPDUのMACアドレスおよびシリアル番号が同一である。1台の電源装置が接続の確立を待っている場合、iPDUは非冗長化と表示されます。
- 接続を待機中 - この情報ステータスは、以下の1つまたは複数の条件を示します。
  - 電源装置をiPDUに接続するために正しくない電源コードが使用された。
  - iPDUとiLOプロセッサーが接続プロセス中である。このプロセスには、iLOプロセッサーまたはiPDUをリセットしてから最大2分かかります。
  - iPDUモジュールにネットワーク（またはIP）アドレスがない。

部品番号

iPDUの製品番号。

シリアル

iPDUのシリアル番号。

MACアドレス

iPDUネットワークポートのMACアドレス。各iPDUが固有のMACアドレスを持っているため、この値を参照すると接続さ

れている各iPDUを特定できます。

iPDUリンク

iPDUのHTTPアドレス（使用できる場合）。インテリジェントモジュラーPDUのWebインターフェイスを開くには、この列のリンクをクリックします。

電力読み取り値

このセクションは、サーバーブレードとSynergyコンピュートモジュールに対して表示されます。

現在の電力読み取り値

サーバーからの最新の電力読み取り値。

この値は、通常、すべてのアクティブな電源装置の出力の合計に等しくなりますが、個々の電源装置を読み取るため、多少変動する場合があります。この値はあくまで参考であり、電力管理ページに表示される値ほど正確ではありません。

詳しくは

サーバー電力使用量の表示

パワーマイクロコントローラー

このセクションは、サーバーブレードとSynergyコンピュートモジュールに対して表示されます。

ファームウェアバージョン

パワーマイクロコントローラーのファームウェアのバージョン。

iLOファームウェアがパワーマイクロコントローラーのファームウェアバージョンを決定するには、サーバーの電源が入っている必要があります。

バッテリバックアップユニットの詳細

バッテリバックアップユニットをサポートするブレード以外のサーバーでは、以下の詳細が表示されます。

- ベイ - バッテリバックアップユニットが設置されているベイ。
- 設置 - バッテリバックアップユニットが設置されているかどうか。値にはOK、バッテリ障害、バッテリ交換があります。
- ステータス - バッテリバックアップユニットのステータス。指定できる値は、OK、劣化、障害、またはその他です。
- 充電 - バッテリバックアップユニットの充電レベル（%）。充電ステータスの値には、充電完了、放電中、充電中、低速充電、充電していませんがあります。
- シリアル番号 - バッテリバックアップユニットのシリアル番号。
- 容量 - バッテリバックアップユニットの容量（ワット）。
- ファームウェア - インストールされているバッテリバックアップユニットのファームウェアバージョン。

Smart Storage Energy Packのリスト

電力情報ページには、Smart Storage Energy Packをサポートするサーバーに関する以下の情報が表示されます。

索引

Energy Pack索引番号です。

装着

Energy Packの装着状態。表示される値は、OKおよび未装着です。

ステータス

Energy Packのヘルスステータス。表示される値は、OK、劣化、障害、またはその他です。

モデル

モデル番号。

スペア

スペアEnergy Packの部品番号。

シリアル番号

Energy Packのシリアル番号。

タイプ

Energy Packのタイプ。

ファームウェア

インストールされているEnergy Packファームウェアのバージョン。

電力監視

iLOは、サーバーとオペレーティングシステムの稼動時間が最大になるように、サーバーの電源装置を監視します。電源装置は低電圧などの電気条件による影響を受ける可能性があります。また、不注意でACコードが外れる場合があります。冗長電源装置が構成されている場合は、これらの条件により冗長性が失われます。冗長電源装置が使用されていない場合は、これらの条件により操作性が失われます。電源装置のハードウェア障害の検出時や、AC電源コードの切断時には、イベントがIMLに記録され、LEDインジケーターが使用されます。

iLOプロセッサーは、Power Discovery Serviceインフラストラクチャの必須コンポーネントです。iLOプロセッサーは、各Platinum Plus電源装置に接続されているiPDUと通信して、ラックおよびデータセンターの電源の冗長について判断します。Power Discovery Serviceインフラストラクチャに iLOプロセッサーが含まれる場合、iLOプロセッサーはサーバーの外部入力電源の冗長化および個々（内部）の電源装置のステータスをインテリジェントに報告します。

詳しくは、次のWebサイトを参照してください。https://www.hpe.com/info/rackandpower

高効率モード

高効率モードは、セカンダリ電源装置をスタンバイモードにすることにより、サーバーの電力効率を改善します。セカンダリ電源装置がスタンバイモードにある場合は、プライマリ電源装置がシステムにすべてのDC電力を供給します。電源装置の出力レベルが高いほど電源装置の効率が上がり（AC入力W当たりのDC出力Wが増加し）、全体的な電力効率が向上します。

高効率モードは、電源の冗長性に影響しません。プライマリ電源装置に障害が発生した場合は、セカンダリ電源装置がただちにシステムへのDC電力の供給を開始し、停止時間を防止します。冗長電源装置モードは、UEFIシステムユーティリティを通じてのみ構成できます。これらの設定をiLOファームウェアから変更することはできません。

サポートされていないモードを使用するように高効率モードが構成されている場合、電源装置効率が低下する可能性があります。

冷却機能の構成と表示

最小ファン速度の構成

前提条件

iLOの設定を構成する権限

このタスクについて

iLOは、取り付けられたファンが構成された設定よりも遅い速度で動作するのを防ぐ最小ファン速度（パーセンテージ）をサポートしています。サーバーが稼働している場合、ファンは構成された速度以上で動作します。

最小ファン速度が温度構成値より大きい場合、最小ファン速度設定によって、温度構成設定がオーバーライドされます。

手順

1. ナビゲーションツリーで電力 & 温度をクリックして、ファンタブまたはファン&冷却モジュールタブをクリックします。

   タブ名は、サーバーがサポートする機能によって異なります。

2. をクリックします。

ファン設定ページが開きます。

3. 取り付けられているすべてのファンの最小ファン速度（%）を入力し、OKをクリックします。

温度構成設定の構成

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーで電力 & 温度をクリックして、ファンタブまたはファン&冷却モジュールタブをクリックします。

   タブ名は、サーバーがサポートする機能によって異なります。

2.  をクリックします。

   ファン設定ページが開きます。

3. 温度構成値を選択します。

4. OKをクリックします。

   変更を適用するにはリセットが必要であることがiLOによって通知されます。

5. はい、リセットを適用しますをクリックします。

   iLOは、変更を保存してリセットします。

   接続が再確立されるまでに、数分かかることがあります。

温度構成設定

最適な冷却

ファンが適切な冷却を行うために必要な最低限の速度に構成されるため、最も効率的な冷却が可能になります。

強化されたCPU冷却

プロセッサーへの冷却を強化することにより、パフォーマンスが向上する可能性があります。

増強した冷却

ファンの速度を上げて動作させます。

最大冷却

システムで使用できる最大の冷却能力を提供します。

温度構成値が最小ファン速度値より大きい場合、温度構成設定によって、最小ファン速度設定がオーバーライドされます。

ファン情報の表示

このタスクについて

ファン情報ページに表示される情報は、サーバー構成によって異なります。

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、最後の電源オフ時のものです。ヘルス情報は、サーバーの電源が入っており、POSTが完了している場合にのみアップデートされます。

手順

1. ナビゲーションツリーで電力 & 温度をクリックして、ファンタブまたはファン&冷却モジュールタブをクリックします。

   タブ名は、サーバーがサポートする機能によって異なります。

2. （オプション）冷却ファンの冗長をサポートしているサーバーでは空のファンベイは表示されません。ファンベイを表示するには、空白のベイを表示をクリックします。空のファンベイが表示されているときにそれらを非表示にするに

は、空白のベイを隠すをクリックします。

ファン概要の詳細

全体のステータス

取り付けられたファンのヘルスステータスの概要。

冗長性

ファンの冗長性ステータス。

最小ファン速度

取り付けられているすべてのファンの最小速度（0～100%）。サーバーが稼働している場合、ファンは構成された速度以上で動作します。

温度構成

温度構成値。

詳しくは

サブシステムおよびデバイスステータスの値

ファンの詳細

ファンごとに、次の詳細が表示されます。

- ファン - ファンの名前。
- 位置 - サーバーシャーシ内の位置が表示されます。
- 冗長化 - ファンのバックアップコンポーネントがあるかどうか。
- ステータス - ファンのヘルスステータス。
- 速度 - ファン速度（%）。

詳しくは

サブシステムおよびデバイスステータスの値

ファン

iLOファームウェアは、ハードウェアとともに、ファンの動作と速度を制御します。ファンはコンポーネントに欠かせない冷却機能によって、信頼性を向上させて動作の継続を維持します。ファンは、システム全体を対象に監視される温度に反応して最小の雑音で十分な冷却機能を提供します。

ファンサブシステムの監視には、十分、冗長化、および非冗長化のファン構成が含まれます。1つまたは複数のファンが故障しても、サーバーは動作を続けるのに十分な冷却機能を提供します。

ファンの動作ポリシーは、ファンの構成や冷却の需要に応じて、サーバーごとに異なります。ファンの制御はシステムの内部温度を監視し、温度を下げるときはファンの回転速度を上げ、十分に下がったときはファンの回転速度を落とします。ファンの障害が発生した場合、ファンの動作ポリシーによっては、他のファンの回転速度を上げ、イベントをIMLに記録したり、LEDインジケーターを点灯させたりします。

非冗長化構成または冗長化構成で複数のファンに障害が発生すると、システムの損傷を防ぎ、データの整合性を保証するために十分な冷却機能を提供できなくなる可能性があります。この場合、冷却ポリシーに加えて、オペレーティングシステムとサーバーの適切なシャットダウンが開始される可能性があります。

HPE液冷モジュール情報の表示

このタスクについて

このページに表示される情報は、サーバー構成によって変化します。

注記: 液冷の情報は、サポートされているプラットフォームでのみ表示されます。

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、最後の電源オフ時のものです。ヘルス情報は、サーバーの電源が入っており、POSTが完了している場合にのみアップデートされます。

手順

ナビゲーションツリーで電力 & 温度をクリックして、ファン&冷却モジュールタブをクリックします。

HPE液冷モジュールの詳細

それぞれのHPE液冷モジュールについて、以下の詳細が表示されます。

- 冷却ポンプ - 冷却ポンプの名前。
- 場所 - 冷却ポンプの場所。
- 冗長 - 冷却ポンプのバックアップコンポーネントがあるかどうか。
- ステータス - 冷却ポンプのヘルスステータス。
- 速度 - 冷却ポンプの速度（パーセント）。

HPE液冷モジュールのサマリーの詳細

全体の状況

取り付けられた冷却ポンプのヘルスステータスの概要。

冗長性

冷却ポンプの冗長性ステータス。

温度情報

温度情報ページには、サーバーシャーシの温度センサーの場所、ステータス、温度、しきい値設定が表示されます。また、使用可能なPCIeサブコンポーネントの温度の詳細も表示されます。

PCIeサブコンポーネントの名前は、補助センサー名から派生します。補助センサー名が使用できない場合、名前はエンティティタイプから派生します。エンティティタイプも使用できない場合は、PCIeサブコンポーネントの名前にNAと表示されます。

PLDMで報告されるアダプター温度センサー（サブコンポーネント）は、主要センサーによって集約された温度情報ページに表示されます。サブコンポーネントがある主要センサーでは、アスタリスク（*）文字が付いたいずれかのサブコンポーネントからの詳細が表示されます。

サーバーの電源がオフの場合、このページのシステムのヘルス情報は、最後の電源オフ時のものです。ヘルス情報は、サーバーの電源が入っており、POSTが完了している場合にのみアップデートされます。

サブトピック

温度グラフの表示

温度センサーデータの表示

温度の監視

温度グラフの表示

手順

1. ナビゲーションツリーで電力&温度をクリックして、温度タブをクリックします。
2. （オプション）グラフ表示をカスタマイズします。
   - 3次元グラフを表示するには、3Dオプションを有効にします。
   - 2次元グラフを表示するには、3Dオプションを無効にします。

- サーバーの前面または背面にあるセンサーを表示するには、フロントビューまたはバックビューを選択します。

3. （オプション）個々のセンサーの詳細を表示するには、マウスカーソルをグラフ上の円に移動します。

   センサーID、ステータス、および温度測定値が表示されます。

サブトピック

温度グラフの詳細

温度グラフの詳細

温度グラフを表示する場合、グラフ上の円形は、センサーデータテーブルに示されるセンサーに対応します。

グラフ上の色は、温度変化の度合いに当たり、緑色から赤色の範囲で示されます。緑色は温度0° C、赤色は「クリティカル」しきい値を表します。センサーが測定する温度が上がると、グラフが緑色からオレンジ色に変わり、さらに温度が上がって「クリティカル」しきい値に近づくと赤色になります。

温度センサーデータの表示

手順

1. ナビゲーションツリーで電力 & 温度をクリックして、温度タブをクリックします。
2. （オプション）サブコンポーネントの詳細を展開または折りたたむには、次の › または⌄ アイコンをクリックします。
3. （オプション）温度が摂氏単位で表示されているときは、° Fをクリックすると、温度が華氏で表示されます。温度が華氏単位で表示されているときは、° Cスイッチをクリックすると、温度が摂氏で表示されます。
4. （オプション）デフォルトでは、取り付けられていないセンサーは非表示です。取り付けられていないセンサーを表示するには、センサーなしの情報を表示をクリックします。見つからないセンサーが表示されているときにそれらを非表示にするには、センサーなしの情報を隠すをクリックします。
5. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

   サブコンポーネントの先頭には番号が付けられ、内部計算に基づいてソートされます。

サブトピック

温度センサーの詳細

温度センサーの詳細

- センサー - 温度センサーのID。センサーの位置も示します。
- 位置 - 温度が測定されている領域。この列では、メモリは次のものを指します。
  - 物理メモリDIMM上の温度センサー。
  - メモリDIMMの近くにあるが、DIMM上には置かれていない温度センサー。これらのセンサーは、追加の温度情報を提供するために、DIMMの近くの通気冷却経路をさらに下った場所に配置されています。

センサー列の温度センサーのIDは、温度センサーの正確な位置を示し、DIMMまたはメモリ領域に関する詳細な情報を提供します。

- X - 温度センサーのx座標。
- Y - 温度センサーのy座標。
- ステータス - 温度ステータス。
- 読み取り値 - 温度センサーによって記録された温度。温度センサーが取り付けられていない場合、読み取り値列にはN/Aという値が表示されます。
- しきい値 - 過熱状態の警告の温度しきい値です。注意とクリティカルの2つのしきい値が示されます。温度センサーが取り付けられていない場合、しきい値列にはN/Aという値が表示されます。ベンダーによってしきい値が制御されるデバイスの場合も値N/Aが表示されます。

注記: CPU温度の履歴を報告する以外に、 iLO6はCPUパッケージの温度も報告します。

温度の監視

次の温度しきい値が監視されます。

- 注意 - サーバーは、温度を「注意」しきい値未満に維持するように設計されています。

  温度が注意しきい値を超えると、ファンの回転速度が最大になります。

  温度が注意しきい値を60秒間超えると、適切なサーバーシャットダウンが試行されます。

- クリティカル - 温度が制御不能になった場合または急上昇した場合、高い動作温度によって電子コンポーネント障害が発生する前に、「クリティカル」温度しきい値によりサーバーを物理的にシャットダウンしてシステム障害の発生を防ぎます。

  この場合、iLO6はすぐにシャットダウンします。 別のメカニズムでは、シャットダウンは約10秒遅れます。

監視ポリシーはサーバーの要件によって異なります。ポリシーには通常、次のものが含まれます。

- ファンの速度を上げて冷却を最大にする。
- IMLで温度イベントをログに記録する。
- LEDインジケータを使用して、イベントを視覚的に示す。
- データの破損を防ぐために、オペレーティングシステムの正常なシャットダウンを開始する。

温度が高すぎる状態を回避すると、追加のポリシーが実装されます。例：

- ファン速度を標準に戻す。
- イベントをIMLに記録する。
- LEDインジケータをオフにする。
- 進行中のシャットダウンをキャンセルする（該当する場合）。

注記:
LinuxおよびVMwareの場合：メモリ温度センサー付きのNVIDIAオプションカードには、ベンダーのドライバーがインストールされ、持続モードが有効になっている必要があります。詳しくは、ベンダーのオプションカードドキュメントを参照してください。

RESTfulインターフェイスツールを使用したユーザー定義のしきい値の構成

手順

1. テキストエディターを開き、ファイルを作成して、ユーザー定義の温度のしきい値を定義します。

   テンプレートとして、次の例を使用します。

   ```
   {
   "path":"/redfish/v1/Chassis/1/Thermal/Actions/Oem/Hpe/HpeThermalExt.SetUserTempThreshold/",
   "body": {"SensorNumber": Supported Temperature Sensor,
   "ThresholdValue": Desired threshold temperature,
   "AlertType": "Warning" or "Critical"
   }
   }
   ```

2. ファイルを*ファイル名*.jsonとして保存します。

3. RESTfulインターフェイスツールを起動します。

   ilorest
   と入力します。

5. iLOシステムにログインします。

   ```
   iLOrest > login iLO host name or IP address -u iLO user name -p iLO password
   ```

6. 次のコマンドを入力して、アラートを構成します。

   ```
   rawpatch ファイル名.json
   ```

パフォーマンス管理機能の使用

サブトピック

パフォーマンス監視

ワークロードアドバイザー

パフォーマンス監視

パフォーマンス - 監視ページには、次のセンサーから収集されたパフォーマンスデータが表示されます。

CPU使用率

このセンサーは、システムに搭載されているすべてのプロセッサーの使用率を報告します。測定値は、プロセッサーの最大演算能力のパーセンテージに基づいています。作業時のプロセッサーの動作速度が考慮されます。この測定値は、プロセッサーがアイドル状態でない頻度によって計算されることがよくある使用率に関して一部のOSが報告する値とは異なる場合があります。

メモリバス使用率

このセンサーは、メモリバスの総帯域幅の使用率を報告します。測定値は、構成の最大メモリ帯域幅のパーセンテージに基づいています。この測定値は、使用可能なシステムメモリのうち使用されている部分、または割り当て済みの部分によって計算されることがよくあるメモリ使用率に関して一部のOSが報告する値とは異なる場合があります。

I/Oバス使用率

このセンサーは、I/Oバスに接続されているすべてのプロセッサー（PCI-eバス総帯域幅）の使用率を報告します。この測定値は、それらのバスの最大総帯域幅のパーセンテージに基づいています。この測定値は、I/Oデバイスのビジー状態の程度を示すものではなく、デバイスが使用しているPCI-e帯域幅の量を示すものです。

CPUインターコネクト使用率

このセンサーは、システム内の複数のプロセッサーソケットを接続するリンクの計算で得られた帯域幅使用率を報告します。これはシステム内のすべてのリンクの集約です。

平均CPU周波数

このセンサーは、全体の平均的なプロセッサー周波数を報告します。ゼロの値は、プロセッサーがアイドル状態であることを意味します。この値は、プロセッサーがアイドル状態でない場合のみ周波数を測定する一部のOSでよく見られる「実行時の周波数」とは異なります。

CPU電力

このセンサーは、プロセッサーが消費する電力を報告します。これはプロセッサー内の電力アキュムレータに基づいており、プロセッサーが電力制限の内部調整に使用する値です。

このページの情報は、電力メーターページの合計CPU電力データとは異なる場合があります。

サブトピック

パフォーマンスデータの表示

パフォーマンスアラートの構成

パフォーマンスデータの表示

前提条件

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

  ライセンスがインストールされていない場合、メッセージが表示されて、10分間のみグラフが表示されます。

- MCTP検出が有効である。
- iLO日付/時刻が正しく設定され、有効なパフォーマンステレメトリーサンプルが確実に収集されている。

このタスクについて

サーバーが電源オフまたはPOST状態のとき、メッセージが表示され、パフォーマンス測定値に0の値が表示されます。サーバーの電源がオンでPOSTが完了していると、パフォーマンスデータがアップデートされます。リセット後、グラフの値が0の場合がありますが、これはサーバーがオフまたはPOSTのときにデータが収集されていなかったことになります。これらの値がサーバーリセットのためであることを確認するには、IMLを調べます。

iLOをリセットすると：

- 10分および1時間間隔のパフォーマンスデータがクリアされます。
- 24時間および1週間グラフのデータが保存され、リセットが完了した後に表示できます。
- リセットが完了した後で24時間および1週間のグラフを表示すると、毎時データがなくなっている場合があります。

手順

1. ナビゲーションツリーでパフォーマンスをクリックし、監視タブをクリックします。
2. 選択されたセンサーメニューでセンサーを選択します。
3. 次のいずれかのオプションをクリックしてグラフの間隔を選択します。
   - 10分
   - 1時間
   - 24時間
   - 1週間

グラフには、要求した間隔のデータが表示されます。

4. （オプション）グラフ上で特定のポイントのデータを表示するには、グラフの下にあるスライダー○ を目的のポイントに移動します。

   スライダーを動かすと、グラフ上の選択ポイントの詳細がグラフの横に表示されます。

5. （オプション）CPU電力または平均CPU周波数を選択した場合、グラフの横にあるCPUリスト内のチェックボックスをオンまたはオフにします。

   CPUのチェックボックスを選択すると、グラフに表示されます。CPUのチェックボックスをクリアすると、グラフから除去されます。

6. （オプション）このページでデータを更新する方法を選択します。

   デフォルトでは、ページを開いた後はページのデータは自動的には更新されません。

   - 選択したグラフタイプのページデータを更新するには、↻ をクリックします。
   - ページの自動更新を開始するには、▷ をクリックします。選択したグラフのタイプに応じて、ページは10秒または5分間隔で更新されます。□ をクリックするか、別のページに移動するまで、ページは自動的に更新されます。

サブトピック

パフォーマンスデータの詳細

パフォーマンス監視のグラフ表示オプション

詳しくは

インストール済みファームウェア情報の表示
MCTP検出の構成

パフォーマンスデータの詳細

パフォーマンスデータセクションには、次の詳細が表示されます。

センサー
: 選択したセンサーの名前。

最大
: 最大の測定値。

最小
: 最小の測定値。

パフォーマンス監視のグラフ表示オプション

選択されたセンサーメニュー

センサーのパフォーマンスデータを表示するには、選択されたセンサーメニューでセンサーを選択します。

グラフタイプ

グラフの期間を指定するには、グラフタイプ名をクリックします。

- 10分 – 直近の10分間のパフォーマンスデータを表示します。iLOファームウェアは、20秒ごとにこのグラフのパフォーマンスデータを収集します。グラフに表示されるサンプルの最大数は30です。
- 1時間 – 直近の1時間のパフォーマンスデータを表示します。iLOファームウェアは、20秒ごとにこのグラフのパフォー

マンスデータを収集します。グラフに表示されるサンプルの最大数は180です。

- 24時間 – 直近の24時間のパフォーマンスデータを表示します。iLOファームウェアは、5分ごとにこのグラフのパフォーマンスデータを収集します。グラフに表示されるサンプルの最大数は288です。
- 1週間 – 先週のパフォーマンスデータを表示します。iLOファームウェアは、30分ごとにこのグラフのパフォーマンスデータを収集します。グラフに表示されるサンプルの最大数は336です。

パフォーマンスグラフを更新

- 選択したグラフタイプのページデータを更新するには、 をクリックします。
- ページの自動更新を開始するには、 をクリックします。

  をクリックするか、別のページに移動するまで、ページは自動的に更新されます。

グラフ上に特定のデータポイントを表示

- グラフ上で特定のポイントのデータを表示するには、グラフの下にあるスライダー を目的のポイントに移動します。

  次の方法でスライダーを移動することもできます。

  - スライダートラックをクリックします。
  - スライダーアイコンをクリックし、キーボードの矢印キーを押します。

  スライダーを動かすと、グラフ上の選択ポイントの詳細がグラフの横に表示されます。
- 自動更新の実行時に、グラフの下にあるスライダー を動かすと、x軸方向の特定の履歴ポイントに該当するデータポイントに焦点が当たります。

パフォーマンスアラートの構成

前提条件

- iLOの設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- MCTP検出が有効である。
- iLO日付/時刻が正しく設定され、有効なパフォーマンステレメトリーサンプルが確実に収集されている。

このタスクについて

構成されたしきい値に達した場合にIMLにイベントをPOSTするパフォーマンスアラートを構成できます。

CPU使用率、メモリバス使用率、およびI/Oバス使用率のセンサーで上限と下限のしきい値がサポートされます。

CPUインターコネクト使用率、CPU電力、およびJitterカウントのセンサーで上限しきい値がサポートされます。

手順

1. ナビゲーションツリーでパフォーマンスをクリックし、監視タブをクリックします。
2. パフォーマンスアラートをサポートするセンサーを選択します。
3. しきい値設定と滞留時間を入力し、適用をクリックします。

   アラートを無効にするには、滞留時間を0に設定します。

サブトピック

パフォーマンスアラートの設定オプション

詳しくは

インストール済みファームウェア情報の表示

パフォーマンスアラートの設定オプション

しきい値下限

イベントがIMLにポストされる前にセンサーが報告できる最小値。

使用率のパーセンテージを入力します。

しきい値上限

イベントがIMLにポストされる前にセンサーが報告できる最大値。

- 使用率のセンサーの場合は、選択したセンサーの使用率のパーセンテージを入力します。
- CPU電力の場合は、値をワット単位で入力します。
- Jitterカウントの場合は、しきい値カウントを入力します。

滞留時間

しきい値に違反するまでの、センサーの測定値が構成済みの値を上回るまたは下回る秒数。しきい値に違反すると、イベントがIMLにポストされます。

たとえば、しきい値上限を70%、滞留時間を40秒に設定した場合、センサーが70%を超える測定値を40秒を超えて報告するとイベントがポストされます。

- アラートを有効にするには、20～64800（20秒～18時間）の範囲で、滞留時間を20の倍数の有効な値に設定します。20の倍数でない値を入力した場合、値は次の20の倍数に切り上げられます。
- アラートを無効にするには、滞留時間を0に設定します。

ワークロードアドバイザー

iLOは選択したサーバーワークロード特性を監視し、監視対象のデータに基づいてパフォーマンス調整の推奨設定を提供します。

サブトピック

サーバーワークロード詳細の表示

パフォーマンスチューニングオプションの構成

サーバーワークロード詳細の表示

前提条件

- ホストBIOS構成権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- サーバーの電源が入っており、POSTが完了している。

監視する時間間隔でサーバーの電源が入れられたことを確認します。例えば、24時間間隔のデータは、サーバーの電源が24時間入っていないと表示されません。

- MCTP検出が有効である。
- iLO日付/時刻が正しく設定され、有効なパフォーマンステレメトリーサンプルが確実に収集されている。

手順

1. ナビゲーションツリーでパフォーマンスをクリックし、ワークロードアドバイザータブをクリックします。
2. 詳細をサーバーワークロードセクションで確認します。

   iLOがリセットされた場合、10分間隔の情報はサーバーの電源が10分入れられた後で、1時間間隔の情報はサーバーの電源が1時間入れられた後で表示されます。
3. （オプション）テーブルを最新情報にアップデートするには、 をクリックします。

サブトピック

サーバーワークロードの詳細

詳しくは

MCTP検出の構成
インストール済みファームウェア情報の表示
iLO SNTP設定の構成

サーバーワークロードの詳細

ワークロードの特性とは、ワークロードがシステムリソースをどのように使用しているかについての質的評価です。これらはパフォーマンス監視イベントから得た定量的な測定値に基づいており、チューニングの決定を行うときの参考として役立ちます。このように観測された特性が、通常はインテリジェントなチューニング決定を行う際に必要となります。たとえば、特定のBIOSオプションがメリットをもたらすのはワークロードのNUMA認識が高い場合に限られます。

以下のワークロード特性が表示されます。

- CPU使用率-サーバー内でプロセッサーはどれだけビジーかです。
- メモリバス使用率-サーバーにより観測されるメモリトラフィックの量です。
- I/Oバス使用率-サーバーにより観測されるI/Oトラフィックの量です。
- NUMA認識-ワークロードがメモリおよびI/Oアクセスを複数のプロセッサーにどのように分散しているかです。NUMA認識が高いということは、I/Oおよびメモリトラフィックがリモートリソースよりもローカルリソースに向けられていることを意味します。

表示される値は高、中、低です。

10分および1時間間隔のサーバーワークロードデータは、iLOがリセットされるとクリアされます。

パフォーマンスチューニングオプションの構成

前提条件

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

- サーバーの電源が入っており、POSTが完了している。

  監視する時間間隔でサーバーの電源が入れられたことを確認します。例えば、24時間間隔のデータおよび推奨事項は、サーバーの電源が24時間入れられるまで使用できません。

- MCTP検出が有効である。
- iLO日付/時刻が正しく設定され、有効なパフォーマンステレメトリーサンプルが確実に収集されている。

手順

1. ナビゲーションツリーでパフォーマンスをクリックし、ワークロードアドバイザータブをクリックします。
2. 選択された間隔メニューで値を選択します。

   10分、1時間、または24時間間隔で収集されたデータに基づいて推奨設定を確認できます。

3. 推奨事項を推奨設定列で確認します。

   iLOがリセットされた場合、10分間隔の情報はサーバーの電源が10分入れられた後で、1時間間隔の情報はサーバーの電源が1時間入れられた後で表示されます。

4. 1つまたは複数の設定を変更するには、設定をクリックします。
5. 必要に応じて、チューニングオプションを変更し、適用をクリックします。

   iLOは、チューニングオプションの変更によってワークロードプロファイル設定がカスタムに変更されることを通知します。

6. はい、適用しますをクリックします。

   iLOは設定を保存し、変更を有効にするにはサーバーの再起動が必要であることを通知します。

7. サーバーを再起動します。

   ステータスバナーのリンクをクリックして、サーバー電源ページに移動できます。

サブトピック

パフォーマンスチューニングの設定

詳しくは

MCTP検出の構成
インストール済みファームウェア情報の表示
iLO SNTP設定の構成

パフォーマンスチューニングの設定

Sub-NUMAクラスタリング

このオプションが有効に設定されている場合、プロセッサーコア、キャッシュ、およびメモリはこの機能によって複数のNUMAドメインに分割されます。NUMAに対応し、最適化されているワークロードでは、この機能を有効にするとパフォーマンスが向上する可能性があります。

この機能を有効にした場合、最大1GBのシステムメモリが使用できなくなる場合があります。

NUMAグループサイズ最適化

このオプションは、NUMAノードのサイズ（論理プロセッサー数）をシステムBIOSが報告する方法を構成します。これは、アプリケーションの使用法に応じてプロセッサーをグループ化（Kgroups）することに関してOSを支援します。デフォルト値のクラスターは、グループがNUMAの境界に沿って最適化されるため、より良いパフォーマンスが提供されます。一部のアプリケーションは、複数のグループにまたがるプロセッサーを利用するように最適化されない場合があります。このような場合、影響を受けるアプリケーションでより多くの論理プロセッサーが使用されるように、フラットオプションを選択することが必要になることがあります。

アンコア周波数のスケーリング

このオプションは、プロセッサーの内部バス（アンコア）の周波数のスケーリングを制御します。このオプションを自動に設定すると、プロセッサーはワークロードに基づいて周波数を動的に変更できます。最大または最小の周波数を設定すると、レイテンシおよび消費電力の調整ができます。

メモリリフレッシュレート

このオプションでは、メモリコントローラーのリフレッシュレートを調整できます。サーバーのメモリのパフォーマンスと耐障害性に影響する場合があります。サーバーの他のドキュメントでデフォルト値 （1xリフレッシュ）の変更が推奨されない限り、Hewlett Packard Enterpriseはデフォルト値の使用をお勧めします。

パワーレギュレーター

このオプションを使用すると、パワーレギュレーターのサポートを構成できます。以下の値を使用できます。

- ダイナミックパワーセービングモード - プロセッサーの利用率に基づいてプロセッサー速度と電力使用量を自動的に変化させます。このオプションにより、パフォーマンスに影響を与えずに全体的な消費電力を減らすことができます。このオプションは、OSのサポートを必要としません。
- スタティックローパワーモード - プロセッサー速度を下げ、電力使用量を減らします。このオプションは、システムの最大電力量の値を低く抑えます。パフォーマンスへの影響は、プロセッサーの使用率が高い環境では増大します。
- スタティックハイパフォーマンスモード - OSの電力管理ポリシーに関係なく、プロセッサーは常に最大電力および最大パフォーマンスで動作します。
- OSコントロールモード - OSが電力管理ポリシーを有効にしない場合、プロセッサーは常に最大電力および最大パフォーマンスで動作します。

注記:
ワークロードパフォーマンスアドバイザーページに表示されるパワーレギュレーター設定には、ブート時の静的構成が反映されます。これには、システムの電源投入後に適用された、この設定への実行時の変更は反映されません。ワークロードパフォーマンスアドバイザーページの推奨設定の変更を適用すると、この設定のブート時の構成だけが変更されます。変更を有効にするには、システムの再起動が必要です。

最小プロセッサーアイドル電力パッケージCステート

このオプションを使用して、オペレーティングシステムが使用するプロセッサーの最小アイドル電力状態（Cステート）を選択します。Cステートを高く設定すればするほど、そのアイドル状態の消費電力は少なくなります。プロセッサーがサポートする最も低いアイドル電力状態は、C6ステートです。

エネルギー/パフォーマンスバイアス

このオプションを使用して、プロセッサーのパフォーマンスと消費電力を最適化するように複数のプロセッサーサブシステムを構成します。以下の値を使用できます。

- 最大パフォーマンス - この設定は、最高のパフォーマンスと最低のレイテンシを必要とし、消費電力にこだわらない環境で使用してください。
- パフォーマンスに最適化 - この設定では、電力効率が最適化されます。Hewlett Packard Enterpriseは、ほとんどの環境でこの設定を推奨します。
- 電力に最適化 - サーバーの使用率に基づいて電力効率が最適化されます。
- 省電力モード - この設定は、消費電力に関する制約が厳しく、パフォーマンスの低下を容認できる環境に適しています。

iLOネットワーク設定の構成

サブトピック

iLOネットワーク設定

ネットワーク構成の概要の表示

ネットワーク共通設定

IPv4設定の構成

IPv6設定の構成

iLO SNTP設定の構成

iLO NIC自動選択

Windowsネットワークフォルダー内のiLOシステムの表示

iLOネットワーク設定

ネットワーク設定にアクセスするには、ナビゲーションツリーでアクティブなNICを選択し、次のページでネットワーク設定を表示または編集します。

- ネットワーク概要
- ネットワーク共通設定
- IPv4設定
- IPv6設定
- SNTP設定

アクティブでないNICを選択すると、そのNICを使用するようにiLOが構成されていないことを通知するメッセージが表示されます。

ネットワーク構成の概要の表示

手順

ネットワーク構成に応じて、ナビゲーションツリーでiLO専用ネットワークポートまたはiLO共有ネットワークポートをクリックします。

ネットワーク概要タブが表示されます。

サブトピック

ネットワーク情報の概要

IPv4概要の詳細

IPv6概要の詳細

IPv6アドレスリスト

ネットワーク情報の概要

情報セクションには、以下の詳細が表示されます。

注記:
iLOホスト名およびNIC設定は、ネットワーク共通設定ページで構成できます。
アクセス設定ページで802.1Xサポート設定を構成できます。

- 使用中のNIC - アクティブなiLOネットワークインターフェイス（iLO専用ネットワークポートまたはiLO共有ネットワークポート）の名前。
- iLOホスト名 - iLOサブシステムに割り当てられた完全修飾ネットワーク名。デフォルトで、ホスト名はILO+システムのシリアル番号および現在のドメイン名です。この値はネットワーク名に使用され、一意である必要があります。
- MACアドレス - 選択しているiLOネットワークインターフェイスのMACアドレス。
- リンク設定 - 選択したiLOネットワークインターフェイスのリンク設定。デフォルト値は自動ネゴシエートです。

  この値は次の場合に表示されません。

  - サーバーが共有ネットワークポートを使用するように構成されている場合。共有ネットワークポートが有効になっている場合、この値はホストオペレーティングシステムで管理する必要があります。
  - サーバーがiLO専用ネットワークポートを使用するように構成されており、かつサーバーモデルでこの値の変更をサポートしていない場合。
- 現在のリンク速度 - ネットワークインターフェイスのリンク速度（メガビット/秒）。

  iLO共有ネットワークポートが有効になっている場合は、物理リンクの実際の速度が表示されます。

  iLO共有ネットワークポート接続は、100 Mbpsを超える速度では動作できません。iLO共有ネットワークポートを使用する場合、iLO仮想メディアを介したデータ転送などのネットワーク集約型タスクは、iLO専用ネットワークポートを使用する構成で実行される同じタスクよりも遅くなる場合があります。
- デュプレックス設定 - 選択しているiLOネットワークインターフェイスのリンクデュプレックス設定。デフォルト値は自動ネゴシエートです。

  この値は次の場合に表示されません。

  - サーバーが共有ネットワークポートを使用するように構成されている場合。共有ネットワークポートが有効になっている場合、この値はホストオペレーティングシステムで管理する必要があります。
  - サーバーがiLO専用ネットワークポートを使用するように構成されており、かつサーバーモデルでこの値の変更をサポートしていない場合。
- 現在のデュプレックス - 全二重または半二重。
- 802.1Xサポート - 802.1Xサポートが有効または無効のどちらに設定されているのか。

IPv4概要の詳細

- DHCPv4ステータス - IPv4でDHCPが有効かどうかを示します。
- アドレス - 現在使用中のIPv4アドレス。値が`0.0.0.0`の場合、IPv4アドレスは設定されていません。
- サブネットマスク - 現在使用中のIPv4アドレスのサブネットマスク。値が`0.0.0.0`の場合、アドレスは構成されていません。
- デフォルトゲートウェイ - IPv4プロトコルで使用されているデフォルトゲートウェイアドレス。値が`0.0.0.0`の場合、ゲートウェイは構成されていません。

IPv6概要の詳細

DHCPv6 ステータス

IPv6でDHCPが有効かどうかを示します。表示される値は、以下のとおりです。

- 有効 - ステートレスおよびステートフルなDHCPv6が有効になっています。
- 有効（ステートレス） - ステートレスなDHCPv6のみが有効になっています。
- 無効 - DHCPv6が無効になっています。

IPv6ステートレスアドレス自動構成（SLAAC）

IPv6でSLAACが有効かどうかを示します。SLAACが無効の場合でも、iLOのSLAACリンクローカルアドレスは必要なため構成されます。

IPv6アドレスリスト

このテーブルには、iLOに対して現在構成されているIPv6アドレスが表示されます。テーブルには、次の情報が表示されます。

ソース

アドレスのタイプ。

IPv6

IPv6アドレス。

プレフィックス長

アドレスプレフィックスの長さ。

ステータス

アドレスのステータス。値には、以下のものがあります。

- アクティブ - アドレスはiLOによって使用中です。
- 保留 - 重複したアドレスの検出が進行中です。
- 障害 - 重複したアドレスの検出に失敗しました。アドレスはiLOによって使用されていません。
- 無効 - アドレスプレフィックスのRA（Router Advertised）有効存続期間は更新されず、期限が切れました。このアドレスはもう使用されていません。

デフォルトゲートウェイ

使用されているデフォルトIPv6ゲートウェイアドレス。IPv6では、iLOは使われる可能性があるデフォルトゲートウェイアドレスのリストを維持します。このリスト内のアドレスは、ルーターアドバタイズメッセージおよびIPv6静的デフォルトゲートウェイ設定を元に生成されます。

静的デフォルトゲートウェイは、IPv6ページで設定します。

ネットワーク共通設定

iLO専用ネットワークポートまたはiLO共有ネットワークポートのネットワーク共通設定ページを使用して、iLOホスト名とNIC設定を構成します。

iLOホスト名の設定

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーでiLO専用ネットワークポートまたはiLO共有ネットワークポートをクリックします。
2. 全般タブをクリックします。

3. iLOサブシステム名（ホスト名）を入力します。

   ホスト名はiLOサブシステムのDNS名です。この名前は、DHCPとDNSがIPアドレスではなくiLOサブシステム名に接続するよう構成されている場合のみ使用されます。

4. DHCPが構成されていない場合は、iLOドメイン名を入力します。

   静的ドメイン名を使用するには、IPv4設定ページおよびIPv6設定ページでDHCPv4が提供するドメイン名を使用とDHCPv6が提供するドメイン名を使用の設定を無効にします。

5. 適用をクリックして変更を保存します。

   1つ以上の保留中の変更を有効にするにはiLOのリセットが必要であることがiLOから通知されます。iLO設定の構成権限がアカウントに割り当てられている場合、iLOのリセットボタンがメッセージに含まれています。

   iLOのリセットが完了するまで、このメッセージはすべてのiLO専用ネットワークポートタブまたはiLO共有ネットワークポートタブに表示されます。

6. （オプション）全般、IPv4、IPv6、SNTPの各タブで、その他のネットワーク設定を構成します。

7. iLOネットワーク設定の構成が完了したら、iLOのリセットをクリックします。

   接続が再確立されるまでに、数分かかることがあります。

詳しくは

Kerberos認証用のiLOホスト名とドメイン名の構成
IPv4設定の構成
IPv6設定の構成

iLOホスト名とドメイン名の制限

iLOホスト名設定を構成する場合は、以下の点に注意してください。

- **ネームサービスの制限** - サブシステム名はDNS名の一部として使用します。
  - DNSでは、英数字とハイフンが使用できます。
  - ネームサービスの制限は、ドメイン名にも適用されます。
- **ネームスペースの問題** - この問題を避けるために、次のガイドラインに従ってください。
  - アンダースコア文字を使用しない
  - サブシステム名を15文字までにする

    iLOではホスト名に最大49文字まで使用できますが、より短い名前を使用することで、環境内の他のソフトウェア製品との相互運用性の問題を回避することができます。
  - IPアドレスとDNS/WINS名でiLOプロセッサーがPINGコマンドで応答があることを確認する
  - NSLOOKUPがiLOネットワークアドレスを正しく解決し、ネームスペースが競合していないことを確認する
  - DNSとWINSの両方を使用している場合は、iLOネットワークアドレスが正しく解決されることを確認する
  - ネームスペースを変更した場合はDNS名を更新する
- Kerberos認証を使用する場合は、ホスト名とドメイン名がKerberos使用の前提条件を満たしていることを確認します。

NIC設定

ネットワーク共通設定タブのNIC設定セクションでiLO専用ネットワークポートまたはiLO共有ネットワークポートを有効にして、関連付けられたNIC設定の構成を行います。

NIC設定セクションは、Synergyコンピュートモジュールでは使用できません。

iLO Webインターフェイスを介したiLO専用ネットワークポートの有効化

前提条件

- iLOの設定を構成する権限
- デフォルトのサーバー構成でリモート管理をサポートしていない場合、オプションのiLOネットワーク有効化モジュールがインストールされています。

手順

1. iLO専用ネットワークポートを、サーバーを管理するLANに接続します。
2. ナビゲーションツリーでiLO専用ネットワークポートをクリックします。
3. 全般タブをクリックします。
4. iLO専用ネットワークポートを使用チェックボックスを選択します。
5. リンク設定を選択します。
6. 仮想LANを使用するには、仮想LAN有効オプションを有効にします。
7. 仮想LANをオプションを有効にした場合は、仮想LANタグを入力します。
8. 適用をクリックして変更を保存します。

   1つ以上の保留中の変更を有効にするにはiLOのリセットが必要であることがiLOから通知されます。iLO設定の構成権限がアカウントに割り当てられている場合、iLOのリセットボタンがメッセージに含まれています。

   iLOのリセットが完了するまで、このメッセージはすべてのiLO専用ネットワークポートタブまたはiLO共有ネットワークポートタブに表示されます。
9. （オプション）全般、IPv4、IPv6、SNTPの各タブで、その他のネットワーク設定を構成します。
10. iLOネットワーク設定の構成が完了したら、iLOのリセットをクリックします。

    接続が再確立されるまでに、数分かかることがあります。

詳しくは

iLOネットワーク接続に関する留意事項
iLOネットワークポートの構成オプション

専用ネットワークポートの全般設定

リンク設定

この値は、iLOネットワークトランシーバーの速度とデュプレックス設定を制御します。

以下の値から選択します。

- 自動（デフォルト） - iLOを有効にして、ネットワークに接続する際に、サポートされる最高リンク速度とデュプレックス設定をネゴシエートします。
- 1000BaseT、全二重 - 全二重を使用した1 Gb接続を強制します（サポートされるサーバーのみ）。
- 100BaseT、全二重 - 全二重を使用する100 Mb接続を強制します。
- 100BaseT、半二重 - 半二重を使用する100 Mb接続を強制します。
- 10BaseT、全二重 - 全二重を使用した10 Mb接続を強制します。
- 10BaseT、半二重 - 半二重を使用した10 Mb接続を強制します。

一部のサーバーモデルでは、専用ネットワークポートが有効になっている場合、リンク速度とデュプレックス設定を変更できません。

VLAN有効

VLANを有効にすると、iLO専用ネットワークポートはVLANの一部になります。物理的に同じLANに接続されている場合でも、異なる仮想LANタグを持つすべてのネットワークデバイスが、独立したLANにあるかのように表示されます。

VLANタグ

相互に通信するネットワークデバイスすべてが、同じ仮想LANタグを持つ必要があります。仮想LANタグは、1～4094の任意の番号です。

iLO Webインターフェイスを介したiLO共有ネットワークポートの有効化

前提条件

- iLOの設定を構成する権限
- デフォルトのサーバー構成がリモート管理をサポートしていない場合は、オプションのiLOネットワーク有効化モジュールがインストールされている。
- サポートされているネットワークカードがシステムで利用可能である。

手順

1. 共有ネットワークポートOCP1、OCP2、または内蔵NICをLANに接続します。
2. ナビゲーションツリーでiLO共有ネットワークポートをクリックして、全般タブをクリックします。
3. 共有ネットワークポートを使用チェックボックスを選択します。
4. 利用可能なオプションのリストからネットワークカードを選択します。
5. ポートメニューから値を選択します。
6. 仮想LANを使用するには、仮想LAN有効オプションを有効にします。
7. 仮想LAN機能を有効にした場合は、VLANタグを入力します。
8. 適用をクリックして変更を保存します。

   1つ以上の保留中の変更を有効にするにはiLOのリセットが必要であることがiLOから通知されます。iLO設定の構成権限がアカウントに割り当てられている場合、iLOのリセットボタンがメッセージに含まれています。

   iLOのリセットが完了するまで、このメッセージはすべてのiLO専用ネットワークポートタブまたはiLO共有ネットワークポートタブに表示されます。
9. （オプション）全般、IPv4、IPv6、SNTPの各タブで、その他のネットワーク設定を構成します。
10. iLOネットワーク設定の構成が完了したら、iLOのリセットをクリックします。

    接続が再確立されるまでに、数分かかることがあります。

    iLOをリセットすると、共有ネットワークポートがアクティブになります。iLOとの間のすべてのネットワークトラフィックが共有ネットワークポートOCP1、OCP2、または内蔵NICポート経由で転送されるようになります。

詳しくは

iLOネットワーク接続に関する留意事項
iLOネットワークポートの構成オプション

共有ネットワークポートの全般設定

NIC

サーバーのNICタイプ。

ポート

1以外のポート番号の選択は、サーバーおよびネットワークアダプターの両方がこの構成をサポートしている場合にのみ機能します。無効なポート番号を入力すると、ポート1が使用されます。

VLAN有効

VLANを有効にすると、iLO共有ネットワークポートがVLANの一部になります。物理的に同じLANに接続されている場合でも、異なる仮想LANタグを持つすべてのネットワークデバイスが、独立したLANにあるかのように表示されます。

VLANタグ

相互に通信するネットワークデバイスすべてが、同じ仮想LANタグを持つ必要があります。仮想LANタグは、1～4094の任意の番号です。

iLOネットワークポートの構成オプション

iLOサブシステムは、以下のネットワーク接続オプションを提供します。

- iLO専用ネットワークポート - iLOネットワークトラフィック専用の独立したNICを使用します。サポートされている場合、このポートはサーバー背面のRJ-45ジャックを使用します。

  RJ-45ジャックにはiLOというラベルが付いています。

  一部のサーバーでは、このオプションはオプションのiLOネットワーク有効化モジュールのインストールによって提供されます。

  専用管理ネットワークは、優先されるiLOネットワーク構成です。

- 共有ネットワークポート - 構成に応じて、次の共有ネットワークポートオプションを使用できます。
  - 共有ネットワークポートOCP1 - OCPスロット1に取り付けられたオプションのオープンコンピュートプロジェクトNICを使用します。このNICは通常、サーバーネットワークトラフィックを処理します。このNICは、共通のSFPまたはRJ-45コネクター経由で同時にiLOネットワークトラフィックも処理するように構成できます。
  - 共有ネットワークポートOCP2 - OCPスロット2に取り付けられたオプションのオープンコンピュートプロジェクトNICを使用します。このNICは通常、サーバーネットワークトラフィックを処理します。このNICは、共通のSFPまたはRJ45コネクター経由で同時にiLOネットワークトラフィックも処理するように構成できます。
  - 共有ネットワークポート内蔵NIC - サーバーに内蔵の固定NICを使用します。このNICは通常、サーバーネットワークトラフィックを処理します。このNICは、共通のRJ45コネクター経由で同時にiLOネットワークトラフィックも処理するように構成できます。

使用しているサーバーでサポートされるNICについて詳しくは、次のWebサイトにあるサーバー仕様を参照してください。https://www.hpe.com/info/qs

共有ネットワークポートに関する考慮事項

共有ネットワークポートオプションを使用することには、いくつかの欠点があります。

- 共有ネットワーク接続では、トラフィックによって、iLOのパフォーマンスが低下することがあります。
- サーバーの起動時、およびオペレーティングシステムNICドライバーのロードおよびアンロード時に、短時間（2～8秒）、ネットワークからiLOにアクセスできません。この短い時間の経過後に、iLOの通信がリストアされ、iLOがネットワークトラフィックに応答します。

  このようなシチュエーションが起きた場合は、リモートコンソールと、接続されているiLO仮想メディアデバイスが切断されることがあります。

- ネットワークコントローラーのファームウェアをアップデートまたはリセットすることも、iLOが短期間、ネットワーク経由で到達不能に陥る原因となる可能性があります。
- iLO共有ネットワークポート接続は、100 Mbpsを超える速度では動作できません。iLO仮想メディアを介したデータ転送などのネットワーク集約型タスクは、iLO専用ネットワークポートを使用する構成で実行される同じタスクよりも遅くなる場合があります。

共有ネットワークポートに関する考慮事項について詳しくは、iLO6トラブルシューティングガイドを参照してください。

iLOネットワーク接続に関する留意事項

- iLOは1つのアクティブなNIC接続のみをサポートしているため、一度に有効にできるのは専用ネットワークポートオプションまたは共有ネットワークポートオプションのいずれか1つのみです。
- デフォルトでは、iLO共有ネットワークポートはサーバーNICのポート1を使用します。サーバーの構成に応じて、このNICはLOM、FlexibleLOM、またはFlexibleLOM/OCPアダプターになります。ポート番号はNIC上のラベルに対応します。これは、オペレーティングシステム内の番号付けとは異なる可能性があります。

  サーバーとNICの両方でポートの選択がサポートされている場合、iLOファームウェアで別のポート番号を選択することができます。ポート1以外のポートが共有ネットワークポート用に選択されていて、その構成がサーバーでサポートされていない場合、iLOは開始時にポート1に戻します。

- 専用ネットワークポートが搭載されていないサーバーでは、標準のハードウェア構成の場合、iLOネットワーク接続はiLO共有ネットワークポート接続のみを介して提供されます。これらのサーバーでは、iLOファームウェアはデフォルトで共有ネットワークポートに設定されています。
- サーバーの補助電源には予算制限があるため、iLO共有ネットワークポート機能で使用される1 Gb/s銅線ネットワークアダプターの一部は、サーバーの電源がオフのときに10/100の速度でしか動作しない可能性があります。この問題を避けるために、Hewlett Packard Enterpriseでは、iLO共有ネットワークポートが接続されるスイッチを自動ネゴシエート用に構成するか、専用ネットワークポートを使用することをお勧めします。ネットワーク接続について詳しくは、Webサイト**https://www.hpe.com/info/qs**にあるiLO仕様書を参照してください。

  iLOが接続されているスイッチポートが1 Gb/sに構成されている場合、一部の銅線iLO共有ネットワークポートアダプターで、サーバーの電源がオフのときに接続が切断される可能性があります。サーバーの電源が再投入されれば、接続は復旧します。
- iLO共有ネットワークポートを無効にしても、システムNICは完全に無効にはなりません。サーバーネットワークトラフィックは、引き続きNICポートを通過できます。iLO共有ネットワークポートが無効の場合、iLOとの間のすべてのデータ通信量は共有ネットワークポートを通過しません。
- 共有ネットワークポートが有効な場合は、リンク設定やデュプレックス設定は変更できません。共有ネットワークポート構成を使用する場合、オペレーティングシステムでこれらの設定を管理する必要があります。
- 一部のサーバーでは、専用管理ネットワーク（デフォルト）または共有ネットワーク接続によるリモート管理のサポートを追加するために、オプションのiLOネットワーク有効化モジュールが必要です。iLOネットワーク有効化モジュールがインストールされていない場合、iLOアクセスは、ホストベース（インバンド）のアクセス方式でのみサポートされます。サポートされているホストベースのアクセス方式の例には、iLO RESTful API、UEFIシステムユーティリティ、iLOサービスポート（利用可能な場合）、および仮想NICが含まれます。

IPv4設定の構成

前提条件

iLOの設定を構成する権限

このタスクについて

これらのIPv4設定を構成するとき、192.0.2.0/24などの特殊な用途のIPv4アドレスは入力しないでください。これらのアドレスはサポートされていません。詳しくは、IETFのWebサイトにあるRFC5735のドキュメントを参照してください。

手順

1. ナビゲーションツリーでiLO専用ネットワークポートまたはiLO共有ネットワークポートをクリックして、IPv4タブをクリックします。
2. DHCPv4構成設定を構成します。
3. 静的IPv4アドレス構成設定を構成します。
4. DNS構成設定を構成します。
5. 静的経路構成設定を構成します。
6. 開始時にゲートウェイにPING設定を構成します。
7. 適用をクリックして変更を保存します。

   1つ以上の保留中の変更を有効にするにはiLOのリセットが必要であることがiLOから通知されます。iLO設定の構成権限がアカウントに割り当てられている場合、iLOのリセットボタンがメッセージに含まれています。

   iLOのリセットが完了するまで、このメッセージはすべてのiLO専用ネットワークポートタブまたはiLO共有ネットワークポートタブに表示されます。
8. （オプション）全般、IPv4、IPv6、SNTPの各タブで、その他のネットワーク設定を構成します。

9. iLOネットワーク設定の構成が完了したら、iLOをリセットをクリックします。

   接続が再確立されるまでに、数分かかることがあります。

DHCPv4構成設定

DHCPv4の設定はデフォルトで有効です。

DHCPv4有効

iLOによるDHCPサーバーからのIPアドレス（およびその他の多くの設定）の取得を有効にします。

DHCPv4が提供するゲートウェイを使用

DHCPサーバーが提供するゲートウェイをiLOが使用するかどうかを指定します。DHCPを使用しない場合は、ゲートウェイIPv4アドレスボックスにゲートウェイアドレスを入力します。

DHCPv4が提供する静的経路を使用

DHCPサーバーが提供する静的経路をiLOが使用するかどうかを指定します。この静的経路を使用しない場合は、静的経路 #1設定、静的経路 #2設定、および静的経路 #3設定の各ボックスに静的経路宛先、マスク、およびゲートウェイアドレスを入力します。

DHCPv4のドメイン名の使用

DHCPサーバーが提供するドメイン名をiLOが使用するかどうかを指定します。DHCPを使用しない場合は、ネットワーク共通設定ページのドメイン名ボックスにドメイン名を入力します。

DHCPv4のDNSサーバーの使用

DHCPサーバーが提供するDNSサーバーリストをiLOが使用するかどうかを指定します。DNSサーバーリストを使用しない場合は、プライマリDNSサーバーボックス、セカンダリDNSサーバーボックス、およびターシャリDNSサーバーボックスにDNSサーバーアドレスを入力します。

DHCPv4が提供する時間設定を使用

DHCPv4が提供するNTPサービスの場所をiLOが使用するかどうかを指定します。

DHCPv4が提供するWINSサーバーを使用

DHCPサーバーが提供するWINSサーバーリストをiLOが使用するかどうかを指定します。WINSサーバーリストを使用しない場合は、プライマリWINSサーバーボックスおよびセカンダリWINSサーバーボックスにWINSサーバーアドレスを入力します。

注記:

DHCPサーバーの予約を作成するには、DHCPクライアント識別子（一意の識別子）が必要です。iLO6システムの場合、DHCPクライアント識別子は、後ろに3バイト（6文字）の0が続くハードウェアMACアドレスです。たとえば場合、iLO6 MACアドレスが00-53-00-AA-BB-CCの場合、関連するDHCPクライアント識別子は `005300AABBCC000000` になります。

静的IPv4アドレス構成設定

IPv4アドレス

iLOのIPアドレス。DHCPを使用する場合、iLOのIPアドレスは自動的に提供されます。DHCPを使用しない場合、静的IPアドレスを入力します。

サブネットマスク

iLO IPネットワークのサブネットマスク。DHCPを使用している場合、サブネットマスクは自動的に提供されます。DHCPを使用しない場合、ネットワークのサブネットマスクを入力します。

ゲートウェイIPv4アドレス

iLOゲートウェイのIPアドレス。DHCPを使用する場合、iLOゲートウェイのIPアドレスは自動的に提供されます。DHCPを使用しない場合は、iLOゲートウェイのIPアドレスを入力します。

IPv4 DNS構成設定

プライマリDNSサーバー

DHCPv4が提供するDNSサーバーを使用が有効な場合、この値は自動的に入力されます。有効でない場合は、プライマリ

DNSサーバーのアドレスを入力します。

セカンダリDNSサーバー

DHCPv4が提供するDNSサーバーを使用が有効な場合、この値は自動的に入力されます。有効でない場合は、セカンダリDNSサーバーのアドレスを入力します。

ターシャリDNSサーバー

DHCPv4が提供するDNSサーバーを使用が有効な場合、この値は自動的に入力されます。有効でない場合は、ターシャリDNSサーバーのアドレスを入力します。

DDNSサーバー登録を有効

このオプションを有効または無効にして、iLOがそのIPv4アドレスと名前をDNSサーバーに登録するかどうかを指定します。

このオプションは、デフォルトで有効になっています。

IPv4の静的経路構成設定

静的経路 #1 設定、静的経路 #2 設定、および静的経路 #3 設定

iLO静的経路の接続先、マスク、およびゲートウェイのアドレス DHCPv4が提供する静的経路を使用が有効な場合、これらの値は自動的に入力されます。そうでない場合は、静的経路の値を入力してください。

その他のIPv4設定

開始時にゲートウェイにping

iLOプロセッサーの初期化時にゲートウェイに4つのICMPエコー要求パケットをiLOが送信するように構成するには、このオプションを有効にします。これにより、iLOとの間のパケット転送を行うルーターで、iLO用のARPキャッシュエントリーが最新であることを保証できます。

このオプションは、デフォルトで有効になっています。

IPv6設定の構成

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーでiLO専用ネットワークポートまたはiLO共有ネットワークポートをクリックします。
2. IPv6タブをクリックします。
3. グローバルIPv6構成設定を構成します。
4. DHCPv6構成設定を構成します。
5. DNS構成設定を構成します。
6. 静的IPv6アドレス構成設定を構成します。
7. 静的経路構成設定を構成します。
8. 適用をクリックして変更を保存します。

   1つ以上の保留中の変更を有効にするにはiLOのリセットが必要であることがiLOから通知されます。iLO設定の構成権限がアカウントに割り当てられている場合、iLOのリセットボタンがメッセージに含まれています。

   iLOのリセットが完了するまで、このメッセージはすべてのiLO専用ネットワークポートタブまたはiLO共有ネットワークポートタブに表示されます。

9. （オプション）全般、IPv4、IPv6、SNTPの各タブで、その他のネットワーク設定を構成します。

10. iLOネットワーク設定の構成が完了したら、iLOのリセットをクリックします。

接続が再確立されるまでに、数分かかることがあります。

グローバルIPv6構成設定

iLOクライアントアプリケーションはIPv6を最初に使用

iLOクライアントアプリケーションでIPv4サービスアドレスもIPv6サービスアドレスも構成されている場合は、このオプションでクライアントアプリケーションへのアクセスの際にiLOがどちらのプロトコルを先に試すかを指定します。この設定は、FQDNを使用してNTPを設定する場合、名前リゾルバーから受信したアドレスリストにも適用されます。

- iLOでIPv6を先に使用する場合、このオプションを有効にします。
- iLOでIPv4を先に使用する場合、このオプションを無効にします。

最初のプロトコルを使用した通信が失敗すると、iLOは自動的に2番目のプロトコルを試します。

このオプションは、デフォルトで有効になっています。

ステートレスアドレス自動構成（SLAAC）を有効

iLOがルーター広告メッセージから自身のIPv6アドレスを作成するように構成するには、このオプションを有効にします。

iLOは、このオプションが有効になっていない場合でも、自身のリンク-ローカルアドレスを作成します。

このオプションは、デフォルトで有効になっています。

DHCPv6構成設定

ステートフルモードDHCPv6を有効（アドレス）

このオプションを有効にすると、iLOは、DHCPv6サーバーから提供されるIPv6アドレスを要求し、構成できます。

このオプションは、デフォルトで有効になっています。

- DHCPv6急速コミットを使用 - このチェックボックスを選択すると、DHCPv6サーバーで高速コミットメッセージングモードを使用するようiLOに指示します。このモードはDHCPv6のネットワークトラフィックを低減しますが、複数のDHCPv6サーバーが応答およびアドレスを提供できるネットワークで使用すると、問題の原因になることがあります。

  このオプションは、デフォルトでは無効になっています。

ステートレスモードDHCPv6を有効（その他）

NTPおよびDNSサービスの場所の設定をiLOがDHCPv6サーバーに要求するように構成するには、このオプションを有効にします。

このオプションは、デフォルトで有効になっています。

- DHCPv6が提供するドメイン名を使用 - このチェックボックスで、DHCPv6サーバーが提供するドメイン名を使用するかどうかを選択します。

  このオプションは、デフォルトで有効になっています。

- DHCPv6が提供するDNSサーバーを使用 - このチェックボックスを選択すると、DNSサーバーの場所に、DHCPv6サーバーによって提供されたIPv6アドレスが使用されます。この設定は、IPv4のDNSサーバーの位置オプションと同時に有効にできます。

  このオプションは、デフォルトで有効になっています。

- DHCPv6が提供するNTPサーバーを使用 - このチェックボックスを選択すると、NTPサーバーの場所に、DHCPv6サーバーによって提供されたIPv6アドレスが使用されます。この設定は、IPv4のNTPサーバーの位置オプションと同時に有効にできます。

  このオプションは、デフォルトで有効になっています。

ステートフルモードDHCPv6を有効（アドレス）を有効にした場合、ステートレスモードDHCPv6を有効（その他）がデフォルトで有効になります。iLOとDHCPv6サーバー間で必要なDHCPv6ステートフルメッセージでは、これが暗黙で了解されているためです。

IPv6 DNS構成設定

プライマリDNSサーバー、セカンダリDNSサーバー、およびターシャリDNSサーバー

DNSサービスのIPv6アドレスを入力します。

IPv4とIPv6の両方のページでDNSサーバーの場所が構成されている場合、両方のソースが使用されます。使用するソースは、iLOクライアントアプリケーションはIPv6を最初に使用構成オプション、プライマリソース、セカンダリリソース、ターシャリリソースの順にこれらの設定に従って選択されます。

DDNSサーバー登録を有効

このオプションを有効または無効にして、iLOがそのIPv6アドレスと名前をDNSサーバーに登録するかどうかを指定します。

このオプションは、デフォルトで有効になっています。

静的IPv6アドレス構成設定

静的IPv6アドレス1、静的IPv6アドレス2、静的IPv6アドレス3、および静的IPv6アドレス4

iLOの最大4つの静的IPv6アドレスとプレフィックス長を入力します。リンク-ローカルアドレスを入力しないでください。

アドレスごとにステータス情報が表示されます。

静的デフォルトゲートウェイ

ネットワーク上にルーター広告メッセージが存在されない場合に対応できるよう、デフォルトIPv6ゲートウェイアドレスを入力します。

IPv6の静的経路構成設定

静的経路#1（宛先）、静的経路#2（宛先）、および静的経路#3（宛先）

静的IPv6経路の宛先のプレフィックスとゲートウェイアドレスのペアを入力します。宛先のプレフィックス長を指定します。リンク-ローカルアドレスは宛先としては許可されませんが、ゲートウェイとしては許可されます。
静的経路の値ごとにステータス情報が表示されます。

IPv6をサポートしているiLOの機能

IPv4アドレスプールが枯渇に向かっている現状に対応するために、IETFがIPv6を導入しました。IPv6では、アドレス不足の問題を解消するために、アドレス長が128ビットに拡張されています。iLOはデュアルスタック実装を導入することで両方のプロトコルの同時使用に対応しています。

以下の機能がIPv6の使用をサポートします

- 共有ネットワークポート接続経由のIPv6
- IPv6静的アドレス割り当て
- IPv6 SLAACアドレス割り当て
- IPv6静的ルート割り当て
- IPv6静的デフォルトゲートウェイエントリー
- DHCPv6ステートフルアドレス割り当て
- DHCPv6ステートレスDNS、ドメイン名、およびNTP構成
- 統合リモートコンソール
- HPEのシングルサインオン
- Webサーバー
- SSHサーバー
- SNTPクライアント
- DDNSクライアント

- RIBCL over IPv6
- SNMP
- アラートメール
- リモートsyslog
- WinDBGサポート
- HPQLOCFG/HPLOMIG over IPv6接続
- URLベースの仮想メディア
- CLI/RIBCLキーインポートover IPv6接続
- LDAPおよびKerberos over IPv6を使用した認証
- iLO連携
- IPMI
- 組み込みリモートサポート

iLO SNTP設定の構成

前提条件

- iLOの設定を構成する権限
- 少なくとも1台のNTPサーバーが、ご使用の管理ネットワーク上で使用できます。
- DHCPv4が提供するNTPサービス構成を使用する場合、IPv4タブでDHCPv4が有効になっている。
- DHCPv6が提供するNTPサービス構成を使用する場合、IPv6タブでDHCPv6ステートレスモードが有効になっている。

手順

1. ナビゲーションツリーでiLO専用ネットワークポートまたはiLO共有ネットワークポートをクリックします。
2. SNTPタブをクリックします。
3. 以下のいずれかを実行します。
   - DHCPが提供するNTPサーバーアドレスを使用するには、DHCPv4が提供する時間設定を使用かDHCPv6が提供する時間設定を使用、あるいは両方を有効にします。
   - プライマリタイムサーバーボックスおよびセカンダリタイムサーバーボックスにNTPサーバーのアドレスを入力します。
4. DHCPv6が提供する時間設定を使用のみを選択したか、プライマリタイムサーバーとセカンダリタイムサーバーを入力した場合は、サーバーのタイムゾーンをタイムゾーンリストから選択します。
5. NTP時間転送設定を構成します。

   ブレード以外のサーバーでは、この設定はNTP時間をホストに転送と呼ばれています。
6. 適用をクリックして変更を保存します。

   1つ以上の保留中の変更を有効にするにはiLOのリセットが必要であることがiLOから通知されます。iLO設定の構成権限がアカウントに割り当てられている場合、iLOのリセットボタンがメッセージに含まれています。

   iLOのリセットが完了するまで、このメッセージはすべてのiLO専用ネットワークポートタブまたはiLO共有ネットワークポートタブに表示されます。
7. （オプション）全般、IPv4、IPv6、SNTPの各タブで、その他のネットワーク設定を構成します。

8. iLOネットワーク設定の構成が完了したら、iLOをリセットをクリックします。

   接続が再確立されるまでに、数分かかることがあります。

サブトピック

SNTPオプション

iLOのクロック同期

DHCP NTPアドレスの選択

詳しくは

IPv4設定の構成
IPv6設定の構成
DHCP NTPアドレスの選択
iLOのクロック同期

SNTPオプション

DHCPv4が提供する時間設定を使用

DHCPv4が提供するNTPサーバーアドレスをiLOが使用するように構成します。

このオプションは、デフォルトで有効になっています。

DHCPv6が提供する時間設定を使用

DHCPv6が提供するNTPサーバーアドレスをiLOが使用するように構成します。

このオプションは、デフォルトで有効になっています。

NTP時間の伝達設定

この設定の名前は、サーバーの種類によって異なります。

- NTP時間をホストに転送 - AC電源が適用された後、またはiLOがデフォルト設定にリセットされた後に初めてPOSTを実行している間に、サーバー時間をiLO時間と同期させるかどうかを決定します。

  すべてのサーバーでは、この設定はiLOがNTPタイムソースから時間を取得できる場合にのみ有効になります（OneView for Synergyサーバーをタイムソースにすることができます）。

- Propagate NTP - AC電源が適用された後、またはiLOがデフォルト設定にリセットされた後に初めてPOSTを実行している間に、サーバー時間をiLO時間と同期させるかどうかを決定します。

このオプションは、デフォルトでは無効になっています。

注記:

- BIOSの時間形式がUTCに設定されている場合は、サーバー時間とともに、サーバーのタイムゾーン設定もiLOのタイムゾーン設定に同期されます。
- AC電源が供給された後の最初のPOST中に、iLOが構成されたNTPサーバーから時間を取得できない場合、iLOの時間とタイムゾーンはBIOSで構成された時間とタイムゾーンに同期します。

プライマリタイムサーバー

指定したアドレスを持つプライマリタイムサーバーを使用するようにiLOを構成します。サーバーアドレスは、サーバーのFQDN、IPv4アドレス、またはIPv6アドレスを使用して入力できます。

セカンダリタイムサーバー

指定したアドレスを持つセカンダリタイムサーバーを使用するようにiLOを構成します。サーバーアドレスは、サーバーのFQDN、IPv4アドレス、またはIPv6アドレスを使用して入力できます。

タイムゾーン

iLOが現地時間を得るためにUTC時を調整する方法と、夏時間（サマータイム）を得るために時間を調整する方法が決まります。iLOログのエントリーに正しい現地時間を表示するために、ユーザーはサーバーが存在する場所のタイムゾーンを指定する必要があり、ログの表示フィルターでローカル時刻表示を選択する必要があります。

SNTPサーバーが提供する時間をiLOで調整なしで使用する場合は、UTC時に調整を加えないタイムゾーンを選択します。さらにそのタイムゾーンは、夏時間の調整が適用されないものである必要があります。この要件に合うタイムゾーンはいくつかあります。iLOで選択可能な1つの例はGreenwich（GMT）です。このタイムゾーンを選択すると、iLO Webインターフェイスのページおよびログエントリーには、SNTPサーバーが提供する時間がそのまま表示されます。

注記:
NTPサーバーを協定世界時（UTC）を使用するように構成してください。

iLOのクロック同期

iLOでは、SNTPを使用して外部の時刻ソースとクロックを同期させることができます。iLOの日付と時刻はPOST実行中にシステムROMによって同期を取ることもできるため、SNTPの構成は省略可能です。

プライマリおよびセカンダリNTPサーバーアドレスは、手動でまたはDHCPサーバーにより構成できます。プライマリサーバーのアドレスに接続できない場合は、セカンダリアドレスが使用されます。

DHCP NTPアドレスの選択

DHCPサーバーを使用してNTPサーバーアドレスを提供する場合は、IPv6ページのiLOクライアントアプリケーションはIPv6を最初に使用設定によって、プライマリおよびセカンダリNTPの値の選択を制御します。iLOクライアントアプリケーションはIPv6を最初に使用を選択した場合、DHCPv6提供のNTPサービスアドレス（使用可能な場合）がプライマリ時刻サーバーに使用され、DHCPv4提供のアドレス（使用可能な場合）がセカンダリ時刻サーバーに使用されます。

プロトコルベースの優先動作を変更して、DHCPv4を最初に使用するには、iLOクライアントアプリケーションはIPv6を最初に使用チェックボックスをクリアします。

DHCPv6アドレスがプライマリアドレスにもセカンダリアドレスにも使用できない場合は、DHCPv4アドレス（使用可能な場合）が使用されます。

iLO NIC自動選択

iLO NIC自動選択を使用すると、iLOがiLO専用ネットワークポートとiLO共有ネットワークポートを選択できるようになります。起動時に、iLOは使用可能なポートのネットワークアクティビティを検索し、ネットワークアクティビティに基づいて使用するポートを自動的に選択します。

この機能によって、ProLiant Gen10以降のサーバーに共通の事前構成を使用することができます。例えば、複数のサーバーがある場合、一部のサーバーを、iLO専用ネットワークポート経由でiLOに接続するデータセンター内にインストールします。他のサーバーは、共有ネットワークポート経由でiLOに接続するデータセンター内にインストールします。iLO NIC自動選択を使用すると、どちらのデータセンターにもサーバーを設置できるようになり、iLOは正しいネットワークポートを選択します。

デフォルトでは、NIC自動選択は無効です。

サブトピック

NIC自動選択のサポート

NIC自動選択が有効になっている場合のiLO起動時の動作

iLO NIC自動選択の有効化

NICフェイルオーバーの構成

詳しくは

[iLO NIC自動選択の有効化]

NIC自動選択のサポート

- ProLiant Gen10以降の非ブレードサーバーはNIC自動選択をサポートします。
- iLO6は、この構成をサポートしているサーバー上で両方の共有ネットワークポートを検索するように設定できます。
- iLO6はNICフェイルオーバーをサポートします。有効にすると、現在の接続が切断されたときに、iLOが自動的にNIC接続の検索を開始します。この機能を使用するには、NIC自動選択を有効にする必要があります。

NIC自動選択が有効になっている場合のiLO起動時の動作

NIC自動選択が有効な場合：

- iLOが電源に接続されると、最初にiLO専用ネットワークポートをテストします。
- iLOがリセットされると、最後に使用したiLOネットワークポートを最初にテストします。
- ネットワークポートのテスト時に、iLOがネットワークのアクティビティを検出した場合、そのポートを選択して使用します。約100秒後までにネットワークアクティビティが検出されない場合は、iLOは反対側のネットワークポートに切り替え、そのポートのテストを開始します。iLOはネットワークアクティビティが検出されるまで、iLO専用ネットワークポートとiLO共有ネットワークポートを交互にテストします。iLOがテストのためにネットワークポートを切り替えるたびに、iLOのリセットが発生します。

  △ 注意:

  物理NICのいずれかがセキュリティ保護されていないネットワークに接続している場合、iLOがiLOネットワークポート間で交互に切り替えたときに不正アクセスが発生する可能性があります。Hewlett Packard Enterpriseでは、必ずiLOを次のようなネットワークに接続することを強くおすすめします。

  - iLOへのアクセスに強力なパスワードを使用している。
  - セキュリティ保護されていないネットワークにiLO専用ネットワークポートを接続しない。
  - iLO共有ネットワークポートがセキュリティ保護されていないネットワークに接続されている場合、iLOのうち共有NICの部分はVLANタギングを使用し、VLANが安全なネットワークに接続されていることを確認する。

- iLOがアクティブなネットワークポートを検索するときは、サーバーのUID LEDが点灯します。検索中にiLOがリセットされた場合、UID LEDが5秒間点滅し、その後アクティブなポートが選択されるか、iLOがリセットされるまで点灯します。
- サーバーがiLOへのLOMおよびFlexibleLOM共有ネットワークポート接続の両方をサポートしている場合、iLOは構成中に選択されたオプションだけをテストします。iLOはLOMおよびFlexibleLOMオプションを交互にテストしません。
- NIC自動選択がDHCPアドレスの割り当てアクティビティを検索するよう構成されており、iLOネットワークポートのうち1つだけでDHCPが有効になっている場合、iLOはDHCP用に構成されていないポートの受信データパケットアクティビティをテストします。

iLO NIC自動選択の有効化

手順

1. 両方のiLOネットワークポートを設定します。

NICの自動選択機能を有効にして使用する前に、両方のiLOネットワークポートをそれぞれのネットワーク環境に合わせて設定する必要があります。

2. 次のいずれかを実行します。
   - CLIコマンド`oemhpe_nicautosel`を使用して、NIC自動選択を設定します。
   - NIC自動選択を有効にするには、MOD_NETWORK_SETTINGSスクリプトにILO_NIC_AUTO_SELECTタグを追加し、スクリプトを実行します。

     （オプション）オプションのNIC自動選択機能を設定するには、MOD_NETWORK_SETTINGSスクリプトにILO_NIC_AUTO_SNP_SCANおよびILO_NIC_AUTO_DELAYタグを追加します。

   詳しくは、HPE iLO 6スクリプティング/コマンドラインガイドを参照してください。
3. サーバーのケーブルを配線し、iLOをリセットします。

   NIC自動選択への変更は、iLOがリセットされるまで反映されません。

詳しくは

iLO NIC自動選択
NIC自動選択のサポート
NIC自動選択が有効になっている場合のiLO起動時の動作

NICフェイルオーバーの構成

前提条件

NIC自動選択が有効になっている。

NICフェイルオーバーを構成するには、次のいずれかのオプションを使用します。詳しくは、 HPE iLO 6スクリプティング/コマンドラインガイドを参照してください。

手順

- CLIコマンド`oemhpe_nicfailover`を使用して、NICフェイルオーバーを設定します。
- `ILO_NIC_FAIL_OVER`タグを`MOD_NETWORK_SETTINGS`スクリプトに追加し、スクリプトを実行します。

詳しくは

iLO NIC自動選択の有効化

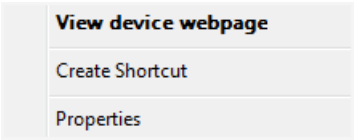
Windowsネットワークフォルダー内のiLOシステムの表示

このタスクについて

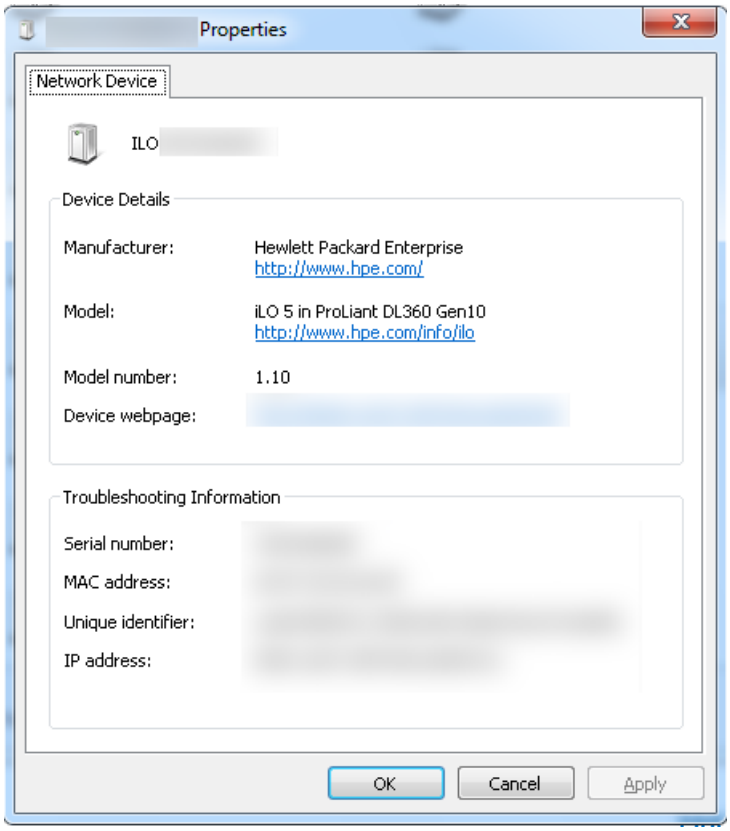
UPnPが構成されている場合、Windowsシステムと同じネットワーク上のiLOシステムがWindowsのネットワークフォルダーに表示されます。

手順

- iLOシステムのWebインターフェイスを起動するには、Windowsのネットワークフォルダーでアイコンを右クリックし、**デバイスのWebページの表示**を選択します。



- iLOシステムのプロパティを表示するには、Windowsのネットワークフォルダーにあるアイコンを右クリックし、プロパティを選択します。



プロパティウィンドウには、以下の設定があります。

  - デバイスの詳細 - iLOのメーカーとバージョン情報。iLO Webインターフェイスを開始するには、デバイスのWebページリンクをクリックします。
  - トラブルシューティング情報 - シリアル番号、MACアドレス、UUID、およびIPアドレス。

リモートサポートの管理

サブトピック

HPE内蔵リモートサポート

HPE iLO 6には、内蔵リモートサポート機能が含まれており、この機能により、サポートされるサーバーをHPEリモートサポートに登録することができます。

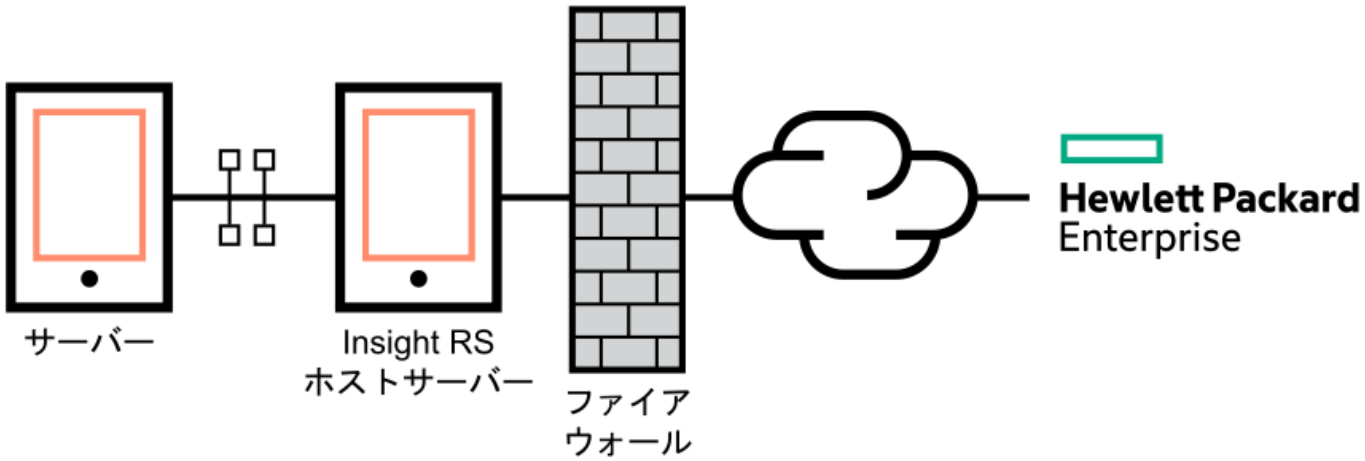
また、iLOを使用してサービスイベントやリモートサポートによるデータ収集を監視することもできます。

Hewlett Packard Enterpriseにデバイスを接続することによって、そのデバイスをリモートでサポートします。また、診断、構成、テレメトリー、および連絡先の情報をHewlett Packard Enterpriseに送信できます。その他のビジネス情報は収集されません。またデータはHewlett Packard Enterpriseのプライバシー声明に従って管理されます。プライバシーポリシーは、次のWebサイト**https://www.hpe.com/info/privacy**で確認できます。

> **重要:**
> HPEは現在Insight Remote Support Central Connectのみをサポートします。HPE Insight Online Direct Connectを使用している場合、Hewlett Packard EnterpriseはInsight Online Direct Connectの登録を解除し、Insight Remote Support Central Connectに登録することをお勧めします。

Insight Remote Support Central Connect

ローカル環境にあるInsight Remote Supportの一元化されたホストサーバーを使用してHewlett Packard Enterpriseにサポート対象のデバイスを登録します。すべての構成およびサービスイベント情報は、ホストサーバーを介してルーティングされます。この情報は、ローカルのInsight RS Consoleを使用して表示できます。



デバイスサポート

組み込みリモートサポートの登録は、以下のデバイスタイプをサポートしています。

> **重要:**
> HPE OneViewを使用してご利用の環境を管理する場合は、これを使用してリモートサポートを登録します。詳しくは、HPE OneViewユーザーガイドを参照してください。

Insight Remote Support Central Connect

- HPE ProLiant Gen10サーバー
- HPE ProLiant Gen10 Plusサーバー
- HPE ProLiant Gen11サーバー

HPEリモートサポートにより収集されるデータ

iLOリモートサポートにより収集されるデータ

サーバーがリモートサポート対象に登録されている場合、iLOがActive Health System情報およびサーバー構成情報を収集した後、iLOまたはInsight RSホストサーバーがHewlett Packard Enterpriseにこの情報を送信します。Active Health System情報は7日ごとに送信され、設定情報は30日ごとに送信されます。以下の情報が含まれます。

登録

サーバーの登録中、iLOは、サーバーハードウェアを一意に識別するためのデータを収集します。登録データには、以下の情報が含まれます。

- サーバーモデル
- シリアル番号
- iLO NICアドレス

サービスイベント

サービスイベントが記録されると、iLOは、関連ハードウェアコンポーネントを識別するためのデータを収集します。サービスイベントデータには、以下の情報が含まれます。

- サーバーモデル
- シリアル番号
- ハードウェアコンポーネントのパーツ番号
- 説明、場所、およびハードウェアコンポーネントを識別するその他の特徴

構成

データの収集中、iLOは、プロアクティブなアドバイスとコンサルティングを可能にするデータを収集します。構成データには、以下の情報が含まれます。

- サーバーモデル
- シリアル番号
- プロセッサーモデル、速度、および使用率
- ストレージ容量、速度、および使用率
- メモリ容量、速度、および使用率
- ファームウェア/BIOS
- インストールされているドライバー、サービス、およびアプリケーション（AMSがインストールされている場合）

Active Health System

データの収集中、iLOは、サーバーのヘルス、構成、およびランタイムテレメトリーに関するデータを収集します。この情報は、問題のトラブルシューティングおよび、品質分析のための閉じたループで使用されます。

詳しくは

Active Health System
リモートサポートのデータ収集
リモートサポートサービスイベント

リモートサポート登録に関する前提条件

手順

1. リモートサポートソリューションのコンポーネントにログインするときに使用する、サポートされるブラウザーをインストールします。
2. Webサイトhttps://www.hpe.com/support/hpescに移動し、リモートサポートに登録する製品に有効なHewlett Packard Enterprise保証または契約があることを確認します。

3. 以下の情報を収集します。この情報は、Insight Remote Support Central Connectのホストサーバーの構成手順で使用します。
   - 連絡先情報。Hewlett Packard Enterpriseは、サポートケースを作成するときにこの情報を使用します。
   - サイト情報 （サイト名、アドレス、およびタイムゾーン）。Hewlett Packard Enterpriseは、サービス担当者または部品をサーバーのある場所に送らなければならないときにこの情報を使用します。
   - Webプロキシ情報（Webプロキシはインターネットにアクセスするために使用されます）。
   - チャネルパートナーがデバイス情報を表示できるようにする場合は、認定サービスプロバイダー、リセラー/ディストリビューター、およびインストーラーのチャネルパートナーID。インストーラーはInsight Remote Support Central Connectのみに必要です。

     パートナーIDは、パートナー登録プロセス中にチャネルパートナーに割り当てられるロケーションIDです。チャネルパートナーIDがわからない場合は、パートナーにお問い合わせの上、その情報を取得してください。
4. リモートサポート登録用のProLiantサーバーをセットアップします。

   サーバーをセットアップしている場合は、それらがサーバーのセットアップ手順で説明されている要件を満たしていることを確認します。
5. iLOのホスト名またはIPアドレスとログイン認証情報（ログイン名およびパスワード）を入手します。

   iLOの設定権限を持っているローカルまたはディレクトリベースのユーザーアカウントを使用することができます。
6. Insight Remote Support Central Connect環境をセットアップします。

サブトピック

HPE組み込みリモートサポートでサポートされるブラウザー

リモートサポート登録用のProLiantサーバーのセットアップ

Insight Remote Support Central Connect環境のセットアップ

HPE組み込みリモートサポートでサポートされるブラウザー

iLO

iLO6は、サポートされるブラウザーにリストされているブラウザーをサポートします。

Insight RS

- Mozilla Firefox：49.x
- Google Chrome：53.x

リモートサポート登録用のProLiantサーバーのセットアップ

前提条件

ProLiantサーバーをセットアップまたはアップデートするために必要なファイルがあることを確認します。

構成によっては、**Service Pack for ProLiant**が必要な場合があります。SPPにはiLOファームウェア、iLO 6 Channel Interfaceドライバー、およびAMSが含まれます。SPPダウンロードページ**https://www.hpe.com/servers/spp/download**からSPPをダウンロードします。

次のWebサイトで、iLO 6 Channel Interfaceドライバー、iLOファームウェア、およびAMSを個別にダウンロードできます。**https://www.hpe.com/support/ilo6**

手順

1. サーバーハードウェアをインストールします。
2. iLOをネットワークに接続します。
3. Intelligent Provisioningを使用してサーバーの構成とOSのインストールを実行します。

   詳しくは、Intelligent Provisioningのユーザーガイドを参照してください。
4. （オプション）AMSをまだインストールしていない場合はインストールします。

   Hewlett Packard EnterpriseはAMSをインストールすることをお勧めします。

   AMSの使用は、iLOがサーバーの名前を取得できる1つの方法です。iLOがサーバー名を取得できない場合、Insight RSで表示されているサーバー名は、サーバーのシリアル番号から得られます。
5. AMSをインストールしていない場合は、Insight RSでサーバー名が正しく表示されることを確認するために、以下のいずれかを実行します。
   - Windowsシステムの場合のみ、オペレーティングシステムを起動します。Insight RSは、サーバーを識別するために、Windowsコンピューター名を使用します。
   - iLO Webインターフェイスのアクセス設定ページで、サーバー名を構成します。

     プライバシーを保護するため、サーバー名に機密情報を使用しないでください。サーバー名はInsight RSに表示されます。
6. Windowsサーバー：iLO 6 Channel Interfaceドライバーをインストールします。

   Red Hat Enterprise LinuxおよびSUSE Linux Enterprise Serverの場合、ドライバーはLinuxディストリビューションに含まれています。
7. タイムゾーンがiLOで設定されていることを確認します。

詳しくは

iLOドライバーのインストール
AMSのインストール
iLOネットワーク設定の構成
iLO SNTP設定の構成
ネットワーク構成の概要の表示
iLO暗号化設定
インストール済みファームウェア情報の表示

Insight Remote Support Central Connect環境のセットアップ

このタスクについて

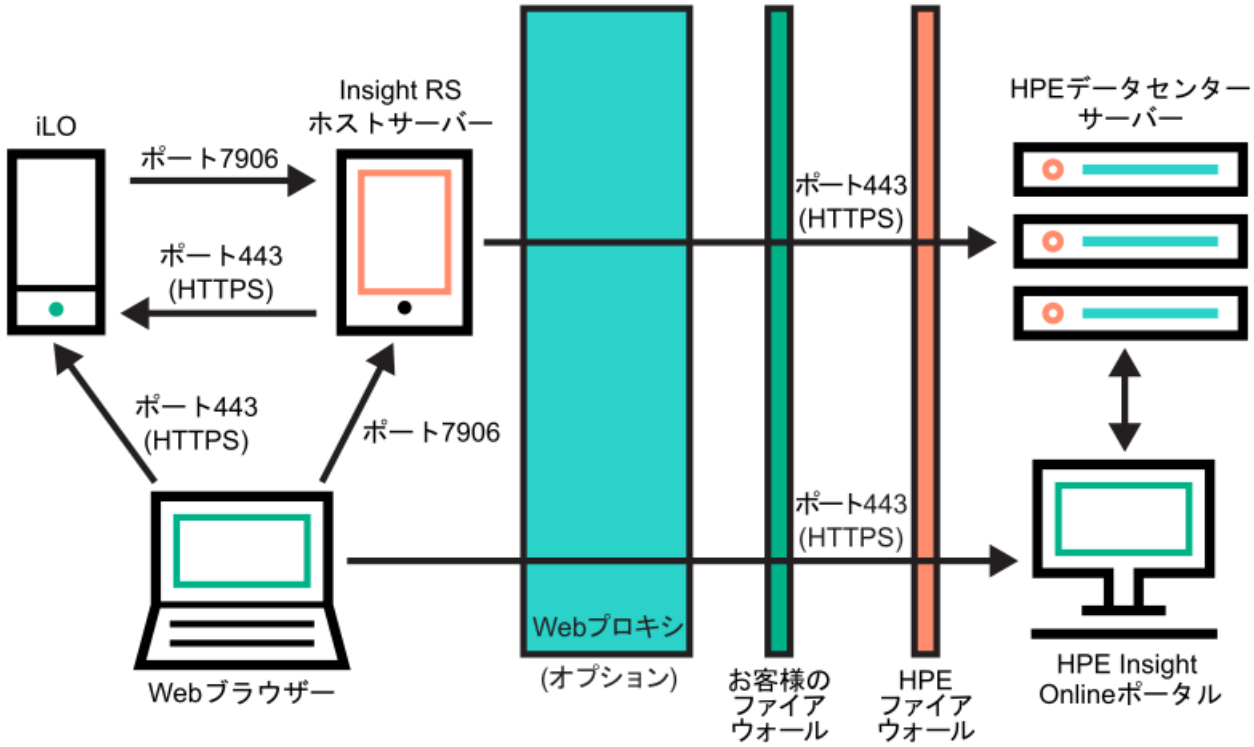
Insight Remote Supportは、サポートサービスの提供については、ご使用の環境とHewlett Packard Enterpriseの間の通信に依存します。

手順

1. Insight RSホストサーバーに使用するサーバーが、Insight Remote Supportのリリースノートに記載されている要件を満たしていることを確認します。

   Insight RSソフトウェアでは、ホストサーバーのことを「ホスティングデバイス」と呼んでいます。
2. ご使用の環境がInsight Remote Support Central Connectのネットワーク要件に示すポート要件を満たしていることを確認します。

図 1. Insight Remote Support Central Connectのネットワーク要件



3. Insight RSホストサーバーを設定します。

   a. ホストサーバー上のInsight RSソフトウェアのバージョンが、登録するProLiantサーバーをサポートしていることを確認します。詳しくは、次のWebサイトを参照してください。https://www.hpe.com/support/InsightRS-Support-Matrix

   b. Insight RSコンソールを使用して、Insight Remote Support Central Connectに登録するProLiantサーバーのRIBCLプロトコルを構成します。

   c. （オプション）HPE SIMをInsight RSとともに使用する場合は、HPE SIMアダプターを設定します。

   詳しくは、Webサイト（https://www.hpe.com/info/insightremotesupport/docs）にあるInsight Remote Supportのインストール/構成ガイドを参照してください。

4. Insight RSホストサーバーとリモートサポートWebサービスとの間の通信を確認します。

   このタスクを完了するには、Insight RSホストサーバーでWebブラウザーを起動して、次のWebサイトに移動します。https://api.support.hpe.com/v1/version/index.html

   サーバーとHPE間の接続が正しく設定されている場合、Webブラウザーには、一部のデータセンターコンポーネントのバージョン（たとえば、`19.1.17.470`）が表示されます。

Insight Remote Support Central Connectの登録

前提条件

- ご使用の環境が内蔵リモートサポート登録の前提条件を満たしている。
- iLOの設定を構成する権限

手順

1. ナビゲーションツリーでリモートサポートをクリックします。

   登録ページが表示されます。

2. ホストサーバーのホスト名またはIPアドレスおよびポート番号を入力します。

   ホスト名、IPv4アドレス、またはIPv6アドレスを入力できます。

   デフォルトポートは7906です。

3. **登録**をクリックします。

   iLOによって、登録プロセスが終了したことが通知されます。

4. （オプション）iLOとHPEリモートサポート間の接続を確認するために、テストイベントを送信します。

5. （オプション）システムイベントに関する電子メールアラートを受け取るには、アラートメールを構成します。

詳しくは

リモートサポート登録に関する前提条件
テストサービスイベントの送信
アラートメールを有効にする
サポートされるデバイスのDirect ConnectからCentral Connectリモートサポートへの変更

Insight Remote Support Central Connectの登録解除

手順

1. Insight RS Consoleにログインします。

2. 次のいずれかを実行します。

   - サーバーの監視を一時的に停止するには、Insight RS Consoleで、デバイス > Device Summaryタブでサーバーを選択し、ACTIONS > DISABLE SELECTEDを選択します。

     iLOのWebインターフェイスからサーバーの登録を直接解除することは、Insight RS Consoleでサーバーを一時的に無効にすることと同じです。

   - サーバーの監視を永久に停止するには、Insight RS Consoleからサーバーを削除します。サーバーを削除するには、Device Summaryタブでサーバーを選択し、次にACTIONS > DELETE SELECTEDを選択します。

3. ナビゲーションツリーでリモートサポートをクリックします。

   登録ページが表示されます。

4. サーバーが登録されていないことを確認します。

リモートサポートサービスイベント

iLOがハードウェア障害（メモリDIMMまたはファンの問題など）を検出すると、サービスイベントが生成されます。サーバーがリモートサポートに登録されている場合、サービスイベントの詳細がサービスイベントログに記録されます。リモートサポートの構成に応じて、詳細はInsight RSホストサーバー（Central Connect）に送信され、これによってHewlett Packard Enterpriseに転送されます。Hewlett Packard Enterpriseがサービスイベントを受信すると、サポートケースが開かれます（保証対象の場合）。計画メンテナンス中にメンテナンスモード機能を有効にすると、計画メンテナンス期間中にサポートケースを開くことができなくなります。

サブトピック

サービスイベントの送信

メンテナンスモードの設定

メンテナンスモードの有効期限の編集

メンテナンスモードのクリア

メンテナンスモードのステータスの表示

テストサービスイベントの送信

サービスイベントログの表示

サービスイベントログのクリア

サービスイベントの送信

サービスイベントが発生した場合は、そのイベントに関する情報がHewlett Packard Enterpriseに送信されます。

サービスイベントの送信障害が発生した場合は、さらに2回追加で送信が試行されます。3回の試行後もイベントを送信できない場合は、次が実行されます。

- SNMPトラップ（`cpqSm2IrsCommFailure 9020`）が生成されます。このSNMPトラップは、`cpqsm2.mib`ファイルで定義されています。
- 失敗がサービスイベントログに記録されます。
- 失敗がiLOイベントログに記録されます。
- サービスイベントはActive Health Systemのログに記録されます。
- 失敗メッセージは、Active Health Systemのログに記録されます。

メンテナンスモードの設定

前提条件

- iLOの設定を構成する権限
- サーバーがリモートサポートに登録されています。

このタスクについて

サーバーでメンテナンスを実行する場合は、メンテナンスモードを使用します。メンテナンスモードが設定されると、Insight RSに送信される通信には、アクションが不要であることを示すフラグが付けられます。この機能により、Hewlett Packard Enterpriseは、サポートケースを開くかどうかを判定できます。

手順

1. ナビゲーションツリーでリモートサポートをクリックし、サービスイベントタブをクリックします。
2. （メンテナンスモードセクション内）をクリックします。

   メンテナンスモード設定の編集ページが開きます。
3. メンテナンスモードチェックボックスを選択します。
4. 失効メニューから時間を選択します。
5. 適用をクリックします。

   iLOによって、メンテナンスモードに設定されたことが通知されます。

   指定した期間を過ぎると、メンテナンスモードは自動的に終了します。必要に応じて、メンテナンスモードを手動でクリアできます。

   メンテナンスモードが設定されるか、期限切れになるか、クリアされると、iLOイベントログにイベントが記録されま

す。

メンテナンスモードの有効期限の編集

前提条件

- iLOの設定を構成する権限
- サーバーがリモートサポートに登録されています。
- メンテナンスモードが有効になっています。

手順

1. ナビゲーションツリーでリモートサポートをクリックし、サービスイベントタブをクリックします。

   サービスイベントページには、メンテナンスモードの残り時間が表示されます。

2. （メンテナンスモードセクション内）をクリックします。

   メンテナンスモード設定の編集ページが開きます。

3. 失効メニューで新しい値を選択し、 適用をクリックします。

   iLOによって、メンテナンスモードに設定されたことが通知されます。

   指定した期間を過ぎると、メンテナンスモードは自動的に終了します。必要に応じて、メンテナンスモードを手動でクリアできます。

   メンテナンスモードが設定されるか、期限切れになるか、クリアされると、iLOイベントログにイベントが記録されます。

メンテナンスモードのクリア

前提条件

- iLOの設定を構成する権限
- サーバーがリモートサポートに登録されています。

手順

1. ナビゲーションツリーでリモートサポートをクリックし、サービスイベントタブをクリックします。
2. （メンテナンスモードセクション内）をクリックします。

   メンテナンスモード設定の編集ページが開きます。

3. メンテナンスモードチェックボックスをクリアして、適用をクリックします。

   メンテナンスモードがクリアされ、イベントがiLOイベントログに記録されることがiLOから通知されます。

メンテナンスモードのステータスの表示

前提条件

サーバーがリモートサポートに登録されています。

手順

ナビゲーションツリーでリモートサポートをクリックし、サービスイベントタブをクリックします。

メンテナンスモードセクションには、現在のメンテナンスモードのステータスが表示されます。

メンテナンスモードが有効になっている場合、残り時間が表示されます。残り時間は、ブラウザーウィンドウを更新するか、テストサービスイベントを送信するとアップデートされます。

テストサービスイベントの送信

前提条件

- iLOの設定を構成する権限
- サーバーがリモートサポートに登録されています。

このタスクについて

リモートサポート設定が正しく機能していることを確認するため、テストイベントを送信できます。

手順

1. ナビゲーションツリーでリモートサポートをクリックし、サービスイベントタブをクリックします。
2. テストイベントの送信をクリックします。
3. 要求を確認するメッセージが表示されたら、はい、送信しますをクリックします。

   送信が完了すると、テストイベントは、サービスイベントログおよびInsight RS Consoleに表示されます。

   テストが成功すると、サービスイベントログの送信ステータスに`エラーなし`と表示されます。

   サービスイベントログの生成時刻列には、構成されたiLOタイムゾーンに基づく日時が表示されます。
4. （オプション）Insight RS Consoleでテストイベントを表示できます。

サブトピック

Insight RS Consoleを使用したテストサービスイベントの表示

詳しくは

Insight RS Consoleを使用したテストサービスイベントの表示

Insight RS Consoleを使用したテストサービスイベントの表示

前提条件

Insight Remote Support Central Connect用に登録されているサーバーで、テストサービスイベントが送信されました。

手順

1. Insight RS Consoleにログインします（https://<Insight RSホストサーバーのIPアドレス>:7906）。
2. デバイスページに移動します。
3. ご使用のサーバーを見つけて、デバイス名をクリックします。
4. サービスイベントタブをクリックします。
5. サービスイベントのリストが表示されます。
6. Insight RSは、サービスイベントの生成時刻の値を、Insight RS Consoleへのアクセスに使用するブラウザーのタイムゾーンに変換します。

7. それ以上の処理は不要であるため、テストイベントは自動的に閉じます。

サービスイベントログの表示

前提条件

サーバーがリモートサポートに登録されています。

手順

ナビゲーションツリーでリモートサポートをクリックし、サービスイベントタブをクリックします。

サブトピック

サービスイベントログの詳細

サポートされるサービスイベントタイプ

サービスイベントログの詳細

サービスイベントログには、サービスイベントごとに以下の情報が表示されます。

- 識別子 – サービスイベントを識別する一意の文字列。
- 生成時刻 – サービスイベントが生成された時刻。この列に、構成されたiLOタイムゾーンに基づいて日時が表示されます。
- イベントID – サービスイベントタイプの一意の番号。
- 認識された重大度 – イベント表示の重大度（たとえば、5-重度、7-致命的）。
- 送信ステータス – イベント送信のステータス。イベントが正常に送信されると、ステータスは`エラーなし`になります。
- 送信先 – Insight Remote SupportのCentral Connect構成の場合、サービスイベントを受信したInsight RSホストサーバーのホスト名またはIPアドレスおよびポート。
- イベントカテゴリ – メッセージレジストリ内のメッセージIDの説明に対応するイベントのカテゴリ。

サポートされるサービスイベントタイプ

HPEリモートサポートソリューションでは、以下のサービスイベントタイプがサポートされています。

イベントID	説明
1	汎用のテストサービスイベント
100	ファン障害サービスイベント
101	システムバッテリ障害サービスイベント
200	電源装置障害サービスイベント
202	電源ヒューズ障害サービスイベント
300	物理ディスクドライブサービスイベント
301	Smartアレイコントローラアクセラレータバッテリ障害イベント
302	Smartアレイコントローラアクセラレータボードステータス変化イベント
303	Smartアレイコントローラステータス変化イベント
304	SAS物理ドライブステータス変化イベント
305	ATAディスクドライブステータス変化イベント
306	ファイバーチャネルホストコントローラーのステータス変化イベント
307	NVMeドライブのステータス変化
308	NVMeドライブの消耗ステータスの変化
309	SSDドライブの消耗ステータスの変化
400	メモリモジュール障害または障害予測イベント
401	NVDIMM障害
500	ストレージシステムのファンステータス変化イベント
501	ストレージシステムの電源装置ステータス変化イベント
600	訂正不能なマシンチェック例外イベント
1000	汎用IMLサービスイベント

サービスイベントログのクリア

前提条件

- iLOの設定を構成する権限
- サーバーがリモートサポートに登録されています。

手順

1. ナビゲーションツリーでリモートサポートをクリックし、サービスイベントタブをクリックします。
2. イベントログのクリアをクリックします。

   iLOが要求を確認するように求めます。
3. はい、クリアしますをクリックします。

iLOによって、サービスイベントログがクリアされたことが通知されます。

リモートサポートのデータ収集

Data Collectionsページを使用して、Remote Supportにサーバーを登録するときにHewlett Packard Enterpriseに送信されるデータに関する情報を表示します。デバイス構成が変更されたときに、次にスケジュールされたデータ収集送信まで待てない場合は、このページを使用してHewlett Packard Enterpriseにデータ収集情報を手動で送信することもできます。

サブトピック

データ収集情報の送信

Active Health Systemが報告する情報の送信

iLOでのデータ収集ステータスの表示

iLOでのActive Health Systemレポートステータスの表示

Insight RS Console（Insight Remote Support Central Connectのみ）でのデータ収集ステータスの表示

データ収集情報の送信

前提条件

iLOの設定を構成する権限

このタスクについて

Insight RSホストサーバーが、保証およびサービス契約に基づく分析およびプロアクティブサービスのために、サーバーのヘルス、構成、およびランタイムテレメトリーに関する情報をHewlett Packard Enterpriseに送信します。

- **Insight Remote Support Central Connect** - データ送信の頻度は、Insight RSコンソールで構成します。詳しくは、Insight RSのオンラインヘルプを参照してください。

次にスケジュールされた送信まで待ちたくない場合は、以下の手順を使用してデータ収集を手動で送信します。

手順

1. ナビゲーションツリーでリモートサポートをクリックし、データ収集タブをクリックします。
2. データ収集の送信をクリックします。
3. 要求を確認するメッセージが表示されたら、はい、送信しますをクリックします。

   送信が完了すると、収集された最新の構成情報送信および収集された最新の構成情報送信ステータスがアップデートされます。この日時は、構成されているiLOタイムゾーンに基づいています。
4. （オプション）Insight RS Consoleでデータ収集ステータスを表示します。

詳しくは

Insight RS Console（Insight Remote Support Central Connectのみ）でのデータ収集ステータスの表示

Active Health Systemが報告する情報の送信

前提条件

iLOの設定を構成する権限

このタスクについて

Insight RSホストサーバーが、サーバーのヘルス、構成、およびランタイムテレメトリーに関する情報をHewlett Packard Enterpriseに送信します。この情報は、問題のトラブルシューティングと閉ループ型の品質解析に使用されます。

- **Insight Remote Support Central Connect** - データは7日ごとに送信されます。Insight RS ConsoleでActive Health Systemレポート送信曜日を変更することができます。詳しくは、Insight RSのオンラインヘルプを参照してください。

次にスケジュールされた送信まで待ちたくない場合は、以下の手順を使用してActive Health Systemレポート情報を手動で送信します。Active Health System情報をActive Health Systemページから直接ダウンロードすることもできます。

手順

1. ナビゲーションツリーでリモートサポートをクリックし、データ収集タブをクリックします。
2. Active Health Systemレポートの送信をクリックします。
3. 要求を確認するメッセージが表示されたら、はい、送信しますをクリックします。

   収集したデータには、最新の7日間のActive Health System情報が含まれます。

   送信が完了すると、最新のActive Health Systemレポート送信および最新のActive Health Systemレポート送信のステータスがアップデートされます。この日時は、構成されているiLOタイムゾーンに基づいています。
4. （オプション）Insight RS ConsoleでActive Health Service Collectionステータスを表示します。

詳しくは

Insight RS Console（Insight Remote Support Central Connectのみ）でのデータ収集ステータスの表示

iLOでのデータ収集ステータスの表示

手順

ナビゲーションツリーでリモートサポートをクリックし、データ収集タブをクリックします。

サブトピック

データ収集の詳細

データ収集の詳細

- 収集された最新の構成情報送信 - 最後にデータが収集された日時。
- 収集された最新の構成情報送信ステータス - 最後のデータ送信のステータス。

iLOでのActive Health Systemレポートステータスの表示

手順

ナビゲーションツリーでリモートサポートをクリックし、データ収集タブをクリックします。

サブトピック

Active Health Systemレポートの詳細

Active Health Systemレポートの詳細

- 最新のActive Health Systemレポート送信 - 最後のActive Health Systemレポートの日時。
- 最新のActive Health Systemレポート送信のステータス - 最新データ送信のステータス。

Insight RS Console（Insight Remote Support Central Connectのみ）でのデータ収集ステータスの表示

手順

1. Insight RS Consoleにログインします（https://<Insight RSホストサーバーのIPアドレスまたはFQDN>: 7906）。
2. デバイスページに移動します。
3. ご使用のサーバーを登録を見つけて、デバイス名をクリックします。
4. 構成情報収集タブをクリックします。

   収集タブには、構成情報収集およびActive Health Systemレポート情報について、次の名前が表示されます。「Server Basic Configuration Collection」と「Active Health Service Collection」という名前が使用されます。収集を展開するには、結果アイコンの左にあるプラス記号（＋）をクリックします。追加情報を表示する、または収集ファイルをダウンロードするには、詳細をクリックします。

   Insight RSでは、iLOデータ送信日時の値が、Insight RS Consoleへのアクセスに使用されているブラウザーのタイムゾーンに変換されます。

サポートされるデバイスのリモートサポート設定の変更

サブトピック

サポートされるデバイスのDirect ConnectからCentral Connectリモートサポートへの変更

サポートされるデバイスのDirect ConnectからCentral Connectリモートサポートへの変更

手順

1. Insight Online Direct Connectからデバイスを登録解除します。
2. Insight Remote Support Central Connectのためにデバイスを登録する正しい時間を決定します。

   iLOとInsight RSホストサーバーが異なるタイムゾーンを使用していて、Insight RSホストサーバーが、iLOより早いタイムゾーンを使用している場合は、デバイスをすぐに再登録しないでください。Insight RSホストサーバーの時刻が、デバイスを登録解除した時刻と同じか、それよりも遅くなるまで待ちます。

   たとえば、iLOシステムをフランスの現地時間に設定し、ホストサーバーをカリフォルニアの現地時間に設定したとします。フランスで現地時間午後5時にデバイスの登録を解除した場合、カリフォルニアでは現地時間午後5時まで待ってからデバイスをInsight Remote Support Central Connectに登録する必要があります。待たない場合、デバイスはInsight Online（有効な場合）に表示されません。
3. 該当する場合は、手順2で決められた時刻まで待ちます。
4. Insight Remote Support Central Connectにデバイスを登録します。

詳しくは

Insight Remote Support Central Connectの登録

iLOの管理機能の使用

サブトピック

iLOユーザーアカウント

iLOディレクトリグループ

ブート順序

ライセンスキーのインストール

iLOでのリモートキーマネージャーの使用

言語パック

ファームウェア検証

Smart Update ManagerをWindows上で使用してカスタムISOを作成する

iLOユーザーアカウント

iLOでは、セキュアメモリにローカルで保存されているユーザーアカウントを管理できます。

ユーザー指定のログイン名と高度なパスワード暗号化を使用してローカル ユーザー アカウントを最大12個作成することができます。権限は各ユーザーの設定を制御し、ユーザーのアクセス要件に合わせてカスタマイズできます。

13ユーザー以上をサポートするには、ディレクトリサービスを使用してユーザーの認証や権限付与を行うようiLOを構成します。

サブトピック

ローカルユーザーアカウントの追加

ローカルユーザーアカウントの編集

ユーザーアカウントの削除

iLOユーザーアカウントオプション

iLOユーザーアカウントの権限

iLOユーザーアカウントロール

パスワードに関するガイドライン

IPMI/DCMIユーザー

ユーザーアカウントの表示

詳しくは

iLOのディレクトリの認証と認可設定

ローカルユーザーアカウントの追加

前提条件

ユーザーアカウント管理権限

手順

1. ナビゲーションツリーでマネジメントをクリックします。

   ユーザー管理タブが表示されます。

2. 新規をクリックします。
3. 次の詳細を入力します。
   - ログイン名
   - ユーザー名
   - 新しいパスワードおよびパスワードの確認
4. （オプション）事前定義されたユーザー権限セットを選択するには、役割メニューで役割を選択します。

   手動で権限を選択する場合は、デフォルトの役割（カスタム）を使用します。

5. 手順4でカスタムを選択した場合 、次の権限から選択します。
   - ログイン
   - リモートコンソール
   - 仮想電源およびリセット
   - 仮想メディア
   - ホストBIOS
   - iLO設定の構成
   - ユーザーアカウント管理
   - ホストNIC構成
   - ホストストレージ構成
   - リカバリセット

   使用できるすべてのユーザーの権限を選択するには、すべてを選択チェックボックスをクリックします。

6. （オプション）アカウントをサポートされているアプリケーションのサービスアカウントとして使用する場合は、サービスアカウントチェックボックスを選択します。

   サポートされているアプリケーションには、iLO Amplifier Packがあります。

   サービスアカウントのプロパティは、最初のユーザーアカウントの作成時にのみ構成できます。既存のユーザーアカウントでこの設定を編集することはできません。

7. 新しいユーザーを保存するには、ユーザーの追加をクリックします。

   iLOはアカウントが追加されたことを通知します。

詳しくは

iLOユーザーアカウントオプション
iLOユーザーアカウントの権限
パスワードに関するガイドライン

ローカルユーザーアカウントの編集

前提条件

ユーザーアカウント管理権限

手順

1. ナビゲーションツリーでマネジメントをクリックします。

   ユーザー管理タブが表示されます。

2. ユーザーアカウントを選択し、編集をクリックします。
3. 必要に応じて、以下の値をアップデートします。
   - ログイン名
   - ユーザー名
4. パスワードを変更するには、パスワードを変更チェックボックスをクリックし、パスワードとパスワードの確認の値をアップデートします。
5. （オプション）ユーザーアカウントの権限を変更する場合は、次のいずれかを実行します。
   - 手動で権限を選択するには、役割メニューでカスタムを選択して、リストから権限を選択します。

     使用できるすべてのユーザーの権限を選択するには、すべてを選択チェックボックスをクリックします。
   - 事前定義されたユーザー権限セットを選択するには、役割メニューからAdministrator、Operator、またはReadOnlyを選択します。
6. ユーザーアカウントの変更を保存するには、ユーザーのアップデートをクリックします。

   iLOは、選択したアカウントがアップデートされたことを通知します。

詳しくは

iLOユーザーアカウントオプション
iLOユーザーアカウントの権限
パスワードに関するガイドライン

ユーザーアカウントの削除

前提条件

ユーザーアカウント管理権限

手順

1. ナビゲーションツリーで管理をクリックします。

   ユーザー管理タブが表示されます。

2. 1つまたは複数の削除するユーザーアカウントの横にあるチェックボックスを選択します。
3. 削除をクリックします。
4. 要求を確認するメッセージが表示されたら、はい、削除しますをクリックします。

   iLOは、選択されたアカウントが削除されたことを通知します。

iLOユーザーアカウントオプション

- ログイン名は、iLOにログインするときに使用する名前です。この名前は、ユーザー管理ページのユーザーリスト、セッ

ションリストページ、ユーザーアイコンをクリックしたときに表示されるメニュー、およびログに表示されます。ログイン名は、ユーザー名と同じである必要はありません。ログイン名の最大長は39文字です。ログイン名には印刷可能な文字を使用する必要があります。

- ユーザー名は、ユーザー管理ページのユーザーリストに表示されます。ログイン名と同じである必要はありません。ユーザー名の最大長は39文字です。ユーザー名には、印字可能な文字を使用する必要があります。わかりやすいユーザー名を割り当てると、各ログイン名の所有者を識別でき便利です。
- 新しいパスワードおよびパスワードの確認では、iLOにログインするために使用するパスワードを設定および確認します。
- 役割では、ユーザーアカウントを追加または編集するときに、事前定義されたユーザー権限セットを選択できます。カスタムオプションを使用して、カスタマイズされた権限セットを定義できます。
- サービスアカウントは、アカウントをサービスアカウントとして指定します。サービスアカウントは、iLOで動作するサポート製品で使用されます。

  サポートされているアプリケーションには、iLO Amplifier Packがあります。

  サービスアカウントのプロパティは、最初のユーザーアカウントの作成時にのみ構成できます。既存のユーザーアカウントでこの設定を編集することはできません。

iLOユーザーアカウントの権限

次の権限は、ユーザーアカウントに適用されます。

- ログイン - iLOにログインできます。
- リモートコンソール - ビデオ、キーボード、マウスの制御を含めホストシステムのリモートコンソールにアクセスできます。

  この権限を持つユーザーはBIOSにアクセスできるため、ホストベースのBIOS、iLO、ストレージ、およびネットワークタスクを実行できる場合があります。
- 仮想電源およびリセット - ホストシステムの電源再投入やリセットを実行できます。これらの操作はシステムの可用性を中断します。この権限を持つユーザーは、システムにNMIを生成ボタンを使用してシステムを診断できます。
- 仮想メディア - ホストシステム上の仮想メディア機能を使用できます。
- ホストBIOS - UEFIシステムユーティリティを使用してホストBIOS設定を構成できます。この権限は、アクティブなシステムROMを冗長システムROMで置き換えるために必要です。

  この権限は、ホストベースのユーティリティを使用した構成には影響しません。
- iLOの設定を構成 - セキュリティ設定を含むほとんどのiLO設定を構成し、iLOファームウェアをアップデートすることができます。この権限は、ローカルユーザーアカウント管理を有効にしません。

  iLOを構成したら、すべてのユーザーからこの権限を取り消して、次のインターフェイスからの再構成を防止します。

  - iLOのWebインターフェイス
  - iLO RESTful API
  - CLI
  - HPQLOCFG

  次のインターフェイスにアクセスできるユーザーは、引き続きiLOを再構成できます。

  - UEFIシステムユーティリティ
  - HPONCFG

ユーザーアカウント管理権限を持つユーザーのみが、この権限を有効または無効にすることができます。

- ユーザーアカウント管理 - ユーザーは、ローカルiLOユーザーアカウントを追加、編集、および削除できます。この権限を持つユーザーは、すべてのユーザーの権限を変更できます。この権限が割り当てられていないと、本人の設定の表示と本人のパスワードの変更しか実行できません。
- ホストNIC構成 - ホストNIC設定を構成できます。

  この権限は、ホストベースのユーティリティを使用した構成には影響しません。
- ホストストレージ構成 - ホストストレージ設定を構成できます。

  この権限は、ホストベースのユーティリティを使用した構成には影響しません。
- リカバリセット - ユーザーがシステムリカバリセットを管理できるようにします。

  デフォルトでは、リカバリセット権限はデフォルトのAdministratorアカウントに割り当てられます。この特権は、既にこの特権を持っているアカウントでアカウントを作成または編集することによってのみ、ユーザーアカウントに追加できます。

  リカバリセット特権を持つユーザーアカウントがなく、この特権を持つアカウントが必要な場合は、管理プロセッサーを工場出荷時のデフォルト設定にリセットしてください。工場出荷時のデフォルトリセットにより、リカバリセット特権を持つデフォルトの管理者アカウントが作成されます。

  システムメンテナンススイッチでiLOセキュリティが無効にされている場合、この権限を使用できません。

次の権限は、CLIまたはRIBCLスクリプトを介して使用できません。

- ホストNIC構成
- ホストストレージ構成
- リカバリセット
- ホストBIOS
- ログイン

次の権限は、UEFIシステムユーティリティのiLO6構成ユーティリティから使用できません。

- リカバリセット
- ログイン

iLOユーザーアカウントロール

Administrator
: リカバリセット以外のすべての権限を有効にします。

Operator
: iLO設定の構成、ユーザーアカウントの管理、およびリカバリセット以外のすべての権限を有効にします。

ReadOnly
: ログイン権限のみを有効にします。

カスタム（デフォルト）
: ユーザーがカスタム権限セットを定義できるようにします。

パスワードに関するガイドライン

Hewlett Packard Enterpriseでは、ユーザーアカウントを作成およびアップデートする場合に、以下のパスワードに関するガイドラインに従うことをお勧めします。

- パスワードを使用する場合：
  - パスワードをメモまたは記録しないでください。
  - パスワードの共有は避けてください。
  - 辞書に載っている言葉を組み合わせたパスワードを使用しないでください。
  - 推測しやすい単語を含むパスワードを使用しないでください。例えば、会社名、製品名、ユーザー名、ログイン名などです。
  - パスワードを定期的に変更します。
  - iLOデフォルト認証情報を安全な場所に保管します。
- 強化パスワードには、少なくとも以下の3つの特性が必要です。
  - 少なくとも1つの大文字ASCII文字
  - 少なくとも1つの小文字ASCII文字
  - 少なくとも1つのASCII数字
  - 少なくとも1つの他の文字タイプ（記号、特殊文字、句読点など）。

  アクセス設定ページのパスワードの複雑さ設定を有効にした場合、ユーザーアカウントを作成または編集するときにiLOによってこれらのパスワード特性が強制されます。
- ユーザーアカウントのパスワードの最低文字数は、アクセス設定ページで設定します。構成された最小パスワード長値によって、パスワードの長さは最小0文字（パスワードなし）から最大39文字まで可能です。Hewlett Packard Enterpriseでは、8文字以上の最小パスワード長を使用することをお勧めします。デフォルト値は8文字です。

> **重要:**
> 保護されたデータセンターの外側に拡大されることのない物理的に安全な管理ネットワークがない場合、最小パスワード長を8文字未満に設定しないでください。

詳しくは

iLOアクセス設定の構成
セキュリティガイドライン

IPMI/DCMIユーザー

iLOファームウェアは、IPMI 2.0仕様に準拠しています。IPMI/DCMIユーザーを追加する場合、ログイン名は最長16文字、パスワードは最長20文字です。

iLOユーザー権限を選択すると、等価なIPMI/DCMIユーザー権限が上記の設定に基づくIPMI/DCMI権限ボックスに表示されます。

- ユーザー - ユーザーは読み取り専用アクセス権を持っています。ユーザーは、iLOの設定または書き込みやシステムの操作は実行できません。

  IPMIユーザー権限については、すべての権限を無効にします。Operatorレベルを満たさない権限の任意の組み合わせは、IPMI Operatorです。
- Operator - Operatorは、システムの操作を実行できますが、iLOを設定したり、ユーザーアカウントを管理したりすることはできません。

  IPMIOperator権限については、リモートコンソール、仮想電源およびリセット、および仮想メディアを有効にします。Administratorレベルを満たさないOperator以上の権限の任意の組み合わせは、IPMI Operatorです。

- Administrator - Administratorは、すべての機能に対する読み取り/書き込みアクセス権を持っています。

  IPMI Administrator権限については、すべての権限を有効にします。

ユーザーアカウントの表示

手順

1. ナビゲーションツリーでマネジメントをクリックします。

   ユーザー管理ページが表示されます。

   ローカルユーザーテーブルには、各ローカルユーザーのログイン名、ユーザー名、および割り当てられている権限が表示されます。

   割り当てられた権限がチェックマークのアイコンで表示され、割り当てられていない権限がXアイコンで表示されます。

   サービスアカウントが構成されている場合、サービステーブルには、各サービスアカウントのログイン名、ユーザー名、および割り当てられている権限が表示されます。サービスアカウントが存在しない場合、このテーブルは表示されません。

2. （オプション）権限の名前を参照するには、カーソルを権限アイコン上に移動します。

詳しくは

iLOユーザーアカウントオプション
iLOユーザーアカウントの権限

iLOディレクトリグループ

iLOディレクトリグループは、Kerberos認証とスキーマフリーディレクトリの統合で使用されます。iLOは最大6つのディレクトリグループをサポートします。

詳しくは

iLOでのKerberos認証
スキーマフリーディレクトリ認証

ディレクトリグループの追加

前提条件

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

手順

1. ナビゲーションツリーで管理をクリックしてから、ディレクトリグループタブをクリックします。
2. 新規をクリックします。
3. グループ情報セクションで、以下の詳細を提供します。
   - グループDN
   - グループSID（Kerberos認証およびActive Directory統合のみ）

4. 次の権限のいずれかを選択します。
   - ログイン
   - リモートコンソール
   - 仮想電源およびリセット
   - 仮想メディア
   - ホストBIOS
   - iLOの設定を構成
   - ユーザーアカウント管理
   - ホストNIC構成
   - ホストストレージ構成
   - リカバリセット
5. 新しいディレクトリグループを保存するには、グループの追加をクリックします。

詳しくは

ディレクトリグループのオプション
ディレクトリグループ権限
Active Directoryの入れ子型グループ（スキーマフリー構成のみ）

ディレクトリグループの編集

前提条件

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

手順

1. ナビゲーションツリーで管理をクリックしてから、ディレクトリグループタブをクリックします。
2. ディレクトリグループセクションでグループを選択し、編集をクリックします。
3. グループ情報セクションで、以下の詳細を提供します。
   - グループDN
   - グループSID（Kerberos認証およびActive Directory統合のみ）
4. 次の権限のいずれかを選択します。
   - ログイン
   - リモートコンソール
   - 仮想電源およびリセット
   - 仮想メディア
   - ホストBIOS
   - iLOの設定を構成
   - ユーザーアカウント管理
   - ホストNIC構成

- ホストストレージ構成
- リカバリセット

5. ディレクトリグループの変更を保存するには、グループのアップデートをクリックします。

詳しくは

ディレクトリグループのオプション
ディレクトリグループ権限
Active Directoryの入れ子型グループ（スキーマフリー構成のみ）

ディレクトリグループの削除

前提条件

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

手順

1. ナビゲーションツリーで管理をクリックしてから、ディレクトリグループタブをクリックします。
2. 削除するディレクトリグループの横にあるチェックボックスを選択します。
3. 削除をクリックします。
4. 要求を確認するメッセージが表示されたら、はい、削除しますをクリックします。

   グループが削除されたことがiLOによって通知されます。

ディレクトリグループのオプション

各ディレクトリグループには、DN、SID、およびアカウントの権限が含まれます。Kerberosログインの場合、グループのSIDは、iLOに設定されているディレクトリグループのSIDと比較されます。ユーザーが複数のグループのメンバーである場合、そのユーザーアカウントにはすべてのグループの権限が付与されます。

グローバルグループおよびユニバーサルグループを使用して権限を設定できます。ドメインローカルグループは、サポートされていません。

ディレクトリグループをiLOに追加するときは、以下の値を設定します。

- グループDN（セキュリティグループDN） - このグループのメンバーには、グループに設定された権限が付与されます。ここで指定するグループは、ディレクトリに存在しなければならず、iLOにアクセスする必要があるユーザーは、このグループのメンバーでなければなりません。ディレクトリに存在するDNを入力します（たとえば、CN=Group1, OU=Managed Groups, DC=domain, DC=extension）。

  短縮されたDNもサポートされます（たとえば、Group1）。短縮されたDNは、一意に一致するものではありません。Hewlett Packard Enterpriseでは、完全修飾のDNを使用することをおすすめします。
- グループSID（セキュリティID） - MicrosoftセキュリティID（SID）は、Kerberosおよびディレクトリグループの権限付与に使用されます。この値は、Kerberos認証に必要です。必要な形式は、S-1-5-2039349です。

Active Directoryの入れ子型グループ（スキーマフリー構成のみ）

多くの組織では、ユーザーや管理者をグループ分けしています。このように整理すると、グループを1つまたは複数のiLOシステムに関連付けることができるので便利です。グループメンバーを追加または削除すると、構成をアップデートできます。

Microsoft Active Directoryでは、あるグループを別のグループ内に配置した入れ子型のグループの作成がサポートされています。

スキーマフリー構成では、間接メンバー（プライマリグループの入れ子型グループであるグループのメンバー）であるユーザーにiLOへのログオンが許可されます。

CAC Smartcard認証を使用する場合は、入れ子型グループがサポートされません。

ディレクトリグループ権限

- ログイン – ディレクトリユーザーがiLOにログインできます。
- リモートコンソール – ディレクトリユーザーが、ビデオ、キーボード、マウスの制御を含めて、ホストシステムのリモートコンソールにアクセスできます。

  この権限を持つユーザーはBIOSにアクセスできるため、ホストベースのBIOS、iLO、ストレージ、およびネットワーク構成タスクを実行できる場合があります。
- 仮想電源およびリセット – ディレクトリユーザーがホストシステムの電源再投入やリセットを実行できます。これらの操作はシステムの可用性を中断します。この権限を持つユーザーは、システムにNMIを生成ボタンを使用してシステムを診断できます。
- 仮想メディア – ディレクトリユーザーがホストシステム上の仮想メディア機能を使用できます。
- ホストBIOS – ディレクトリユーザーがUEFIシステムユーティリティを使用することでホストBIOS設定を構成できます。

  この権限は、ホストベースのユーティリティを使用した設定には影響しません。
- iLOの設定を構成 – ディレクトリユーザーはセキュリティ設定を含むほとんどのiLO設定を構成し、iLOファームウェアをアップデートすることができます。この権限は、ローカルユーザーアカウント管理を有効にしません。

  iLOを構成したら、すべてのユーザーからこの権限を取り消して、iLO Webインターフェイス、iLO RESTful API、HPQLOCFG、またはCLIによる再構成を防止します。UEFIシステムユーティリティまたはHPONCFGにアクセスできるユーザーは、引き続きiLOを再構成することができます。ユーザーアカウント管理権限を持つユーザーのみがこの権限を有効または無効にできます。
- ユーザーアカウント管理 – ディレクトリユーザーはローカルのiLOユーザーアカウントを追加、編集、および削除できます。
- ホストNIC構成 – ディレクトリユーザーがホストNIC設定を構成できます。

  この権限は、ホストベースのユーティリティを使用した設定には影響しません。
- ホストストレージ構成 – ディレクトリユーザーがホストストレージ設定を構成できます。

  この権限は、ホストベースのユーティリティを使用した設定には影響しません。
- リカバリセット – ディレクトリユーザーがシステムリカバリセットを管理できます。

  デフォルトでは、この権限はデフォルトの管理者アカウントに割り当てられます。この権限を別のアカウントに割り当てるには、すでにこの権限を持つアカウントでログインします。

  セッションを開始したときにシステムメンテナンススイッチがiLOセキュリティを無効にするように設定されている場合、この権限を使用できません。

ディレクトリグループの表示

手順

1. ナビゲーションツリーで管理をクリックしてから、ディレクトリグループタブをクリックします。

   ディレクトリグループテーブルには、各グループのグループDN、グループSID、および割り当てられた権限が表示されます。

   割り当てられた権限がチェックマークのアイコンで表示され、割り当てられていない権限がXアイコンで表示されます。
2. （オプション）権限の名前を参照するには、カーソルを権限アイコン上に移動します。

詳しくは

ディレクトリグループのオプション
ディレクトリグループ権限

ブート順序

ブート順序機能を使用すると、サーバーのブートオプションを設定できます。

ブートモード、ブート順序、あるいはワンタイムブートステータスの変更を行うと、サーバーのリセットが必要になります。リセットが必要な場合は、iLOによって通知されます。

サーバーがPOSTのときにサーバーのブート順序を変更しようとすると、エラーが発生します。POST中はブート順序を変更できません。このエラーが発生した場合、POSTが終了するのを待ってから、再試行してください。

Gen11以降では、UEFIブートモードのみがサポートされています。

サブトピック

サーバーブートモードの設定

サーバーブート順序の構成

ワンタイムブートステータスの変更

ROMベースユーティリティを次回のリセット時に起動

サーバーブートモードの設定

前提条件

- iLOの設定を構成する権限

このタスクについて

ブートモード設定を使用して、サーバーでOSブートファームウェアを検索する方法を定義します。UEFIモードを選択します。

手順

1. ナビゲーションツリーで管理をクリックして、ブート順序タブをクリックします。
2. Unified Extensible Firmware Interface (UEFI) を選択し、適用をクリックします。

   iLOに、変更の確認を求めるメッセージが表示されます。この設定を変更すると、サーバーをリセットするまで、ブート順序のページで変更を追加することはできません。
3. OKをクリックします。
4. サーバーをリセットします。

サーバーブート順序の構成

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーで管理をクリックして、ブート順序タブをクリックします。

仮想メディアが接続されると、iLOのWebインターフェイスのページ上部の仮想フロッピー/USBキーおよび仮想CD/DVD-ROMのテキストの横に仮想メディアタイプが表示されます。

2. デバイスのブート順序を上下に移動するには、サーバーのブート順序リストでデバイスを選択し、上へまたは下へをクリックします。

   UEFIモードでは、使用可能なブートデバイスのリストからオプションを選択します。

   > **注記:**
   > フロッピードライブはサポートされるiLO仮想メディアデバイスですが、ブート可能なデバイスとしてはサポートされていません。

3. 適用をクリックします。

   iLOによって、ブート順序が正常にアップデートされたことが確認されます。

ワンタイムブートステータスの変更

このタスクについて

ワンタイムブートステータス機能を使用して、定義済みのブート順序を変更せずに、次回のサーバーリセット時に起動するメディアタイプを設定します。

サブトピック

UEFIモードでのワンタイムブートステータスの変更

UEFIモードでのワンタイムブートステータスの変更

前提条件

- iLOの設定を構成する権限
- サーバーが、iLOファームウェアまたはシステムROMのアップデート後、再起動された。
- サーバーが、UEFIブートモードを使用するように構成された後、再起動された。

手順

1. ナビゲーションツリーで管理をクリックして、ブート順序タブをクリックします。
2. ワンタイムブートオプションを選択リストから、オプションを選択します。
3. ワンタイムブートオプションを選択リストでUEFI Targetを選択した場合、UEFI Targetオプションを選択：リストからブートデバイスを選択します。

   例えば、2つのブート可能パーティションがあるハードドライブがある場合、次回のサーバーリセットで使用するパーティションを選択できます。

4. 適用をクリックします。

   iLOは、ワンタイムブートオプションが正常にアップデートされたことを確認します。

   現在のワンタイムブートオプションの値がアップデートされ、選択内容が示されます。

サブトピック

UEFIモードのワンタイムブートオプション

UEFIモードのワンタイムブートオプション

次のUEFIモードワンタイムブートオプションがサポートされています。

> **注記:**
> フロッピードライブはサポートされるiLO仮想メディアデバイスですが、ブート可能なデバイスとしてはサポートされていません。

- ワンタイムブートなし
- CD/DVDドライブ
- USBストレージデバイス
- ハードディスクドライブ
- ネットワークデバイス - BIOSは、有効にされたネットワークデバイスがないかスキャンします。サーバーは、成功するまで、検出されたデバイスから一度に1つずつ起動を試みます。
- Intelligent Provisioning
- HTTP Boot - ブート可能イメージのURIがROMベースのシステムユーティリティで定義されている場合、サーバーはHTTP URIで起動します。

  このオプションは、ネットワーク設定の構成にDHCPサーバーを使用する構成でサポートされます。
- UEFI Target - このオプションを選択した場合、UEFI Targetオプションを選択リストの使用可能なブートデバイスの一覧から選択できます。
- Embedded UEFI Shell - サーバーは、UEFIシステムユーティリティから分離した組み込みシェル環境から起動します。
- 内蔵iPXE - サーバーは内蔵iPXEアプリケーションで起動します。

  内蔵iPXEは、システムBIOSに組み込まれたオープンソースのネットワークブートアプリケーションです。このオプションを使用して、ネットワークブートを実行できます。

ROMベースユーティリティを次回のリセット時に起動

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーで管理をクリックして、ブート順序タブをクリックします。
2. ROMベースのセットアップユーティリティを次回のサーバーのリセット時に読み込むには、システムセットアップユーティリティを起動をクリックします。

ライセンスキーのインストール

前提条件

- iLOの設定を構成する権限
- iLOライセンスが、そのライセンスをインストールするサーバーでサポートされている。

詳しくは、HPE iLOライセンスガイドを参照してください。

手順

1. ナビゲーションツリーで管理をクリックし、ライセンスタブをクリックします。
2. アクティベーションキーボックスにライセンスキーを入力します。

   アクティベーションキーボックスで、セグメント間でカーソルを移動するには、Tabキーを押す、またはボックスのセグメントの内側をクリックします。 アクティベーションキーボックスのセグメントにデータを入力すると、カーソルは自動的に次に進みます。

   すでにキーがインストールされているサーバー上でライセンスキーをインストールした場合、現在のキーは新しいキーに置き換えられます。

   ライセンスキーをインストールすると、iLOに最後の5桁のみが表示されます。Hewlett Packard Enterpriseでは、後で必要になる場合に備えて、ライセンスキー情報を記録して保存することをお勧めします。
3. インストールをクリックします。

   エンドユーザー使用許諾契約を読み、合意したことを確認するプロンプトがiLOで表示されます。

   エンドユーザー使用許諾契約の詳細は、ライセンスパックオプションキットに記載されています。
4. 同意するをクリックします。

   これで、ライセンスキーは有効になります。

サブトピック

ライセンス情報の表示

iLOライセンス

ライセンス情報の表示

手順

ナビゲーションツリーで管理をクリックし、ライセンスタブをクリックします。

サブトピック

ライセンスの詳細

ライセンスの詳細

- ライセンス – ライセンス名
- ステータス – ライセンスのステータス
- アクティベーションキー – インストールされているキー

  セキュリティ保護のため、ライセンスキーの下5桁のみが表示されます。

iLOライセンス

iLO標準機能はすべてのサーバーに搭載され、サーバーのセットアップ、サーバーヘルスの監視、電力および温度制御の監

視、およびリモートサーバー管理を簡素化します。

iLOライセンスは、マルチユーザーコラボレーション用のグラフィカルリモートコンソール、ビデオの録画と再生のような機能や他の多くの機能を有効にします。

- 製品をインストールして使用するサーバーごとに1つのiLOライセンスが必要です。
- ライセンスは譲渡できません。
- iLO AdvancedライセンスはSynergyコンピュートモジュールに自動的に付属します。
- iLO Advancedのライセンスは、2020年6月1日以降に出荷されたProLiant e910サーバーブレードに自動的に含まれています。
- ライセンスキーを失くした場合、HPE iLOライセンスガイドに記載されている、失くしたライセンスキーに対する手順に従います。
- 詳しくは、https://www.hpe.com/support/ilo-docsでHPE iLOライセンスガイドを参照してください。
  - 無料iLOトライアルライセンスの入手
  - ライセンスキーの購入、登録、引き換え。

iLOのライセンスキーを登録することの利点

ライセンスの登録は重要な手順です。以下のような利点があります。

- Hewlett Packard Enterpriseサポートセンターへのアクセス（https://www.hpe.com/support/hpesc）。
- マイHPEソフトウェアセンター Webサイトからのソフトウェアアップデートへのアクセス（https://www.hpe.com/downloads/software）。
- マイHPEソフトウェアセンター Webサイトから、1つの便利な場所ですべてのHewlett Packard Enterprise製品ライセンスを追跡（https://www.hpe.com/software/hpesoftwarecenter）。
- 重要な製品アラートの受信。
- 一意のHewlett Packard Enterpriseサポート契約ID（SAID）のアクティブ化。

  Hewlett Packard Enterpriseが迅速かつ個々に応じたサポートを提供できるように、SAIDはお客様を識別し、お客様の製品を追跡します。

> **注記:**
> 現時点のマイHPEソフトウェアセンターポータルでは、SAID契約を追跡しません。

iLOでのリモートキーマネージャーの使用

iLO6は、リモートキーマネージャーをサポートします。これは、HPEストレージコントローラーと組み合わせて使用できます。

リモートキーマネージャーは、データ暗号化キーの生成、保存、操作、制御、アクセスの監査を行います。これを使用して、ビジネスクリティカルで機密性のある保存済みデータの暗号化キーへのアクセスを保護し維持することができます。

iLOが、リモートキーマネージャーと他の製品との間のキー交換を管理します。iLOは、リモートキーマネージャーとの通信に、自身のMACアドレスに基づいた一意のユーザーアカウントを使用します。このアカウントを最初に作成するために、iLOは、管理者権限を持つ、リモートキーマネージャーに以前から存在する展開ユーザーアカウントを使用します。展開ユーザーアカウントについて詳しくは、リモートキーマネージャーのドキュメントを参照してください。

サブトピック

サポートされているキーマネージャー

リモートキー管理の構成

キーマネージャーサーバーの構成

キーマネージャー構成の詳細の追加

キーマネージャー構成のテスト

キーマネージャーイベントの表示

キーマネージャーログのクリア

サポートされているキーマネージャー

iLOは以下のキーマネージャーをサポートしています。

- Utimaco Enterprise Secure Key Manager（ESKM）4.0以降

  FIPSセキュリティ状態が有効になっている場合は、ESKM 5.0以降が必要です。

  注意:
  ESKMを使用する場合は、アップデートされたコード署名証明書が含まれているソフトウェアアップデートを必ずインストールしてください。必要なアップデートをインストールしないと、ESKMは2019年1月1日後に再起動するとエラー状態になります。詳しくは、**ESKMのドキュメント**を参照してください。

- Thales TCT KeySecure for Government G350v（旧称SafeNet AT KeySecure G350v 8.6.0）
- Thales KeySecure K150v（旧称SafeNet KeySecure 150v 8.12.0）
- Thales CipherTrust Manager 2.2.0、K170v（仮想）およびK570（物理）アプライアンス

注記:
CNSAセキュリティ状態を使用するようiLOが構成されている場合、キーマネージャーの使用はサポートされません。

リモートキー管理の構成

手順

1. キー管理ソフトウェアをキーサーバーにインストールして構成します。
   a. ローカルユーザーを作成します。
   b. ローカルグループを作成します。
   c. マスターキーを作成します。

   詳しくは、サポートされているキーマネージャーソフトウェアのドキュメントを参照してください。
2. リモートキー管理をサポートするようにiLOを構成します。
   a. キーマネージャーサーバーを構成します。
   b. キーマネージャー構成の詳細を追加します。
   c. （オプション）キーマネージャーの構成をテストします。
3. リモートキー管理モードで動作するように、サポートされているデバイスを構成します。
   - NVMeドライブについては、UEFIシステムユーティリティユーザーガイドを参照してください。
   - MRXXXストレージコントローラーについては、HPE MegaRAID MRコントローラーユーザーガイドを参照してくださ

い。

これらのドキュメントは、Webサイトhttps://www.hpe.com/support/hpescで入手できます。

4. （オプション）SRXXXストレージコントローラーの場合のみ：iLOのストレージ情報ページで、暗号化ステータスが暗号化済と表示されていることを確認します。

キーマネージャーサーバーの構成

前提条件

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

手順

1. ナビゲーションツリーで管理をクリックして、キーマネージャータブをクリックします。
2. （キーマネージャーサーバーセクション内）をクリックします。

   キーマネージャーサーバー設定を編集ページが開きます。
3. 次の情報を入力します。
   - プライマリキーサーバーアドレス
   - プライマリキーサーバーポート
   - セカンダリキーサーバーアドレス
   - セカンダリキーサーバーポート
4. （オプション）プライマリおよびセカンダリキーサーバーを使用した構成でサーバーの冗長化を確認するには、冗長化が必要オプションを有効にします。

   Hewlett Packard Enterpriseでは、このオプションを有効にすることをお勧めします。
5. OKをクリックします。

   Thales CipherTrust Manager 2.2.0について詳しくは、[Remote Key Manager Support for Cipher Trust Manager](#)構成ガイドを参照してください。

サブトピック

[キーマネージャーサーバーのオプション](#)

キーマネージャーサーバーのオプション

プライマリキーサーバーアドレス

プライマリキーサーバーのホスト名、IPアドレス、またはFQDN。この文字列の最大長は79文字です。

プライマリキーサーバーポート

プライマリキーサーバーポート。

セカンダリキーサーバーアドレス

セカンダリキーサーバーのホスト名、IPアドレス、またはFQDN。この文字列の最大長は79文字です。

セカンダリキーサーバーポート

セカンダリキーサーバーポート。

冗長化が必要

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

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

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

キーマネージャー構成の詳細の追加

前提条件

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

手順

1. ナビゲーションツリーで管理をクリックして、キーマネージャータブをクリックします。
2. （キーマネージャー構成セクション内）をクリックします。

   キーマネージャー構成設定を編集ページが開きます。
3. 次の情報をキーマネージャー上のiLOアカウントセクションに入力します。
   - アカウントグループ
   - （オプション）キーマネージャーローカルCA証明書名

   アカウント名の値は読み取り専用です。
4. 次の情報をキーマネージャー管理者アカウントセクションに入力します。
   - ログイン名
   - パスワード
5. OKをクリックします。

   iLOは情報要求をキーマネージャーサーバーに送信します。
   - ilo-<iLOのMACアドレス>というアカウント名が存在しない場合：
     - キーマネージャー管理者アカウントセクションで入力したユーザーアカウントが、アカウント名を作成して、キーマネージャーのローカルユーザーとその生成済みパスワードに関連付けます。
     - アカウント名は、手順3で入力したアカウントグループに追加されます。
   - ilo-<iLOのMACアドレス>というアカウント名が存在する場合：
     - キーマネージャー管理者アカウントセクションで入力したユーザーアカウントが、キーマネージャーのローカルユーザーにアカウント名を関連付けて、新しいパスワードが生成されます。

- キーマネージャー管理者アカウントセクションで入力したユーザーアカウントが、ilo-<iLOのMACアドレス>アカウントに関連付けられたアカウントグループのメンバーでない場合、そのアカウントがアカウントグループに追加されます。
- ilo-<iLOのMACアドレス>がすでに、キーマネージャーのローカルグループのメンバーである場合、手順3で入力したグループは無視されます。キーマネージャーでの既存のグループ割り当てが使用され、 iLOのWebインターフェイスに表示されます。新しいグループの割り当てが必要な場合は、iLO設定をアップデートする前にキーマネージャーをアップデートする必要があります。

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

サブトピック

キーマネージャー構成の詳細

キーマネージャー構成の詳細

アカウント名

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

アカウントグループ

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

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

キーマネージャーローカルCA証明書名

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

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

ログイン名

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

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

パスワード

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

キーマネージャー構成のテスト

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- キーマネージャーがセットアップされ、iLOでキーマネージャーの構成が完了している。

このタスクについて

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

- キーマネージャーソフトウェアのバージョンがiLOと互換性があることを確認します。
- TLSを使用してプライマリキーマネージャーサーバー（および構成されている場合はセカンダリキーマネージャーサーバー）に接続します。
- 構成済みの認証情報およびアカウントを使用して、キーマネージャーに認証します。

手順

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

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

キーマネージャーイベントの表示

前提条件

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

手順

1. ナビゲーションツリーで管理をクリックして、キーマネージャータブをクリックします。
2. キーマネージャーイベントセクションまでスクロールします。

   各イベントがタイムスタンプと説明とともに一覧表示されます。

キーマネージャーログのクリア

前提条件

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

手順

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

   iLOが要求を確認するように求めます。
3. はい、クリアしますをクリックします。

言語パック

言語パックを使用すると、iLOのWebインターフェイスの表示言語を英語から、ユーザーが希望するサポート言語に変更できます。言語パックは、iLO Webインターフェイスと統合リモートコンソールの翻訳を提供します。

言語パックを使用する場合は、以下の点に注意してください。

- 提供されている言語パックは、日本語と簡体字中国語です。
- 英語版はアンインストールできません。
- 複数の言語パックをインストールできます。

  言語パックがインストールされている場合、同じ言語の新しい言語パックをインストールすると、インストールされている言語パックが置き換わります。
- 統合リモートコンソールは、現在のiLOセッションの言語を使用します。
- インストールされている言語パックにテキスト文字列の翻訳が含まれていない場合、テキストは英語で表示されます。
- iLOファームウェアをアップデートする場合は、Hewlett Packard Enterpriseでは言語パックの内容がiLOのWebインターフェイスに対応するように、最新の言語パックをダウンロードすることをおすすめします。

iLOがセッションの言語を決定する方法

iLOは、次のプロセスに基づいてWebインターフェイスセッションの言語を決定します。

1. iLO Webインターフェイスへのログインに使用するコンピューターおよびブラウザーが前回と同じで、ユーザーがCookieを消去していない場合は、当該のiLOプロセッサーとの最後のセッションの言語設定が使用されます。
2. Cookieがない場合は、現在のブラウザーの言語が使用されます。ただし、その言語がiLOでサポートされ、必要な言語パックがインストールされていなければなりません。
3. Cookieがなく、ブラウザーの言語もOSの言語もサポートされていない場合、iLOは設定済みのデフォルト言語を使用します。

フラッシュファームウェア機能で言語パックをインストール

前提条件

iLOの設定を構成する権限

手順

1. 次のWebサイトから言語パックをダウンロードします。https://www.hpe.com/support/ilo6
2. 言語パックの`LPK`ファイルを抽出します。
   - Windowsコンポーネントの場合：ダウンロードしたファイルをダブルクリックし、解凍ボタンをクリックします。ファイルを抽出する位置を選択して、OKをクリックします。
   - Linuxコンポーネントの場合：ファイル形式によって異なりますが、次のいずれかのコマンドを入力します。
     - `#rpm2cpio <language_pack_file_name>.rpm | cpio -id`

   言語パックのファイル名は次のような形式です。`lang_<言語>_<バージョン>.lpk`
3. ナビゲーションツリーでファームウェア & OSソフトウェアをクリックし、ファームウェアアップデートクリックします。

   フラッシュファームウェアコントロールが表示されます。
4. 使用するブラウザーに応じて、参照またはファイルの選択をクリックします。
5. `lang_<言語>_<バージョン>.lpk`を選択し、開くをクリックします。
6. （オプション）言語パックファイルのコピーをiLOレポジトリに保存するには、同様に、iLOレポジトリに保存チェックボックスを選択します。
7. フラッシュをクリックします。

iLOは、インストール要求の確認を求めるメッセージを表示します。

8. OKをクリックします。

   iLOによって言語パックがインストールされ、リセットを開始し、ブラウザー接続が終了します。

   接続が再確立されるまでに、数分かかることがあります。

詳しくは

ファームウェアおよびソフトウェアの表示および管理

言語パックの選択

このタスクについて

次のいずれかの方法を使用して、インストール済みの言語パックを選択します。

手順

- ログインページに移動し、言語メニューで言語を選択します。
- iLOのWebインターフェイスページの一番上にある言語アイコンをクリックして、言語を選択します。
- ナビゲーションツリーで管理をクリックし、言語タブをクリックします。インストールされた言語リストで言語をクリックします。

デフォルト言語設定の構成

前提条件

- iLOの設定を構成する権限
- 使用する言語の言語パックがインストールされていること。
- 使用する言語がブラウザーにインストールされ、他のインストール済みのブラウザー言語よりもこの言語が優先されるように設定されていること。

このタスクについて

このiLOファームウェアインスタンスのユーザー用のデフォルト言語を構成するには、以下の手順に従います。

手順

1. ナビゲーションツリーで管理をクリックして、言語タブをクリックします。
2. デフォルト言語メニューで値を選択します。

   選択できる言語は英語です。英語以外の言語も言語パックがインストールされていれば選択できます。

3. 適用をクリックします。

   デフォルト言語が変更されたことが、iLOによって通知されます。

   以降のiLO Webインターフェイスセッションでは、前のセッションからのブラウザーのCookieがなく、ブラウザーまたはOSの言語をサポートしていない場合、iLO Webインターフェイスに構成済みのデフォルト言語を使用します。

詳しくは

フラッシュファームウェア機能で言語パックをインストール

現在のiLO Webインターフェイスセッション言語の構成

前提条件

使用する言語の言語パックがインストールされていること。

手順

1. ナビゲーションツリーで管理をクリックして、言語タブをクリックします。

2. インストールされた言語リストで言語の名前をクリックします。

   現在のブラウザーセッションのiLO Webインターフェイスが、選択された言語に変更されます。

詳しくは

フラッシュファームウェア機能で言語パックをインストール

言語パックのアンインストール

前提条件

- iLOの設定を構成する権限
- 削除する言語がデフォルト言語として構成されていません。
- 削除する言語が言語パックとしてインストールされました。英語は削除できません。

手順

1. ナビゲーションツリーで管理をクリックして、言語タブをクリックします。
2. 削除する言語の横にある をクリックします。
3. 要求を確認するメッセージが表示されたら、はい、削除をクリックします。

   iLOによって選択した言語パックが削除され、再起動し、ブラウザー接続が終了します。

   接続が再確立されるまでに、数分かかることがあります。

ファームウェア検証

ファームウェア検証機能では、オンデマンドスキャンを実行したり、スケジュールされたスキャンを実施できます。

検出された問題に対処するために、iLOを次のように構成できます。

- 結果を記録する。
- 結果を記録し、リカバリインストールセットを使用する修復処置を開始する。

スキャン結果に応じて、情報はActive Health Systemログとインテグレーテッドマネジメントログに記録されます。

次のファームウェアタイプがサポートされています。

- iLOファームウェア
- システムROM（BIOS）
- システムプログラマブルロジックデバイス（CPLD）
- サーバープラットフォームサービス（SPS）ファームウェア（サポート対象のサーバーのみ）
- サーバープラットフォームサービスのフルリカバリイメージ（サポート対象のサーバーのみ）

ファームウェア検証スキャンの実行中は、ファームウェアアップデートをインストールしたり、iLOレポジトリにファームウェアをアップロードしたりすることはできません。

無効なiLOまたはシステムROM（BIOS）のファームウェアが検出された場合は、無効なファイルがiLOレポジトリの隔離領域に保存されます。無効なファイルをダウンロードし、その種類と発生元を調べることができます。隔離されたイメージはiLOレポジトリページに表示されず、フラッシュファームウェア機能を使用すると選択できません。

破損したサーバープラットフォームサービス（SPS）記述子が検出された場合、破損したファームウェアイメージはiLOレポジトリの隔離領域に移動します。サーバープラットフォームサービスのフルリカバリイメージがシステムリカバリセットにあり、ファームウェア検証ページでログおよび自動的に修復が選択されている場合、リカバリが自動的に実行されます。リカバリが実行されると、イベントがIMLとセキュリティログに記録されます。破損したSPS記述子の自動リカバリには、iLO Advancedライセンスが必要です。

サポートされる管理ツールがシステムリカバリイベントをリスンするように構成されている場合は、リカバリイベントをこのページから送信できます。

ファームウェア検証設定の構成

前提条件

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

手順

1. 管理ページに移動し、ファームウェア検証タブをクリックします。
2. スキャン設定アイコン ☼ をクリックします。
3. バックグランドスキャンを有効を有効または無効の状態に設定します。
4. 整合性障害のアクションを選択します。
5. スキャン間隔を日数で設定します。

   有効な値は1～365日です。
6. 送信をクリックします。

ファームウェア検証スキャンオプション

オンデマンドスキャンオプションは、サポートされているプラットフォームでのみ使用できます。

- バックグランドスキャンを有効 - ファームウェア検証スキャンを有効または無効にします。有効なとき、iLOがサポート対象のインストールファームウェアでファイル破損をスキャンします。
- 整合性障害のアクション - ファームウェア検証スキャン中に問題が見つかったときiLOが実行するアクションを決定します。
  - 結果を記録するには、ログのみを選択します。
  - 結果を記録して修復アクションを開始するには、ログおよび自動的に修復を選択します。

    サポート対象のファームウェアタイプについて問題が検出された場合、iLOが保護されたインストールセットで影響を受けるファームウェアタイプがあるかを調べます。デフォルトでは、このセットはリカバリセットです。ファームウェアイメージを使用可能な場合、iLOがそのファームウェアイメージをフラッシュして修復を完了します。
- スキャン間隔（日数） - バックグラウンドスキャン頻度（日数）を設定します。有効な値は1～365です。

詳しくは

システムリカバリセット

ファームウェア検証スキャンの実行

前提条件

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

手順

1. 管理ページに移動し、ファームウェア検証タブをクリックします。

2. スキャンを実行をクリックします。

   ファームウェア検証スキャンの実行中は、ファームウェアアップデートをインストールしたり、iLOレポジトリにファームウェアをアップロードしたりすることはできません。

   スキャン結果がページの上部に表示されます。

   障害が発生した場合、ファームウェア検証ページのファームウェアの状態が障害/オフラインに変わり、システムヘルスのステータスがクリティカルに変わり、イベントがIMLに記録されます。ファームウェア検証スキャン機能がログおよび自動的に修復に構成されている場合は、障害が発生したファームウェアはフラッシュされます。成功すると、ファームウェアの状態とシステムヘルスのステータスがアップデートされ、IMLイベントは修正済みステータスに変わります。

   自動修復が構成されていない場合は、手動で修復を実行する必要があります。

ファームウェアヘルスステータスの表示

前提条件

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

手順

管理ページに移動し、ファームウェア検証タブをクリックします。

ファームウェアヘルスステータスの詳細

サポートされる各ファームウェアタイプについて、次の情報が表示されます。

ファームウェア名

インストールされているファームウェアの名前。

ファームウェアバージョン

ファームウェアバージョン。

ヘルス

ファームウェアのヘルスステータス。

状態

ファームウェアのステータス。値には、以下のものがあります。

- 有効 - ファームウェアは検証されており、有効です。
- スキャニング - ファームウェア検証スキャンが進行中か、起動しようとします。
- フラッシング - ファームウェアアップデートが進行中です。
- 障害/オフライン - ファームウェアは検証できず、修復されませんでした。

リカバリセットバージョン

システムリカバリセットのファームウェアのバージョン。

このファームウェアタイプがシステムリカバリセットにない場合や、システムリカバリセットがない場合は、存在しませんが表示されます。

隔離されたファームウェアの表示

前提条件

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

手順

管理ページに移動し、ファームウェア検証タブをクリックします。

隔離されたファームウェアファイルは、隔離セクションに表示されます。

隔離されたファイルがない場合は、`There are no items under quarantine`（検疫中のアイテムはありません。）というメッセージが表示されます。

隔離されたファームウェアの詳細

隔離セクションには、無効なファームウェアファイルに関する以下の情報が表示されます。

名前

無効なファームウェアファイルの名前。

作成日

無効なファイルの作成日。

サイズ

無効なファイルサイズ。

個々の隔離されたファイルの詳細

リストのファイルをクリックすると、以下の詳細が表示されます。

- 名前 - 隔離されたファイルの名前。
- 作成日 - 無効なファイルの作成日。
- ファイル名 - iLOレポジトリによって使用される名前。
- イメージの URI - 隔離されたファイルの場所。
- サイズ - 無効なファイルサイズ。
- デバイス クラス - iLOレポジトリのリソースとファームウェアのインベントリデータの間で関係付ける際に使用可能なID。

隔離されたファームウェアのダウンロード

前提条件

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

このタスクについて

iLOレポジトリのQuarantineエリアにファイルを保存するかどうか、オフライン分析のためにファイルをダウンロードすることができます。

手順

1. 管理ページに移動し、ファームウェア検証タブをクリックします。
2. 隔離セクションで、ダウンロードするファイルの横にある をクリックします。

   ステータスメッセージには、ダウンロードの進捗状況が表示されます。
3. ファイルを保存または開くには、ブラウザーの指示に従います。

隔離されたファームウェアの削除

前提条件

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

手順

1. 管理ページに移動し、ファームウェア検証タブをクリックします。
2. 隔離セクションで、削除するファイルの横にある🗑 をクリックします。

   iLOが要求を確認するように求めます。
3. はい、削除をクリックします。

フルシステムリカバリの開始

前提条件

- iLOの設定を構成する権限
- 仮想メディア権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- システムリカバリセットがiLOレポジトリに存在する。
- サポートされる管理ツール（iLO Amplifier Pack 1.15以降など）がサーバーを管理するように構成されている。

このタスクについて

別の管理ツールを起動してフルシステムリカバリを開始するリカバリイベントを、iLOを使用して生成することができます。リカバリは、サーバーオペレーティングシステムのイメージの再構築に続き、システムリカバリセットのインストールを含めます。

> △ **注意:**
> サーバーのイメージの再構築によって、既存のデータが失われる場合があります。

手順

1. リカバリプロセスに、サーバーのシャットダウンが必要なコンポーネントが含まれている場合は、サーバーをシャットダウンします。
2. 管理ページに移動し、ファームウェア検証タブをクリックします。
3. リカバリイベントを送信をクリックします。
4. リカバリイベントを送信ペインで、はい、リカバリイベントを作成しますチェックボックスを選択して、リカバリイベントを送信をクリックします。

   リカバリイベントは、リカバリイベントをリスンするように構成されている管理ツールに送信されます。

   イベントが正常に送信されると、以下の情報イベントがIMLに記録されます。

   `Firmware recovery is requested by Administrator.`（管理者がファームウェアリカバリを要求しています。）

詳しくは

システムリカバリセット

Smart Update Managerを使用してWindows上でカスタムISOを作成する

このタスクについて

> **注記:** HPE Smart Update Manager（SUM）は、HTTPサーバーを起動し、そのサーバーと通信するためのブラウザーを開始します。ポート63001～63002をブロックしないでください。

詳しくは、Smart Update Managerユーザーガイドを参照してください。

手順

1. サポートされるService Pack for ProLiant、Synergy Service Pack、またはSynergyカスタムSPPをダウンロードしてベースラインとして使用します。ファームウェアバンドルを仮想CDドライブにマウントします。
2. 必要なすべての追加コンポーネント（ファームウェアとドライバー）を、必要な署名ファイルと一緒にダウンロードします。
3. ダウンロードしたファイルを1つのローカルフォルダーにコピーします。
4. マウントされたファームウェアバンドルの最上位フォルダーから、`.\launch_sum.bat`コマンドを実行します。Smart Update Managerがブラウザーで開きます。
5. メインメニューから、ベースラインライブラリを選択します。ベースラインインベントリが自動的に開始されます。ベースラインインベントリが完了するのを待ちます（ローカルシステムからこのバンドルのインベントリを初めて作成するときはさらに時間がかかります）。

   ベースラインインベントリが自動的に開始されなかった場合：

   a. ベースラインを追加をクリックし、位置の詳細に、マウントされたファームウェアバンドルからのパッケージパスを入力します。（例：F:¥packages）。
   b. 追加をクリックします。ベースラインインベントリが追加されます。
6. ベースラインを追加をクリックして、追加コンポーネントフォルダーを（カスタムではなく）ベースラインとして追加します。
7. 位置の詳細で、追加コンポーネントフォルダーの場所を入力し、追加をクリックします。

   期待されるすべての追加コンポーネントとバージョンが存在することを確認します。
8. メニューからアクション、次にカスタムを作成オプションを選択します。
9. 以下のオプションを入力します：
   - 説明
   - バージョン
   - ターゲットの位置（空のフォルダーが必要）
   - ブート可能なISOファイルの作成（はい - チェック済み）
   - 解凍したソースISOの位置（起動しているファームウェアバンドル仮想CDの最上位フォルダー）

   注記: バージョン文字列では日付が必須です。日付をクリックして日付を編集します。
10. ステップ1 - ベースラインのソースで、元のベースラインと追加のベースラインの両方が選択されていることを確認します。
11. **重要**: カスタムISOが使用できなくなる可能性があるため、他のコンポーネントを削除しないでください。

    オプションで、ステップ3 - レビューで、フィルター適用をクリックして、追加ファームウェアとドライバーが選択されていることを確認します。元のベースラインに競合するパッケージがある場合は、それらをクリアできます。
12. ISOの作成をクリックし、次にクリックしますベースラインの保存をクリックします。このプロセスは、完了するまでにかなりの時間がかかります。

    このプロセスが完了すると、次のメッセージが表示されます。

    ```
    ベースラインは正常に保存されました。ISOの作成は成功しました。ベースラインは正常に追加されました。
    ```

    変更を失うことなくダイアログボックスを閉じることができます。ISOファイルが作成された後：
    - SUMは、新しく作成されたファームウェアバンドルのインベントリを作成します。

- ISOファイル名はbp-date-version.isoになります。得られたISOファイルの名前を変更できます。内容を保持する必要はありません。マウントされたISOのタイトルは、元のファームウェアバンドル名を保持します。
- ISOファイルはターゲットの位置にその構成内容と一緒にあります。オプションで、キーワードまたはバージョンを検索して、追加コンポーネントがISOインベントリの一部であることを確認します。

  この時点で、仮想CDをマウントしてコンテンツを調べることができます。適切なコンピュートモジュールを使用してISOを起動することもできます。

iLOのセキュリティ機能の使用

サブトピック

セキュリティガイドライン

iLOをセットアップして使用する場合は、セキュリティを最大化するために、次のガイドラインを考慮してください。

- 専用の管理ネットワーク上にiLOを構成します。

  Hewlett Packard Enterpriseでは、データネットワークとは別のプライベート管理ネットワークを確立することをお勧めします。管理ネットワークは、管理者のみがアクセスできるように構成します。

共有ネットワークにiLOデバイスを接続する場合、iLOデバイスを個々のサーバーと考え、それらのデバイスをセキュリティおよびネットワークの監査対象に含まれるようにします。

- iLOは、インターネットに直接接続しないでください。

  iLOプロセッサーは、運用管理ツールであり、インターネットのゲートウェイではありません。ファイアウォール保護を提供する企業VPNを使用してインターネットに接続します。

  > **重要:**
  > iLOがインターネットに直接接続されている場合、iLOユーザーアカウントのパスワードをすぐに変更してください。

- 認証機関（CA）によって署名されたSSL証明書をインストールして、デフォルトの自己署名証明書を置き換えてください。

  SSL証明書情報ページでこのタスクを実行できます。

- 信頼済みCA証明書をインストールして、LDAPなどの外部サービスの証明書の検証を有効にします。
- デフォルトのユーザーアカウントを含め、ユーザーアカウントのパスワードを変更します。

  サーバーの管理者パスワードと同じガイドラインに従ってiLO管理パスワードを変更してください。

  このタスクは、ユーザー管理ページからも実行できます。

  > **重要:**
  > ユーザーアカウントを作成およびアップデートする場合、iLOユーザーアカウントのパスワードに関するガイドラインに従います。

- すべての権限を持つユーザーアカウントを作成する代わりに、権限の数が少ないアカウントを複数作成します。
- iLOおよびサーバーファームウェアを常に最新の状態に保持します。
- できればTwo-Factor認証の認証サービス（Active DirectoryやOpenLDAPなど）を使用します。

  この機能により、ネットワーク全体で同じログインプロセスを使用して認証および承認を行うことができます。同時に複数のiLOデバイスを制御する方法を提供します。ディレクトリは、時刻と位置に基づく非常に特殊なロールおよび権限で、iLOへのロールベースのアクセスを提供します。

- Two-Factor認証を実装します。

  この機能により、さらにセキュリティが強化されます。特に、リモートで、またはローカルネットワークの外で接続できる場合に有効です。

- SNMPトラフィックを保護します。

  管理パスワードと同じガイドラインに従ってコミュニティストリングをリセットします。また、特定の送信元と送信先のアドレスのみを受け入れるようにファイアウォールまたはルーターを設定します。必要ない場合は、サーバーでSNMPを無効にします。

- 使用しないポートおよびプロトコル（SNMPやIPMI/DCMI over LANなど）を無効にします。

  アクセス設定ページでこのタスクを実行できます。

- .NETリモートコンソールにHTTPSを使用します。

  このオプションを構成するには、認証局（CA）によって署名された信頼済みのSSL証明書をインストールし、IRCはiLO内の信頼済みの証明書を要求します設定を有効にします。

  これらの構成手順は、それぞれ、セキュリティタブのSSL証明書情報ページとリモートコンソール&メディアページで完了することができます。

- 使用しない機能（リモートコンソールなど）を無効にします。

  アクセス設定ページでこのタスクを実行できます。

- サーバーOSコンソールを自動的にロックするようにリモートコンソールを構成します。

  このオプションを構成するには、リモートコンソール&メディアページのセキュリティタブにある、リモートコンソールのコンピューターロック設定を構成します。

- 暗号化設定ページで、より高いセキュリティ状態を構成してください。
- UEFIシステムユーティリティでiLO6構成ユーティリティを無効にするか、ユーザーがアクセスする場合にログイン認証情報を要求するようにiLOを構成します。

  アクセス設定ページでこのタスクを実行できます。

- 認証エラーを記録するようiLOを構成します。

  アクセス設定ページでこのタスクを実行できます。

- ファームウェア検証スキャンを有効にします。

  このタスクは、ファームウェア検証ページで実行できます。

- セキュリティダッシュボードページを使用して、セキュリティリスクと推奨事項を監視します。
- セキュリティログを使用して、セキュリティ関連のイベントを監視します。
- ホスト認証が必要機能を有効にします。

  アクセス設定ページでこのタスクを実行できます。

- ダウングレードポリシーを、ダウングレードにはリカバリセットの権限が必要ですに設定します 。

  アクセス設定ページでこのタスクを実行できます。

- リカバリセットを最新の状態に保ちます。
- HTTP接続経由のアクセスを防ぐようにiLOを構成します。

  この動作を構成するには、認証局（CA）によって署名された信頼済みのSSL証明書をインストールし、IRCはiLO内の信頼済みの証明書を要求します設定を有効にします。

  これらの構成手順は、それぞれ、セキュリティタブのSSL証明書情報ページとリモートコンソール&メディアページで完了することができます。

  この構成では、iLO Webインターフェイスにアクセスすると、iLOが応答ヘッダーでHTTP Strict Transport Security（HSTS）フラグを返します。これにより、ブラウザーはHTTP要求をHTTPSに自動的にリダイレクトできます。

詳しくは、次を参照してください。

- **HPE iLO 6の上位10のセキュリティ設定**。
- **HPE iLO 6の推奨されるセキュリティ設定**。
- 次のWebサイトにあるHPE Gen11以降のセキュリティリファレンスガイド：**https://www.hpe.com/support/ilo-docs**

重要なセキュリティ機能

次のWebインターフェイスページで、iLOセキュリティ機能を設定します。

アクセス設定

- iLOインターフェイスおよび機能を有効または無効にします。
- iLOが使用するTCP/IPポートをカスタマイズします。
- 認証失敗ログおよび遅延を設定します。

- iLO6構成ユーティリティを保護します。

iLOサービスポート

iLOサービスポートの可用性、認証、およびサポートされるデバイスを構成します。

セキュアシェルキー

SSHキーをiLOユーザーアカウントに追加し、セキュリティを強化します。

証明書マッピングおよびCACスマートカード

CACスマートカード認証を設定して、ローカルユーザーのスマートカード証明書を設定します。

SSL証明書

X.509 CA署名証明書をインストールして、暗号化通信を有効にします。

ディレクトリ

Kerberos認証とディレクトリ統合を構成します。

iLOは、ディレクトリサービスを使用してユーザーの認証や権限付与を行えるように設定することができます。この構成により、ユーザーの数の制限がなくなります。また、この構成は、エンタープライズ内のiLOデバイスの数に合わせて、簡単に拡張できます。ディレクトリによりiLOデバイスとユーザーを集中的に管理することもでき、より強力なパスワードポリシーを適用できます。

暗号化

iLOのセキュリティ状態をデフォルト値（製品）から強力な設定に変更して、高度なセキュリティ環境を実装します。

HPE SSO

サポートされているツールで、iLOによるシングルサインオンを設定します。

ログインセキュリティバナー

次の場合に表示されるセキュリティ通知を追加します。

- iLO Webインターフェイスログインページに移動します。
- HTML5スタンドアロンリモートコンソールを起動します。
- SSH接続を介してiLOに接続します。

iLOの機能によって使用されるポート

ネットワーク設定とポート

表: iLO経由で構成可能なネットワーク設定とポートにリストされている値を、サイトの要件またはセキュリティのイニシアチブに適合するように構成できます。これらの設定は、iLOアクセス設定ページで構成できます。

表 1. iLO経由で構成可能なネットワーク設定とポート

説明	デフォルト設定またはポート	プロトコルタイプ
IPMI/DCMI over LANポート	623	UDP
IPMI/DCMI over LAN LAN経由のiLOとのIPMI/DCMI 通信を許可するかどうかを指定します。	無効	
リモートコンソールポート	17990	TCP
リモートコンソール iLOリモートコンソール経由のアクセスを有効または無効にすることができます。	有効	
セキュアシェル（SSH）ポート	22	TCP
セキュアシェル（SSH） SSH機能を有効または無効にすることができます。 SSHは、iLOコマンドラインプロトコル（CLP）に暗号化されたアクセスを提供します。	有効	
SNMPポート	161	UDP
SNMP Trap Port	SNMPアラートの場合は162（送信のみ）。	UDP
SNMP iLOが外部のSNMP要求に応答するかどうかを指定します。	有効	
仮想メディアポート	17988	TCP
仮想メディア 仮想メディアを有効にするか無効にするかを指定できます。	有効	
Webサーバー非SSLポート（HTTP）	80	TCP
WebサーバーSSLポート（HTTPS）	443	TCP
Webサーバー [1] iLO Webサーバー経由のアクセスを有効または無効にすることができます。	有効	

[1] iLO Webインターフェイス、リモートコンソール、iLO RESTful API、iLO連携、ファームウェアアップデート、およびRIBCLをサポートします。

その他の発信ポート

セキュリティ管理者は、表: iLOが使用するその他のポートにリストされているポートを知っておく必要がある場合があります。これらのポートは、サードパーティの送信サービス用です。

表 2. iLOが使用するその他のポート

説明	既定のポート	プロトコルタイプ	iLOのWebインターフェイスの場所
DNS解決	53	UDP	該当なし
iLO連携/SSDPマルチキャスト	1900	UDP	該当なし
DHCPv4	67、68	UDP	該当なし
DHCPv6	547	UDP	該当なし
NTP	123	UDP	該当なし
NetBIOSネームサービス/WINS	137	UDP	iLO専用ネットワークポート > IPv4 iLO共有ネットワークポート > IPv4
Kerberos KDCサーバーポート	88	TCP、UDP	セキュリティ > ディレクトリ
ディレクトリサーバーLDAP SSLポート	636	TCP	セキュリティ > ディレクトリ
アラートメールSMTPポート	25	TCP	管理 > アラートメール
Remote Syslog Port	514	UDP	管理 > リモートSyslog
キーマネージャーのポート	9000	TCP	管理 > キーマネージャー
リモートサポートのポート	7906	TCP	リモートサポート > 登録

iLOでサポートされていないポート

iLOは、表: サポートされていないポートにリストされている一般的に使用されるポートをサポートしていません。

表 3. サポートされていないポート

説明	ポート	プロトコルタイプ	注記
セキュリティ保護されていないLDAP • 接続（TCP） • コネクションレス（UDP）	389	TCP/UDP	iLOは発信LDAP接続にセキュアポート636を使用します。
グローバルカタログに対してセキュリティ保護されていないLDAP • 接続（TCP） • コネクションレス（UDP）	3268	TCP/UDP	iLOはセキュアLDAP接続を使用します。

セキュリティプロトコルおよびデータモデル

iLOは、SPDM（Security Protocol and Data Model）を使用して、コンポーネントの完全性を検証し、オプションカードを認証します。すべてのコンポーネントがSPDMをサポートしているわけではありません。SPDMが有効になっている場合、サポートされていない、または正規品ではないコンポーネントによって、iLOのセキュリティステータスがリスクに変化します。

各コンポーネントの認証のステータスは、セキュリティログで確認できます。

サブトピック

グローバルコンポーネントの完全性

コンポーネントの完全性ポリシー

詳しくは

デバイスステータスの値
サポートされるSPDMアルゴリズム

グローバルコンポーネントの完全性

グローバルコンポーネントの完全性オプションを有効にすると、iLOはSPDMを使用してサーバー内のコンポーネントを認証できます。このオプションが有効になっている場合、iLOはSPDMを使用して、サーバー内の該当するすべてのコンポーネントを検証および認証します。

このオプションは、デフォルトでは無効になっています。無効になっている場合、iLOはSPDM認証のためにコンポーネントを検証せず、SPDMをサポートしているカードでも未サポートと報告されます。

アクセス設定ページでこのオプションを有効にできます。

サブトピック

グローバルコンポーネントの完全性の有効化

グローバルコンポーネントの完全性の有効化

前提条件

- SPDM対応のオプションカード
- オプションカードのCAがiLOファームウェア内で利用可能であること

手順

1. アクセス設定ページに移動します。
2. をクリックします（iLO設定で）。
3. グローバルコンポーネントの完全性チェックボックスを選択して、このオプションを有効にします。

コンポーネントの完全性ポリシー

コンポーネントの完全性ポリシーは、サーバー内のデバイスのSPDM認証結果に基づいてシステムブートポリシーを制御します。

サブトピック

サポートされるポリシー

サポートされるポリシー

サポートされているポリシーは次の2つです。

- SPDM障害時にブートを停止します - SPDM認証の失敗時にシステムブートを停止するには、このオプションを選択します。
- ポリシーなし - システムを通常モードで起動するには、このオプションを選択します。

必要なコンポーネントの完全性ポリシーを設定するには、アクセス設定ページに移動し、 をクリックします（iLO設定で）。

サーバーID

サーバーID（DevID）は、ネットワーク全体でサーバーを一意に識別するための標準（IEEE 802.1ARに基づく）方法です。DevIDはサーバーに一意にバインドされているため、サーバーは、通信デバイスを認証、プロビジョニング、および権限付与するさまざまな業界標準およびプロトコルでそのIDを証明できます。

iLOは、工場出荷時にプロビジョニングされたサーバーID（iLO IDevID）およびユーザー定義のサーバーID（iLO LDevID）を使用することをサポートしています。iLOは、システム証明書（システムIDevIDおよびシステムIAK）も保存します。

次は、さまざまなサーバー管理IDです。

- iLO IDevID
- iLO LDevID
- システムIDevID証明書

サブトピック

iLO IDevID

iLO LDevID

システムIDevID証明書

システムIAK証明書

プラットフォーム証明書

iLO IDevID

iLOは、工場でサーバーIDを使用してプロビジョニングできます。この工場でプロビジョニングされたサーバーIDはiLO IDevIDと呼ばれます。HPEサーバーは、802.1X認証用のIDevIDを使用して、顧客ネットワークに安全にオンボーディングできます。iLO IDevIDは生涯有効であり、不変です。

サブトピック

iLO IDevIDの機能

iLO IDevIDの機能

iLO IDevIDは不変であるため、アップデートまたは削除することはできません。

iLO IDevID証明書は、RESTful API GETコマンドを使用して表示できます。

```
"/redfish/v1/Managers/1/SecurityService/iLOIDevID/Certificates/1"
```

iLO LDevID

IDevIDは、iLO LDevIDと呼ばれるユーザー定義のサーバーIDで補完できます。iLO LDevIDは、サーバーが使用される管理ド

メインで一意のものです。HPEサーバーは、802.1X認証用のLDevIDを使用して、顧客ネットワークに安全にオンボーディングできます。iLO LDevIDは、iLO IDevIDを持たないサーバーで使用できます。

LDevIDは、ローカルネットワーク管理者による登録（認証情報の認証および認可）を容易にするのに役立ちます。iLOでは、ファクトリ外でLDevIDをインポート、表示、および削除できます。

サブトピック

LDevID証明書のインポート

このタスクについて

手順

1. LDevIDの証明書署名リクエスト（CSR）を生成します。iLOでは、RESTful API POSTコマンドを使用して、LDevIDのPEM形式でCSRを作成できます。

   `"/redfish/v1/CertificateService/Actions/CertificateService.GenerateCSR"`

   ```
   {
       "Action": "CertificateService.GenerateCSR",
       "CertificateCollection": {
           "@odata.id": "/redfish/v1/Managers/1/SecurityService/iLOLDevID/Certificates/"
       }
   }
   ```

2. このCSRを認証機関に送信して、信頼済みの証明書を取得します。
3. 信頼済みのLDevID証明書をiLOにインポートします。iLOを使用すると、RESTful API POSTコマンドを使用して、LDevID証明書をPEM形式でインポートできます。

   `"/redfish/v1/Managers/1/SecurityService/iLOLDevID/Certificates/"`

   ```
   {
       "CertificateType": "PEM",
       "CertificateString": <Contents of the trusted certificate>
   }
   ```

   インポートする前に、 iLOは、次のパラメーターを使用して入力証明書を検証します。
   - 証明書の公開キーは、対応するCSRで生成されたものと一致します。
   - 証明書で使用される署名およびハッシュアルゴリズムはFIPSに準拠しています。

   注記: iLOは、サイズが最大16KBのLDevID証明書のインポートをサポートします。

インポートされたLDevID証明書の表示

インポートされたLDevID証明書を表示するには、次のRESTful API GETコマンドを使用します。

`"/redfish/v1/Managers/1/SecurityService/iLOLDevID/Certificates/1"`

インポートされたLDevID証明書の削除

インポートされたLDevID証明書を削除するには、次のRESTful API DELETEコマンドを使用します。

`”/redfish/v1/Managers/1/SecurityService/iLOLDevID/Certificates/1”`

LDevID証明書の置き換え

LDevID証明書をアップデートすることはできません。証明書を置き換えるには、既存のLDevID証明書を削除して、新しい証明書を生成する必要があります。LDevID証明書のインポートを参照してください。

注記: One-buttonセキュア消去が原因でLDevID証明書が失われた場合は、バックアップとリストア機能を使用してリストアするか、置き換えることができます。

システムIDevID証明書

iLOは、サーバーホストIDを使用してプロビジョニングでき、オペレーティングシステムで使用できます。この工場でプロビジョニングされたシステムIDはシステムIDevIDと呼ばれ、対応する秘密キーがTPMに保存されます。システムIDevIDは、IDevIDのTPM2.0インプリメンテーションに関するTCG提案に従います。

iLOでは、証明書をアップデートまたは削除することはできません。証明書は、RESTful API GETコマンドを使用してのみ表示できます。

`“/redfish/v1/Managers/1/SecurityService/SystemIDevID/Certificates/1”`

システムIAK証明書

iLOは、工場でシステム初期認証キー（IAK）証明書を使用してプロビジョニングできます。これはシステムIDevIDに似ていますが、TPMベースの認証に使用されます。対応する秘密キーはTPMに保存されます。システムIAKは、IDevIDのTPM2.0インプリメンテーションに関するTCG提案に従います。

iLOでは、証明書をアップデートまたは削除することはできません。証明書は、RESTful API GETコマンドを使用してのみ表示できます。

`“/redfish/v1/Managers/1/SecurityService/SystemIAK/Certificates/1”`

注記: iLOIDevID、 iLO LDevID、システムIDevID、およびシステムIAKは、 iLOセキュリティ状態の遷移全体で保持され、工場出荷時のデフォルト値にリセットされます。

プラットフォーム証明書

iLOは、サプライチェーンの改ざんを検出するために使用されるハードウェアシャーシまたは構成の署名付きマニフェストとして機能する属性証明書であるプラットフォーム証明書を使用してプロビジョニングできます。この証明書はTCGに準拠しています。

iLOでは、証明書をアップデートまたは削除することはできません。証明書は、RESTful API GETコマンドを使用してのみ表示できます。

`“/redfish/v1/Managers/1/SecurityService/PlatformCert/Certificates/1”`

DevIDとシステムIAKのOne-buttonセキュア消去

iLO IDevID、iLO LDevID、システムIDevID、システムIAKは、One-buttonセキュア消去後に削除されます。

Hewlett Packard Enterpriseは、iLOの手動バックアップを実行して、One-buttonセキュア消去後のiLO IDevID、iLO LDevID、システムIDevID、およびシステムIAKの損失の影響を最小限に抑えることをお勧めします。手動バックアップでは、iLOのバックアップサービスにすべての証明書が含まれます。これらの証明書は、バックアップファイルから復元できます。

システムボードの交換

ボードを交換すると、iLO IDevID、iLO LDevID、システムIDevID、およびシステムIAKが無効になります。新しいボードでこれらをすべて交換する必要があります。工場出荷時にプロビジョニングされた証明書（iLO IDevID、システムIDevID、およびシステムIAK）は、工場外では新しいボード上で交換できません。

ボードを交換する場合、新しいLDevIDを作成できます。詳しくは、LDevID証明書のインポートを参照してください。新しいボードでは、iLO LDevIDは、認証と認可のための唯一のサーバーIDになります。

802.1XおよびiLO

IEEE 802.1Xは、ポートベースのネットワークアクセス制御のメカニズムであり、ネットワークへのアクセスを規制し、ネットワークにアクセスする身元不明および認可を受けていない関係者から保護します。

802.1Xは、認証プロセス中のメッセージ交換に拡張認証プロトコル（EAP）を使用します。EAP-トランスポート層セキュリティ（EAP-TLS）は、認証に証明書またはスマートカードを使用するEAPタイプです。

HPE iLO6は、802.1Xアクセス制御ネットワークへのオンボーディングのためのEAP-TLSベースの認証をサポートします。ファクトリでプロビジョニングされたサーバーID（iLO IDevID）を使用して、HPEサーバーは、802.1X認証用に、ゼロタッチ（無人自律操作）で安全にオンボードしてIDを確立できます。iLOは、ユーザーが802.1X認証用にプロビジョニングしたサーバーID（iLO LDevID）もサポートしています。iLO IDevIDとiLO LDevIDの両方がシステムに存在する場合、iLO LDevIDはEAP-TLS認証に使用されます。

802.1X認証のデフォルト設定は「有効」です。ただし、システムにiLO IDevIDまたはiLO LDevIDがない場合、iLO6はEAP-TLS認証を開始したり、認証要求に応答したりしません。

詳しくは、iLO IDevIDおよびiLO LDevIDを参照してください。

サブトピック

802.1X認証の前提条件

802.1X認証の前提条件

- 安全なデバイスID（iLO IDevIDまたはiLO LDevID）がプリインストールされています。
- iLO DevID証明書を受け入れるように認証、認可、およびアカウンティング（AAA）サーバーを構成します（たとえば、EAP-TLSをサポートするように構成し、RADIUSサーバーにDevID発行者証明書をインストールします）。

iLOアクセス設定

アクセス設定のデフォルト値は、ほとんどの環境に適しています。アクセス設定ページで変更できる値を使用すると、特殊環境向けのiLO外部アクセス方法をカスタマイズできます。

アクセス設定ページに入力された値は、すべてのiLOユーザーに適用されます。

サブトピック

iLOアクセス設定の構成

前提条件

- すべてのアクセス設定の変更に関する前提条件：
  - iLOの設定を構成する権限
- アップデートサービス設定の変更に関する追加の前提条件：
  - リカバリセット権限
  - この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- ダウンロード可能な仮想シリアルポートログまたは仮想シリアルポートログover CLI設定を変更するための追加の前提条件は、以下の通りです。
  - この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

このタスクについて

この手順は、iLO機能を除くすべてのアクセス設定を対象とします。iLO機能を無効にするには、iLO機能の無効化を参照してください。

手順

1. ナビゲーションツリーでセキュリティをクリックします。

   アクセス設定ページが表示されます。

2. アップデートしたいアクセス設定カテゴリの隣にある をクリックします。

   以下から選択します。

   - サーバー
   - アカウントサービス
   - iLO

- アップデートサービス
- ネットワーク

編集*設定 タイプ*ページが開きます。

3. 必要に応じて、設定をアップデートし、OKをクリックします。

   変更した設定のタイプに応じて、以下が実行される場合があります。

   - iLOが、アップデートが完了したことを通知します。
   - iLOが、保留中の変更を有効にするにはリセットを必要であることを通知します。

     設定によっては、リセットが完了する前に、設定の変更時に即座に影響することがあります。たとえば、リモートコンソールを介したアクセスを無効にした場合、OKをクリックするとリモートコンソールセッションを開始できません。構成の変更を完了するには、リセットが必要です。

     リセットが必要なその他の設定では、リセットを行わずに手動で構成を元の状態に戻すことができます。これらの設定の場合は、手動で変更を元に戻して、✕ をクリックして、リセットメッセージを無視します。たとえば、仮想NIC機能を有効にした場合、保留中の変更にリセットが必要であることが、iLOから通知されます。仮想NICオプションを無効にリセットして手動でこの変更を元に戻すと、保留中のリセットメッセージは残され、✕ をクリックして、メッセージを無視できます。

     画面またはダイアログボックスで✕ をクリックすると、リセットメッセージは破棄されますが、iLO構成が前の設定に戻されることはありません。変更を元に戻す場合は、手動で変更を元に戻す必要があります。

4. （オプション）2～3の手順を繰り返して、追加のアクセス設定をアップデートします。
5. リセットが必要な場合、アクセス設定のアップデートが完了したら、iLOをリセットをクリックします。

   iLOが要求を確認するように求めます。

6. はい、iLOをリセットしますをクリックします。

   接続が再確立されるまでに、数分かかることがあります。

詳しくは

iLO機能の無効化

iLO機能の無効化

前提条件

iLOの設定を構成する権限

このタスクについて

iLO機能設定は、iLO機能が使用可能かどうかを制御します。

- この設定が有効（デフォルト）になっている場合、iLOネットワークを使用でき、オペレーティングシステムドライバーとの通信がアクティブです。
- この設定が無効になっている場合、iLOネットワークと、オペレーティングシステムドライバーとの通信が切断されます。

  iLO機能は、ProLiantサーバーブレードまたはSynergyコンピュートモジュールでは無効にできません。

この手順を使用して、iLO機能の設定を変更します。他のiLOアクセス設定をアップデートするには、iLOアクセス設定の構成を参照してください。

手順

1. ナビゲーションツリーでセキュリティをクリックします。

アクセス設定ページが表示されます。

2. （iLOセクションの横）をクリックします。

   iLO設定の編集ページが表示されます。

3. アドバンスト設定を表示をクリックします。

4. iLO機能セクションで無効をクリックします。

   iLOが要求を確認するように求めます。

5. iLOの機能の無効の確認チェックボックスを選択します。

6. はい、iLOの機能を無効にしますをクリックします。

   注意:

   このボタンをクリックした場合、iLOにはどのインターフェイスからもアクセスできなくなります。iLOの機能をリストアするには、UEFIシステムユーティリティを使用できます。

   iLOはセッションを終了します。iLO機能設定を再度有効にするまで、どのiLOインターフェイスからも接続できません。

7. （オプション）iLO機能を再度有効にするには、UEFIシステムユーティリティまたはシステムメンテナンススイッチを使用します。

   Hewlett Packard Enterpriseでは、UEFIシステムユーティリティを使用してこの作業を実行することをお勧めします。

サブトピック

iLO機能を有効にする方法

詳しくは

iLOアクセス設定の構成
iLOセキュリティを無効にする理由

iLO機能を有効にする方法

iLO機能が無効になっている場合、iLO Webインターフェイスから機能を再度有効にすることはできません。UEFIシステムユーティリティまたはシステムメンテナンススイッチを使用して、iLO機能を再度有効にすることができます。

UEFIシステムユーティリティ

Hewlett Packard Enterpriseでは、UEFIシステムユーティリティを使用してiLO機能を再度有効にすることをお勧めします。

詳しくは、UEFIシステムユーティリティドキュメントを参照してください。

システムメンテナンススイッチ

iLO機能をリストアする別の方法は、システムメンテナンススイッチを使用してiLOセキュリティを無効にするというものです。

iLOセキュリティを無効にすると、iLOのネットワーク構成が工場出荷時のデフォルト設定にリセットされます。工場出荷時のデフォルトネットワークインターフェイスがネットワークに接続されている場合、iLOはネットワーク上で利用可能です。この変更はiLOセキュリティをリストアした後も持続します。

注意:

セキュリティを無効にし、iLOが本番環境のセキュリティ状態を使用している場合、どのユーザーもiLOにアクセスして構成を変更することができます。システムメンテナンススイッチを使用してセキュリティを無効にする場合、Hewlett Packard Enterpriseでは、この構成でiLOを使用する時間をできるだけ短くすることを強くお勧めします。

サーバーアクセス設定オプション

アクセス設定ページのサーバーセクションでは、以下の設定を構成できます。

サーバー名

ホストサーバー名を指定することができます。この値を手動で割り当てることができますが、オペレーティングシステムをロードするとホストソフトウェアによって上書きされることがあります。

最大 49 バイトのサーバー名を入力できます。

サーバーのFQDN/IPアドレス

サーバーのFQDNまたはIPアドレスを指定できます。この値を手動で割り当てることができますが、オペレーティングシステムをロードするとホストソフトウェアによって上書きされることがあります。

最大 255 バイトの FQDN または IP アドレスを入力できます。

アカウントサービスのアクセス設定オプション

アクセス設定ページのアカウントサービスセクションでは、以下の設定を構成できます。

遅延前の認証の失敗時

iLOがログイン遅延を課すまでに許容されるログインの失敗数を設定できます。

有効な値は次のとおりです。

- 毎回の失敗時でも遅延なし - ログイン試行の最初の失敗後、ログイン遅延が発生します。
- 1回目の失敗時では遅延なし（デフォルト） - ログイン試行に2回失敗するまで、ログイン遅延は発生しません。
- 3回目の失敗時では遅延なし - ログイン試行に4回失敗するまで、ログイン遅延は発生しません。
- 5回目の失敗時では遅延なし - ログイン試行に6回失敗するまで、ログイン遅延は発生しません。

認証の失敗時の遅延時間

ログインに失敗した後のiLOログイン遅延の継続期間を構成できます。

有効な値は2、5、10、および30秒です。デフォルト値は10秒です。

認証失敗ログ

認証失敗のログ記録条件を構成できます。すべてのログインタイプがサポートされ、それぞれのログインタイプは個別に動作します。

以下の設定が有効です。

- 有効-毎回失敗時 - ログインに失敗するたびに、失敗したログインログエントリーが記録されます。
- 有効-2回の失敗ごと - ログイン試行に2回失敗するごとに、ログインの失敗のログエントリーが記録されます。
- 有効-3回の失敗ごと（デフォルト） - ログイン試行に3回失敗するごとに、ログインの失敗のログエントリーが記録されます。
- 有効-5回の失敗ごと - ログイン試行に5回失敗するごとに、ログインの失敗のログエントリーが記録されます。
- 無効 - ログインの失敗のログエントリーは記録されません。

最小パスワード長

ユーザーパスワードの設定または変更の際に許可される文字の最小数を指定します。

指定する文字数は、0～39文字の値でなければなりません。デフォルト値は8です。

パスワードの複雑さ設定を有効にした場合、iLOは、最小パスワード長を満たすパスワードを許可しないことがあります。たとえば、最小パスワード長を1に設定した場合、1文字のパスワードはパスワードの複雑さ要件を満たさないた

め無効になります。

パスワードの複雑さ

ユーザーアカウントおよびiLO連携グループを作成するときのパスワードの複雑さチェックの動作を制御します。

この設定を有効にすると、新しいまたはアップデートしたユーザーアカウントパスワードには、次の特性のうちの3つが含まれる必要があります。

- 少なくとも1つの大文字ASCII文字
- 少なくとも1つの小文字ASCII文字
- 少なくとも1つのASCII数字
- 少なくとも1つの他の文字タイプ（記号、特殊文字、句読点など）

この設定を無効（デフォルト）にした場合、これらのパスワード特性は適用されません。

iLOアクセス設定オプション

アクセス設定ページのiLOセクションでは、以下の設定を構成できます。

グローバルコンポーネントの完全性

SPDMを使用してサーバー内の該当するすべてのコンポーネントを認証する●機能●を有効または無効にします。

この設定は、デフォルトでは無効になっています。

このオプションを有効にすると、iLOはSPDMを使用してサーバー上のコンポーネントを検証できます。

コンポーネントの完全性ポリシー

デバイスのコンポーネントの完全性ポリシー設定に基づいてシステムブートポリシーを指定します。ポリシーは次の2つです。

- SPDM障害時にブートを停止します - SPDM認証の失敗時にシステムブートを停止するには、このオプションを選択します。
- ポリシーなし - システムを通常モードで起動するには、このオプションを選択します。

ダウンロード可能な仮想シリアルポートログ

iLO Webインターフェイスを介してダウンロードできるファイルに仮想シリアルポートのログを収集する機能を有効または無効にします。

この設定を有効にすると、仮想シリアルポートのアクティビティが、アクセス設定ページからダウンロードできるファイルに記録されます。

この設定は、デフォルトでは無効になっています。

この機能にはライセンスが必要です。この機能をサポートするライセンスがインストールされていない場合、このオプションは表示されません。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

CLIで表示できるファイルに仮想シリアルポートを記録する方法については、ネットワークアクセス設定オプションを参照してください。

アイドル接続タイムアウト（分）

iLOセッションで、ユーザーの操作がないまま経過し、自動的に終了するまでの時間を指定します。

各接続は別個のセッションであるため、iLO Webインターフェイスおよび.NET IRCは、アイドル時間を別々に追跡します。アイドル接続タイムアウトに達すると、アイドル状態のセッションのみが終了します。

iLO WebインターフェイスとHTML5コンソールは、1つのiLOセッションを共有します。アイドル接続タイムアウトに達すると、共有セッションは終了します。

有効な値は次のとおりです。

- 15、30、60、120分間 - デフォルト値は30分です。

- 無限 – 非アクティブなユーザーはログアウトされません。

異なるサイトにアクセスしたりブラウザーウィンドウを閉じたりすることによってiLOからログアウトしなかった場合も、アイドル接続になります。iLOファームウェアがサポートする接続数には制限があります。無限タイムアウトオプションを乱用すると、他のユーザーがiLOにアクセスできなくなる場合があります。アイドル接続は、期限が切れると再利用されます。

この設定は、ローカル/ディレクトリのユーザーに適用されます。ディレクトリサーバータイムアウト設定は、iLO設定を優先的に使用する場合があります。

設定を変更しても、現在のユーザーセッションでただちに有効にならない場合がありますが、すべての新しいセッションでただちに強制設定されます。

iLO機能

この設定については、iLO機能の無効化を参照してください。

iLO RIBCLインターフェイス

iLOとの通信にRIBCLコマンドを使用できるかどうかを指定します。

この設定は、デフォルトで有効になっています。

この機能を無効にすると、HTTP/HTTPSを介したRIBCLとインバンド通信経由のRIBCLは機能しません。

無効の場合、RIBCLを使用しようとすると次のメッセージが表示されます。

```
<?xml version="1.0"?>
<RIBCL VERSION="2.23">

<RESPONSE
STATUS="0x00FC"
MESSAGE='RIBCL is disabled.'
/>
</RIBCL>
```

この値を変更するときは、iLOをリセットする必要があります。

注記: Synergyコンピューティングモジュールのデフォルト設定を変更することはできません。デフォルト設定を変更しようとすると、エラーメッセージが表示されます。
RIBCLは、HPE OneViewとiLOの間の適切な通信のために有効にする必要があります。

iLO ROMベースセットアップユーティリティ

UEFIシステムユーティリティのiLO構成オプションを有効または無効にします。

- この設定が有効（デフォルト）になっている場合、UEFIシステムユーティリティへのアクセス時にiLO構成オプションを使用できます。
- この設定が無効になっている場合、UEFIシステムユーティリティへのアクセス時にiLO構成オプションを使用できません。

システムBIOSでオプションROMのプロンプトが無効になっている場合、この設定を有効にできません。

iLO Webインターフェイス

iLOと通信するためにiLO Webインターフェイスを使用できるかどうかを指定します。

この設定は、デフォルトで有効になっています。

この値を変更するときは、iLOをリセットする必要があります。リセットの完了後は、UEFIシステムユーティリティまたはiLO RESTful APIを使用してこの設定を再度有効にするまで、Webブラウザー経由でiLOインターフェイスにアクセスすることはできません。

リモートコンソールサムネイル

iLOでリモートコンソールのサムネイルイメージの表示を有効または無効にします。

サムネイルを無効にしても、リモートコンソール機能は無効になりません。

この設定を無効にすると、Webインターフェイスがサムネイルの表示を中止するのに約30秒かかります。

この設定を有効にする場合は、ブラウザーウィンドウを更新してサムネイルを表示します。iLOからログアウトしてか

らログインし直して、サムネイルを表示することもできます。

ホスト認証が必要

管理プロセッサーにアクセスするホストベースの構成ユーティリティを使用するために、iLOユーザー認証情報が必要かどうかを決定します。これらのユーティリティは、管理者またはrootのホストコンテキストで、ホストOSのコマンドラインから実行します。

- この設定を有効にすると、すべてのコマンドで有効な資格情報が必要になります。
- この設定を無効にした場合は、有効な認証情報は必要でなく、管理者権限でコマンドは実行します。

  iLOが本番環境または高セキュリティより高いセキュリティ状態を使用するように構成されている場合、この設定は無効にできません。

iLO RBSUへのログインが必要

UEFIシステムユーティリティのiLO構成オプションにユーザーがアクセスしたときに、ユーザー認証情報が必要かどうかを決定します。

- この設定が無効（デフォルト）になっている場合、UEFIシステムユーティリティのiLO構成オプションにユーザーがアクセスするときに、ログインは不要です。

  この設定が無効になっている場合でも、iLOのセキュリティ状態が本番環境または高セキュリティよりも高い場合、UEFIシステムユーティリティのiLO構成オプションにアクセスするには、ユーザー資格情報が必要です。
- この設定が有効になっている場合、UEFIシステムユーティリティのiLO構成オプションにユーザーがアクセスするときに、ログインダイアログボックスが開きます。

シリアルコマンドラインインターフェイス速度

CLI機能のシリアルポートの速度を変更できます。

以下の速度（ビット/秒）が有効です。

- 9600（デフォルト）

  Synergyコンピュートモジュールの場合のみ：Synergyコンソールおよび Composer CLIで、この値を9600に設定する必要があります。
- 19200
- 38400 - UEFIシステムユーティリティのiLO構成オプションではこの値はサポートされていません。
- 57600
- 115200

正常に動作させるには、シリアルポート構成をパリティなし、データビット8、ストップビット1（N/8/1）に設定する必要があります。

この値は、UEFIシステムユーティリティで構成されたシリアルポート速度と一致するように設定します。

シリアルコマンドラインインターフェイスステータス

シリアルポート経由でのCLI機能のログインモデルを変更できます。

以下の設定が有効です。

- 有効-認証が必要（デフォルト） - ホストシリアルポートに接続された端末からSMASH CLPにアクセスできます。有効なiLOユーザー証明書が必要です。
- 有効-認証は不要 - ホストシリアルポートに接続された端末からSMASH CLPにアクセスできます。iLOユーザー証明書は不要です。
- 無効 - ホストシリアルポートからSMASH CLPへのアクセスを無効にします。物理シリアルデバイスを使用する予定の場合は、このオプションを使用してください。

POST中にiLO IPを表示

ホストサーバーのPOST中にiLOのネットワークIPアドレスを表示できます。

- この設定が有効（デフォルト）になっている場合、POST実行中にiLOのIPアドレスが表示されます。

- この設定が無効になっている場合、POST実行中にiLOのIPアドレスが表示されません。

外部モニターにサーバーヘルスを表示

外部モニターでサーバーヘルスサマリー画面の表示を有効にします。

- この設定が有効になっている場合は、サーバーのUIDボタンを押して放して、外部モニターにサーバーヘルスサマリー画面を表示できます。
- この設定が無効になっている場合は、サーバーのUIDボタンを押して放しても、サーバーヘルスサマリー画面は開きません。

> △ **注意:**
> この機能を使用するには、UIDボタンを押して放します。5秒以上押し続けると、適切なiLOの再起動またはハードウェアiLOの再起動が開始されます。ハードウェアiLOの再起動中にデータの損失やNVRAMの破損が発生する可能性があります。

この機能は、Synergyコンピュートモジュールではサポートされません。

サーバーヘルスサマリー画面について詳しくは、HPE iLO 6トラブルシューティングガイドを参照してください。

VGAポート検出オーバーライド

システムのビデオポートに接続されているデバイスの検出方法を制御します。動的検出によってシステムが異常なポート電圧から保護されます。

- この設定が有効になっている場合（デフォルト）、iLOファームウェアは、ビデオ出力の使用を開始する前に、接続されているデバイスを検出します。
- この設定が無効になっている場合、iLOハードウェアは、ビデオ出力の使用を開始する前に、接続されているデバイスを検出します。

この設定は、ディスプレイ、KVMコンセントレーター、またはアクティブなドングルへのビデオ出力がない場合のトラブルシューティングで使用できます。

この設定は、Synergyコンピュートモジュールではサポートされません。

仮想NIC

USBサブシステム経由で仮想NICを使用してホストオペレーティングシステムからiLOにアクセスできるかどうかを決定します。

- この設定が有効になっている場合は、以下のことができます。
  - ホストOSで動作しているRESTfulインターフェイスツールまたは別のクライアントからiLO RESTful APIコマンドを開始する。
  - ホストOSで動作しているSSHクライアントでiLOに接続する。
  - ホストOSで動作しているサポート対象のブラウザーを使用してiLO Webインターフェイスにアクセスする。
  - 概要ページで仮想NICのIPアドレスを表示する。
- この設定が無効になっている場合、仮想NICを使用してiLOにアクセスすることはできません。

  工場出荷時のデフォルトの仮想NIC設定は、iLOのほとんどのバージョンで無効になっています。iLO6では、この設定はデフォルトで有効になっています。iLOを工場出荷時のデフォルト設定にリセットすると、仮想NIC設定は、iLOのインストールされているバージョンのデフォルト設定に戻ります。ファームウェアのアップグレードまたはダウングレードでは、この設定は変更されません。

サービスアクセス設定オプションのアップデート

ダウングレードポリシー

iLOからアップデートできるファームウェアタイプをダウングレードする要求をiLOがどのようにして処理するかを指定します。

この機能にはライセンスが必要です。この機能をサポートするライセンスがインストールされていない場合、このオプションは表示されません。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。

以下の値から選択します。

- ダウングレードの許可（デフォルト）-iLO設定の構成権限を持つすべてのユーザーがファームウェアをダウングレードできます。
- ダウングレードにはリカバリセットの権限が必要です-iLO設定の構成権限とリカバリセット権限を持つユーザーのみがファームウェアをダウングレードできます。
- ダウングレードを永遠に不許可-ユーザーはファームウェアをダウングレードできません。

> △ **注意:**
>
> この設定を構成するとiLOに対して永続的な変更が行われます。永遠にダウングレードを禁止するようiLOを構成した後は、iLOのどのインターフェイスやユーティリティからもこの設定の構成を変更することができなくなります。iLOを出荷時のデフォルト設定に設定しても、この値はリセットされません。

サードパーティーのファームウェアアップデートパッケージの受け入れ

iLOで、デジタル署名されていないサードパーティのファームウェアアップデートパッケージを受け入れるかどうかを指定します。Platform Level Data Model（PLDM）ファームウェアパッケージがサポートされています。

この設定は、デフォルトでは無効になっています。

ネットワークアクセス設定オプション

アクセス設定ページのネットワークセクションでは、iLOの機能を有効および無効にしたり、それらの機能で使用するポートを構成したりできます。

iLOが使用するTCP/IPポートは構成可能であり、ポート設定に関する任意のサイト要件およびセキュリティのイニシアチブに適合できます。これらの設定は、ホストシステムには影響しません。iLOで有効なポートの値の範囲は1～65535です。使用されているポートの番号を入力すると、iLOにより別の値を入力するよう求められます。

通常、これらの設定を変更するには、標準の通信とSSL通信に使用されるWebブラウザーの構成を変更する必要があります。

匿名データ

この設定は、以下を制御します。

- 基本システム情報の匿名要求への応答でiLOが提供するXMLオブジェクト。
- `/redfish/v1`に対するRedfishの匿名呼び出しへの応答で提供される情報。

この設定が有効になっている（デフォルト）場合は、次のようになります。

- 他のソフトウェアは、ネットワーク上のiLOシステムを検出および特定できます。iLOが提供するXML応答を表示するには、XMLを表示をクリックします。
- `/redfish/v1`に対するRedfishの匿名呼び出しには、次のような情報が含まれます。

```
"ManagerFirmwareVersion": "1.10",
"ManagerType": "iLO 6",
"Status": {"Health": "OK"}
```

- iLOのヘルスステータスが劣化の場合は、iLOのヘルスステータスと問題の説明がログインページに表示されます。iLOヘルスステータスは、iLO診断セルフテストを組み合わせた結果に基づいています。セキュリティ侵害の可能性があるセルフテスト障害は、説明には表示されません。

このオプションが無効になっている場合は、次のようになります。

- iLOは空のXMLオブジェクトを使用して要求に応答します。

- iLOのバージョン情報はログインページに表示されません。
- `/redfish/v1`に対するRedfishの匿名呼び出しに次の情報は含まれません。`ManagerFirmwareVersion`、`ManagerType`、および`Status`。

本番環境または高セキュリティより高いセキュリティ状態を有効にすると、この設定は自動的に無効になります。

拡張されたダウンロードパフォーマンス

iLOのスクリプト化可能な仮想メディアとURLベースのファームウェアアップロードのダウンロードパフォーマンスを向上させることができます。

このオプションを有効にすると、イメージをホストしているWebサーバーとiLOの通信が最適化されます。この設定は、このオプションを変更した後、新しい仮想メディア接続とファームウェアアップデート操作が開始された場合にのみ有効になります。

この設定は、デフォルトで有効になっています。

拡張されたダウンロードパフォーマンス設定を編集するには、アクセス設定ページに移動し、 （ネットワーク設定）をクリックします。

IPMI/DCMI over LAN

業界標準のIPMIおよびDCMIコマンドをLAN経由で送信できます。

この設定は、デフォルトでは無効になっています。

この設定が無効になっていると、iLOはLAN経由でIPMI/DCMIを無効にします。この機能が無効にされても、サーバー側のIPMI/DCMIアプリケーションは依然として機能します。

この設定が有効になっている場合、iLOでは、クライアント側のアプリケーションを使用してLAN経由でIPMI/DCMIコマンドを送信できます。

IPMI/DCMI over LANが無効にされている場合、ポートスキャナーを使用して、セキュリティの脆弱性をスキャンするセキュリティ監査で、構成されているIPMI/DCMI over LANポートが検出されません。

本番環境または高セキュリティより高いセキュリティ状態を有効にすると、この設定は自動的に無効になります。

IPMI/DCMI over LANポート

IPMI/DCMIポート番号を設定します。

デフォルト値はUDP 623です。

リモートコンソール

iLOリモートコンソール経由のアクセスを有効または無効にすることができます。

このオプションを無効にすると、グラフィカルリモートコンソールとテキストベースのリモートコンソールが無効になります。ポートスキャナーを使用して、セキュリティの脆弱性をスキャンするセキュリティ監査で、構成されているリモートコンソールポートが検出されません。

リモートコンソールを無効にしても、リモートコンソールサムネイルは無効になりません。リモートコンソールサムネイルを無効にするには、iLOのアクセス設定セクションでリモートコンソールサムネイルオプションを編集します。

この設定は、デフォルトで有効になっています。

リモートコンソールポート

リモートコンソールポートを設定します。

デフォルト値はTCP 17990です。

セキュアシェル（SSH）

SSH機能を有効または無効にすることができます。

SSHは、iLOコマンドラインプロトコル（CLP）に暗号化されたアクセスを提供します。

この設定は、デフォルトで有効になっています。

セキュアシェル（SSH）ポート

SSHポートを設定します。

デフォルト値はTCP 22です。

SNMP

iLOが外部のSNMP要求に応答するかどうかを指定します。

SNMPアクセスを無効にすると、iLOはそのまま動作を続行し、iLO Webインターフェイスに表示される情報はアップデートされます。この状態では、警告は生成されず、SNMPアクセスは許可されません。

SNMPアクセスが無効になっている場合、SNMP設定ページのほとんどのボックスは使用できません。

本番環境または高セキュリティより高いセキュリティ状態を有効にすると、この設定は自動的に無効になります。

SNMPポート

SNMPポートを設定します。

SNMPアクセスのデフォルト値はUDP 161です。

SNMPポートの値をカスタマイズすると、標準以外のSNMPポートの使用をサポートしない一部のSNMPクライアントが、iLOで正しく動作しない場合があります。

SNMPオプションが無効になっている場合、この値をアップデートすることはできません。

SNMPトラップポート

SNMPトラップポートを設定します。

SNMPアラート（またはトラップ）のデフォルト値はUDP 162です。

SNMPトラップポートをカスタマイズすると、標準以外のSNMPトラップポートの使用をサポートしない一部のSNMP監視アプリケーションが、iLOで正しく動作しない場合があります。

HPE SIM 7.2以降でSNMP v3を使用するには、SNMPトラップポートの値を50005に変更します。

SNMPオプションが無効になっている場合、この値をアップデートすることはできません。

仮想メディア

iLO仮想メディア機能を有効または無効にすることができます。

このオプションを無効にすると、仮想メディア機能が無効になります。ポートスキャナーを使用してセキュリティの脆弱性をスキャンするセキュリティ監査で、構成されている仮想メディアポートが検出されません。

仮想メディアポート

iLOが着信ローカル仮想メディア接続をリスンするために使用するポート。

デフォルト値はTCP 17988です。

仮想シリアルポートログover CLI

CLIを使用して表示できる仮想シリアルポートの記録を有効または無効にします。

この設定が有効になっている場合、仮想シリアルポートの動作がiLOメモリ内の150ページの循環バッファーに記録されます。CLIコマンド`vsp log`を使用して、記録された情報を表示できます。仮想シリアルポートのバッファーサイズは128 KBです。

この設定は、デフォルトでは無効になっています。

この機能にはライセンスが必要です。この機能をサポートするライセンスがインストールされていない場合、このオプションは表示されません。使用可能なライセンスタイプ、およびサポートされている機能については、次のWebサイトにあるライセンス文書を参照してください：https://www.hpe.com/support/ilo-docs。

iLO Webインターフェイスを介してダウンロードできるファイルに仮想シリアルポートを記録する方法については、iLOアクセス設定オプションを参照してください。

Webサーバー

iLO Webサーバー経由のアクセスを有効または無効にすることができます。

注意:
この値を無効に設定した場合、iLOは、構成済みのWebサーバー非SSLポート（HTTP）またはWebサーバーSSLポート（HTTPS）での通信をリスンしません。
Webサーバーが無効になっている場合、次の機能は正常に動作しません。

- iLOのWebインターフェイス
- リモートコンソール
- iLO RESTful API
- RIBCL

このオプションを無効にすると、ポートスキャナーを使用してセキュリティ脆弱性をスキャンするセキュリティ監査で、構成されているWebサーバー非SSLポート（HTTP）およびWebサーバーSSLポート（HTTPS）が検出されません。

Webサーバー非SSLポートを有効

HTTPポートを無効にします。

Webサーバー非SSLポート（HTTP）

HTTPポートを設定します。

デフォルト値はTCP 80です。

WebサーバーSSLポート（HTTPS）

HTTPSポートを設定します。

デフォルト値はTCP 443です。

注記: Synergyコンピューティングモジュールのデフォルト設定を変更することはできません。デフォルト設定を変更しようとすると、エラーメッセージが表示されます。
このオプションを無効にすると、iLOは構成済みのWebサーバーからの通信の検出に失敗し、RIBCLが無効になります。
RIBCLは、HPE OneViewとiLOの間の適切な通信のために有効にする必要があります

Webプロキシ

Webプロキシサーバーを有効にするかどうかを指定します。

アクセス設定ページからWebプロキシを有効にするには、以下の手順を使用します。

- （ネットワーク設定）をクリックし、Webプロキシチェックボックスを選択します。
- Webプロキシサーバー名、Webプロキシポート番号、Webプロキシユーザー名、およびWebプロキシパスワードを入力します。
  - Webプロキシサーバー - プロキシサーバーのホスト名またはIPアドレスを示します。
  - Webプロキシポート - Webプロキシポート番号を指定します。iLOで有効なポートの値の範囲は1～65535です。
  - Webプロキシユーザー名 - Webプロキシのユーザー名を示します。
  - Webプロキシパスワード - Webプロキシのパスワードを示します。
- OKをクリックしてプロキシサーバーを有効にします。

Webプロキシ設定をデフォルト値にリセットするには、Webプロキシチェックボックスを選択解除にし、OKをクリックします。

802.1Xサポート

iLOで802.1Xベースの認証をサポートするかどうかを指定します。この機能では、出荷時にプロビジョニングされたID（iLO IDevID）またはユーザー定義のサーバーID（iLO LDevID）を認証に使用することをサポートしています。

サブトピック

SSHクライアントによるiLOログイン

SSHクライアントによるiLOログイン

SSHクライアントでiLOにログインすると、表示されるログインプロンプトの回数は、認証失敗ログオプションの値（無効の場合は3）に一致します。SSHクライアントはログインが失敗すると実装も遅延するため、SSHクライアント設定は、プロンプトの回数に影響を与える場合があります。

たとえば、デフォルト値（有効-3回目の失敗時）でSSH認証失敗ログを生成するには、SSHクライアントが、3回に設定されたパスワードプロンプトで構成されている場合、連続した3回のログイン失敗が次のように発生します。

1. SSHクライアントを起動し、正しくないログイン名とパスワードでログインします。

   パスワードプロンプトが3回表示されます。正しくないパスワードを3回入力すると、接続が終了し、最初のログイン失敗が記録されます。SSHログイン失敗カウンターが1に設定されます。

2. SSHクライアントを起動し、正しくないログイン名とパスワードでログインします。

   パスワードプロンプトが3回表示されます。正しくないパスワードを3回入力すると、接続が終了し、2番目のログイン失敗が記録されます。SSHログイン失敗カウンターが2に設定されます。

3. SSHクライアントを起動し、正しくないログイン名とパスワードでログインします。

   パスワードプロンプトが3回表示されます。正しくないパスワードを3回入力すると、接続が終了し、3番目のログイン失敗が記録されます。SSHログイン失敗カウンターが3に設定されます。

iLOファームウェアは、失敗したSSHログインログエントリーを記録し、SSHログイン失敗カウンターを0に設定します。

iLOサービスポート

サービスポートは、サポートされているサーバーおよびコンピュートモジュールで**iLO**のラベルが付けられているUSBポートです。

お使いのサーバーまたはコンピュートモジュールがこの機能に対応しているか調べるには、次のWebサイト（https://www.hpe.com/info/qs）にあるサーバーの仕様ドキュメントを参照してください。

サーバーに物理的にアクセスできる場合、サービスポートを使用して次のことができます。

- サポートされているUSBフラッシュドライブにActive Health Systemログをダウンロードします。

  この機能を使用する場合、接続されているUSBフラッシュドライブにホストオペレーティングシステムはアクセスできません。

- サポートされるUSBイーサーネットアダプターにクライアント（ノートパソコンなど）を接続して以下にアクセスします。
  - iLOのWebインターフェイス
  - リモートコンソール
  - iLO RESTful API
  - CLI
  - RIBCLスクリプト

iLOサービスポートを使用すると、次のようになります。

- 操作がiLOイベントログに記録されます。
- サービスポートのステータスを示すようにサーバーのUIDが点滅します。

  RESTクライアントとiLO RESTful APIを使用してサービスポートのステータスを取得することもできます。

- サービスポートを使用してサーバー内のデバイスまたはサーバー自体を起動することはできません。

- サービスポートに接続してサーバーにアクセスすることはできません。
- 接続されているデバイスにサーバーからアクセスすることはできません。

iLOサービスポート経由でのActive Health Systemログのダウンロード

前提条件

iLOサービスポートおよびUSBフラッシュドライブオプションがiLOサービスポートページで有効になっている。

手順

1. `command.txt`という名前のテキストファイルを作成し、Active Health Systemログをダウンロードするための必須の内容を記述します。
2. サポートされているUSBフラッシュドライブのルートディレクトリにファイルを保存します。
3. USBフラッシュドライブをiLOサービスポート（サーバーの前面にある、**iLO**のラベルが付けられているUSBポート）に接続します。

   ファイルシステムがマウントされ、`command.txt`ファイルが読み込まれて実行されます。

   iLOサービスポートのステータスがビジーに変わり、UIDが中速で4回点滅してから1秒オフを繰り返します。

   コマンドが成功した場合は、iLOサービスポートのステータスが完了に変わり、UIDが高速で1回点滅してから3秒オフを繰り返します。

   コマンドが失敗した場合は、iLOサービスポートのステータスがエラーに変わり、UIDが高速で8回点滅してから1秒オフを繰り返します。

   ファイルシステムがマウント解除されます。
4. USBフラッシュドライブを取り外します。

   iLOサービスポートのステータスが準備完了に変わります。UIDは点滅を停止するか、リモートコンソールアクセスやファームウェアアップデートの進行中などの状態を示して点滅します。
5. （オプション）ファイルをHPE InfoSight for Serversにアップロードします。

   HPE InfoSight for ServersでAnalyze Logsページにアクセスするには、Compute見出しの下のInfrastructure > Analyze Logsを選択します。

   詳しくは、次のWebサイトにあるHPE InfoSight for Serversユーザーガイドを参照してください：https://www.hpe.com/support/infosight-servers-docs

詳しくは

iLOサービスポート設定の構成
iLOサービスポートのサポート対象デバイス
iLOサービスポートを通じたActive Health Systemログダウンロードのサンプルテキストファイル

iLOサービスポートを通じてiLOにクライアントを接続する

前提条件

- iLOサービスポートおよびUSBイーサーネットアダプターオプションがiLOサービスポートページで有効になっている。
- クライアントNICがサービスポート機能をサポートするように構成されている。
- サーバーに物理的にアクセスできる。

手順

1. サポートされているUSBイーサーネットアダプターを使用して、クライアントをサービスポート（サーバーの前面にある、**iLO**のラベルが付けられているUSBポート）に接続します。

   クライアントNICにリンクローカルアドレスが割り当てられます。このプロセスには、数秒かかることがあります。

2. IPv4アドレス
   `169.254.1.2`
   を使用して、iLOに接続します。

   サービスポートを介してサーバーにクライアントを接続するときは、同じIPアドレスが使用されます。このアドレスを変更することはできません。

   サービスポートのステータスがビジーに変わり、UIDが中速で4回点滅してから1秒オフを繰り返します。

3. 作業を終了したら、クライアントをサービスポートから外します。

   サービスポートのステータスが準備完了に変わります。UIDは点滅を停止するか、リモートコンソールアクセスやファームウェアアップデートの進行中などの状態を示して点滅します。

詳しくは

iLOサービスポート設定の構成
iLOサービスポートを通じて接続するクライアントを設定する

iLOサービスポート設定の構成

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーでセキュリティクリックして、iLO サービスポートタブをクリックします。
2. 以下の設定を行います。
   - iLOサービスポート
   - USBフラッシュドライブ
   - 認証が必要
   - USBイーサーネットアダプター
3. 適用をクリックします。

   アップデートされた設定はすぐに有効になり、構成変更に関する情報がiLOイベントログに記録されます。

iLOサービスポートオプション

- iLOサービスポート – iLOサービスポートを有効または無効にすることができます。デフォルト設定は有効です。この機能を無効にすると、このページのマスストレージオプションセクションまたはネットワークオプションセクションの機能を構成することはできません。

  使用中のiLOサービスポートを無効にしないでください。データがコピーされているときにこのポートを無効にすると、データが破損する可能性があります。

- USBフラッシュドライブ – USBフラッシュドライブをiLOサービスポートに接続してActive Health Systemログをダウンロードできます。デフォルト設定は有効です。

  iLOサービスポートを使用しているときにこの設定を無効にしないでください。データがコピーされているときにUSBフラッシュドライブを無効にすると、データが破損する可能性があります。

  この設定が無効のときにUSBフラッシュドライブをiLOサービスポートに挿入した場合、デバイスは無視されます。

- 認証が必要 – iLOサービスポートを使用してActive Health SystemログをダウンロードするときにiLOユーザー認証情報を`command.txt`ファイルに入力する必要があります。デフォルト設定は、無効です。

  iLOセキュリティを無効にするようシステムメンテナンススイッチが設定されている場合、ユーザー認証情報は不要です。

- USBイーサーネットアダプター – USBイーサーネットアダプターを使用してノートパソコンをiLOサービスポートに接続

し、統合リモートコンソールにアクセスできます。デフォルト設定は有効です。

この設定が無効な場合にノートパソコンを接続すると、デバイスは無視されます。

iLOサービスポートを通じて接続するクライアントを設定する

手順

1. IPv4自動構成アドレスを自動的に取得するクライアントNICを構成します。

   詳しくは、オペレーティングシステムのドキュメントを参照してください。

2. 次のいずれかを実行します。

   - プロキシ例外を追加します。次のいずれかの形式を使用します。
     - Edge、Chrome：`169.254.*`
     - Firefox：`169.254.0.0/16`
   - クライアント上でWebプロキシ設定を無効にします。

   プロキシ設定について詳しくは、オペレーティングシステムのドキュメントを参照してください。

iLOサービスポートのサポート対象デバイス

大容量ストレージデバイス

iLOサービスポートは、以下の特性を持つUSBキーをサポートします。

- 高速USB 2.0準拠。
- FAT32フォーマット（512バイトブロックを推奨）。
- 1つのLUN。
- 最大サイズ127 GBの1つのパーティションと、Active Health Systemログをダウンロードするのに十分な空き領域。
- 有効なFAT32パーティションテーブル。

  USBキーのマウントに失敗した場合、無効なパーティションテーブルがあることが考えられます。Microsoft DiskPartなどのユーティリティを使用して、パーティションを削除して再作成してください。
- 読み取り保護されていない。
- ブート可能ではない。

NANDが搭載されていないサーバーでは、大容量ストレージデバイスはサポートされません。

USBイーサーネットアダプター

iLOサービスポートは、ASIX Electronics Corporationの次のいずれかのチップを内蔵したUSBイーサーネットアダプターをサポートします。

- AX88772
- AX88772A
- AX88772B
- AX88772C

Hewlett Packard Enterpriseは、HPE USBイーサーネットアダプター（部品番号Q7Y55A）を使用することをお勧めします。

iLOサービスポートを通じたActive Health Systemログダウンロードのサンプルテキストファイル

iLOサービスポートを使用してActive Health Systemログをダウンロードする場合は、`command.txt`というテキストファイルを作成し、サポートされているUSBデバイスにファイルを保存します。USBデバイスをサーバーに接続すると、`command.txt`ファイルが実行され、ログファイルがダウンロードされます。

command.txtファイルのファイルテンプレート

`command.txt`ファイルのテンプレートとして、次の例を使用します。

```
{
  "/ahsdata/" : {
    "POST" : {
      "downloadAll"  : "0",
      "from"         : "2016-08-25",
      "to"           : "2016-08-26",
      "case_no"      : "ABC0123XYZ",
      "contact_name" : "My Name",
      "company"      : "My Company, Inc.",
      "phone"        : "281-555-1234",
      "email"        : "my.name@mycompany.com",
      "UserName"     : "my_username",
      "Password"     : "my_password"
    }
  }
}
```

command.txtファイルのパラメーター

以下の値をカスタマイズできます。

- `downloadAll` - ダウンロード範囲を制御します。日付の範囲のログをダウンロードするには、
  `0`
  を入力します。ログ全体をダウンロードするには、
  `1`
  を入力します。
- `from` - 日付範囲に対応するログをダウンロードする場合の開始日。
- `to` - 日付範囲に対応するログをダウンロードする場合の終了日。
- `case_no`（オプション） - 開いているHPEサポートケースのケース番号。この値の最大長は14文字です。この値を入力すると、それがダウンロードしたファイルに含まれます。
- `contact_name`（オプション） - このサーバーの連絡担当者。この値を入力すると、それがダウンロードしたファイルに含まれます。この値の最大長は255文字です。
- `company`（オプション） - このサーバーを所有する会社。この値を入力すると、それがダウンロードしたファイルに含まれます。この値の最大長は255文字です。
- `phone`（オプション） - このサーバーの連絡担当者の電話番号。この値を入力すると、それがダウンロードしたファイルに含まれます。この値の最大長は39文字です。
- `email`（オプション） — このサーバーの連絡担当者のメールアドレス。この値を入力すると、それがダウンロードしたファイルに含まれます。この値の最大長は255文字です。
- `UserName` - iLOが大容量ストレージデバイスでのiLOサービスポートのアクションに認証を要求するように構成されている場合は、iLOアカウントのユーザー名を入力します。iLOセキュリティを無効にするようシステムメンテナンススイッチが設定されている場合、ユーザー名は不要です。
- `Password` - iLOが大容量ストレージデバイスでのiLOサービスポートのアクションに認証を要求するように構成されている場合は、入力したユーザー名のパスワードを入力します。iLOセキュリティを無効にするようシステムメンテナンススイッチが設定されている場合、パスワードは不要です。

command.txtファイルのファイル要件

- ファイルは、有効なJSON形式でなければなりません。

  Hewlett Packard Enterpriseは、オンラインのJSONフォーマッターを使用して、ファイルの構文を確認することをおすすめします。Webサイト**http://www.freeformatter.com/json-formatter.html**で無料のユーティリティを入手できます。

- ファイル内にコメントを含めないでください。
- ファイル内のテキストでは大文字と小文字が区別されます。
- ファイルではプレーンテキストのみサポートされます。追加の書式設定プロパティを埋め込むアプリケーションを使用してファイルを作成しないでください。

SSHキーの管理

サブトピック

Webインターフェイスを使用した新しいSSHキーの認証

CLIを使用した新しいSSHキーの認証

SSHキーの削除

HPE SIMサーバーからのSSHキーを認証するための要件

SSHホストキーの表示

認証済みSSHキーの表示

SSHキー

サポートされているSSHキー形式の例

Webインターフェイスを使用した新しいSSHキーの認証

前提条件

ユーザーアカウント管理権限

手順

1. `ssh-keygen`、`puttygen.exe`、または別のSSHキーユーティティを使用して、2,048ビットのDSAキーまたはRSAキーを生成します。

   iLOがCNSAセキュリティ状態を使用するように構成されている場合、NIST P-384曲線を使用するECDSA 384ビットキーが必要です。

2. `key.pub`という名前で公開キーを保存します。
3. `key.pub`ファイルの内容をコピーします。
4. ナビゲーションツリーでセキュリティをクリックして、セキュアシェルキータブをクリックします。
5. SSHキーを追加するユーザーアカウントの左にあるチェックボックスを選択します。

   各ユーザーアカウントに割り当てられるキーは1つだけです。

6. 新しいキーの認証をクリックします。
7. 公開キーボックスに公開キーを貼り付けます。
8. 公開キーのインポートをクリックします。

   認証済みSSHキーテーブルがアップデートされ、ユーザーアカウントに関連付けられたSSH公開キーのハッシュが表示されます。

CLIを使用した新しいSSHキーの認証

前提条件

ユーザーアカウント管理権限

手順

1. `ssh-keygen`、`puttygen.exe`、または別のSSHキーユーティリティを使用して、2,048-bit DSAまたはRSA SSHキーを生成します。

   iLOがCNSAセキュリティ状態を使用するように構成されている場合、NIST P-384曲線を使用するECDSA 384ビットキーが必要です。

2. `key.pub`ファイルを生成します。
3. アクセス設定ページでセキュアシェル（SSH）アクセスが有効になっていることを確認します。
4. `putty.exe`を使用して、ポート22を使用したSSHセッションを開きます。
5. `/Map1/Config1`ディレクトリに変更します。
6. 次のコマンドを入力します。

   ```
   load sshkey type "oemhpe_loadSSHkey -source
   <protocol://username:password@hostname:port/filename>"
   ```

   このコマンドを使用するときは次の点に留意してください。

   - `protocol`の値は必須で、HTTPまたはHTTPSを指定します。
   - `hostname`および`filename`の値は必須です。
   - `username:password`および`port`の値は省略可能です。

   CLIでは、入力した値の構文は大まかにしか検証されません。よく見て、URLが正しいことを確認してください。次の例でコマンド構造を示します。

   ```
   oemhpe_loadSSHkey -source http://192.168.1.1/images/path/sshkey.pub
   ```

SSHキーの削除

前提条件

ユーザーアカウント管理権限

このタスクについて

SSHキーを1つ以上のユーザーアカウントから削除するには、以下の手順を使用します。

SSHキーをiLOから削除すると、SSHクライアントは、iLOに対して、対応するプライベートキーを使用して認証できなくなります。

手順

1. ナビゲーションツリーでセキュリティをクリックして、セキュアシェルキータブをクリックします。
2. 認証済みSSHキーリストで、1つまたは複数のユーザーアカウントの左にあるチェックボックスを選択します。
3. 選択したキーの削除をクリックします。

   iLOが要求を確認するように求めます。

4. はい、削除しますをクリックします。

選択したSSHキーがiLOから削除されます。

HPE SIMサーバーからのSSHキーを認証するための要件

`mxagentconfig`ユーティリティを使用すると、HPE SIMサーバーからSSHキーを認証できます。

- キーを認証するには、`mxagentconfig`を使用する前に、iLOでSSHが有効になっている必要があります。
- `mxagentconfig`に入力したユーザー名とパスワードは、iLO設定の構成権限を持つユーザーアカウントに対応する必要がありますこのユーザーは、ディレクトリユーザーであってもローカルユーザーであってもかまいません。
- キーは、iLOで認証され、`mxagentconfig`コマンドで指定されるユーザー名に対応します。

`mxagentconfig`について詳しくは、iLOスクリプティング/CLIガイドを参照してください。

SSHホストキーの表示

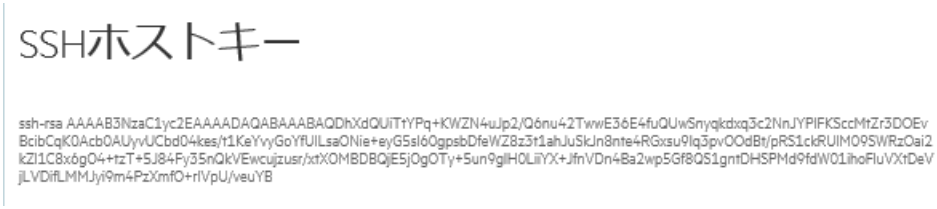
このタスクについて

iLOによって報告されるSSHホストキーを表示するには、以下の手順に従ってください。

手順

1. ナビゲーションツリーでセキュリティをクリックして、セキュアシェルキータブをクリックします。

   SSHホストキーが表示されます。

2. （オプション）ホスト名/IPアドレスとSSHホストキーをSSHクライアント構成ファイルに追加します。

   以下に例を示します。

   - LinuxのOpenSSHユーザー：`.ssh/known_hosts`ファイルをアップデートします。
   - WindowsのPuTTYユーザー：Windowsレジストリ（`HKEY_CURRENT_USER\SoftWare\SimonTatham\PuTTY\SshHostKeys`）をアップデートします。

3. （オプション）接続が安全であることを確認するには、SSHホストキーの値をSSHクライアントから報告された値と比較します。

   以下に例を示します。

   ```
   Linux-client:~ # grep ilo.example.com .ssh/known_hosts
   ilo.example.com,[redacted] ssh-rsa
   AAAAB3NzaC1yc2EAAAADAQABAAABAQC9E/XDH9xPU+NdMyTu5Oylw9AN6mJlH7woMqcf79lda6DeS1D+vX1I
   Wg3GwDKFUobabQ+gZtkBrxWFzwAf51CPitsybQCK2hvLztsypb/W3p+MPZ9zU6/voCHzL2v0bAxeXuX8ack/8RA
   w0l1agB5xY6B3pjP/qaeFJb29sGqPwoaXps6g5t/YFhxIQ8is8N+LnfuTzMtQDj74rfq6pcXGnXq+ErmbkcfHn
   AdSMveT6rXPM1U+Je1B9VOVS23fUL7mfoshLnSHrJJtP7XkZ1rKf1QPKCChWLfpdmTprsaJrxDrwCNxX4+pPh
   UXqHYLTlvPA8xsqaPxPZfHxZWTZrCp
   ```

4. キーが一致しない場合は、一致しない理由を確認してから続行してください。

   考えられる理由のいくつかを以下に示します。

   - 手順1で表示したiLOシステムが、SSHクライアントで接続したシステムと同じではない。

- SSH接続はリダイレクトされている。ネットワークが接続をリダイレクトするよう構成されているか管理者に尋ねてください。ネットワークが接続をリダイレクトするように構成されていない場合、ネットワークセキュリティが低下する可能性があります。
- iLOが出荷時のデフォルト設定にリセットされたために、アクセスしようとしているシステムのiLO SSHホストキーが変更された。あなたは自分のSSHクライアント構成を変更していません。

認証済みSSHキーの表示

手順

1. ナビゲーションツリーでセキュリティをクリックして、セキュアシェルキータブをクリックします。

   認証済みSSHキーテーブルには、各ユーザーアカウントに関連付けられたSSH公開キーのハッシュが表示されます。

2. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。

SSHキー

SSHキーをiLOに追加すると、iLOファームウェアによってキーがローカルユーザーアカウントに関連付けられます。

サポートされているSSHキーフォーマット

- RFC 4716
- OpenSSHキー形式
- レガシーiLO形式

SSHキーの操作

- iLO Webインターフェイスおよびcliでは、サポートされているSSHキー形式がサポートされます。
- RIBCLスクリプトでは、レガシーiLO形式のみがサポートされています。
- 対応するプライベートキーを使用して認証されるSSH接続は、キーの所有者として認証され、同じ権限を持ちます。
- iLOファームウェアは、最大1,366バイトの長さのSSHキーをインポートすることができます。キーの長さが1,366バイトを超える場合、認証に失敗することがあります。認証に失敗する場合は、SSHクライアントソフトウェアを使用して、より短いキー生成してください。
- iLOのWebインターフェイスを使用してパブリックキーを入力する場合は、パブリックキーに関連付けられたユーザーを選択します。
- iLO RESTful APIを使用してパブリックキーを入力する場合は、パブリックキーとともにユーザー名がPOST本文で提供されます。
- CLIを使用してパブリックキーを入力する場合は、パブリックキーが、iLOにログインするために入力したユーザーに結び付けられます。
- HPQLOCFGおよびRIBCLスクリプトを使用してパブリックキーを入力する場合は、パブリックキーデータにiLOユーザー名を追加します。パブリックキーは、ユーザー名とともに格納されます。
- ユーザーに対してSSHキーが認証された後にそのユーザーが削除されると、SSHキーが削除されます。

サポートされているSSHキー形式の例

RFC 4716

```
---- BEGIN SSH2 PUBLIC KEY ---- CRLF
Comment: "Administrator"CRLF
AAAAB3NzaC1kc3MAAACAT27C04Dy2zr7fWhUL7TwHDKQdEdyuAlNLIivLFP3IoKZCRLF
ZtzF0VInP5x2VFVYmTvdVjSupD92CTlxxAtarOPON2qUqoOajKRtBWLmxcfqsLCTCRLF
3wI3ldxQvPYnhTYyhPQuoeJ/vYhoam+y0zi8D03pDv9KaeNA3H/zEL5mf9Ktgts8CRLF
/UAAAAVAJ4efo8ffq0hg4a/eTGEuHPCb3INAAAAgCbnhADYXu+Mv4xuXccXWP0PcCRLF
j477YiZgos3jt/Z0ezFX6/cN/RwwZwPC1HCsMuwsVBIqi7bvn1XczFPKOt06gVWcCRLF
jFteBY3/bKpQkn61SGPC8AhSu8ui0KjyUZrxL4LdBrtp/K2+lm1fqXHnzDIEJ0RHCRLF
g8ZJazhY920PpkD4hNbAAAAgDN3lba1qFVl0UlRjj21MjXgr6em9TETSOO5b7SQ8CRLF
hX/Z/axobbrHCj/2s66VA/554chkVimJT2IDRRKVkcV8OVC3nb4ckpfFEZvKkAWYCRLF
aiFDLqRbHhh4qyRBIfBKQpvvhDj1aecdFbaO2UvZltMir4n8/E0hh19nfi3tjXAtCRLF
STV CRLF
---- END SSH2 PUBLIC KEY ---- CRLF
```

OpenSSHキー形式

```
ssh-dss
AAAAB3NzaC1kc3MAAACAYjEd8Rk8HLCLqDIlI+RkA1UXjVS28hNSk8YDljTaJpw1VOlBirrLGPdSt0avN
Sz0DNQuU7gTPfjj/8cXyHe3y95Oa3Rics1fARyLiNFGqFjr7w2ByQuoYUaXBzzghIYMQcmpc/W/kDMC0d
VOf2XnfcLpcVDIm3ahVPRkxFV9WKkAAAAVAI3J61F+oVKrbNovhoHh8pFfUa9LAAAAgA8pU5/M9F0s5Qx
qkEWPD6+FVz9cZ0GfwIbiuAI/9ARsizkbwRtpAlxAp6eDZKFvj3ZIyNjcQODeYYqOvVU45AkSkLBMGjpF
05cVtnWEGEvrW7mAvtG2zwMEDFSREw/V526/jR9TKzSNXTH/wqRtTc/oLotHeyV2jFZFGpxDOvNWAAAAg
Ff6pvWaco3CDELmH0jT3yUkRSaDztpqtoo4D7ev7VrNPPjnKKKmpzHPmAKRxz3g5S80SfWSnWM3n/pekB
a9QI9lH1r3Lx4JoOVwTpkbwb0by4eZ2cqDw20KQ0A5J84iQE9TbPNecJ0HJtZH/K8YnFNwwYy2NSJyjLw
A0TSmQEOW Administrator CRLF
```

レガシーiLO形式

iLOレガシー形式のキーは、RIBCLで必要なBEGINおよびENDヘッダーで囲まれたOpenSSHキーです。

この形式は、BEGIN SSH KEYのテキストとEND SSH KEYのテキストの間に1行で記す必要があります。

```
-----BEGIN SSH KEY----- CRLF
ssh-dss
AAAAB3NzaC1kc3MAAACBANA45qXo9cM1asav6ApuCREt1UvP7qcMbw+sTDrx9lV22XvonwijdFiOM/0Vv
uzVhM9oKdGMC7sCGQrFV3zWDMJcIb5ZdYQSDt44X6bvlsQcAR0wNGBN9zHL6YsbXvNAsXN7uBM7jXwHwr
ApWVuGAI0QnwUYvN/dsE8fbEYtGZCRAAAAFQDofA47q8pIRdr6epnJXSNrwJRvaQAAAIBY7MKa2uH82I0
KKYTbNMi0o5mOqmqy+tg5s9GC+HvvYy/S7agpIdfJzqkpHF5EPhm0jKzzVxmsanO+pjju7lrE3xUxojev
lokTERSCMxLa+OVVbNcgTe0xpvc/cF6ZvsHs0UWz6gXIMCQ9Pk118VMOw/tyLp42YXOaLZzGfi5pKAAAA
IEAl7FsO7sDbPj02a5jO3qFXa762lWvu5iPRZ9cEt5WJEYwMO/ICaJVDWVOpqF9spoNb53Wl1pUARJg1s
s8Ruy7YBv8Z1urWWAF3fYy7R/SlQqrsRYDPLM5eBkkLO28B8C6++HjLuc+hBvj90tsqeNVhpCfO9qrjYo
mYwnDC4m1IT4= ASmith CRLF
-----END SSH KEY-----CRLF
```

CAC Smartcard認証

Common Access Card（CAC）とは、米国防総省（DoD）の多要素認証スマートカードです。Common Access Cardは、現役軍人、予備員、軍属、DoD外政府職員、州兵、指定業者社員の標準IDとして発行されます。IDカードとして使用されるだけでなく、共通アクセスカードは官庁施設やコンピューターネットワークへアクセスする際に必要です。

各CACに埋め込まれているスマートカード証明書は、iLO Webインターフェイスでローカルユーザーアカウントと関連付けられなければなりません。証明書マップページのコントロールを使用して、スマートカード証明書をアップロードし、アカウントと関連付けます。

LDAPディレクトリサポートを備えたCAC認証ではディレクトリサービスに対して認証するサービスアカウントを使用し、ユーザーアカウントは設定されたディレクトリサーバーと同じドメイン内に存在する必要があります。さらに、ユーザーアカウントは、設定されたグループまたは拡張スキーマロールの直接メンバーでなければなりません。クロスドメイン認証とネスト化グループはサポートされません。

Two-Factor認証

連邦政府認証を満たすために必要な要件の一部がTwo-Factor認証です。Two-Factor認証は、CACの二重認証です。たとえば

CACでは、実際にカードを所有していてそのカードに関連付けられたPIN番号を知っていなければならないことで、Two-Factor認証が成立します。CAC認証に対応するためには、スマートカードがPINを必要とするように構成されていなければなりません。

CAC Smartcard認証設定の構成

前提条件

- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- （オプション）LDAPサーバーCA証明書がディレクトリ統合のためにインストールされている。
- （オプション）LDAPディレクトリ統合がディレクトリデフォルトスキーマモードで構成されている。

手順

1. ナビゲーションツリーでセキュリティをクリックし、CAC/Smartcardタブをクリックします。
2. 信頼済みCA証明書のインポート

   この証明書は、iLOに提示される証明書の検証に使用します。証明書は構成されているiLOセキュリティ状態に準拠していなければなりません。
3. 以下の認証オプションを設定します。
   a. CAC Smartcard認証を有効にします。
   b. （オプション）CAC厳密モードを有効にします。
4. （オプション）CAC厳密モードの有効時にセキュリティを強化するために、Hewlett Packard Enterpriseでは、次を有効にすることをお勧めします。
   - ホスト認証が必要 - この設定はアクセス設定ページで構成できます。
   - FIPSセキュリティ状態 - この設定は暗号化ページで構成できます。
5. （オプション）ディレクトリ統合を使用している場合は、ディレクトリユーザー証明書名マッピングセクションでオプションを選択します。

   この設定は、ユーザー証明書のどの部分がディレクトリユーザーアカウントの識別に使用されるかを特定します。
6. 認証オプションおよびディレクトリユーザー証明書名マッピング設定を保存するには、適用をクリックします。

   CAC厳密モードを有効にした場合、iLOでは、iLOのリセットを必要とする要求の確認が求められます。

   CAC厳密モードを有効にしていない場合、iLOでは、変更が保存されたことが通知されます。
7. 変更を確認してリセットを開始するようにiLOから求められたら、はい、適用およびリセットをクリックします。
8. （オプション）証明書失効リスト（CRL）をインポートします
9. （オプション）オンライン証明書ステータスプロトコル（OCSP）を使用してユーザー証明書を確認するには、OCSP設定セクションにHTTPまたはHTTPS URLを入力して、適用をクリックします。
10. スマートカード証明書をアップロードしてローカルiLOユーザーアカウントにマップします（iLOをローカルユーザー認証で使用する場合のみ）。

詳しくは

CAC Smartcard認証用の信頼済みの証明書の管理
新しいローカルユーザー証明書の承認
スキーマフリーディレクトリ認証

CACスマートカード認証設定

CACスマートカード認証

共通アクセススマートカードを使用した認証を有効または無効にします。

CAC厳密モード

iLOへの接続ごとにクライアント証明書を要求するCAC厳密モードを有効または無効にします。このモードが有効になっている場合、iLOはユーザー名やパスワードを受け付けず、キーベースの認証方法のみが許可されます。

> **注記:**
> 信頼済みの証明書がない場合、iLOにアクセスできません。iLO Webインターフェイスにアクセスしようとすると、エラーが生成されます。

ディレクトリユーザー証明書名マッピング

ディレクトリユーザー名の場合を設定すると、ユーザー証明書の部分を選択して、ご自分のディレクトリのユーザー名として使用できます。

- 証明書SAN UPNを使用 - サブジェクト代替名（SAN）の、userPrincipalName（UPN）タイプの最初のフィールドをユーザー名として使用します。これには、ユーザー名とドメイン名がメールアドレス形式で含まれています。たとえば、`upn:testuser@domain.com`の場合、`testuser@domain.com`となります。
- 証明書件名CNを使用 - サブジェクトのCNまたはCommonNameの部分だけをユーザー名として使用します。たとえば、`cn = test user, ou = users, dc = domain, dc = com`というDNでは、共通名は`test user`です。
- 完全な証明書のSubject DNを使用 - ディレクトリサービスでユーザーを検索するとき、完全な識別名をユーザー名として使用します。たとえば、識別名は`cn = test user, ou = users, dc = domain, dc = com`と表されます。
- 証明書SAN RFC822名を使用 - SANの、rfc822Nameタイプの最初のフィールドをユーザー名として使用します。これにはメールアドレスが含まれています。たとえば、`rfc822Name:testuser@domain.com`の場合、ユーザー名は`testuser@domain.com`となります。

OCSP設定

この機能を使用すると、オンライン証明書ステータスプロトコル（OCSP）を使用してユーザー証明書をチェックできます。

HTTPおよびHTTPS URLが受け付けられます。

応答が`不明`または`失効`状態の場合、認証は失敗します。

CAC Smartcard認証用の信頼済みの証明書の管理

信頼済みCA証明書のインポート

前提条件

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

  証明書は、PEMでエンコードされたBase64フォーマットでなければなりません。

手順

1. ナビゲーションツリーでセキュリティをクリックし、CAC/Smartcardタブをクリックします。
2. ダイレクトインポートセクションに信頼済みCA証明書を貼り付けます。
3. 適用をクリックします。

   操作が正常に実行されていないように思われる場合は、ページの上部にスクロールして、エラーメッセージが表示されていないかどうかを確認します。

信頼済みCA証明書の削除

前提条件

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

手順

1. ナビゲーションツリーでセキュリティをクリックし、CAC/Smartcardタブをクリックします。
2. 信頼できるCA証明書を管理セクションまでスクロールします。
3. 削除する証明書の横にあるチェックボックスを選択します。
4. 削除をクリックします。

   iLOが要求を確認するように求めます。
5. はい、削除しますをクリックします。

   証明書が削除されます。

   操作が正常に実行されていないように思われる場合は、ページの上部にエラーメッセージが表示されていないかどうかを確認します。

証明書失効リスト（CRL）をURLからインポート

前提条件

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

このタスクについて

取り消された発行済み証明書を無効にするには、CRLをインポートします。

手順

1. ナビゲーションツリーでセキュリティをクリックし、CAC/Smartcardタブをクリックします。
2. 失効リストのインポートセクションにURLを入力するか貼り付けます。

   CRLのサイズ制限は100 KBであり、CRLはDERフォーマットでなければなりません。
3. 適用をクリックします。

   CRLの変更は、将来のCACログインセッションに適用されます。

   既存のCACログインセッションにCRLの変更を強制的に適用するには、次のいずれかを実行します。

   - iLOをリセットします。
   - アクティブセッションリストで目的のCACセッションを特定し、それらの接続を解除します。

   証明書失効リスト（CRL）セクションに、CRLの説明とシリアル番号が表示されます。

証明書失効リストの削除

前提条件

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

い。

手順

1. ナビゲーションツリーでセキュリティをクリックし、CAC/Smartcardタブをクリックします。
2. 証明書失効リスト（CRL）セクションまで下にスクロールします。
3. 削除をクリックします。

   iLOが要求を確認するように求めます。
4. はい、削除しますをクリックします。

SSL証明書の管理

SSL（Secure Sockets Layer）プロトコルは、データがネットワークを移動しているときに、他人がデータを見たり、変更したりできないようにデータを暗号化するための規格です。SSL証明書は、暗号化キー（サーバーの公開キー）とサーバー名をデジタル的に結合した小さなコンピューターファイルです。対応するプライベートキーを所有するサーバーのみが、ユーザーとサーバー間で認証済みの双方向通信を実現できます。

証明書は署名がないと有効になりません。認証機関（CA）によって署名され、そのCAが信頼される場合、CAによって署名されるすべての証明書も信頼されます。自己署名証明書は、証明書の所有者がそれ自身のCAとして機能する証明書です。

iLOは、SSL接続で使用するために自己署名の電子証明書をデフォルトで作成します。この電子証明書により、構成手順を追加することなく、iLOの動作を有効にすることができます。

重要:
自己署名証明書を使用するよりも、信頼済み証明書をインポートするほうが安全です。Hewlett Packard Enterpriseでは、信頼済み証明書をインポートしてiLOユーザーアカウント認証情報を保護することをお勧めします。

iLOのバックアップおよび復元機能を使用する場合、証明書が含まれます。

サブトピック

SSL証明書情報の表示

手順

ナビゲーションツリーでセキュリティをクリックし、SSL証明書タブをクリックします。

サブトピック

SSL証明書の詳細

SSL証明書の詳細

- 発行先 - 証明書の発行先の名前。

  iLO自己署名証明書を表示する際、この値は、Hewlett Packard Enterpriseヒューストンオフィスに関する情報を表示します。

- 発行元 - 証明書を発行したCA。

  iLO自己署名証明書を表示する際、この値は、Hewlett Packard Enterpriseヒューストンオフィスに関する情報を表示します。

- 有効期間の開始 - 証明書の有効期限の開始日。
- 有効期間の終了 - 証明書の有効期限の終了日。
- シリアル番号 - 証明書に割り当てられたシリアル番号。この値は、自己署名証明書の場合はiLOによって生成され、信頼済みの証明書の場合はCAによって生成されます。

自動証明書登録

iLOは、Simple Certificate Enrollment Protocol（SCEP）を使用したSSL証明書の自動取得と更新をサポートするようになりました。現在、iLOは、Microsoftネットワークデバイス登録サービス（NDES）でこれらの機能をサポートしています。

iLOの証明書登録を有効にするには、最初に、証明書登録サーバーで次のサービスを構成する必要があります。

- 認証局（CA）を構成します。CAは、証明書サービスを実行し、証明書を発行するサーバーです。
- NDESを構成します。NDESは証明書登録サーバーです。

注記:
この機能は、iLOがCNSAセキュリティ状態にある場合はサポートされません。

デフォルトで、この機能は無効です。この機能の有効化について詳しくは、自動証明書登録の有効化セクションを参照してください。

信頼済みのSSL証明書

このタスクについて

SSL証明書をカスタマイズするには、次のいずれかのオプションを選択します。

- 信頼済みのSSL証明書のインポート - 信頼済みのSSL証明書を手動でインポートするには、このオプションを使用します。
- SSL証明書を自動的に管理 - SSL証明書の自動生成または更新を管理するには、このオプションを使用します。
- 証明書のカスタマイズをクリックします。証明書のカスタマイズプロセスのための新しいページが開きます。

証明書のカスタマイズ

SSL証明書の手動での取得とインポート

自動証明書登録の有効化

SSL証明書の取得とインポート

前提条件

iLOの設定を構成する権限

このタスクについて

iLOでは、iLOにインポートする信頼済みのSSL証明書を取得するために認証機関（CA）に送信できる証明書署名要求（CSR）を作成できます。

iLOは、最大20 KBのサイズのSSL証明書チェーン（PEM形式）のインポートをサポートします。

SSL証明書は、対応するCSRを使用して生成されたキーがないと動作しません。iLOが工場出荷時のデフォルト設定にリセットされる場合、または前のCSRに対応する証明書がインポートされる前に別のCSRが生成される場合、証明書は動作しません。その場合には、CAから新しい証明書を取得するために、新しいCSRを生成する必要があります。

手順

1. CAから信頼済みの証明書を取得します。
2. 信頼済みの証明書をiLOにインポートします。

CAからの信頼済み証明書の取得

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーでセキュリティをクリックし、SSL証明書タブをクリックします。
2. 証明書のカスタマイズをクリックします。
3. 次の値を入力します。
   - 国（C）
   - 州または県(ST)
   - 都市または地域(L)
   - 組織名(O)
   - 組織ユニット(OU)
   - 共通名(CN)
4. （オプション）iLO IPアドレスをCSRに含めるには、iLOのIPアドレスを含みますチェックボックスを選択します。

   注記:
   多くの認証機関（CA）では、この入力を受け入れることができません。使用中のCAでこの入力を受け入れることがわかっていない場合は、このオプションを選択しないでください。

   このオプションが有効な場合、iLOのIPアドレスがCSRサブジェクト代替名（SAN）の拡張子に含まれます。
5. CSRの生成をクリックします。

   CSRを生成中であり、その処理に最大で10分かかる可能性があることを伝えるメッセージが表示されます。

6. 数分（最大10分）後に、CSRの生成を再度クリックします。

   CSRが表示されます。

7. CSRテキストを選択してコピーします。
8. ブラウザーウィンドウを開き、第三者認証機関に移動します。
9. 画面の指示に従って、CSRをCAに送信します。
   - 証明書の目的を選択するように求められたら、必ずサーバー証明書のオプションを選択してください。
   - CSRをCAに送信するときに、ご使用の環境でサブジェクト代替名の指定が要求される可能性があります。必要に応じて、iLO DNS名を入力します。

   CAは証明書を生成します。証明書署名ハッシュは、CAによって決定されます。

10. 証明書を取得したら、以下の事項を確認してください。
    - CNがiLO FQDNと一致している。この値は、概要ページにiLOホスト名として表示されます。
    - 証明書がBase64でエンコードされたX.509証明書である。
    - 証明書に開始行と終了行が含まれている。

CSR入力の詳細

CSRを作成するときは、次の詳細情報を入力します。

- 国（C） - このiLOサブシステムを所有する会社または組織が存在する国を識別する2文字の国番号。2文字の省略表記を大文字で入力します。
- 州（ST） - このiLOサブシステムを所有する会社または組織が存在する州または県。
- 都市または地域（L） - このiLOサブシステムを所有する会社または組織が存在する市町村。
- 組織名（O） - このiLOサブシステムを所有する会社または組織の名前。
- 組織ユニット（OU） - （省略可能）このiLOサブシステムを所有する会社または組織の中の単位。
- 共通名（CN） - このiLOサブシステムのFQDN。

  FQDNは、共通名（CN）ボックスに自動的に入力されます。

  iLOがCSRにFQDNを入力できるように、ネットワーク共通設定ページでドメイン名を設定します。

- iLOのIPアドレスを含みます - CSRにiLO IPアドレスを含めるには、このチェックボックスを選択します。

> **注記:**
> 多くのCAでは、この入力を受け入れられません。使用中のCAでこの入力を受け入れることがわかっていない場合は、このオプションを選択しないでください。

証明書署名要求

CSRには、クライアントブラウザーとiLO間の通信を検証するパブリックキーとプライベートキーのペアが含まれています。iLOは、SHA-256を使用して署名された2048ビットRSAキーまたはCNSA準拠キーを生成します。生成されたCSRは、新しいCSRが生成されるか、iLOが工場出荷時のデフォルト設定にリセットされるか、または証明書がインポートされるまで、メモリに保持されます。

信頼済みの証明書のインポート

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーでセキュリティをクリックし、SSL証明書タブをクリックします。
2. 証明書のカスタマイズをクリックします。
3. 証明書のインポートをクリックします。
4. 証明書のインポートウィンドウで、テキストボックスに証明書を貼り付けて、インポートをクリックします。

   iLOが要求を確認してiLOをリセットするように求めます。
5. はい、適用およびリセットをクリックします。

   iLOは、証明書をインポートしてからリセットします。

自動証明書登録の有効化

前提条件

- 証明書登録サーバーのURL
- チャレンジパスワード
- 証明書登録サーバーのCA証明書。
- CSRを構成する。
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- iLO設定の構成権限。

このタスクについて

手順

1. ナビゲーションツリーでセキュリティをクリックし、SSL証明書タブをクリックします。

   iLO自己署名証明書はデフォルトの証明書です。
2. SSL証明書を自動的に管理を選択します。
3. 証明書のカスタマイズをクリックします。自動証明書登録ページが開きます。
4. 証明書の登録設定に次の値を入力します。
   - サーバーのURL - 証明書登録サーバーのURL。
   - チャレンジパスワード - 証明書登録サーバーから取得され、証明書の登録および更新中にiLOの認証に使用されるチャレンジパスワード。
   - CA証明書 - 証明書登録サーバーのCA証明書。CA証明書は、iLOと証明書登録サーバー間の信頼を確立するために使用されます。

     注記:
     - サーバーのURL、チャレンジパスワード、およびCA証明書は、証明書登録の必須フィールドです。
     - iLOは、最大6 KBのサイズのCA証明書（PEM形式）のインポートをサポートします。
     - iLOは、最大63文字のチャレンジパスワードをサポートします。
   - 国（C） - このiLOサブシステムを所有する会社または組織が存在する国/地域を識別する2文字の国/地域番号。2文字の省略表記を大文字で入力します。

- 都道府県（ST） – このiLOサブシステムを所有する会社または組織が存在する都道府県。
- 市町村（L） – このiLOサブシステムを所有する会社または組織が存在する市町村。
- 組織名（O） – このiLOサブシステムを所有する会社または組織の名前。
- 組織ユニット（OU） – （省略可能）このiLOサブシステムを所有する会社または組織の中の単位。
- 共通名（CN） – このiLOサブシステムのFQDN。

  FQDNは、共通名（CN）ボックスに自動的に入力されます。

  iLOがCSRにFQDNを入力できるように、ネットワーク共通設定ページでドメイン名を設定します。

注記: CSRフィールドは、SSL証明書の手動インポートと自動インポートの両方に共通です。

5. （オプション）iLO IPアドレスをCSRに含めるには、iLOのIPアドレスを含みますチェックボックスを選択します。

注記:
一部の認証局（CA）は、このCSRフィールドをサポートしていない場合があります。使用中のCAでこの入力が受け入れられるかわからない場合は、このオプションを選択しないでください。

このオプションが有効な場合、iLOのIPアドレスがCSRサブジェクト代替名（SAN）の拡張子に含まれます。

6. 有効をクリックして、登録プロセスを開始します。

証明書登録サービスが有効になるとすぐに、証明書の登録ステータスは 進行中になります。

数分（最大10分）後に、ページを更新すると、最新の証明書登録ステータスが取得されます。登録が成功すると、証明書の登録ステータスは 成功になります。また、証明書登録サービスが正常に有効になったことを通知するメッセージが表示されます。登録が成功した後、 iLOを手動でリセットする必要があります。新しく信頼された証明書は、 iLOがリセットされた後でのみ使用されるようになります。

登録が失敗すると、証明書の登録ステータスは 失敗になります。失敗の原因と推奨されるアクションについて詳しくは、「セキュリティログ」ページを参照してください。

注記: 登録サービスが有効になっている場合、証明書の削除と手動インポートは許可されません。

証明書の登録設定のアップデート

前提条件

iLO設定の構成権限。

このタスクについて

手順

1. ナビゲーションツリーでセキュリティをクリックし、SSL証明書タブをクリックします。

   信頼済みのSSL証明書が使用中であることを通知するメッセージが表示されます。

2. 信頼済みのSSL証明書の下には、デフォルトでSSL証明書を自動的に管理オプションが選択されています。
3. 証明書のカスタマイズをクリックします。自動証明書登録ページが開きます。
4. フィールドを編集して、アップデートをクリックします。

注記: 設定をアップデートしても、証明書の登録は開始されません。登録を開始するには、最初にサービスを無効にしてから再度有効にします。

自動的に管理されるSSL証明書の更新

このタスクについて

証明書登録サービスが有効になっていて、証明書の有効期限が近づいている場合（つまり、有効期限から30日）、iLOは証明書の更新を自動的に開始します。iLOが証明書の更新を開始するとすぐに、証明書の登録ステータスは進行中になります。

更新が成功すると、証明書の登録ステータスは成功になります。更新ステータスについては、「セキュリティログ」ページを参照してください。更新が成功した後、iLOを手動でリセットする必要があります。新しく信頼された証明書は、iLOがリセットされた後でのみ使用されるようになります。

更新が失敗すると、証明書の登録ステータスは失敗になります。失敗の原因と推奨されるアクションについて詳しくは、「セキュリティログ」ページを参照してください。

登録サービスの無効化

前提条件

iLO設定の構成権限。

このタスクについて

登録サービスを無効にしても、サービスを使用して生成された証明書は削除されません。証明書を削除するには、SSL証明書の削除を参照してください。

サービスが無効になっている場合、iLOは証明書の更新を自動的に開始しません。

手順

1. 信頼済みのSSL証明書の下には、デフォルトでSSL証明書を自動的に管理オプションが選択されています。
2. 証明書のカスタマイズをクリックします。自動証明書登録ページが開きます。
3. サービスの無効をクリックします。
4. はい、無効にしますをクリックして、無効にすることを確認します。証明書の登録ステータスも無効になります。

   証明書登録の有効化については、 自動証明書登録の有効化セクションを参照してください。

SSL証明書の削除

前提条件

iLOの設定を構成する権限

このタスクについて

この機能を使用して、SSL証明書を削除し、iLO自己署名証明書を再生成します。

> **注記**: 証明書登録サービスが有効になっている場合、証明書の削除と手動インポートは許可されません。

次の理由から、証明書を削除する場合があります。

- 証明書の有効期限が切れた。
- 証明書に無効な情報が含まれている。
- 証明書に関してセキュリティ上の問題がある。

- 実績のあるサポート組織から証明書を削除するよう勧められた。

手順

1. ナビゲーションツリーでセキュリティをクリックし、SSL証明書タブをクリックします。
2. 削除をクリックします。

   iLOが既存の証明書を削除し、iLOをリセットしてから、新しい自己署名証明書を生成することを確認するように求めます。
3. はい、削除しますをクリックします。

   iLOがカスタムSSL証明書を削除し、リセットしてから、新しい自己署名証明書を生成します。

   iLOで新しい証明書を生成するには数分かかる場合があります。
4. 推奨：信頼済みの証明書を取得してインポートします。

   Hewlett Packard Enterpriseでは、信頼済みの証明書をインポートすることをお勧めします。

詳しくは

SSL証明書の取得とインポート
自動証明書登録の有効化

iLOのディレクトリの認証と認可設定

iLOファームウェアは、Microsoft Active DirectoryによるKerberos認証をサポートします。また、Active DirectoryやOpenLDAPディレクトリサーバーとのディレクトリ統合もサポートします。

ディレクトリ統合を構成するときに、スキーマフリー構成とHPE拡張スキーマ構成を選択できます。HPE拡張スキーマは、Active Directoryの場合のみサポートされます。iLOファームウェアは、ディレクトリサービスに接続する場合に、SSL接続を使用してディレクトリサーバーのLDAPポートに接続します。

ディレクトリサーバー証明書検証機能は、CA証明書をインポートすると有効にできます。この機能により、iLOがLDAP認証時に正しいディレクトリサーバーに接続できます。

iLOの認証およびディレクトリサーバー設定の構成は、ディレクトリまたはKerberos認証を使用するためのiLO構成プロセスの手順の1つです。これらの機能を使用するように環境をセットアップするには、追加の手順が必要です。

サブトピック

認証およびディレクトリサーバー設定を構成するための前提条件

iLOでKerberos認証の設定を構成します

iLOにおけるスキーマフリーディレクトリ設定の構成

iLOにおけるHPE拡張スキーマディレクトリ設定の構成

ディレクトリユーザーコンテキスト

ディレクトリサーバーCA証明書

ディレクトリサーバーCA証明書の削除

Kerberos認証およびディレクトリ統合によるローカル ユーザー アカウント

ディレクトリテストの実行

認証およびディレクトリサーバー設定を構成するための前提条件

手順

1. ご使用のiLOユーザーアカウントにiLO設定の構成権限があることを確認します。
2. この機能をサポートするライセンスをインストールします。
3. Kerberos認証またはディレクトリ統合をサポートするように環境を構成します。

詳しくは

Kerberos認証の設定
ディレクトリ統合の設定（スキーマフリー構成）
ディレクトリ統合の設定（HPE拡張スキーマ構成）

iLOでKerberos認証の設定を構成します

前提条件

- ご使用の環境がこの機能を使用するための前提条件を満たしていること。
- 環境のセットアップタスク中に作成したKerberosキータブファイルを使用できること。

手順

1. ナビゲーションツリーでセキュリティをクリックし、ディレクトリタブをクリックします。
2. Kerberos認証を有効にします。
3. Kerberos認証と同時にローカルユーザーアカウントを使用する場合は、ローカルユーザーアカウントを有効に設定します。
4. Kerberosレルムの名前を入力します。
5. Kerberos KDCサーバーアドレスを入力します。
6. Kerberos KDCサーバーポートを入力します。
7. Kerberosキータブファイルを追加するには、参照またはファイルを選択（ブラウザーによって異なる）をクリックして、画面の指示に従います。
8. 設定の適用をクリックします。
9. ディレクトリグループを構成するには、ディレクトリグループリンクをクリックします。

サブトピック

Kerberosの設定

詳しくは

認証およびディレクトリサーバー設定を構成するための前提条件
iLOディレクトリグループ
Kerberos認証の設定

Kerberosの設定

- Kerberos認証 - Kerberosログインを有効または無効にします。Kerberosログインが有効で、正しく構成されている場合、ログインページにゼロサインインボタンが表示されます。
- Kerberosレルム — iLOプロセッサーが動作しているKerberosレルムの名前。この値は最大127文字です。レルム名は、通常、大文字に変換されたDNS名です。レルム名は、大文字と小文字が区別されます。

- Kerberos KDCサーバーアドレス – Key Distribution Center（KDC）のIPアドレスまたはDNS名。この値は最大127文字です。各レルムには、認証サーバーおよびチケット交付サーバーを含む1つ以上のKey Distribution Center（KDC）がある必要があります。これらのサーバーは、結合させることができます。
- Kerberos KDCサーバーポート – KDCがリスンしているTCPまたはUDPポート番号。デフォルト値は88です。
- Kerberosキータブ – サービスプリンシパル名と暗号化されたパスワードのペアが含まれているバイナリファイル。Windows環境下では、`ktpass`ユーティリティを使用してキータブファイルを生成します。

iLOにおけるスキーマフリーディレクトリ設定の構成

前提条件

ご使用の環境がこの機能を使用するための前提条件を満たしていること。OpenLDAPベースのディレクトリサーバーを構成するには、OpenLDAPソフトウェアの管理者ガイドを参照してください。

手順

1. ナビゲーションツリーでセキュリティをクリックし、ディレクトリタブをクリックします。
2. LDAPディレクトリ認証メニューでディレクトリデフォルトスキーマを使用を選択します。
3. ディレクトリ統合と同時にローカルユーザーアカウントを使用する場合は、ローカルユーザーアカウントを有効に設定します。
4. OpenLDAPユーザーのみ：汎用LDAPを有効にします。

   この設定は、ディレクトリデフォルトスキーマを使用を選択している場合のみ使用可能です。
5. CAC/Smartcard認証が有効な構成では、CAC LDAPサービスアカウントとパスワードをiLOオブジェクト識別名CAC LDAPサービスアカウントおよびiLOオブジェクトパスワードボックスに入力します。
6. ディレクトリサーバーアドレスボックスに、ディレクトリサーバーのFQDNまたはIPアドレスを入力します。
7. ディレクトリサーバーLDAPポートボックスにディレクトリサーバーのポート番号を入力します。
8. （オプション）新しいCA証明書をインポートします。
   a. 証明書ステータスボックスでインポートをクリックします。
   b. Base64でエンコードされたX.509証明書データを証明書のインポートウィンドウに貼り付けてインポートをクリックします。
9. （オプション）既存のCA証明書を置き換えます。
   a. 証明書ステータスボックスで一覧をクリックします。
   b. 証明書詳細ウィンドウで新規をクリックします。
   c. Base64でエンコードされたX.509証明書データを証明書のインポートウィンドウに貼り付けてインポートをクリックします。
10. 1つまたは複数のディレクトリユーザーコンテキストボックスに有効な検索コンテキストを入力します。
11. 設定の適用をクリックします。
12. ディレクトリサーバーとiLO間の通信をテストするには、設定のテストをクリックします。
13. ディレクトリグループを構成するには、ディレクトリグループリンクをクリックします。

サブトピック

スキーマフリーディレクトリの設定

詳しくは

認証およびディレクトリサーバー設定を構成するための前提条件
iLOディレクトリグループ
ディレクトリテストの実行
ディレクトリユーザーコンテキスト
ディレクトリサーバーCA証明書
Kerberos認証およびディレクトリ統合によるローカル ユーザー アカウント
ディレクトリ統合の設定（スキーマフリー構成）

スキーマフリーディレクトリの設定

- ディレクトリデフォルトスキーマを使用 — ディレクトリ内のユーザーアカウントを使用するディレクトリ認証および権限付与を選択します。ユーザーの認証と権限付与には、ユーザーアカウントとグループメンバーシップが使用されます。

  この構成では、Active DirectoryおよびOpenLDAPがサポートされます。

- 汎用LDAP - この構成ではOpenLDAPでサポートされているBINDメソッドを使用することを指定します。
- iLOオブジェクト識別名/CAC LDAPサービスアカウント — CAC/Smartcard認証が構成され、スキーマフリーディレクトリオプションで使用される場合の、CAC LDAPサービスアカウントを指定します。

  iLOがディレクトリサーバーにアクセスするときに、ユーザー検索コンテキストはiLOオブジェクトDNに適用されません。

- iLOオブジェクトパスワード — CAC/Smartcard認証が構成され、スキーマフリーディレクトリオプションで使用される場合の、CAC LDAPサービスアカウントのパスワードを指定します。
- ディレクトリサーバーアドレス - ディレクトリサーバーのネットワークDNS名またはIPアドレスを指定します。ディレクトリサーバーアドレスは最大127文字です。

  FQDNを入力する場合、iLOでDNS設定が構成されていることを確認します。

  Hewlett Packard Enterpriseは、ディレクトリサーバーを定義するときにDNSラウンドロビンを使用することをおすすめします。

- ディレクトリサーバーLDAPポート - サーバー上の安全なLDAPサービス用のポート番号を指定します。デフォルト値は636です。ディレクトリサービスが別のポートを使用するように構成されている場合は、別の値を指定できます。セキュリティ保護された安全なLDAPポートを入力することを確認します。iLOセキュリティ保護されていないLDAPポートには接続できません。
- ディレクトリユーザーコンテキスト - これらのボックスを使用して、ユーザーがログイン時に完全なDNを入力する必要がないように、共通のディレクトリサブコンテキストを指定できます。すべてのディレクトリユーザーコンテキストの合計で1904文字の制限があります。
- 証明書ステータス - ディレクトリサーバーのCA証明書がロードされているかどうかを示します。

  ステータスがロード済の場合は、一覧をクリックするとCA証明書の詳細が表示されます。CA証明書がロードされていない場合、ステータスは未ロードと表示されます。iLOは、7 KBまでのサイズのSSL証明書をサポートしています。

iLOにおけるHPE拡張スキーマディレクトリ設定の構成

前提条件

ご使用の環境がこの機能を使用するための前提条件を満たしていること。

手順

1. ナビゲーションツリーでセキュリティをクリックし、ディレクトリタブをクリックします。
2. LDAPディレクトリ認証メニューでHPE拡張スキーマを使用を選択します。
3. ディレクトリ統合と同時にローカルユーザーアカウントを使用する場合は、ローカルユーザーアカウントを有効に設定します。
4. ディレクトリツリー内のこのiLOインスタンスの位置をiLOオブジェクト識別名/CAC LDAPサービスアカウントボックスに入力します。
5. ディレクトリサーバーアドレスボックスに、ディレクトリサーバーのFQDNまたはIPアドレスを入力します。
6. ディレクトリサーバーLDAPポートボックスにディレクトリサーバーのポート番号を入力します。
7. （オプション）新しいCA証明書をインポートします。
   a. 証明書ステータステキストボックスでインポートをクリックします。
   b. Base64でエンコードされたX.509証明書データを証明書のインポートウィンドウに貼り付けてインポートをクリックします。
8. （オプション）既存のCA証明書を置き換えます。
   a. 証明書ステータステキストボックスで一覧をクリックします。
   b. 証明書詳細ウィンドウで新規をクリックします。
   c. Base64でエンコードされたX.509証明書データを証明書のインポートウィンドウに貼り付けてインポートをクリックします。
9. 1つまたは複数のディレクトリユーザーコンテキストボックスに有効な検索コンテキストを入力します。
10. 設定の適用をクリックします。
11. ディレクトリサーバーとiLO間の通信をテストするには、設定のテストをクリックします。

サブトピック

HPE拡張スキーマディレクトリの設定

詳しくは

認証およびディレクトリサーバー設定を構成するための前提条件
ディレクトリテストの実行
ディレクトリユーザーコンテキスト
Kerberos認証およびディレクトリ統合によるローカル ユーザー アカウント
ディレクトリ統合の設定（HPE拡張スキーマ構成）

HPE拡張スキーマディレクトリの設定

- HPE拡張スキーマを使用 - HPE拡張スキーマで作成されたディレクトリオブジェクトを使用するディレクトリ認証および権限付与を選択します。HPE拡張スキーマを使用してディレクトリが拡張されている場合は、このオプションを選択します。HPE拡張スキーマは、Microsoft Windowsのみで動作します。この構成では、Active Directoryをサポートしています。
- iLOオブジェクト識別名/CAC LDAPサービスアカウント - HPE拡張スキーマ構成で、この設定はこのiLOインスタンスがディレクトリツリーのどこにリストされるかを指定します。例：

  ```
  cn=Mail Server iLO,ou=Management Devices,o=ab
  ```

  iLOがディレクトリサーバーにアクセスするときに、ユーザー検索コンテキストはiLOオブジェクトDNに適用されません。
- ディレクトリサーバーアドレス - ディレクトリサーバーのネットワークDNS名またはIPアドレスを指定します。ディレ

クトリサーバーアドレスは最大127文字です。

FQDNを入力する場合、iLOでDNS設定が構成されていることを確認します。

Hewlett Packard Enterpriseは、ディレクトリサーバーを定義するときにDNSラウンドロビンを使用することをおすすめします。

- ディレクトリサーバーLDAPポート - サーバー上の安全なLDAPサービス用のポート番号を指定します。デフォルト値は636です。ディレクトリサービスが別のポートを使用するように構成されている場合は、別の値を指定できます。セキュリティ保護された安全なLDAPポートを入力することを確認します。iLOセキュリティ保護されていないLDAPポートには接続できません。
- 証明書ステータス - ディレクトリサーバーのCA証明書がロードされているかどうかを示します。

  ステータスがロード済の場合は、一覧をクリックするとCA証明書の詳細が表示されます。CA証明書がロードされていない場合、ステータスは未ロードと表示されます。iLOは、7 KBまでのサイズのSSL証明書をサポートしています。
- ディレクトリユーザーコンテキスト - これらのボックスを使用して、ユーザーがログイン時に完全なDNを入力する必要がないように、共通のディレクトリサブコンテキストを指定できます。すべてのディレクトリユーザーコンテキストの合計で1904文字の制限があります。

ディレクトリユーザーコンテキスト

固有DNを使用すると、ディレクトリに表示されるすべてのオブジェクトを識別できます。ただし、DNが長かったり、ユーザーが自分のDNを知らなかったり、ユーザーが異なるディレクトリコンテキストにアカウントを持っている場合があります。ユーザーコンテキストを使用した場合、iLOはDNでディレクトリサービスへの接続を試みたあと、ログインに成功するまで順番に検索コンテキストを適用します。

- **例1** - 検索コンテキスト
  `ou=engineering,o=ab`
  を入力すると、`cn=user,ou=engineering,o=ab`の代わりに
  `ユーザー`
  としてログインできます。
- **例2** - IM、サービス、およびトレーニング部門がシステムを管理している場合、次の検索コンテキストを使用することでこれらの部門のユーザーが彼らの共通名を使用してログインすることが可能となります。
  - `ディレクトリユーザーコンテキスト1:ou=IM,o=ab`
  - `ディレクトリユーザーコンテキスト2:ou=Services,o=ab`
  - `ディレクトリユーザーコンテキスト3:ou=Training,o=ab`

  ユーザーが`IM`部門と`トレーニング`部門の両方に所属する場合は、最初に`cn=user,ou=IM,o=ab`としてログインが試みられます。
- **例3（Active Directory専用）** - Microsoft Active Directoryでは、代替ユーザー認証情報フォーマットを使用できます。ユーザーは、`user@domain.example.com`としてログインすることができます。検索コンテキスト
  `@domain.example.com`
  を入力すると、`ユーザー`としてログインできます。成功したログイン試行のみが、この形式の検索コンテキストをテストできます。
- **例4（OpenLDAP ユーザー）** - ユーザーがDN `UID=user, ou=people, o=ab`を持っており、かつ検索コンテキストを
  `ou=people, o=ab`
  を入力した場合、ユーザーはDNを入力する代わりに
  `ユーザー`
  としてログインすることができます。
  この形式を使用するには、セキュリティ - ディレクトリページで汎用LDAPを有効にする必要があります。

ディレクトリサーバーCA証明書

LDAP認証時にiLOがディレクトリサーバー証明書を、CA証明書がすでにインポートされている場合に検証します。証明書が正しく検証されるように、必ず正しいCA証明書をインポートしてください。証明書の検証が失敗すると、iLOログインが拒否されてイベントが記録されます。CA証明書がインポートされていない場合、ディレクトリサーバー証明書の検証手順はスキップされます。

ディレクトリサーバーとiLO間のSSL通信を検証するには、設定のテストをクリックします。

ディレクトリサーバーCA証明書の削除

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーでセキュリティをクリックし、ディレクトリタブをクリックします。
2. 証明書ステータステキストボックスで一覧をクリックします。
3. 証明書詳細ウィンドウで削除をクリックします。

   iLOが要求を確認するように求めます。
4. OKをクリックします。

   証明書が削除されたことがiLOによって通知されます。

Kerberos認証およびディレクトリ統合によるローカル ユーザー アカウント

iLOがディレクトリまたはKerberos認証を使用するように設定した場合、ローカルユーザーアカウントをアクティブにすることができます。この構成では、ローカルおよびディレクトリベースのユーザーアクセスを使用できます。

以下事項に留意してください。

- ローカルユーザーアカウントが有効になっている場合、設定されているユーザーはローカルに保存されたユーザー認証情報を使用してログインできます。
- ローカルアカウントが無効になっている場合、ユーザーアクセスは有効なディレクトリ認証情報に制限されます。
- Kerberosまたはディレクトリを介して有効なアクセスを確保するまでは、ローカルユーザーアクセスを無効にしないでください。
- Kerberos認証またはディレクトリの統合を使用する場合、Hewlett Packard Enterpriseは、ローカルユーザーアカウントを有効にして管理者権限を持つユーザーアカウントを構成することをおすすめします。iLOがディレクトリサーバーと通信できない場合、このアカウントを使用できます。
- ローカルユーザーアカウントを介したアクセスは、ディレクトリサポートが無効になっている場合、またはライセンスが取り消された場合に有効になります。

ディレクトリテストの実行

このタスクについて

ディレクトリテストを使用すると、設定が済んだディレクトリの設定を検証できます。ディレクトリテストの結果は、ディ

レクトリ設定が保存されるとき、またはディレクトリテストが開始されるときにリセットされます。

手順

1. ナビゲーションツリーでセキュリティをクリックし、ディレクトリタブをクリックします。
2. ディレクトリページの下部にある設定のテストをクリックします。

   iLOにより、ディレクトリ設定の有効性を確認するために設計された一連の簡単なテストの結果が表示されます。ディレクトリ設定を正しく構成した後にこれらのテストを再実行する必要はありません。ディレクトリテストページでは、ディレクトリユーザーとしてログインする必要はありません。
3. ディレクトリテスト制御セクションで、ディレクトリ管理者識別名ボックスとディレクトリ管理者パスワードボックスに、ディレクトリ管理者のDNおよびパスワードを入力します。

   Hewlett Packard Enterpriseでは、ディレクトリ内にiLOオブジェクトを作成する際に使用するものと同じ識別名とパスワードを使用することをおすすめします。これらの識別情報は、iLOに保存されるものではなく、iLOオブジェクトとユーザー検索コンテキストを確認するために使用されます。
4. ディレクトリテスト制御セクションで、テストユーザー名ボックスとテストユーザーパスワードボックスに、テストユーザーの名前およびパスワードを入力します。
5. テストの開始をクリックします。

   複数のテストがバックグラウンドで開始し、最初にサーバーとのSSL接続を確立し、ユーザー権限を評価して、ネットワーク経由でのディレクトリユーザーに対するPingが実行されます。

   テストの実行中、ページは定期的に更新されます。テストはいつでも停止でき、ページを手動で更新することもできます。

サブトピック

ディレクトリテストの入力値

ディレクトリテストのステータス値と制御

ディレクトリテスト結果

iLOディレクトリテスト

ディレクトリテストの入力値

ディレクトリテストを実行するときに次の値を入力します。

- ディレクトリ管理者識別名 – iLOオブジェクト、ロール、および検索コンテキストについてディレクトリを検索します。このユーザーは、ディレクトリ読み取り権限を持っている必要があります。
- ディレクトリ管理者パスワード – ディレクトリ管理者を認証します。
- テストユーザー名およびテストユーザーパスワード – iLOへのログインとアクセス権をテストします。ユーザー検索コンテキストを適用できるため、ユーザー名は完全修飾である必要はありません。このユーザーは、このiLOのロールに関連付けられている必要があります。

  通常、このアカウントは、テスト対象のiLOプロセッサーへのアクセスに利用します。これはディレクトリ管理者アカウントでも構いませんが、スーパーユーザーアカウントではテストでユーザー認証を検証できません。iLOには、これらの認証情報が保存されません。

注記:

- ディレクトリ管理者識別名とテストユーザー名の最大長は128文字です。
- ディレクトリ管理者識別名とテストユーザーパスワードの最大長は64文字です。

ディレクトリテストのステータス値と制御

iLOに以下のディレクトリテストのステータス値が表示されます。

- 実行中 – ディレクトリテストが現在バックグラウンドで実行されていることを示します。

  現在のテストを取り消すには、テストの中止 をクリックします。最新の結果でページの内容をアップデートするには、更新 をクリックします。テストの中止ボタンを使用しても、テストがただちに終了されない場合があります。

- 未テスト – ディレクトリテストは最新であり、新しいパラメーターを指定してテストを再度実行できることを示します。

  テストの開始ボタンを使用してテストを開始し、現在のテスト制御値を使用することができます。ディレクトリテストは、すでに実行中の場合には、開始できません。

- 停止中 – ディレクトリテストがまだ停止できる段階に達していないことを示します。ステータスが未テストに変わるまでは、テストを再開できません。テストが完了したかどうかを確認するには、更新ボタンを使用してください。

ディレクトリテスト結果

ディレクトリテスト結果セクションには、ディレクトリテストのステータスが最後のアップデート日時とともに表示されます。

- 全体のステータス – テストの結果の要約が示されます。
  - 未実行 – テストは実行されていません。
  - 不明 – 結果は報告されませんでした。
  - パス – エラーは報告されませんでした。
  - 問題が見つかりました – 問題が報告されました。
  - 失敗 – 特定のサブテストが失敗しました。問題を特定するには、画面上のログを調べます。
  - 警告 – 1つ以上のディレクトリテストが、警告ステータスを報告しました。
- テスト – 各テストの名前。
- 結果 – 特定のディレクトリ設定のステータス、または1つまたは複数のディレクトリ設定による動作のステータスが報告されます。これらの結果は、テストシーケンスを実行すると生成されます。結果は次の場合に停止します。
  - テストが完了するまで実行した。
  - テストの障害によって進行が妨げられた。
  - テストが停止した。

  テスト結果は次のようになります。
  - パス – テストは正常に実行されました。複数のディレクトリサーバーがテストされた場合は、テストを実行したすべてのサーバーで成功しています。
  - 未実行 – テストは実行されませんでした。
  - 失敗 – 1つまたは複数のディレクトリサーバーについてテストが成功しませんでした。それらのサーバーでは、ディレクトリサポートを使用できない可能性があります。
  - 警告 – テストが実行され、証明書エラーなどの警告状態を報告しました。注意列で、警告状態を解消するために推奨される処置を確認してください。

- 注意 – ディレクトリテストのさまざまな段階の結果を示します。データは、エラーの詳細と、ディレクトリサーバー証明書のサブジェクトや、評価されたロールなどの情報によってアップデートされます。

iLOディレクトリテスト

ディレクトリサーバーDNS名

ディレクトリサーバーがFQDNフォーマット（directory.company.com）で定義されている場合、iLOは、名前をFQDNフォーマットからIPフォーマットに解決し、設定されたDNSサーバーに問い合わせます。

iLOが、構成されたディレクトリサーバーのIPアドレスを取得した場合、テストは成功します。iLOがディレクトリサーバーのIPアドレスを取得できない場合、このテストと以後のテストすべてが失敗します。

ディレクトリサーバーがIPアドレスで構成されている場合、iLOはこのテストを省略します。

ディレクトリサーバーへのPing

iLOは、設定されたディレクトリサーバーに対するpingを開始します。

iLO がping応答を受信する場合、テストは成功します。ディレクトリサーバーがiLOに応答しない場合、テストは失敗します。

テストが失敗した場合、iLOは以後のテストを続行します。

ディレクトリサーバーへの接続

iLOは、ディレクトリサーバーとのLDAP接続交渉を試みます。

iLOが接続を開始できた場合、テストは成功します。

指定したディレクトリサーバーとのLDAP接続をiLOが開始できなかった場合、テストは失敗します。以後のテストは、停止します。

SSLを使用しての接続

iLOは、ポート636経由でSSLハンドシェーク、交渉、およびディレクトリサーバーとのLDAP通信を開始します。

iLOとディレクトリサーバー間のSSLハンドシェークと交渉が成功した場合、テストは成功します。

LDAPサーバー証明書の検証エラーはこのテストの結果に報告されます。

ディレクトリサーバーへのバインド

このテストでは、接続は、テストコントロールに指定したユーザー名とバインドされます。ユーザーを指定しない場合、 iLO は匿名バインドを実行します。

ディレクトリサーバーがバインドを受け付けると、テストは成功します。

ディレクトリ管理者のログイン

ディレクトリ管理者識別名とディレクトリ管理者パスワードを指定した場合、iLOは、これらの値を使用して、管理者としてディレクトリサーバーにログインします。これらの値の指定は省略できます。

ユーザー認証

iLOは、指定したユーザー名とパスワードでディレクトリサーバーに認証されます。

提供したユーザー認証情報が正しい場合、テストは成功します。

ユーザー名および/またはパスワードが正しくない場合、テストは失敗します。

ユーザー承認

このテストは、指定したユーザー名が指定したディレクトリグループに属し、ディレクトリサービスの設定中に指定したディレクトリ検索コンテキストに含まれることを確認します。

ディレクトリユーザーコンテキスト

ディレクトリ管理者識別名を指定した場合、iLOは、指定したコンテキストを検索しようと試みます。

iLOが管理者認証情報を使用し、ディレクトリ内のコンテナーを検索してコンテキストを見つけると、テストは成功します。

@記号で始まるコンテキストをテストできる唯一の方法はユーザーログインです。

失敗は、コンテナーが見つからなかったことを示します。

LOMオブジェクトの存在

このテストは、セキュリティ – ディレクトリページで構成されたiLOオブジェクト識別名を使用して、ディレクトリサーバー内のiLOオブジェクトを検索します。

iLOがそれ自体を表現するオブジェクトを見つけると、テストは成功します。

このテストは、LDAPディレクトリ認証が無効になっていても実行されます。

iLOセキュリティ状態

本番環境（デフォルト）

iLOがこのセキュリティ状態に設定されている場合、次のようになります。

- iLOは工場出荷時のデフォルトの暗号化設定を使用します。
- iLOセキュリティをバイパスするためのシステムメンテナンススイッチ設定（iLOセキュリティオーバーライドスイッチと呼ばれる場合もある）は、iLOへのログインに関するパスワード要件を無効にします。
- リモートコンソールデータは、AES-128双方向暗号化を使用します。

高セキュリティ

iLOがこのセキュリティ状態に設定されている場合、次のようになります。

- iLOは、以下を経由した安全なHTTP伝送を含め、安全なチャネル経由のAES暗号の使用を強制します。
  - ブラウザー
  - SSHポート
  - iLO RESTful API
  - RIBCL

  サポートされている暗号を使用してこの安全なチャネル経由でiLOに接続します。このセキュリティ状態は、安全でないチャネル経由の通信と接続には影響しません。
- ホストシステムから実行される次のコマンドに対するユーザー名とパスワードの制限が適用されます。
  - iLO RESTful API
  - RIBCL
- リモートコンソールデータは、AES-128双方向暗号化を使用します。
- HPQLOCFGユーティリティは、iLOとのSSL接続をネゴシエーションした後、利用可能な最強の暗号を使用してRIBCLスクリプトをネットワーク経由でiLOに送信します。
- TLS 1.2をサポートしていないネットワークベースのツールを使用してサーバーに接続することはできません。
- iLOセキュリティをバイパスするためのシステムメンテナンススイッチ設定（iLOセキュリティオーバーライドスイッチと呼ばれる場合もある）は、iLOへのログインに関するパスワード要件を無効にしません。

FIPS

Common Criteriaコンプライアンス、Payment Card Industryコンプライアンス、またはその他の標準にはFIPSセキュリティ状態が必要になる場合があります。

iLOがこのセキュリティ状態に設定されている場合、次のようになります。

- iLOは、FIPS 140-2レベル1の要件への準拠を目的とするモードで動作します。

  FIPSは、米国政府機関および契約業者によって適用を義務付けられている一連のコンピューターセキュリティ規格で

す。

FIPSのセキュリティ状態は、FIPS承認済みと同じではありません。FIPS承認済みは、Cryptographic Module Validation Programを完了することにより承認を受けたソフトウェアを意味します。

- iLOは、以下を経由した安全なHTTP伝送を含め、安全なチャネル経由のAES暗号の使用を強制します。
  - ブラウザー
  - SSHポート
  - iLO RESTful API
  - RIBCL

  サポートされている暗号を使用してこの安全なチャネル経由でiLOに接続します。このセキュリティ状態は、安全でないチャネル経由の通信と接続には影響しません。
- ホストシステムから実行される次のコマンドに対するユーザー名とパスワードの制限が適用されます。
  - iLO RESTful API
  - RIBCL
- リモートコンソールデータは、AES-128双方向暗号化を使用します。
- HPQLOCFGユーティリティは、iLOとのSSL接続をネゴシエーションした後、利用可能な最強の暗号を使用してRIBCLスクリプトをネットワーク経由でiLOに送信します。
- TLS 1.2をサポートしていないネットワークベースのツールを使用してサーバーに接続することはできません。
- iLOセキュリティをバイパスするためのシステムメンテナンススイッチ設定（iLOセキュリティオーバーライドスイッチと呼ばれる場合もある）は、iLOへのログインに関するパスワード要件を無効にしません。

CNSA

CNSAセキュリティ状態（SuiteBモードとも呼ばれる）は、FIPSセキュリティ状態が有効になっている場合にのみ使用できます。

iLOがこのセキュリティ状態に設定されている場合、次のようになります。

- iLOは、NSAによって定義されたCNSA要件への準拠を目的とするモードで動作します。
- iLOは、米国政府機密として分類されたデータを保持するシステムの保護を目的とするモードで動作します。
- TLS 1.2をサポートしていないネットワークベースのツールを使用してサーバーに接続することはできません。
- iLOセキュリティをバイパスするためのシステムメンテナンススイッチ設定（iLOセキュリティオーバーライドスイッチと呼ばれる場合もある）は、iLOへのログインに関するパスワード要件を無効にしません。
- iLOへの接続に使用するソフトウェアまたはユーティリティはすべて、CNSAに準拠している必要があります。

  以下に例を示します。
  - ファームウェアアップデートユーティリティ
  - SSHクライアント
  - HPEおよび他社製のスクリプティングツールとコマンドラインツール
  - HPEおよび他社製の管理ツール
  - アラートメール、syslog、LDAP、またはキーマネージャーサーバー
  - リモートサポート ソフトウェア
- HTML5リモートコンソールを使用していることを確認してください。このコンソールでは、AES-256ビットCNSA準拠の暗号の使用が強制されます。.NET IRCはCNSAに準拠していません。

準拠を確認するには、ソフトウェアのベンダーに確認するか、Wiresharkなどのユーティリティを使用します。

iLO暗号化設定

すべてのGen11サーバーに付属しているHPE iLO Standardによって、お客様は次の3つのセキュリティ状態のいずれかでサーバーを構成することができます。iLO Advancedのライセンスでは、CNSAの最上位レベルの暗号化機能を必要とするお客様は4つ目のセキュリティ状態を利用できます。

セキュリティの段階が上がると、サーバーは、Webページ、SSH、およびネットワーク通信に対してより強力な暗号化規則を適用します。各ネットワーク接続の両端が暗号化規則をサポートしている必要があることに注意してください。そうでないと通信はできず、インターフェイスによっては潜在的なセキュリティ上の脅威を制限するためにシャットダウンされます。

次のセキュリティ状態を利用できます。

- 本番環境
- 高セキュリティ
- FIPS
- CNSA

サブトピック

本番環境セキュリティ状態の有効化

前提条件

iLOの設定を構成する権限

手順

1. （オプション）必要に応じてファームウェアおよびソフトウェアのアップデートをインストールします。
2. ナビゲーションツリーでセキュリティをクリックして、暗号化タブをクリックします。

   以下の 現在の設定が表示されます。
   - ネゴシエートされた暗号 – ネゴシエートされた暗号が表示されます。
   - セキュリティ状態 – 選択したセキュリティ状態が表示されます。
   - 有効なTLSバージョン – 有効なTLSバージョンが表示されます。

3. セキュリティ設定のアップデートのセキュリティ状態メニューで本番環境を選択します。

   デフォルトでは、 TLS 1.0、 TLS 1.1、 TLS 1.2が本番環境モードで有効になります。TLS 1.2はどのモードでも無効にすることはできません。

4. （オプション）TLS 1.0、TLS 1.1、または両方を本番環境モードで無効にすることができます。

   注記:
   - TLSバージョン1.0および1.1は、本番環境モードでのみ有効または無効にできます。
   - TLSバージョン1.0および1.1は、より高いセキュリティモードでは無効になります。
   - TLS 1.2をサポートしていないツールは、TLS 1.0および1.1が無効になっている場合、iLOに接続できません。

5. 適用をクリックします。

   iLOは、新しい設定を適用するためにiLOの再起動を確認するよう要求します。

6. 使用中のブラウザー接続を終了し、iLOを再起動するには、はい、適用してリセットしますをクリックします。

   接続が再確立されるまでに、数分かかることがあります。

7. 開いているブラウザーウィンドウをすべて閉じます。

   ブラウザーセッションが開いたままになっていると、設定されたセキュリティ状態に誤った暗号が使用される場合があります。

詳しくは

iLOアクセス設定の構成
iLOセキュリティ状態

高セキュリティセキュリティ状態の有効化

前提条件

iLOの設定を構成する権限

手順

1. （オプション）必要に応じてファームウェアおよびソフトウェアのアップデートをインストールします。
2. ナビゲーションツリーでセキュリティをクリックして、暗号化タブをクリックします。

   以下の 現在の設定が表示されます。
   - ネゴシエートされた暗号 – ネゴシエートされた暗号が表示されます。
   - セキュリティ状態 – 選択したセキュリティ状態が表示されます。
   - 有効なTLSバージョン – 有効なTLSバージョンが表示されます。
3. セキュリティ設定のアップデートのセキュリティ状態メニューで高セキュリティを選択します。
4. 適用をクリックします。

   iLOは、新しい設定を適用するためにiLOの再起動を確認するよう要求します。

5. 使用中のブラウザー接続を終了し、iLOを再起動するには、はい、適用してリセットしますをクリックします。

   接続が再確立されるまでに、数分かかることがあります。

6. 開いているブラウザーウィンドウをすべて閉じます。

   ブラウザーセッションが開いたままになっていると、設定されたセキュリティ状態に誤った暗号が使用される場合があ

ります。

7. アクセス設定ページで匿名データが無効になっていることを確認します。

FIPSおよびCNSAセキュリティ状態を有効にする

前提条件

- iLOの設定を構成する権限
- オプションのCNSAセキュリティ状態を有効にする予定の場合は、この機能をサポートするライセンスがインストールされていること。
- デフォルトのiLOユーザー認証情報があること。

このタスクについて

この手順は、FIPSまたはCNSAのセキュリティ状態を構成するためのものです。iLOをFIPS承認済み環境に構成するには、iLOによるFIPS承認済み環境の構成を参照してください。

手順

1. （オプション）現在のiLO構成をバックアップします。

   HPONCFGを使用して、この手順を実行できます。

2. （オプション）必要に応じてファームウェアおよびソフトウェアのアップデートをインストールします。
3. ナビゲーションツリーでセキュリティをクリックして、暗号化タブをクリックします。

   以下の 現在の設定が表示されます。
   - ネゴシエートされた暗号 – ネゴシエートされた暗号が表示されます。
   - セキュリティ状態 – 選択したセキュリティ状態が表示されます。
   - 有効なTLSバージョン – 有効なTLSバージョンが表示されます。
4. セキュリティ設定のアップデートのセキュリティ状態メニューでFIPSを選択し、適用をクリックします。

   iLOが要求を確認するように求めます。

   注意:

   FIPSセキュリティ状態を有効にするとiLOが工場出荷時のデフォルト設定にリセットされます。ユーザーデータとほとんどの構成設定を含むすべてのiLO設定が消去されます。iLOイベントログ、IML、セキュリティログも消去されます。インストール済みのライセンスキーは保持されます。

   FIPSセキュリティ状態を無効にする唯一の方法は、iLOを工場出荷時のデフォルト設定にリセットすることです。

5. FIPSセキュリティ状態を有効にする要求を確認するためには、はい、適用およびリセットをクリックします。

   iLOがFIPSセキュリティ状態を有効にした状態で再起動します。接続の再確立が試みられるまでに90秒以上かかります。

6. （オプション）CNSAセキュリティ状態を有効にします。
   a. デフォルトのユーザー認証情報を使用してiLOにログインします。
   b. ナビゲーションツリーでセキュリティをクリックして、暗号化タブをクリックします。

      以下の 現在の設定が表示されます。
      - ネゴシエートされた暗号 – ネゴシエートされた暗号が表示されます。
      - セキュリティ状態 – 選択したセキュリティ状態が表示されます。

- 有効なTLSバージョン – 有効なTLSバージョンが表示されます。

c. セキュリティ設定のアップデートのセキュリティ状態メニューでCNSAを選択し、適用をクリックします。

iLOが要求を確認するように求めます。

d. CNSAセキュリティ状態を有効にする要求を確認するためには、はい、適用およびリセットをクリックします。

iLOがCNSAセキュリティ状態を有効にした状態で再起動します。接続の再確立が試みられるまでに90秒以上かかります。

e. デフォルトのiLO認証情報を使用してiLOに再度ログインします。

CNSAのセキュリティ状態を有効にした後、ライセンスが期限切れになるか、ライセンスをダウングレードした場合、iLOは構成されたセキュリティ状態で引き続き動作します。期限切れになったライセンス、またはダウングレードしたライセンスによってアクティブ化された他のすべての機能は使用できなくなります。

7. 信頼済みの証明書をインストールします。

FIPSセキュリティ状態が有効な場合、デフォルトの自己署名SSL証明書は許可されません。FIPSセキュリティ状態を使用するようにiLOを設定すると、以前にインストールされた信頼済みの証明書（手動インポートまた自動証明書登録のいずれかでインストール）は削除されます。

8. アクセス設定ページでIPMI/DCMI over LANアクセス、匿名データ、およびSNMPアクセスオプションを無効にします。

重要:

IPMIおよびSNMPの標準準拠実装など、一部のiLOインターフェイスは、FIPSに準拠しておらず、FIPS準拠にすることはできません。

構成がFIPSに準拠しているかどうかを確認するには、構成をiLO FIPS妥当性確認プロセスの一部であったセキュリティポリシードキュメントと照合してください。

検証済みバージョンのiLOのセキュリティポリシードキュメントは、**NISTのWebサイト**にあります。iLO6 FIPS情報にアクセスするには、検証済みモジュールの検索ページで証明書番号3122を入力します。

9. （オプション）iLO構成をバックアップしている場合は、それをリストアします。

HPONCFGを使用して、この手順を実行できます。

10. （オプション）構成をリストアした場合は、ローカルiLOユーザーアカウントに新しいパスワードを設定します。

11. （オプション）構成をリストアした場合は、アクセス設定ページでIPMI/DCMI over LANアクセス、匿名データ、およびSNMPアクセスが無効になっていることを確認します。

これらの設定は、構成をリストアするとリセットされる可能性があります。

12. （オプション）ログインセキュリティバナーを構成してiLOユーザーにシステムがFIPSセキュリティ状態を使用していることを知らせます。

詳しくは

iLOのデフォルトのDNS名とユーザーアカウント
iLOのバックアップとリストア
iLOアクセス設定の構成
SSL証明書の取得とインポート
ログインセキュリティバナーの構成

高いセキュリティ状態を使用する場合のiLOへの接続

デフォルト値（本番環境）よりも高いセキュリティ状態を有効にすると、iLOは、AES暗号を使用して安全なチャネルを通じて接続することを要求します。

iLOがCNSAセキュリティ状態を使用するように構成されている場合、AES 256 GCM暗号が必要です。

Webブラウザー

ブラウザーがTLS 1.2およびAES暗号をサポートするよう設定します。ブラウザーがAES暗号を使用していない場合、iLOに接続できません。

ブラウザーが異なると、交渉済み暗号を選択する方法も異なります。詳しくは、ブラウザーのドキュメントを参照してください。

ブラウザーの暗号設定を変更する前に、現在のブラウザーを通じてiLOからログアウトしてください。iLOにログインしている間に行った暗号設定の変更により、ブラウザーでAES以外の暗号がそのまま使用できる場合があります。

SSH接続

使用可能な暗号の設定については、SSHユーティリティのドキュメントを参照してください。

RIBCL

- HPQLOCFGは、以下のような暗号詳細を出力表示します。

```
Detecting iLO...
Negotiated cipher: 256-bit Aes256 with 0-bit Sha384 and 384-bit 44550
```

- HPONCFGでは、「高セキュリティ」、FIPS、またはCNSAのセキュリティ状態が有効なときユーザー認証情報が必要になります。必要なユーザーの権限が割り当てられていない場合は、エラーメッセージが表示されます。

  ホスト認証が必要のアクセス設定は、ホストベースの構成ユーティリティに次の影響を与えます。

  - 有効 – すべてのiLOセキュリティ状態のホストベースの構成ユーティリティを使用するには、有効な認証情報が必要です。
  - 無効 – iLOが製品または高セキュリティのセキュリティ状態を使用するように設定されている場合、有効な認証情報は必要ありません。

  ホスト認証が必要の設定は、FIPSまたはCNSAセキュリティ状態が使用されている場合は無効にすることはできません。

iLO RESTful API

TLS 1.2とAES暗号をサポートするユーティリティを使用します。

iLOによるFIPS承認済み環境の構成

このタスクについて

以下の手順を使用して、iLOをFIPS検証済み環境で操作します。FIPSセキュリティ状態をiLOで使用するには、FIPSおよびCNSAセキュリティ状態を有効にするを参照してください。

重要なのは、FIPS検証済みバージョンのiLOがご使用の環境に必要かどうか、あるいはiLOをFIPSセキュリティ状態を有効にして実行することで十分かどうかを判断することです。検証プロセスに時間がかかるため、FIPS検証済みバージョンのiLOが、新機能とセキュリティ強化が加わった非検証バージョンに置き換えられている場合があります。このような状況では、FIPS検証済みバージョンのiLOが最新バージョンよりも安全性が低くなる場合があります。

手順

FIPS検証済みバージョンのiLOによる環境をセットアップするには、iLO FIPS承認プロセスの一部であったセキュリティポリシードキュメントの手順に従ってください。

検証済みのセキュリティポリシードキュメントは、**NISTのWebサイト**にあります。iLO6 FIPS情報にアクセスするには、検証済みモジュールの検索ページで証明書番号3122を入力します。

FIPSセキュリティ状態の無効化

手順

1. FIPSセキュリティ状態を無効にするには（たとえばサーバーを運用停止する場合）、iLOを工場出荷時のデフォルト設定に設定します。

   このタスクを実行するには、RIBCLスクリプト、iLO RESTful API、またはiLO6構成ユーティリティを使用します。

   > △ **注意:**
   >
   > iLOを工場出荷時のデフォルト設定にリセットすると、すべてのiLO設定が消去されます。消去される設定は、ユーザーデータ、ライセンスデータ、構成設定、ログなどです。サーバーに工場でインストールされたライセンスキーがある場合、このライセンスキーは保持されます。
   >
   > この手順によりiLOログ内のすべてのデータが消去されるため、リセットに関するイベントはログに記録されません。

2. サーバーのオペレーティングシステムを再起動します。

   工場出荷時のデフォルト設定へのリセット中に、SMBIOSレコードはクリアされます。メモリおよびネットワーク情報は、サーバーOSの再起動が完了するまでiLO Webインターフェイスに表示されません。

詳しくは

iLOの工場出荷時デフォルト設定へのリセット（iLO6構成ユーティリティ）

CNSAセキュリティ状態の無効化

手順

1. CNSAセキュリティ状態を無効にするには、次のいずれかを実行します。

   - CNSAセキュリティ状態を無効にして、FIPSセキュリティ状態を引き続き使用するには、セキュリティ状態をCNSAからFIPSに変更します。
   - CNSAおよびFIPSセキュリティ状態を無効にするには、iLOを工場出荷時のデフォルト設定に設定します。

     このタスクを実行するには、RIBCLスクリプト、iLO RESTful API、またはiLO6構成ユーティリティを使用します。

     > △ **注意:**
     >
     > iLOを工場出荷時のデフォルト設定にリセットすると、すべてのiLO設定が消去されます。消去される設定は、ユーザーデータ、ライセンスデータ、構成設定、ログなどです。サーバーに工場でインストールされたライセンスキーがある場合、このライセンスキーは保持されます。
     >
     > この手順によりiLOログ内のすべてのデータが消去されるため、リセットに関するイベントはログに記録されません。

2. iLOを工場出荷時のデフォルト設定にリセットした場合、サーバーのオペレーティングシステムを再起動します。

   工場出荷時のデフォルト設定へのリセット中に、SMBIOSレコードはクリアされます。メモリおよびネットワーク情報は、サーバーOSの再起動が完了するまでiLO Webインターフェイスに表示されません。

詳しくは

iLOの工場出荷時デフォルト設定へのリセット（iLO6構成ユーティリティ）

iLOセキュリティ状態

本番環境（デフォルト）

iLOがこのセキュリティ状態に設定されている場合、次のようになります。

- iLOは工場出荷時のデフォルトの暗号化設定を使用します。
- iLOセキュリティをバイパスするためのシステムメンテナンススイッチ設定（iLOセキュリティオーバーライドスイッチと呼ばれる場合もある）は、iLOへのログインに関するパスワード要件を無効にします。
- リモートコンソールデータは、AES-128双方向暗号化を使用します。

高セキュリティ

iLOがこのセキュリティ状態に設定されている場合、次のようになります。

- iLOは、以下を経由した安全なHTTP伝送を含め、安全なチャネル経由のAES暗号の使用を強制します。
  - ブラウザー
  - SSHポート
  - iLO RESTful API
  - RIBCL

  サポートされている暗号を使用してこの安全なチャネル経由でiLOに接続します。このセキュリティ状態は、安全でないチャネル経由の通信と接続には影響しません。
- ホストシステムから実行される次のコマンドに対するユーザー名とパスワードの制限が適用されます。
  - iLO RESTful API
  - RIBCL
- リモートコンソールデータは、AES-128双方向暗号化を使用します。
- HPQLOCFGユーティリティは、iLOとのSSL接続をネゴシエーションした後、利用可能な最強の暗号を使用してRIBCLスクリプトをネットワーク経由でiLOに送信します。
- TLS 1.2をサポートしていないネットワークベースのツールを使用してサーバーに接続することはできません。
- iLOセキュリティをバイパスするためのシステムメンテナンススイッチ設定（iLOセキュリティオーバーライドスイッチと呼ばれる場合もある）は、iLOへのログインに関するパスワード要件を無効にしません。

FIPS

Common Criteriaコンプライアンス、Payment Card Industryコンプライアンス、またはその他の標準にはFIPSセキュリティ状態が必要になる場合があります。

iLOがこのセキュリティ状態に設定されている場合、次のようになります。

- iLOは、FIPS 140-2レベル1の要件への準拠を目的とするモードで動作します。

  FIPSは、米国政府機関および契約業者によって適用を義務付けられている一連のコンピューターセキュリティ規格です。

  FIPSのセキュリティ状態は、FIPS承認済みと同じではありません。FIPS承認済みは、Cryptographic Module Validation Programを完了することにより承認を受けたソフトウェアを意味します。
- iLOは、以下を経由した安全なHTTP伝送を含め、安全なチャネル経由のAES暗号の使用を強制します。
  - ブラウザー
  - SSHポート
  - iLO RESTful API
  - RIBCL

  サポートされている暗号を使用してこの安全なチャネル経由でiLOに接続します。このセキュリティ状態は、安全でないチャネル経由の通信と接続には影響しません。
- ホストシステムから実行される次のコマンドに対するユーザー名とパスワードの制限が適用されます。

- iLO RESTful API
- RIBCL

- リモートコンソールデータは、AES-128双方向暗号化を使用します。
- HPQLOCFGユーティリティは、iLOとのSSL接続をネゴシエーションした後、利用可能な最強の暗号を使用してRIBCLスクリプトをネットワーク経由でiLOに送信します。
- TLS 1.2をサポートしていないネットワークベースのツールを使用してサーバーに接続することはできません。
- iLOセキュリティをバイパスするためのシステムメンテナンススイッチ設定（iLOセキュリティオーバーライドスイッチと呼ばれる場合もある）は、iLOへのログインに関するパスワード要件を無効にしません。

CNSA

CNSAセキュリティ状態（SuiteBモードとも呼ばれる）は、FIPSセキュリティ状態が有効になっている場合にのみ使用できます。

iLOがこのセキュリティ状態に設定されている場合、次のようになります。

- iLOは、NSAによって定義されたCNSA要件への準拠を目的とするモードで動作します。
- iLOは、米国政府機密として分類されたデータを保持するシステムの保護を目的とするモードで動作します。
- TLS 1.2をサポートしていないネットワークベースのツールを使用してサーバーに接続することはできません。
- iLOセキュリティをバイパスするためのシステムメンテナンススイッチ設定（iLOセキュリティオーバーライドスイッチと呼ばれる場合もある）は、iLOへのログインに関するパスワード要件を無効にしません。
- iLOへの接続に使用するソフトウェアまたはユーティリティはすべて、CNSAに準拠している必要があります。

  以下に例を示します。

  - ファームウェアアップデートユーティリティ
  - SSHクライアント
  - HPEおよび他社製のスクリプティングツールとコマンドラインツール
  - HPEおよび他社製の管理ツール
  - アラートメール、syslog、LDAP、またはキーマネージャーサーバー
  - リモートサポート ソフトウェア
- HTML5リモートコンソールを使用していることを確認してください。このコンソールでは、AES-256ビットCNSA準拠の暗号の使用が強制されます。.NET IRCはCNSAに準拠していません。

準拠を確認するには、ソフトウェアのベンダーに確認するか、Wiresharkなどのユーティリティを使用します。

SSH暗号、キー交換、およびMACのサポート

iLOは、安全なCLPトランザクションのために、SSHポート経由の強化された暗号化を提供します。

構成されているセキュリティ状態に基づいて、iLOは以下をサポートします。

本番稼働

- AES256-CBC、AES128-CBC、3DES-CBC、およびAES256-CTR暗号
- diffie-hellman-group-exchange-sha256、diffie-hellman-group14-sha1、diffie-hellman-group1-sha1キー交換、およびecdh-sha2-nistp384キー交換
- hmac-sha1またはhmac-sha2-256 MAC

FIPSまたは高セキュリティ

- AES256-CTR、AEAD_AES_256_GCM、およびAES256-GCM暗号
- diffie-hellman-group-exchange-sha256、diffie-hellman-group14-sha1キー交換、およびecdh-sha2-nistp384キー交換
- hmac-sha2-256またはAEAD_AES_256_GCM MAC

CNSA

- AEAD_AES_256_GCMおよびAES256-GCM暗号
- ecdh-sha2-nistp384キー交換
- AEAD_AES_256_GCM MAC

Synergyセキュリティモード

- AEAD_AES_256_GCMおよびAES256-GCM暗号
- ecdh-sha2-nistp384キー交換
- AEAD_AES_256_GCM MAC

サポートされるSPDMアルゴリズム

構成されているセキュリティ状態に基づいて、iLOは、SPDMアルゴリズムを次のように分類します。

本番環境、FIPS、高セキュリティ

BaseAsymAlgo(4)

- TPM_ALG_RSASSA_2048
- TPM_ALG_RSAPSS_2048
- TPM_ALG_RSASSA_3072
- TPM_ALG_RSAPSS_3072
- TPM_ALG_ECDSA_ECC_NIST_P256
- TPM_ALG_RSASSA_4096
- TPM_ALG_ECDSA_ECC_NIST_P384

BaseHashAlgo (4)

- TPM_ALG_SHA_256
- TPM_ALG_SHA_384
- TPM_ALG_SHA_512

CNSA

BaseAsymAlgo(4)

- TPM_ALG_RSASSA_3072
- TPM_ALG_RSAPSS_3072
- TPM_ALG_RSASSA_4096
- TPM_ALG_ECDSA_ECC_NIST_P384

BaseHashAlgo (4)

- TPM_ALG_SHA_384

SSL暗号およびMACのサポート

iLOは、分散型IT環境でのリモート管理用に強化されたセキュリティを提供します。SSL暗号化により、Webブラウザーのデータが保護されます。SSLで提供されるHTTPデータの暗号化により、データがネットワーク経由で転送されるときのデータの安全性が保証されます。

ブラウザーからiLOにログインすると、ブラウザーとiLOは、セッション中に使用する暗号設定をネゴシエートします。ネゴシエートされた暗号は暗号化ページに表示されます。

サポートされている暗号の次の一覧は、LDAPサーバー、キーマネージャーサーバー、SSOサーバー、Insight Remote Supportサーバー、仮想メディアで使用されるhttps:// URL、iLO RESTful API、CLIコマンド、iLO連携グループのファームウェアアップデートへの接続など、すべてのiLO SSL接続に適用されます。

構成されているセキュリティ状態に基づいて、iLOは以下の暗号をサポートします。

本番稼働

- RSA、ECDH、およびAEAD MAC（ECDHE-RSA-AES256-GCM-SHA384）による256ビットAES-GCM
- RSA、ECDH、およびSHA384 MAC（ECDHE-RSA AES256-SHA384）による256ビットAES
- RSA、ECDH、およびSHA1 MAC（ECDHE-RSA-AES256-SHA）による256ビットAES
- RSA、DH、およびAEAD MAC（DHE-RSA-AES256-GCM-SHA384）による256ビットAES-GCM
- RSA、DH、およびSHA256 MAC（DHE-RSA AES256-SHA256）による256ビットAES
- RSA、DH、およびSHA1 MAC（DHE-RSA-AES256-SHA）による256ビットAES
- RSAおよびAEAD MAC（AES256-GCM-SHA384）による256ビットAES-GCM
- RSAおよびSHA256 MAC（AES256-SHA256）による256ビットAES
- RSAおよびSHA1 MAC（AES256-SHA）による256ビットAES
- RSA、ECDH、およびAEAD MAC（ECDHE-RSA-AES128-GCM-SHA256）による128ビットAES-GCM
- RSA、ECDH、およびSHA256 MAC（ECDHE-RSA-AES128-SHA256）による128ビットAES
- RSA、ECDH、およびSHA1 MAC（ECDHE-RSA-AES128-SHA）による128ビットAES
- RSA、DH、およびAEAD MAC（DHE-RSA-AES128-GCM-SHA256）による128ビットAES-GCM
- RSA、DH、およびSHA256 MAC（DHE-RSA-AES128-SHA256）による128ビットAES
- RSA、DH、およびSHA1 MAC（DHE-RSA-AES128-SHA）による128ビットAES
- RSAおよびAEAD MAC（AES128-GCM-SHA256）による128ビットAES-GCM
- RSA、およびSHA256 MAC（AES128-SHA256）による128ビットAES
- RSAおよびSHA1 MAC（AES128-SHA）による128ビットAES
- RSA、ECDH、およびSHA1 MAC（ECDHE-RSA-DES-CBC3-SHA）による168ビット3DES
- RSA、DH、およびSHA1 MAC（EDH-RSA-DES-CBC3-SHA）による168ビット3DES
- RSAおよびSHA1 MAC（DES-CBC3-SHA）による168ビット3DES

高セキュリティ

これらのセキュリティ状態にはTLS 1.2が必要です。

- RSA、ECDH、およびAEAD MAC（ECDHE-RSA-AES256-GCM-SHA384）による256ビットAES-GCM
- RSA、DH、およびAEAD MAC（DHE-RSA-AES256-GCM-SHA384）による256ビットAES-GCM
- RSA、ECDH、およびAEAD MAC（ECDHE-RSA-AES128-GCM-SHA256）による128ビットAES-GCM
- RSA、DH、およびAEAD MAC（DHE-RSA-AES128-GCM-SHA256）による128ビットAES-GCM

FIPS

これらのセキュリティ状態にはTLS 1.2が必要です。

- RSA、ECDH、およびAEAD MAC（ECDHE-RSA-AES256-GCM-SHA384）による256ビットAES-GCM
- RSA、ECDH、およびSHA384 MAC（ECDHE-RSA AES256-SHA384）による256ビットAES
- RSA、DH、およびAEAD MAC（DHE-RSA-AES256-GCM-SHA384）による256ビットAES-GCM
- RSA、DH、およびSHA256 MAC（DHE-RSA AES256-SHA256）による256ビットAES
- RSA、ECDH、およびAEAD MAC（ECDHE-RSA-AES128-GCM-SHA256）による128ビットAES-GCM
- RSA、ECDH、およびSHA256 MAC（ECDHE-RSA-AES128-SHA256）による128ビットAES
- RSA、DH、およびAEAD MAC（DHE-RSA-AES128-GCM-SHA256）による128ビットAES-GCM
- RSA、DH、およびSHA256 MAC（DHE-RSA-AES128-SHA256）による128ビットAES

CNSA

このセキュリティ状態にはTLS 1.2が必要です。

- ECDSA、ECDH、およびAEAD MAC（ECDHE-ECDSA-AES256-GCM-SHA384）による256ビットAES-GCM
- クライアントのみ：RSA、ECDH、およびAEAD MAC（ECDHE_RSA_AES256_GCM_SHA384）による256ビットAES-GCM

Synergyセキュリティモード

- ECDSA、ECDH、およびAEAD MAC（ECDHE-ECDSA-AES256-GCM-SHA384）による256ビットAES-GCM
- クライアントのみ：RSA、ECDH、およびAEAD MAC（ECDHE_RSA_AES256_GCM_SHA384）による256ビットAES-GCM

HPE SSO

HPE SSOを使用すると、HPE SSO準拠アプリケーションから、ログイン手順を間に挟むことなくiLOに直接接続できます。

この機能を使用するには、以下の手順に従ってください。

- サポートされるバージョンの、HPE SSOに準拠したアプリケーションが必要です。
- SSO準拠アプリケーションを信頼するようにiLOを構成します。
- CAC厳密モードが有効な場合は、信頼済み証明書をインストールします。

iLOには、HPE SSO証明書の最小要件を決定するためにHPE SSOアプリケーションのサポートが含まれます。HPE SSO準拠アプリケーションの中には、iLOに接続したときに自動的に信頼証明書をインポートするものがあります。この機能を自動的に実行しないアプリケーションの場合は、HPE SSOページを使用してSSO設定を構成してください。

サブトピック

HPE SSO用のiLOの設定

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーでセキュリティをクリックし、HPE SSOタブをクリックします。
2. SSO信頼モード設定を構成します。

   Hewlett Packard Enterpriseでは証明書による信頼モードを使用することをおすすめします。
3. 各役割のiLO権限は、シングルサインオン設定セクションで設定します。
4. 適用をクリックします。
5. 証明書による信頼または名前による信頼を選択した場合は、信頼済みの証明書またはDNS名をiLOに追加します。

   手順については、信頼済みの証明書の追加または直接DNS名のインポートを参照してください。
6. （オプション）HPE SSO準拠アプリケーションにログインし、iLOをブラウズして、SSO接続をテストします。

   たとえば、HPE SIMにログインし、システムページに移動してiLOプロセッサーを見つけて、詳細情報セクションのiLOリンクをクリックします。

   SSO信頼モードが信頼なしに設定されている場合、信頼できるサーバーのリストは使用されません。iLOはSSOサーバー証明書失効を強制しません。

サブトピック

シングルサインオン信頼モードオプション

SSOユーザー権限

シングルサインオン信頼モードオプション

シングルサインオン信頼モードは、HPE SSO要求に対するiLOの応答方法に影響します。

- 信頼なし（SSO無効）（デフォルト） - すべてのSSO接続要求を拒否します。
- 証明書による信頼（最も安全） - iLOに事前にインポートされている証明書と一致させて、HPE SSO対応アプリケーションからSSO接続を有効にします。
- 名前による信頼 - 直接インポートされたIPアドレスまたはDNS名を一致させて、HPE SSO準拠アプリケーションからSSO接続を有効にします。
- すべて信頼（最も安全性が低い） - どのHPE SSO対応アプリケーションから開始されたSSO接続も、すべて受け入れます。

SSOユーザー権限

HPE SSO準拠アプリケーションにログインする場合、HPE SSO準拠アプリケーションの役割割り当てに基づいて認可されます。割り当てられている役割は、SSOが試みられるときに、iLOに渡されます。

SSOはシングルサインオン設定セクションで割り当てられた権限のみを受け入れようとします。iLOディレクトリ設定は適用されません。

デフォルトの権限設定は以下のとおりです。

- ユーザー – ログインのみ
- オペレーター – ログイン、リモートコンソール、仮想電源およびリセット、仮想メディア、およびホストBIOS構成。
- 管理者 – ログイン、リモートコンソール、仮想電源およびリセット、仮想メディア、ホストBIOS構成、iLOの設定の構成、ユーザーアカウント管理、ホストNIC構成、およびホストストレージ構成。

信頼済みの証明書の追加

前提条件

iLOの設定を構成する権限

このタスクについて

証明書レポジトリは、標準的な証明書を5つ保持できます。標準的な証明書が発行されない場合、証明書のサイズは一定ではありません。割り当てられた保管領域がすべて使われると、それ以上のインポートは受け付けられません。

特定のHPE SSO対応アプリケーションから証明書を抽出する方法については、HPE SSO対応アプリケーションのドキュメントを参照してください。

手順

1. ナビゲーションツリーでセキュリティをクリックし、HPE SSOタブをクリックします。
2. インポートをクリックします。
3. 次のいずれかの方法を使用して、信頼済みの証明書を追加します。
   - **ダイレクトインポート** – Base64でエンコードされた証明書のX.509データをコピーし、ダイレクトインポートセクションのテキストボックスに貼り付けてから、適用をクリックします。
   - **インダイレクトインポート** – DNS名、IPアドレス、または証明書URLをURLからのインポートセクションのテキストボックスに入力してから、適用をクリックします。

     iLOはネットワーク経由でHPE SSO対応アプリケーションに接続して、証明書を取得して保存します。

HPE SIM SSO証明書の取得

前提条件

HPE SIM 7.4以降

このタスクについて

次の方法でHPE SIM SSO証明書を取得できます。詳しくは、HPE SIMのドキュメントを参照してください。

手順

- Webブラウザーで次のリンクの1つを入力します。

  ```
  http://<HPE SIM name or network address>:280/GetCertificate?certtype=sso
  ```

  ```
  https://<HPE SIM name or network address>:50000/GetCertificate?certtype=sso
  ```

  すべての要求パラメーターは大文字と小文字が区別されます。小文字の `certtype` パラメーターを大文字にすると、このパラメーターは読み込まれず、HPE SIMは信頼済みの証明書ではなくデフォルトのHPE SIMサーバー証明書を返します。
- HPE SIMから証明書をエクスポートするには、以下の手順に従ってください。

この手順を完了するには、オプション > セキュリティ > 証明書 > HPE Systems Insight Managerシングルサインオンサーバー証明書の順に選択して、エクスポートをクリックします。

直接DNS名のインポート

前提条件

iLO設定の構成権限

手順

1. ナビゲーションツリーでセキュリティをクリックし、HPE SSOタブをクリックします。
2. インポートをクリックします
3. 直接DNS名のインポートセクションにDNS名またはIPアドレスを入力し（最大64文字）、適用をクリックします。

信頼済みの証明書とレコードの表示

このタスクについて

信頼済み証明書および記録を管理テーブルに、現在のiLO管理プロセッサーでSSOを使用するように構成されている信頼済みの証明書およびレコードのステータスが表示されます。

手順

ナビゲーションツリーでセキュリティをクリックし、HPE SSOタブをクリックします。

サブトピック

信頼済みの証明書およびレコードの詳細

信頼済みの証明書およびレコードの詳細

ステータス

証明書またはレコードのステータス。表示される可能性があるステータスの値は、以下のとおりです。

- 証明書またはレコードは有効です。
- 証明書またはレコードに問題があります。考えられる原因は、以下のとおりです。
  - レコードにDNS名が含まれており、信頼モードが証明書による信頼に設定されています（証明書のみが有効）。
  - 証明書が構成されており、信頼モードが名前による信頼に設定されています（直接インポートされたIPアドレスまたはDNS名のみが有効）。
  - 信頼なし（SSO無効）が選択されています。
  - 証明書は構成されているiLOセキュリティ状態に準拠していません。
- 証明書またはレコードが無効です。考えられる原因は、以下のとおりです。
  - 証明書の期限が切れています。証明書の詳細で詳細情報を確認してください。
  - iLOのクロックが設定されていないか、正しく設定されていません。iLOのクロックは、証明書の発効日と有効期限で示される範囲内に含まれている必要があります。

証明書

レコードに証明書が保存されていることを示します。アイコンの上にマウスカーソルを移動すると、証明書の詳細情報（サブジェクト（被認証者）、発行元、日付など）が表示されます。

説明

サーバーの名前または証明書のサブジェクト（被認証者）。

信頼済みの証明書とレコードの削除

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーでセキュリティをクリックし、HPE SSOタブをクリックします。
2. 信頼済みの証明書および記録を管理テーブルから1つ以上の信頼済みの証明書またはレコードを選択します。
3. 削除をクリックします。

   iLOに、選択した証明書またはレコードの削除を確認するプロンプトが表示されます。

   リモート管理システムの証明書を削除すると、iLOでリモート管理システムを使用する際に正常に機能しないことがあります。
4. はい、削除しますをクリックします。

ログインセキュリティバナーの構成

前提条件

iLOの設定を構成する権限

このタスクについて

ログインセキュリティバナー機能を使用すると、iLO Webインターフェイスと HTML5スタンドアロンリモートコンソールログインページに表示されるセキュリティバナーを構成できます。このセキュリティバナーは、SSH接続を介してiLOに接続したときにも表示されます。例えば、メッセージとサーバー所有者の連絡先情報を入力できます。

手順

1. ナビゲーションツリーでセキュリティをクリックして、ログインセキュリティバナーをクリックします。
2. ログインセキュリティバナーを有効設定を有効にします。

   iLOは、ログインセキュリティバナーに以下のデフォルトテキストを使用します。

   ```
   This is a private system. It is to be used solely by authorized users
   and may be monitored for all lawful purposes. By accessing this system,
   you are consenting to such monitoring.
   ```
3. （オプション）セキュリティメッセージをカスタマイズするには、セキュリティメッセージテキストボックスにカスタムメッセージを入力します。

   テキストボックスの上にあるバイトカウンターに、メッセージに使用できる残りのバイト数が表示されます。最大は1,500バイトです。

   空白スペースまたは空白行をセキュリティメッセージに追加しないでください。空白スペースと空白行はバイト数にカウントされ、ログインページのセキュリティバナーには表示されません。

ヒント:

デフォルトのテキストをリストアするには、デフォルトのメッセージを使用をクリックします。

4. 適用をクリックします。

次のログイン時にセキュリティメッセージが表示されます。

システムメンテナンススイッチ

Hewlett Packard Enterpriseサーバーとコンピューティングモジュールには、さまざまなセキュリティ機能と構成を制御するハードウェアシステムメンテナンススイッチがあります。

システムメンテナンススイッチは、シャーシ内のシステムボード上にあります。スイッチにアクセスするには、デバイスをオフラインにし、電源を切り、アクセスカバーを取り外す必要があります。

次のシステムメンテナンススイッチはデフォルトでオフになっています。製品のセキュリティ動作を変更する場合は、これらのスイッチをオンに設定できます。システムメンテナンススイッチの設定は、アクセスパネルのラベルと製品のユーザーガイドに記載されています。

iLOセキュリティ（位置1）

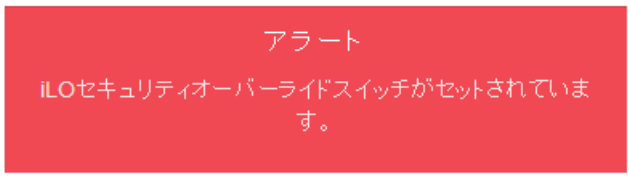
システムメンテナンススイッチのiLOセキュリティ設定により、システムボードを物理的に制御できる管理者が、緊急時にアクセスすることができます。

iLOセキュリティを制御するシステムメンテナンススイッチ位置は、iLOセキュリティオーバーライドスイッチと呼ばれることがあります。

このスイッチがオフの場合（デフォルト）、iLOは構成されている認証設定を適用します。

このスイッチを無効にすると、次のような影響があります。

- iLOが本番環境セキュリティ状態を使用するように構成されている場合、すべてのログイン証明書検証が無効になります。
- iLOが、高セキュリティ、FIPS、またはCNSAのセキュリティ状態を使用するように構成されている場合、すべてのログイン証明書検証が適用されます。
- ホストサーバーがリセットされると、UEFIシステムユーティリティソフトウェアが実行されます。
- iLOネットワーキング、iLO Webインターフェイス、およびROMベースのシステムユーティリティは、以前に無効にされていた場合でもアクセスできます。
- システムリカバリ特権が適用されます。この特権を必要とするアクションを実行するには、特権が有効にされているユーザーアカウントで認証する必要があります。
- iLO Webインターフェイスページに、iLOセキュリティが無効であることを示す警告メッセージが表示されます。



- iLOのログに、iLOセキュリティの変更を記録するエントリーが追加されます。
- SNMPアラートの送信先が構成されている場合、iLOがiLOセキュリティ構成の変更後に起動するとアラートが送信されます。

詳しくは、ご使用の製品のメンテナンス&サービスガイドを参照してください。

サブトピック

iLOセキュリティを無効にする理由

次の状況で、システムメンテナンススイッチを使用して、iLOセキュリティを無効にすることができます。

- ユーザーアカウント管理権限を持つすべてのユーザーアカウントがロックアウトされた。
- 不適切な設定により、ネットワーク上にiLOが表示されず、ROMベースの構成ユーティリティが無効になっている。
- iLOに、iLO のNICがオフになっているか、iLOネットワーク構成が正しくないため、ネットワーク経由で到達できない。UEFIシステムユーティリティを使用して構成を修正することが不可能であるか、または不便である。

  iLOセキュリティを無効にすると、 iLOのネットワーク構成が工場出荷時のデフォルト設定にリセットされます。
  - ほとんどのサーバーでは、このアクションによってDHCPおよびiLO専用ネットワークポートが有効になります。
  - iLO専用ネットワークポートがオプションのアドオンカードであるサーバーでは、このアクションによってDHCPおよび共有ネットワークポートが有効になります。
  - iLOネットワーク有効化モジュールのあるサーバーでは、このアクションによってDHCPおよびiLO専用ネットワークポートが有効になります。
- 設定されたユーザー名は1つのみで、パスワードを忘れてしまった。
- バッテリ駆動のSRAMメモリデバイスに保存されている構成情報を消去したい。

  iLOを起動すると、バッテリ駆動のSRAMメモリデバイスに保存されている構成情報が不揮発性フラッシュメモリ（NAND）にバックアップされます。SRAMが削除されると、構成が自動的にリストアされます。iLOセキュリティを無効にすると、SRAMデータが自動的にリストアされません。

iLOマネジメント設定の構成

サブトピック

RESTアラート

IPMIアラート

iLOアラートメール

リモートsyslog

HPE Compute Ops Management

Agentless ManagementとAMS

Agentless Managementは、セキュリティと安定性を強化するためにアウトオブバンド通信を使用します。Agentless Managementでは、ヘルス監視とアラート通知機能がシステムに内蔵され、サーバーに電源コードを接続するとただちに動作を開始します。

iLOと直接通信できないデバイスおよびコンポーネントから情報を収集するには、Agentless Management Service (AMS) をインストールします。

AMSがある場合とAMSがない場合のAgentless Managementにより提供される情報

コンポーネント	Agentless Management（AMSがない場合）	AMSがインストールされている場合に提供される追加情報
サーバーヘルス	• ファン • 温度 • 電源装置 • メモリ • CPU • NVDIMM	該当なし
ストレージ	• Smartアレイ • SMARTドライブ監視（Smartアレイに接続） • Smartアレイに接続されている内蔵および外付けドライブ • Smart Storage Energy Pack監視（サポート対象のサーバーのみ） • MCTPをサポートするNVMeドライブ	• SMARTドライブ監視 • iSCSI（Windows） • NVMeドライブ
ネットワーク	• NC-SI over MCTPをサポートしている内蔵NICのMACアドレス • NC-SI over MCTPをサポートしているNICの物理リンク接続性およびリンクアップ/リンクダウントラップ • Hewlett Packard Enterpriseベンダー定義のMCTPコマンドをサポートするファイバーチャネルアダプター	• 独立型および内蔵NICのMACアドレスおよびIPアドレス • リンクアップ/リンクダウントラップ • NICチーミングおよびブリッジング情報（WindowsおよびLinux） • サポートされるファイバーチャネルアダプター • 仮想LAN情報（WindowsおよびLinux）
その他	• iLOデータ • ファームウェアインベントリ • デバイスインベントリ	• OS情報（ホストSNMP MIB） • ドライバー/サービスインベントリ • OSログへのイベントの記録 [1]、[2]、[3]
事前障害警告アラート	• メモリ • ドライブ（物理および論理）	該当なし

1 Linuxの場合、AMSベースのOSログ記録（Red Hat Enterprise LinuxおよびSUSE Linux Enterprise Serverでは/var/log/messages、VMwareでは/var/log/syslog）。
Windowsの場合、Windowsシステムログ。
2 Smartアレイのログ記録はサポートされます。
3 Gen11サーバーでは、IMLおよびセキュリティログイベントが、OSログに記載されます。

Agentless Management Service

- AMSをWindowsシステムにインストールすると、Agentless Management Serviceのコントロールパネルがインストールされます。コントロールパネルを使用すると、SNMPの設定を行い、AMSを有効化/無効化を行い、AMSの削除を行うことができます。

- AMSは、オペレーティングシステムの構成情報およびクリティカルイベントをActive Health Systemログに記録します。
- AMSをインストールする前に、iLOドライバーをインストールします。
- iLO6では、AMSにオプションのSystem Management Assistantが含まれます。iLO Agentless ManagementとAMSによって提供される情報を処理するためにOSベースのSNMPサービスを使用する場合は、System Management Assistantを使用できます。
- AMSがインストールされていない場合：
  - iLOは、ナビゲーションツリーのシステム情報およびファームウェア & OSソフトウェアセクションに含まれるコンポーネント情報ページにすべてのデータを表示するとは限りません。
  - iLOは、OS固有の情報にはアクセスできません。

サブトピック

AMSのインストール

AMSのインストールの確認

AMSの再起動

System Management Assistant

詳しくは

iLOドライバーのインストール
System Management Assistant

AMSのインストール

手順

1. 次のいずれかのソースからAMSを取得します。
   - SPP（Windows、Red Hat Enterprise Linux、SUSE Linux Enterprise Server）をSPPダウンロードページ**https://www.hpe.com/servers/spp/download**からダウンロードします。
   - **https://www.hpe.com/support/hpesc**のHewlett Packard Enterpriseサポートセンター（Windows、Red Hat Enterprise Linux、SUSE Linux Enterprise Server、VMware）からソフトウェアをダウンロードします。
   - Software Delivery RepositoryのWebサイト**https://vibsdepot.hpe.com**（VMware）のvibsdepotセクションからソフトウェアをダウンロードします。

     AMSは、Hewlett Packard Enterprise独自のVMware ISOイメージ（**https://www.hpe.com/info/esxidownload**）にも含まれています。
2. ソフトウェアをインストールします。

   SPPの使用方法については、**https://www.hpe.com/info/spp/documentation**にあるSPPのドキュメントを参照してください。

   他のダウンロードタイプの場合、ソフトウェアに付属のインストール手順を実行します。

AMSのインストールの確認

サブトピック

AMSステータスの確認：iLOWebインターフェイス

AMSステータスの確認：Windows

AMSステータスの確認：SUSE Linux Enterprise ServerおよびRed Hat Enterprise Linux

AMSステータスの確認：VMware

AMSステータスの確認：Ubuntu

AMSステータスの確認：iLOWebインターフェイス

手順

ナビゲーションツリーでシステム情報をクリックします。

AMSがヘルスサマリーページのサブシステムとデバイステーブルにリストされています。値には、以下のものがあります。

- 利用不可 - AMSが検出されなかった、サーバーがPOSTを実行している、またはサーバーの電源が入っていないため、AMSは使用できません。
- OK - AMSがインストールされており、実行中です。

AMSステータスの確認：Windows

手順

1. Windowsのコントロールパネルを開きます。

   AMSコントロールパネルがあると、AMSはインストールされています。
2. AMSコントロールパネルを開きます。
3. サービスタブをクリックします。

   AMSが有効になっている場合は、次のメッセージが表示されます。

   ```
   Agentless Management Service (AMS) は有効です。
   ```

AMSステータスの確認：SUSE Linux Enterprise ServerおよびRed Hat Enterprise Linux

手順

1. AMSがインストールされていることを確認するには、コマンド
   `rpm -qi amsd`
   を入力します。
2. AMSが動作していることを確認するには、コマンド
   `systemctl status amsd smad [cpqIde cpqFca cpqScsi cpqiScsi mr_cpqScsi]`
   を入力します。

AMSステータスの確認：VMware

手順

1. AMSがインストールされていることを確認します。
   a. VMware vSphereクライアントからVMwareホストにアクセスします。
   b. サーバーのインベントリ > 構成 > 健全性ステータスタブに移動します。
   c. ソフトウェアコンポーネントの横にあるプラス記号（+）をクリックします。

      ホストにインストールされているソフトウェアのリストが表示されます。AMSコンポーネントには、`amsd`という文字列が含まれています。

      AMSコンポーネントのフルネームは、サポートされるESX/ESXiバージョンごとに異なります。
2. AMSが動作していることを確認するには、コマンド
   `/etc/init.d/ams.sh status`
   を入力します。

AMSステータスの確認：Ubuntu

手順

1. AMSがインストールされていることを確認するには、コマンド
   `dpkg -l amsd`
   を入力します。
2. AMSが動作していることを確認するには、コマンド
   `sudo systemctl status smad; systemctl status amsd`
   を入力します。

AMSの再起動

手順

- **Windows** – Windowsのサービスページに移動して、AMSを再起動します。
- **SUSE Linux Enterprise ServerおよびRed Hat Enterprise Linux** – コマンドとして`systemctl restart amsd smad`を入力します。
- **VMware** – 次のコマンドを入力します。
  - **ESXi 6.xおよび7.0の場合**：
    `/etc/init.d/amsd.sh restart`
  - **ESXi 7.0 U1以降の場合**：
    `esxcli daemon control restart -s amsd`

System Management Assistant

iLO6では、OSベースのSNMPエージェントはサポートされていません。System Management Assistant（SMA）は、OSからSNMP情報を取得するアプリケーションを実行するユーザー向けのAgentless Management Service機能です。

セキュリティ

SMAはセキュアなiLOチャネル経由で通信します。

AMSモード

- **AMS（フォワードモード）** – AMSの標準構成では、OSからiLOに情報が転送されます。
- **SMA（リバースモード）** – SMAが有効な場合は、iLOからOSに情報が転送されます。

インストール

SMAはAMSパッケージの一部としてインストールされ、デフォルトで無効になっています。

SMAの有効化

OSからiLOに情報を転送するには、デフォルトのAMS構成を使用します。iLOからOSに情報を転送するには、SMAを有効にします。AMSの標準構成とSMAは、同時に有効にすることができます。

SMA機能

SMAが有効になっている場合は、次のように処理されます。

- **Linux** – iLOとホストベースのSNMPマスター間でAgentXプロトコル要求がプロキシ転送されます。
- **Windows、Linux** – iLOとホストベースのSNMPサービス間でSNMPプロトコル要求がプロキシ転送されます。

  この方法は、ホストベースのSNMPサービスでAgentXサブエージェントがサポートされていない場合に使用されます。
- **VMware** – iLOおよびAMSからのSNMPトラップを、ESXiホストOSのSNMPサービスを通じて構成されているトラップの宛先に提供します。

SNMPマスター

デフォルトのAMS構成では、AMSはSNMPマスターとしてiLOを使用します。SMAでは、SNMPマスターとして動作するホストベースのサービスが必要です。

SMAが有効になっている場合に提供される情報

- **WindowsおよびLinux** – SMAは、AMSがある場合とAMSがない場合のAgentless Managementにより提供される情報テーブルのAgentless Management（AMSがある場合）列で一覧表示されている情報と同じものを提供します。
- **VMware** – SMAはSNMPトラップのみを提供します。

サブトピック

System Management Assistantの使用（Windows）

System Management Assistantの無効化（Windows）

VMware用System Management Assistantの使用

System Management Assistantの無効化（VMware）

Linux用System Management Assistantの使用

System Management Assistantの使用（Windows）

前提条件

AMSがインストールされています。

このタスクについて

AMSの対話型インストール時にSMAを有効にするかどうかを選択できます。サイレントインストール時には、SMAが有効になりません。

SMAを使用するには、SMAサービスを起動し、Windows SNMPサービスがインストールされ、構成されていることを確認します。

手順

1. Windows SNMPサービスをインストールします。

a. サーバーマネージャーを開きます。
b. 役割と機能の追加を選択します。
c. 開始する前にセクションで次へをクリックします。
d. インストールの種類セクションで次へをクリックします。
e. サーバーの選択セクションで次へをクリックします。
f. サーバーの役割セクションで次へをクリックします。
g. リモートサーバー管理セクションを展開します。
h. 機能管理ツールを展開します。
i. SNMPツールが選択されていることを確認します。
j. SNMPサービスオプションの左側にあるチェックボックスを選択します。
k. 次へをクリックします。
l. インストールをクリックし、インストールが完了するまで待機します。

2. Windows SNMPサービスを構成します。
a. Windowsのサービスウィンドウに移動します。
b. SNMPサービスを右クリックします。
c. セキュリティタブをクリックします。
d. 受け付けるコミュニティ名セクションで追加をクリックします。
e. コミュニティの権利セクションでアクセスタイプを選択します。
f. コミュニティ名セクションでコミュニティ名を入力します。
g. 追加をクリックします。
h. トラップタブをクリックします。
i. コミュニティ名セクションでコミュニティ名を入力し、一覧に追加をクリックします。
j. トラップ先セクションで、追加をクリックし、トラップ送信先のIPアドレスを入力します。
k. OKをクリックします。

3. SMAサービスを開始します。
a. Windowsのサービスウィンドウに移動します。
b. System Management Assistantを右クリックし、プロパティを選択します。
c. スタートアップの種類メニューで自動を選択し、OKをクリックします。
d. System Management Assistantを右クリックし、開始を選択します。

注記:

次の方法でも、SMAサービスを開始できます。

- `<Program Files>\OEM\AMS\Service`に移動して、次のコマンドを実行します。`EnableSma.bat /f`
- コマンドプロンプトウィンドウでコマンド
  `sc config sma start=auto`
  および
  `net start sma`
  を入力します。

System Management Assistantの無効化（Windows）

手順

1. Windowsのサービスウィンドウに移動します。
2. System Management Assistantを右クリックし、プロパティを選択します。
3. スタートアップの種類メニューで無効を選択し、OKをクリックします。
4. System Management Assistantを右クリックし、停止をクリックします。

注記:

`<Program Files>\OEM\AMS\Service`に移動し、`DisableSma.bat /f`コマンドを実行して、SMAサービスを無効化することもできます。

VMware用System Management Assistantの使用

前提条件

AMSがインストールされています。

手順

1. ホスト上でSNMPを有効にし、トラップ先を指定します。

   例：

   ```
   esxcli system snmp set -e 1 -c public -t <trap dest IP address>@162/public
   ```

2. 次のコマンドを入力して、SNMPが有効になっていることを確認します。

   ```
   esxcli system snmp get
   ```

3. 次のコマンドを入力して、SMAを有効にして起動します。

   ```
   esxcli sma enable
   ```

4. 次のコマンドを入力して、SMAが動作していることを確認します。

   ```
   esxcli sma status
   ```

5. SMAプロセス（`smad_rev`）が動作していることを確認します。

System Management Assistantの無効化（VMware）

手順

次のコマンドを実行します。`esxcli sma disable`

Linux用System Management Assistantの使用

前提条件

- AMSがインストールされています。
- ホストSNMPサービスが構成されています。
- ホストとSNMPクライアント間でSNMPパケットが転送されるようにネットワークが構成されています。

手順

1. `/etc/snmp/snmpd.conf`ファイルに最初の非コメント行として次の行を追加して、AgentXサブエージェントがサポートされるようにホストを構成します。

   ```
   master agentx
   ```

2. System Management Assistantを有効にします。
   - **SUSE Linux Enterprise ServerおよびRed Hat Enterprise Linux** - コマンドとして`systemctl enable amsd_rev`を入力します。
3. Agentless Management Serviceを有効にして、起動します。
   - **SUSE Linux Enterprise ServerおよびRed Hat Enterprise Linux** - コマンドとして
     `systemctl enable amsd_rev; systemctl start amsd_rev`
     を入力します。

SNMP設定の構成

前提条件

iLOの設定を構成する権限

このタスクについて

このページで構成する設定は、デフォルトのAgentless ManagementとAMS構成用です。System Management AssistantとOSベースのSNMPサービスを使用する場合は、ホストで同様の設定を構成しなければなりません。

手順

1. ナビゲーションツリーのマネジメントをクリックします。

   SNMP設定ページが表示されます。

2. SNMP設定セクションに次の値を入力します。
   - システムの位置
   - システム連絡先
   - システムの役割

- システムの役割詳細
- 読み込みコミュニティ1
- 読み込みコミュニティ2
- 読み込みコミュニティ3

このページのSNMPポート値およびSNMPステータス値は読み取り専用です。この値は、アクセス設定ページで変更できます。

3. 構成を保存するには、適用をクリックします。

サブトピック

SNMPオプション

詳しくは

System Management Assistant
iLOアクセス設定の構成

SNMPオプション

- システムの位置 – サーバーの物理的位置を指定する最大49文字の文字列。
- システム連絡先 – システム管理者またはサーバーの所有者を指定する最大49文字の文字列。文字列には、名前、メールアドレス、または電話番号を含めることができます。
- システムの役割 – サーバーの役割または機能を記述する最大64文字の文字列。
- システムの役割詳細 – サーバーが実行する場合がある具体的なタスクを記述する最大512文字の文字列。
- 読み込みコミュニティ1、読み込みコミュニティ2、および読み込みコミュニティ3 – 構成されているSNMP読み取り専用コミュニティ文字列。

  次の形式がサポートされています。

  - コミュニティ文字列（たとえば、`public`）。
  - コミュニティ文字列とそれに続くIPアドレスまたはFQDN（たとえば、`public 192.168.0.1`）。

    指定したIPアドレスまたはFQDNからのSNMPアクセスが許可されることを指定するには、このオプションを使用します。

    IPv4アドレス、IPv6アドレス、またはFQDNを入力できます。

  これらの値は、SNMPアラートセクションでSNMPv1が有効になっている場合にのみ編集できます。
- ステータス – SNMPアクセス設定のステータス（有効または無効）。この値は読み取り専用ですが、アクセス設定ページで変更できます。

  アクセス設定ページに移動するには、ステータスリンクをクリックします。
- SNMPポート – SNMP通信に使用されるポート。この値は読み取り専用ですが、アクセス設定ページで変更できます。

  アクセス設定ページに移動するには、SNMPポートリンクをクリックします。

SNMPv3認証

SNMPv3の次のセキュリティ機能によって、iLO SNMPエージェントから安全にデータ収集できます。

- メッセージの整合性により、パケット送信中の改ざんを防ぎます。
- 暗号化により、パケットののぞき見を防ぎます。
- 認証により、パケットが有効なソースから送信されたものであることを確認します。

デフォルトでは、SNMPv3はユーザーベースのセキュリティモデルをサポートします。このモデルでは、セキュリティパラメーターがSNMPエージェントレベル（iLO）とSNMPマネージャーレベル（クライアントシステム）の両方で構成されます。SNMPエージェントとマネージャーの間でやり取りされるメッセージは、データ整合性チェックおよびデータ発信元認証で管理されます。

iLOは、8つのユーザープロファイルをサポートしており、ユーザーはこのプロファイル内でSNMPv3 USMパラメーターを設定できます。

SNMPアラートの送信先の追加

前提条件

- iLOの設定を構成する権限
- SNMPv1アラートの送信先を構成する場合、SNMPv1が有効であること。
- SNMPv3アラートの送信先を構成する場合、少なくとも1人のSNMPv3ユーザーが構成されていること。

このタスクについて

iLOでは、最大8つのSNMPアラート送信先をサポートしています。

手順

1. ナビゲーションツリーのマネジメントをクリックします。

   SNMP設定ページが表示されます。
2. SNMPアラートの送信先セクションで新規をクリックします。
3. 以下の値を入力します。
   - SNMPアラートの送信先
   - トラップコミュニティ （SNMPv1アラートの送信先のみ）
   - SNMPプロトコル
   - SNMPv3ユーザー
4. 追加をクリックします。

サブトピック

SNMPアラートの送信先のオプション

SNMPアラートの送信先のオプション

- SNMPアラートの送信先 - iLOからSNMPアラートを受信する管理システムのIPアドレスまたはFQDN。この値の最大長は255文字です。

  FQDNを使用してSNMPアラートの送信先を構成し、DNSがFQDNに対してIPv4とIPv6の両方のアドレスを提供する場合、iLOは、IPv6ページのiLOクライアントアプリケーションはIPv6を最初に使用設定で指定されたアドレスにトラップを送信します。iLOクライアントアプリケーションはIPv6を最初に使用を有効にすると、トラップはIPv6アドレス（使用可能な場合）に送信されます。iLOクライアントアプリケーションはIPv6を最初に使用を無効にすると、トラップはIPv4

アドレス（使用可能な場合）に送信されます。

- トラップコミュニティ – 構成されているSNMPトラップコミュニティ文字列。
- SNMPプロトコル – 構成されているアラート送信先で使用されるSNMPプロトコル（SNMPv1トラップ、SNMPv3トラップ、またはSNMPv3通知）。

  SNMPアラートセクションでSNMPv1が無効になっている場合、SNMPv1トラップオプションは利用できません。
- SNMPv3ユーザー – 構成されているアラート送信先と関連付けられているSNMPv3ユーザー。

  この値はSNMPプロトコルがSNMPv3に設定されている場合にのみ使用できます。

SNMPアラート送信先の編集

前提条件

- iLOの設定を構成する権限
- SNMPv1トラッププロトコルオプションを使用するようにアラート送信先を変更する場合、SNMPv1が有効になっていること。
- SNMPv3トラッププロトコルオプションまたはSNMPv3通知プロトコルオプションを使用するようにアラート送信先を変更する場合、少なくとも1人のSNMPv3ユーザーが構成されていること。

このタスクについて

iLOでは、最大8つのSNMPアラート送信先をサポートしています。

手順

1. ナビゲーションツリーのマネジメントをクリックします。

   SNMP設定ページが表示されます。
2. SNMPアラートの送信先セクションで、アラート送信先の横のチェックボックスを選択して、編集をクリックします。
3. 以下の値をアップデートします。
   - SNMPアラートの送信先
   - トラップコミュニティ （SNMPv1アラートの送信先のみ）
   - SNMPプロトコル
   - SNMPv3ユーザー
4. アップデート をクリックします。

SNMPアラート送信先の削除

前提条件

iLO設定の構成権限

手順

1. ナビゲーションツリーのマネジメントをクリックします。

   SNMP設定ページが表示されます。
2. SNMPアラート送信先セクションで、削除するSNMPアラート送信先の横のチェックボックスを選択し、削除をクリックし

ます。

3. 要求を確認するメッセージが表示されたら、はい、削除しますをクリックします。

SNMPv3ユーザーの構成

前提条件

iLO設定の構成権限

このタスクについて

iLOでは、最大8人のSNMPv3ユーザーをサポートしています。

手順

1. ナビゲーションツリーのマネジメントをクリックします。

   SNMP設定ページが表示されます。

2. SNMPv3ユーザーセクションで、次のいずれかの操作を実行します。
   - SNMPv3ユーザーを追加するには、新規をクリックします。
   - 構成済みのSNMPv3ユーザーを編集するには、ユーザーの横のチェックボックスを選択し、編集をクリックします。
3. 以下の値を入力します。
   - セキュリティ名
   - 認証プロトコル
   - 認証パスフレーズ
   - プライバシプロトコル
   - プライバシーパスフレーズ
   - ユーザーエンジンID
4. ユーザープロファイルを保存するには、次のいずれかの操作を実行します。
   - 新規ユーザープロファイルを保存するには、追加をクリックします。
   - 編集したユーザープロファイルを保存するには、アップデートをクリックします。

サブトピック

SNMPv3ユーザーオプション

SNMPv3ユーザーオプション

- セキュリティ名 – ユーザープロファイルの名前。1～32文字の範囲で英数字の文字列を入力します。
- 認証プロトコル – 認証パスフレーズのエンコーディングに使用するメッセージダイジェストアルゴリズムを設定します。メッセージダイジェストはSNMPメッセージの該当部分を対象に算出され、受信者に送信するメッセージの一部として、メッセージに含まれます。

  MD5、SHA、またはSHA256を選択します。

  FIPSまたはCNSAセキュリティ状態を使用するようiLOを構成すると、MD5がサポートされません。

- 認証パスフレーズ – 署名操作に使用するパスフレーズを設定します。8～49文字の範囲で値を入力します。
- プライバシープロトコル – プライバシーパスフレーズのエンコーディングに使用する暗号化アルゴリズムを設定します。SNMPメッセージの一部は、送信前に暗号化されます。AESまたはDESを選択します。

  FIPSまたはCNSAセキュリティ状態を使用するようiLOを構成すると、DESがサポートされません。
- プライバシーパスフレーズ – 暗号化操作に使用するパスフレーズを設定します。8～49文字の範囲で値を入力します。
- ユーザーエンジンID – SNMPv3通知パケット用のユーザーエンジンIDを設定します。この値は、「INFORM」メッセージで使用されるリモートアカウントの作成のみに使用されます。

  この値が設定されていない場合、「INFORM」メッセージはデフォルト値または構成されたSNMPv3エンジンIDで送信されます。

  この値は10～64文字で構成される16進数文字列で、文字数は先頭の2文字の0xを除いて偶数でなければなりません。

  例：
  ```
  0x01020304abcdef
  ```

SNMPv3ユーザーの削除

前提条件

iLO設定の構成権限

手順

1. ナビゲーションツリーのマネジメントをクリックします。

   SNMP設定ページが表示されます。
2. SNMPv3ユーザーセクションで、削除するユーザープロファイルの横のチェックボックスを選択し、削除をクリックします。

   △ **注意:**

   選択したSNMPv3ユーザープロファイルがSNMPアラート送信先について構成されている場合、ユーザープロファイルを削除した後、そのアラートは送信されなくなります。
3. 要求を確認するメッセージが表示されたら、はい、削除しますをクリックします。

SNMPv3設定の構成

前提条件

iLO設定の構成権限

このタスクについて

SNMPv3エンジンIDおよびSNMPv3通知設定を構成するには、SNMPv3設定セクションを使用します。

iLOでは、業界標準のSNMPv3通知機能をサポートしています。SNMPv3通知を送信する際、通知は保存され、受信者が肯定応答をiLOに送信するまで、または最大再試行回数に達するまで定期的に再送信されます。

手順

1. ナビゲーションツリーのマネジメントをクリックします。

   SNMP設定ページが表示されます。

2. SNMPv3エンジンIDボックスに値を入力します。

   値を指定しない場合は、このボックスを空白にすることができます。

3. SNMPv3通知設定を構成するには、以下の値を入力します。

   - SNMPv3通知リトライ
   - SNMPv3通知時間間隔

4. 適用をクリックします。

サブトピック

SNMPv3の設定オプション

SNMPv3の設定オプション

SNMPv3エンジンID

SNMPエージェントエンティティに属するSNMPエンジンの一意の識別子。

この値は6～48文字で構成される16進数文字列で（先頭の0xはカウントしない）、文字数は偶数でなければなりません（例：`0x01020304abcdef`）。この設定を構成しない場合、値はシステムで生成されます。

SNMPv3通知リトライ

受信者が肯定応答をiLOに送信しない場合にiLOがアラートを再送する回数。

0～5の値を入力します。デフォルト値は2です。

SNMP通知時間間隔

SNMPv3通知アラートの再送を試行する時間間隔の秒数。

5～120秒の範囲で値を入力します。デフォルト値は15秒です。

SNMPアラートの構成

前提条件

iLOの設定を構成する権限

手順

1. ナビゲーションツリーのマネジメントをクリックします。

   SNMP設定ページが表示されます。

2. SNMPアラートセクションで、iLOホスト名またはOSホスト名を選択して、トラップソース識別子を構成します。

3. 以下の値を構成します。

   - iLO SNMPアラート
   - SNMPv1
   - コールドスタートトラップブロードキャスト
   - 定期的なHSAトラップ構成

4. （オプション）テストアラートを作成し、構成済みのSNMPアラート送信先にこれを送信するには、テストアラートの送信をクリックします。

テストアラートは、構成済みのSNMPアラート送信先アドレスとのiLOのネットワーク接続を確認するために使用されます。アラートが生成されたら、アラート送信先でアラートの受信を確認します。

5. 構成を保存するには、適用をクリックします。

サブトピック

SNMPアラートの設定

SNMPアラートの設定

トラップソース識別子

iLOがSNMPトラップを生成するときにSNMPで定義されたsysName変数に使用されるホスト名を決定します。デフォルト設定は、iLOホスト名です。

ホスト名はOSの構成要素です。ハードドライブが新しいサーバープラットフォームに移動される場合など、サーバーに固定されているわけではありません。ただし、iLOのsysNameは、システムボードに固定されています。

iLO SNMPアラート

ホストオペレーティングシステムとは関係なくiLOによって検出されたアラート状態は、指定されたSNMPアラート送信先に送信できます。このオプションが無効になっている場合、トラップは構成されたSNMPアラートの送信先に送信されません。

SNMPv1

iLOを有効にすると、外部SNMPv1要求を受信し、アラート送信先に構成されているリモート管理システムにSNMPv1トラップを送信します。

コールドスタートトラップブロードキャスト

次の条件のいずれかを満たす場合、コールドスタートトラップは、サブネットブロードキャストアドレスにブロードキャストされます。

- SNMPアラートの送信先が構成されていない。
- SNMPアラートの送信先は構成されているが、SNMPプロトコルが無効である。
- iLOが一部のSNMPアラートの送信先をIPアドレスに解決できなかった。

IPv4ホストのサブネットブロードキャストアドレスは、サブネットマスクとホストIPアドレスのビット成分間のビット論理 `OR` 演算を実行することで取得されます。たとえば、サブネットマスクが `255.255.252.0` のホスト `192.168.1.1` のブロードキャストアドレスは、`192.168.1.1 | 0.0.3.255 = 192.168.3.255` になります。

定期的なHSAトラップ構成

デフォルト構成では、iLOはコンポーネントのステータスが変更された場合（たとえば、ファンステータスが障害に変更された場合）に限り、ヘルスステータスアレイ（HSA）トラップを送信します。

サポートされているコンポーネントが障害または機能低下状態のとき、HSAトラップを定期的に（日次、週次、月次）送信するようiLOを構成できます。この設定は、デフォルトでは無効になっています。

AMSコントロールパネルを使用したSNMPおよびSNMPアラートの設定（Windows専用）

手順

1. Agentless Management Serviceのコントロールパネルを開きます。
2. SNMPタブをクリックします。
3. SNMP設定をアップデートします。

4. （オプション）テストアラートを作成し、構成済みのトラップの宛先にこれを送信するには、テストトラップの送信をクリックします。

   テストアラートは、iLOのトラップ先アドレスとのネットワーク接続を確認するために使用されます。アラートが生成されたら、アラート送信先でアラートの受信を確認します。

5. 構成を保存するには、適用をクリックします。

SNMPトラップ

次の表に、（対応するインテグレーテッドマネジメントログまたはiLOイベントログのクラスおよびコードとともに）iLO6およびサポートされるProLiantサーバーによってサポートされているSNMPトラップを示します。

SNMPトラップとRESTアラート情報を相互参照するには、RESTアラートを参照してください。

イベントのトラブルシューティング情報を確認するには、イベントクラスおよびイベントコードの値を、Webサイトhttps://www.hpe.com/support/ilo-docsにあるIMLメッセージおよびトラブルシューティングガイドの値と照合してください。

トラップID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
0	該当なし	該当なし	`Cold Start Trap` SNMPが初期化され、システムでPOSTが完了した、またはAMSが起動しました。	該当なし
4	該当なし	該当なし	`Authentication Failure Trap` SNMPが認証失敗を検出しました。	該当なし
1006	5h	3h	`cpqSeCpuStatusChange` 訂正不可能なマシンチェック例外がプロセッサーで検出されました。	メジャー
1010	28h	2h	`cpqSeUSBStorageDeviceReadErrorOccurred` 接続されているUSBストレージデバイスで読み取りエラーが発生しました。	OK
1011	28h	3h	`cpqSeUSBStorageDeviceWriteErrorOccurred` 接続されているUSBストレージデバイスで書き込みエラーが発生しました。	OK
1012	28h	4h	`cpqSeUSBStorageDeviceRedundancyLost` USBストレージデバイスの冗長性が失われました。	警告
1013	28h	4h	`cpqSeUSBStorageDeviceRedundancyRestored` USBストレージデバイスの冗長性が回復しました。	OK
1014	28h	5h	`cpqSeUSBStorageDeviceSyncFailed` USBストレージデバイスの冗長性を回復するための同期操作に失敗しました。	警告
1015	33h	5h	`cpqSePCIeDiskTemperatureFailed` PCIeディスクの温度が上限クリティカルしきい値を超えました。	クリティカル

トラップID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
1016	33h	5h	`cpqSePCIeDiskTemperatureOk` PCIeディスクの温度は正常です。	OK
1017	33h	2h	`cpqSePCIeDiskConditionChange` PCIeディスクのステータスが変化しました。	クリティカル
1018	33h	3h	`cpqSePCIeDiskWearStatusChange` PCIeディスク消耗ステータスが変化しました。	クリティカル
1019	33h	4h	`cpqSePciDeviceAddedOrPoweredOn` PCIデバイスが追加されたか、電源がオンになりました。	OK
1020	33h	5h	`cpqSePciDeviceRemovedOrPoweredOff` PCIデバイスが削除されたか、電源がオフになりました。	OK
1021	Ah	3152h	`cpqSeNVMeSecureEraseFailed` NVMeドライブのセキュア消去に失敗しました。	クリティカル
1022	32h	3020h 3021h	`cpqSePcieTrainingFailed` PCI Expressスロットは、連結に失敗しました。	クリティカル
1023	Ah	3158h	`cpqSePciResetFail` システムはスロットのPCIコントローラーでリセットを実行できません。	クリティカル
2014	2h	2Dh	`cpqSiIntrusionInstalled` システム侵入ハードウェアが取り付けられました。	OK
2015	2h	2Eh	`cpqSiIntrusionRemoved` システム侵入ハードウェアが取り外されました。	OK
2016	2h	30h	`cpqSiHoodReplaced` システムフードが交換されました。	OK
2017	Ah	401h	`cpqSiHoodRemovedOnPowerOff` サーバーの電源オフ時にシステムフードが取り外されました。	メジャー
2018	35h	1h	`cpqSiSysTelemetryThresholdAlert` システムテレメトリのメトリック値が上限しきい値を超過したか、または下限しきい値より低くなっています。	情報
3033	13h	12h	`cpqDa6CntlrStatusChange` Smartアレイコントローラーのステータスの変化が検出されました。	クリティカル
3034	13h	21h	`cpqDa6LogDrvStatusChange` Smartアレイ論理ドライブのステータスの変化が検出されました。	クリティカル
3038	13h	17h	`cpqDa6AccelStatusChange` Smartアレイキャッシュモジュールのステータスの変化が検出されました。	クリティカル

トラップID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
3039	13h	23h	cpqDa6AccelBadDataTrap Smartアレイキャッシュモジュールのバックアップ電源が失われました。	クリティカル
3040	13h	24h	cpqDa6AccelBatteryFailed Smartアレイキャッシュモジュールのバックアップ電源が故障しました。	クリティカル
3046	13h	14h	cpqDa7PhyDrvStatusChange Smartアレイ物理ドライブのステータスの変化が検出されました。	クリティカル
3047	13h	2Ch	cpqDa7SpareStatusChange Smartアレイスペアドライブのステータスの変化が検出されました。	クリティカル
3049	13h	15h	cpqDaPhyDrvSSDWearStatusChange Smartアレイ物理ドライブのSSD Wearステータスの変化が検出されました。	クリティカル
3903	Ah	3151h	cpqDaSmartArraySecureEraseFailed Smartアレイのセキュア消去に失敗しました。	クリティカル
5022	13h	1Eh	cpqSasPhyDrvStatusChange AMSが、SASまたはSATA物理ドライブのステータスが変化したことを検出しました。	クリティカル
5026	13h	1Fh	cpqSasPhyDrvSSDWearStatusChange AMSが、SASまたはSATA物理ドライブのSSD Wearステータスが変化したことを検出しました。	クリティカル
6026	2h	38h	cpqHe3ThermalConfirmation 温度上昇のためにサーバーがシャットダウンされましたが、現在は稼働しています。	OK
6027	Ah	101h	cpqHe3PostError 1つまたは複数のPOSTエラーが発生しました。	警告
6032	Bh	36h	cpqHe3FltTolPowerRedundancyLost 指定されたシャーシのフォールトトレラント電源装置の冗長性が失われました。	メジャー
6033	Bh	31h	cpqHe3FltTolPowerSupplyInserted フォールトトレラント電源装置が取り付けられました。	OK
6034	Bh	2Ch	cpqHe3FltTolPowerSupplyRemoved フォールトトレラント電源装置が取り外されました。	メジャー
6035	2h	1Ah	cpqHe3FltTolFanDegraded フォールトトレラントファン状態が、劣化に設定されました。	クリティカル
6036	2h	17h	cpqHe3FltTolFanFailed フォールトトレラントファン状態が、障害に設定されました。	クリティカル

トラップID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
6037	2h	23h	cpqHe3FltTolFanRedundancyLost フォールトトレラントファンの冗長性が失われました。	メジャー
6038	2h	1Fh	cpqHe3FltTolFanInserted フォールトトレラントファンが取り付けられました。	OK
6039	2h	1Bh	cpqHe3FltTolFanRemoved フォールトトレラントファンが取り外されました。	メジャー
6040	2h	27h	cpqHe3TemperatureFailed サーバーの温度を超えました。	クリティカル
6041	2h	14h	cpqHe3TemperatureDegraded 温度ステータスが劣化に設定され、温度が正常な動作範囲にありません。システム構成によっては、このシステムがシャットダウンされる可能性があります。	クリティカル
6042	2h	13h	cpqHe3TemperatureOk 温度ステータスが、OKに設定されました。	OK
6048	Bh	28h	cpqHe4FltTolPowerSupplyOk フォールトトレラント電源装置の状態がOKに設定されました。	OK
6049	Bh	15h	cpqHe4FltTolPowerSupplyDegraded フォールトトレラント電源装置の状態が、劣化に設定されました。	クリティカル
6050	Bh	28h	cpqHe4FltTolPowerSupplyFailed フォールトトレラント電源装置の状態が、障害に設定されました。	クリティカル
6051	該当なし	該当なし	cpqHeResilientMemMirroredMemoryEngaged アドバンストメモリプロテクションサブシステムが、メモリ障害を検出しました。ミラーメモリがアクティブになりました。	メジャー
6054	Bh	36h	cpqHe3FltTolPowerRedundancyRestore フォールトトレラント電源装置が冗長化の状態に回復しました。	OK
6055	2h	23h	cpqHe3FltTolFanRedundancyRestored フォールトトレラントファンが冗長化の状態に回復しました。	OK
6061	該当なし	該当なし	cpqHeManagementProcInReset 管理プロセッサーはリセット中です。	マイナー
6062	該当なし	該当なし	cpqHeManagementProcReady 管理プロセッサーは使用可能です。	情報
6064	該当なし	該当なし	cpqHe5CorrMemReplaceMemModule メモリエラーが訂正されました。メモリモジュールを取り付けます。	メジャー

トラップID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
6069	Bh	52h	cpqHe4FltTolPowerSupplyACpowerloss 指定されたシャーシおよびベイのフォールトトレラント電源装置がAC電源の消失を報告しました。	クリティカル
6070	Bh	3Eh	cpqHeSysBatteryFailed HPE Smartストレージバッテリが故障しました。	警告
6071	Bh	1Eh	cpqHeSysBatteryRemoved HPE Smartストレージバッテリが取り外されました。	警告
6072	27h	4h	cpqHeSysPwrAllocationNotOptimized iLOは所要電力を特定できませんでした。サーバーの電力割り当てが最適化されていません。	警告
6073	Bh	24h	cpqHeSysPwrOnDenied ハードウェアを識別できないために、サーバーの電源をオンにできませんでした。	クリティカル
6074	14h	7h	cpqHePowerFailureError デバイスの電源障害が検出されました。	クリティカル
6075	29h	1h	cpqHeInterlockFailureError デバイスがシステムボードにない、または適切に取り付けられていません。	クリティカル
6076	Ah	340h	cpqHeNvdimmBackupError NVDIMMバックアップエラーが検出されました。	クリティカル
6077	Ah	341h	cpqHeNvdimmRestoreError NVDIMMの復元エラーが検出されました。	クリティカル
6078	Ah	342h	cpqHeNvdimmUncorrectableMemoryError 訂正不能なメモリエラーが検出されました。	クリティカル
6079	Ah	343h	cpqHeNvdimmBackupPowerError NVDIMMのバックアップ電源エラーが発生しました。バックアップ電源を使用できません。これ以上のバックアップは不可能です。	クリティカル
6080	Ah	344h	cpqHeNvdimmNVDIMMControllerError NVDIMMコントローラーのエラーが発生しました。OSではNVDIMMは使用されません。	クリティカル
6081	Ah	345h	cpqHeNvdimmEraseError NVDIMMを消去できませんでした。これ以上のバックアップは不可能です。	クリティカル
6082	Ah	346h	cpqHeNvdimmArmingError NVDIMMを取り付けることができませんでした。これ以上のバックアップは不可能です。	クリティカル
6083	Ah	355h	cpqHeNvdimmSanitizationOk このNVDIMM-Nがサニタイズ/消去の対象として選択されました。NVDIMMに保存されているデータはすべて消去されました。	OK

トラップID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
6084	Ah	356h	cpqHeNvdimmSanitizationError このNVDIMM-Nはサニタイズ/消去の対象として選択されましたが、このプロセスが正常に終了しませんでした。	クリティカル
6085	Ah	364h	cpqHeNvdimmControllerFirmwareError NVDIMMコントローラーファームウェアのエラーが発生しました。コントローラーファームウェアが壊れているため、OSでNVDIMMは使用されません。	クリティカル
6086	Ah	374h	cpqHeNvdimmErrorInterleaveOn メモリの初期化エラーまたは訂正不能エラーが発生しました。プロセッサーのNVDIMMはすべて無効です。	クリティカル
6087	Ah	375h	cpqHeNvdimmInterleaveOff メモリの初期化エラーまたは訂正不能エラーが発生しました。NVDIMMは無効になっています。	クリティカル
6088	Ah	394h	cpqHeNvdimmEventNotifyError このNVDIMMのイベント通知を設定できません。	クリティカル
6089	Ah	395h	cpqHeNvdimmPersistencyLost NVDIMMの持続性が失われました。これ以上のデータバックアップは不可能です。	クリティカル
6090	Ah	396h	cpqHeNvdimmPersistencyRestored NVDIMMの持続性が復元されました。これ以上のデータバックアップが可能です。	情報
6091	Ah	397h	cpqHeNvdimmLifecycleWarning NVDIMMライフサイクルの警告。NVDIMMの寿命に達しました。	メジャー
6092	Ah	430h	cpqHeNvdimmLogicalNvdimmError 論理NVDIMMのエラーが発生しました。	メジャー
6093	Ah	354h	cpqHeNvdimmConfigurationError NVDIMM構成エラーが発生しました。	クリティカル
6094	Ah	351h	cpqHeNvdimmBatteryNotChargedwithWait スマートバッテリは、取り付けられたNVDIMMをサポートするほど十分に充電されていません。	OK
6095	Ah	352h	cpqHeNvdimmBatteryNotChargedwithNoWait スマートバッテリは、取り付けられたNVDIMMをサポートするほど十分に充電されていません。	OK
6096	Ah	388h	cpqHeDimmMemoryMapChanged 訂正不能なメモリエラー - 障害が発生しているメモリモジュールを判別できませんでした。	警告
6098	Ah	483h	cpqHeNvdimmInitializationError 内部エラーのため、1つまたは複数のNVDIMMを初期化できません。	警告

トラップID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
6099	Bh	54h	cpqHePwrSupplyError システム電源装置のエラーが発生しました。	警告
6100	Bh	54h	cpqHePwrSupplyErrorRepaired システム電源装置のエラーが修復されました。	OK
6101	Bh	55h	cpqHeBbuError バッテリバックアップユニットのエラーが発生しました。	警告
6102	Bh	55h	cpqHeBbuErrorRepaired バッテリバックアップユニットのエラーが修復されました。	OK
6103	Bh	1Ch	cpqHeNoPowerSupplyDetected 電源装置または電源バックプレーンは検出されませんでした。	メジャー
6104	Bh	1Bh	cpqHePowerProtectionFault システムボードの電源保護障害が発生しました。	クリティカル
6105	14h	9h	cpqHePowerFuseDegraded 電源の劣化が検出され、サーバーシステムボードを交換する必要があります。	クリティカル
6106	Ah	3134h	cpqHeTPMSecureEraseFailed Trusted Platform Moduleのセキュア消去に失敗しました。	クリティカル
6107	Ah	3140h	cpqHeSPISecureEraseFailed システムファームウェア構成のセキュア消去に失敗しました。	クリティカル
6109	28h	6h	cpqHeNANDSecureEraseFailed 管理プロセッサーの内蔵メディアデバイスのセキュア消去に失敗しました。	クリティカル
6110	Ah	3143h 3145h 3146h	cpqHeSedPassphrasefail デバイスの暗号化エラー。暗号化の有効化または無効化あるいはパスフレーズの変更に失敗しました。	クリティカル
6111	Ah	3148h	cpqHeSedUnlockfail 自己暗号化デバイスのロックを解除する不正な試行が3回実行されました。デバイスは次回のリブートまでロックされます。	メジャー
6116	0xA	0x460	cpqHePMMCorrErrThreshold 訂正可能なメモリエラーのしきい値を超過した	メジャー
6118	2h	39h	cpqHeInletAmbientPreCautionThresAlert インレット周囲センサーの読み取り値がユーザー定義の値以上です。	マイナー
6119	0x2	0x3C	cpqHeCoolingModuleDegraded 指定されたシャーシの冷却モジュールの状態が劣化に設定されています。	メジャー

トラップID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
6120	0x2	0x3B	`cpqHeCoolingModuleFailed` 指定されたシャーシの冷却モジュールの状態が失敗に設定されています。	クリティカル
6121	0x2	0x3D	`cpqHeCoolingModuleRedundancyLost` 冷却モジュールは、指定されたシャーシの冗長性を失いました。	メジャー
6122	0x2	0x3D	`cpqHeCoolingModuleRedundancyRestored` 冷却モジュールは、指定されたシャーシの冗長化の状態に戻りました。	情報
6123	0xB	0x90	`cpqHeUnsupportedPwrSupplyDetected` サポートされない電源装置構成です。	クリティカル
6124	0xB	0x90	`cpqHeUnSupportedPwrSupplyRemoved` サポートされない電源装置が取り外されました。	情報
6125	0x2	0x3F	`cpqHeUserTempThreshWarning` ユーザー定義の注意温度しきい値を超えました。	マイナー
6126	0x2	0x40	`cpqHeUserTempThreshCritical` ユーザー定義のクリティカル温度しきい値を超えました。	クリティカル
8029	13h	28h	`cpqSs6FanStatusChange` ストレージエンクロージャーのファンステータスが変化しました。	クリティカル
8030	13h	29h	`cpqSs6TempStatusChange` ストレージエンクロージャーの温度ステータスが変化しました。	クリティカル
8031	13h	2Ah	`cpqSs6PwrSupplyStatusChange` ストレージエンクロージャーの電源ステータスが変化しました。	クリティカル
8032	13h	2Bh	`cpqSsConnectionStatusChange` ストレージエンクロージャーのステータスが変化しました。	クリティカル
9001	23h	5h	`cpqSm2ServerReset` サーバー電源がリセットされました。	クリティカル
9003	23h	1100h	`cpqSm2UnauthorizedLoginAttempts` 認証されないログイン試行回数の最大値を超えました。	情報
9005	23h	1101h	`cpqSm2SelfTestError` iLOがセルフテストエラーを検出しました。	クリティカル
9012	23h	104h	`cpqSm2SecurityOverrideEngaged` iLOが、セキュリティオーバーライドジャンパーが接続位置に切り替えられていることを検出しました。	情報

トラップID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
9013	23h	105h	`cpqSm2SecurityOverrideDisengaged` iLOが、セキュリティオーバーライドジャンパーが切断位置に切り替えられていることを検出しました。	情報
9017	23h	3h	`cpqSm2ServerPowerOn` サーバーの電源が入れられました。	OK
9018	23h	1h	`cpqSm2ServerPowerOff` サーバーの電源が切られました。	OK
9019	23h	1102h	`cpqSm2ServerPowerOnFailure` 電源オン要求がありましたが、サーバーが障害状態にあったために電源を入れることができませんでした。	クリティカル
9020	23h	1138h	`cpqSm2IrsCommFailure` Insight Remote Supportとの通信に失敗しました。	警告
9021	32h	3h	`cpqSm2FirmwareValidationScanFailed` ファームウェア検証エラーが発生しました（iLO、IE、またはSPSファームウェア）。	クリティカル
9022	32h	3h	`cpqSm2FirmwareValidationScanErrorRepaired` 報告されたファームウェア整合性スキャンの問題は修復されました。	OK
9023	32h	4h	`cpqSm2FirmwareValidationAutoRepairFailed` ファームウェアのリカバリ時にエラーが発生しました。	警告
9024	14h	2h	`cpqSm2AutoShutdownInitiated` iLOがオペレーティングシステムの自動シャットダウンを開始しました。	メジャー
9025	14h	2h	`cpqSm2AutoShutdownCancelled` オペレーティングシステムの自動シャットダウンがキャンセルされました。	OK
9026	23h	448h	`cpqSm2FwUpdateUploadFailed` ファームウェアアップデートまたはアップロードに失敗しました。	警告
9027	23h	464h	`cpqSm2SecurityStateChange` iLOセキュリティの状態が変化しました。	OK
9028	23h	B3h	`cpqSm2WDTimerReset` iLOがウォッチドッグタイマーのタイムアウトを検出しました。オペレーティングシステムに装備された後は、フェイルセーフタイマーは定期的に扱われません。	メジャー
9029	23h	491h	`cpqSm2OverallSecStateAtRisk` システムセキュリティ状態にリスクがあります。	メジャー
9030	23h	490h	`cpqSm2OverallSecStatusChange` 全体セキュリティステータスが変更されました。	メジャー

トラップID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
11003	1h	1h	cpqHo2GenericTrap 汎用トラップ。SNMP設定、クライアントSNMPコンソール、およびネットワークが正しく動作していることを確認します。iLOのWebインターフェイスを使用すると、このアラートを生成して、SNMPコンソールでアラートが受信されることを確認できます。	情報
11018	23h	CEh	cpqHo2PowerThresholdTrap 電力しきい値を超えました。	メジャー
11020	該当なし	該当なし	cpqHoMibHealthStatusArrayChangeTrap サーバーのヘルスステータスが変化しました。	該当なし
14004	13h	20h	cpqIdeAtaDiskStatusChange AMSが、ATAディスクドライブのステータスが変化したことを検出しました。	クリティカル
14007	Ah	3150h	cpqIdeAtaSecureEraseFailed SATAドライブのセキュア消去に失敗しました。	クリティカル
16028	11h	Bh	cpqFca3HostCntlrStatusChange AMSが、ファイバーチャネルホストコントローラーのステータスが変化したことを検出しました。	クリティカル
18011	11h	Ah	cpqNic3ConnectivityRestored 論理ネットワークアダプターとの接続が回復しました。	OK
18012	11h	Ah	cpqNic3ConnectivityLost 論理ネットワークアダプターのステータスが障害に変化しました。	警告
18013	11h	Ch	cpqNic3RedundancyIncreased AMSが、接続されている論理アダプターグループ内の障害が発生していた物理アダプターが良好ステータスに復帰したことを検出しました。	OK
18014	11h	Ch	cpqNic3RedundancyReduced AMSが、論理アダプターグループ内の物理アダプターが障害ステータスに変化したが、少なくとも1台の物理アダプターがOKステータスで残っていることを検出しました。	警告
18015	11h	Dh	cpqNicAllLinksDown ネットワークアダプターのすべてのリンクがダウンしています。	メジャー
18016	Bh	Eh	cpqNicAllLinksDownRepaired ネットワークアダプターの1つまたは複数のリンクが修復されました。	OK
18017	32h	3023h	cpqNicFlexLomTrainingFailed Flexlomスロットは、連結に失敗しました。	クリティカル
169001	12h	1h	cpqiScsiLinkUp iSCSIリンクがアップしています。	OK

トラップID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
169002	12h	2h	`cpqiScsiLinkDown` iSCSIリンクがダウンしています。	メジャー

これらのSNMPトラップについて詳しくは、HPE SIM用のInsight Management MIBアップデートキットに含まれている以下のMIBファイルを参照してください。

`cpqida.mib`	ドライブアレイ
`cpqhost.mib`	サーバーホストシステムの詳細
`cpqhlth.mib`	サーバーヘルスシステム
`cpqsm2.mib`	Remote Insight/Integrated Lights-Out
`cpqide.mib`	IDEサブシステム
`cpqscsi.mib`	SCSIシステム
`cpqiscsi.mib`	iSCSIシステム
`cpqnic.mib`	システムNIC
`cpqstsys.mib`	ストレージシステム
`cpqstdeq.mib`	サーバー標準装置
`cpqfca.mib`	ファイバーチャネルアレイ
`cpqsinfo.mib`	システム情報
`cpqstsys.mib`	Smart Arrayストレージ

RESTアラート

次の表に、iLO6およびサポートされるProLiantサーバーによってサポートされているRESTアラートを示します。RESTアラートとSNMPトラップ情報を相互参照するには、SNMPトラップを参照してください。

トラップID	RESTアラートID	RESTの重大度
0	該当なし	該当なし
4	`SNMPAuthenticationFailure`	OK

1006	`ProcessorStatusUnknown`
	`ProcessorStatusOK`
	`ProcessorStatusDegraded`
	`ProcessorStatusDisabled`
	`ProcessorStatusFailed`
		警告
		OK
		警告
		警告
		クリティカル

1010	`USBStorageDeviceReadError`	OK
1011	`USBStorageDeviceWriteError`	OK

トラップID	RESTアラートID	RESTの重大度
1012	USBStorageDeviceRedundancyLost	警告
1013	USBStorageDeviceRedundancyRestored	OK
1014	USBStorageDeviceSyncFailed	警告
1015	PCIeDiskTemperatureFailed	クリティカル
1016	PCIeDiskTemperatureOk	OK
1017	PCIeDriveConditionOk PCIeDriveConditionDegraded PCIeDriveConditionFailed	OK 警告 クリティカル
1018	PCIeDriveWearStatusOk PCIeDriveWearStatusFiftySixDayThreshold PCIeDriveWearStatusFivePercentThreshold PCIeDriveWearStatusTwoPercentThreshold PCIeDriveWearStatusWearOut	OK 警告 警告 警告 クリティカル
1019	PCIeDriveAddedOrPowerOn	OK
1020	PCIeDriveRemovedOrPowerOff	OK
1021	NVMeSecureEraseFailed	クリティカル
1022	該当なし	該当なし
1023	PciResetFail	クリティカル
1193	BIOSSafeModeEngaged	OK
1194	該当なし	該当なし
1197	IntelligentDiagnosticsEnabled	OK
1198	IntelligentDiagnosticsExit	OK
1328	BIOSSafeModeExit	OK
1329	該当なし	該当なし
2014	IntrusionHWInstalled	OK
2015	IntrusionHWRemoved	OK
2016	HoodReplaced	OK
2017	HoodRemovedOnPowerOff	警告
2018	MetricValueExceededUpperThreshold MetricValueBelowLowerThreshold	警告 警告
3033	DrvArrControllerFailed DrvArrControllerOK	クリティカル OK

トラップID	RESTアラートID	RESTの重大度
3034	DrvArrLogDrvFailed	クリティカル
	DrvArrLogDrvUnconfigured	クリティカル
	DrvArrLogDrvRecovering	警告
	DrvArrLogDrvReadyRebuild	警告
	DrvArrLogDrvRebuilding	警告
	DrvArrLogDrvWrongDrive	クリティカル
	DrvArrLogDrvBadConnect	クリティカル
	DrvArrLogDrvOverheating	警告
	DrvArrLogDrvShutdown	クリティカル
	DrvArrLogDrvExpanding	OK
	DrvArrLogDrvNotAvailable	警告
	DrvArrLogDrvQueuedForExpansion	警告
	DrvArrLogDrvMultiPathAccessDegraded	警告
	DrvArrLogDrvErasing	警告
	DrvArrLogDrvPredictiveSpareRebuildReady	OK
	DrvArrLogDrvRapidParityInitializationInProgress	警告
	DrvArrLogDrvRapidParityInitializationPending	警告
	DrvArrLogDrvNoAccessEncryptedMissingKey	クリティカル
	DrvArrLogDrvUnencryptedToEncryptedTransformationInProgress	警告
	DrvArrLogDrvRekeyInProgress	警告
	DrvArrLogDrvNoAccessEncryptedWithControllerEncryptionNotEnabled	クリティカル
	DrvArrLogDrvUnencryptedToEncryptedTransformationNotStarted	OK
	DrvArrLogDrvNewLogDrvKeyRekeyRequestReceived	OK
	DrvArrLogDrvOK	OK

トラップID	RESTアラートID	RESTの重大度
3038	DrvArrayAccBoardInvalid	警告
	DrvArrayAccBoardEnabled	OK
	DrvArrayAccBoardTempDisabled_BadConfiguration	クリティカル
	DrvArrayAccBoardTempDisabled_LowBatteryPower	クリティカル
	DrvArrayAccBoardTempDisabled_DisableCommandIssued	警告
	DrvArrayAccBoardTempDisabled_NoResourcesAvailable	警告
	DrvArrayAccBoardTempDisabled_BoardNotConnected	クリティカル
	DrvArrayAccBoardPermDisabled_BadMirrorData	警告
	DrvArrayAccBoardPermDisabled_ReadFailure	警告
	DrvArrayAccBoardPermDisabled_WriteFailure	警告
	DrvArrayAccBoardPermDisabled_ConfigCommand	警告
	DrvArrayAccBoardTempDisabled_ExpandInProgress	OK
	DrvArrayAccBoardTempDisabled_SnapshotInProgress	OK
	DrvArrayAccBoardTempDisabled_RedundantLowBattery	OK
	DrvArrayAccBoardTempDisabled_RedundantSizeMismatch	警告
	DrvArrayAccBoardTempDisabled_RedundantCacheFailure	クリティカル
	DrvArrayAccBoardPermDisabled_ExcessiveECCErrors	クリティカル
	DrvArrayAccBoardTempDisabled_RAID_ADG_EnablerModuleMissing	OK
	DrvArrayAccBoardPermDisabled_PostECCErrors	クリティカル
	DrvArrayAccBoardPermDisabled_BackupPowerSourceHotRemoved	クリティカル
	DrvArrayAccBoardPermDisabled_CapacitorChargeLow	警告
	DrvArrayAccBoardPermDisabled_NotEnoughBatteries	警告
	DrvArrayAccBoardPermDisabled_NotSupportedByFirmware	クリティカル
	DrvArrayAccBoardPermDisabled_BatteryNotSupported	クリティカル
	DrvArrayAccBoardPermDisabled_NoCapacitorAttached	警告
	DrvArrayAccBoardPermDisabled_FlashBackedBackupFailed	クリティカル
	DrvArrayAccBoardPermDisabled_FlashBackedRestoreFailed	クリティカル
	DrvArrayAccBoardPermDisabled_FlashBackedHardwareFailure	クリティカル
	DrvArrayAccBoardPermDisabled_CapacitorFailedToCharge	クリティカル
	DrvArrayAccBoardPermDisabled_IncompatibleCacheModule	クリティカル
	DrvArrayAccBoardPermDisabled_ChargerCircuitFailure	警告
	DrvArrayAccBoardTempDisabled_MegaCellNotCabled	
	DrvArrAcceleratorFlashMemoryNotAttached	
3039	DrvArrayAccBoardBadData	クリティカル
3040	DrvArrayAccBoardBatteryFailed	クリティカル

トラップID	RESTアラートID	RESTの重大度
3046	DrvArrPhysDrvFailed	クリティカル
	DrvArrPhysDrvPredictiveFailure	警告
	DrvArrPhysDrvWearOut	警告
	DrvArrPhysDrvErasing	警告
	DrvArrPhysDrvNotAuthenticated	警告
	DrvArrPhysDrvEraseDone	警告
	DrvArrPhysDrvEraseQueued	警告
	DrvArrPhysDrvOK	OK
3047	DrvArrSpareDriveFailed	クリティカル
	DrvArrSpareDriveInactive	OK
	DrvArrSpareDriveBuilding	クリティカル
	DrvArrSpareDriveActive	OK
3049	DrvArrSolidStateDiskFiftySixDayThresholdPassed	警告
	DrvArrSolidStateDiskFivePercentThresholdPassed	警告
	DrvArrSolidStateDiskTwoPercentThresholdPassed	警告
	DrvArrSolidStateDiskWearOut	クリティカル
	DrvArrSolidStateDiskWearOK	OK
3903	SmartArraySecureEraseFailed	クリティカル
5022	該当なし	該当なし
5026	該当なし	該当なし
6026	ServerOperational	警告
6027	POSTErrorsOccurred	警告
6032	PowerRedundancyLost	警告
6033	PowerSupplyInserted	OK
6034	PowerSupplyRemoved	警告
6035	FanDegraded	クリティカル
6036	FanFailed	クリティカル
6037	FanRedundancyLost	警告
6038	FanInserted	OK
6039	FanRemoved	警告
6040	ThermalStatusFailure	クリティカル
6041	ThermalStatusDegradedSysShutdown	クリティカル
	ThermalStatusDegradedSysContinue	クリティカル
6042	ThermalStatusOK	OK

トラップID	RESTアラートID	RESTの重大度
6048	PowerSupplyOK	OK
6049	PowerSupplyDegraded	クリティカル
6050	PowerSupplyFailed	クリティカル
6051	MirroredMemoryEngaged	警告
6054	PowerRedundancyRestored	OK
6055	FanRedundancyRestored	OK
6061	該当なし	該当なし
6062	該当なし	該当なし
6064	CorrectableOrUncorrectableMemoryErrors	警告
6069	PowerSupplyACPowerLoss	クリティカル
6070	SystemBatteryFailed	警告
6071	SystemBatteryRemoved	警告
6072	SystemPowerAllocationNotOptimized	クリティカル
6073	SystemPowerOnDenied	クリティカル
6074	PowerFailureErrorTempAboveCritical PowerFailureErrorInputPowerLoss PowerFailureErrorBadFuse PowerFailureStandby PowerFailureRuntime PowerFailurePowerOn PowerFailureUnknown PowerFailureCpuThermalTrip	クリティカル クリティカル クリティカル クリティカル クリティカル クリティカル クリティカル クリティカル
6075	InterlockFailureErrorStandby InterlockFailureErrorRuntime InterlockFailureErrorPowerOn InterlockFailureErrorUnknown	クリティカル クリティカル クリティカル クリティカル
6076	NvdimmBackupError	クリティカル
6077	NvdimmRestoreError	クリティカル
6078	NvdimmUncorrectableMemoryError	クリティカル
6079	NvdimmBackupPowerError	クリティカル
6080	NvdimmControllerError	クリティカル
6081	NvdimmEraseError	クリティカル
6082	NvdimmArmingError	クリティカル

トラップID	RESTアラートID	RESTの重大度
6083	HeNvdimmSanitizationOk	警告
6084	NvdimmSanitizationError	クリティカル
6085	HeNvdimmControllerFirmwareError	クリティカル
6086	NvdimmInterleaveOn	クリティカル
6087	NvdimmInterleaveOff	クリティカル
6088	NvdimmEventNotifyError	クリティカル
6089	NvdimmPersistencyLost	クリティカル
6090	NvdimmPersistencyRestored	OK
6091	HeNvdimmLifecycleWarning	警告
6092	NvdimmLogicalNvdimmError	警告
6093	NvdimmConfigurationError	クリティカル
6094	NvdimmBatteryNotChargedwithWait	警告
6095	NvdimmBatteryNotChargedwithNoWait	警告
6096	NvdimmMemoryMapChanged	警告
6097	NvdimmPersistantMemoryAddressError	クリティカル
6098	NvdimmInitializationError	警告
6099	PwrSupplyError	警告
6100	PwrSupplyErrorRepaired	OK
6101	BatteryBackupUnitError	クリティカル
6102	BatteryBackupUnitErrorRepaired	OK
6103	NoPowerSupplyDetected	クリティカル
6104	PowerProtectionFault	クリティカル
6105	PowerDegradedEventDetected	クリティカル
6106	TPMSecureEraseFailed	クリティカル
6107	SPISecureEraseFailed	クリティカル
6108	AEPSecureEraseFailed	クリティカル
6109	EmbeddedMediaSecureEraseFailed	クリティカル
6110	SEDPassPhraseFailed	クリティカル
6111	SEDUnlockFailed	警告
6118	InletAmbientPreCautionThresAlert	OK

トラップID	RESTアラートID	RESTの重大度
8029	StorageSystemFanFailed	クリティカル
	StorageSystemNoFan	警告
	StorageSystemFanDegraded	クリティカル
	StorageSystemFanOK	OK
8030	StorageSystemTemperatureFailed	クリティカル
	StorageSystemTemperatureDegraded	クリティカル
	StorageSystemNoTemperature	警告
	StorageSystemTemperatureOK	OK
8031	StorageSystemPwrSupplyDegraded	クリティカル
	StorageSystemNoPwrSupply	警告
	StorageSystemPwrSupplyOK	OK
8032	該当なし	該当なし
9001	ServerResetDetected	警告
9003	UnauthorizedLoginAttempts	OK
9005	該当なし	該当なし
9012	SecurityOverrideEngaged	OK
9013	SecurityOverrideDisengaged	OK
9017	ServerPoweredOn	OK
9018	ServerPoweredOff	OK
9019	ServerPowerOnFailure	クリティカル
9020	ILOToInsightRemoteSupportCommunicationFailure	警告
9021	FirmwareValidationScanFailed	クリティカル
9022	FirmwareValidationScanErrorRepaired	OK
9023	FirmwareValidationAutoRepairFailed	警告
9024	AutoShutdownInitiated	クリティカル
9025	AutoShutdownCancelled	OK
9026	該当なし	該当なし
9027	該当なし	該当なし
9028	IPMIWatchdogTimerReset	警告
9029	OverallSecStateAtRisk	警告
9030	OverallSecStatusChange	警告
11003	TestAlert	OK
11018	PowerThresholdBreach	警告

トラップID	RESTアラートID	RESTの重大度
11020	該当なし	該当なし
14004	該当なし	該当なし
14007	IdeAtaSecureEraseFailed	クリティカル
16028	該当なし	該当なし
18011	NicConnectivityRestored	OK
18012	NicConnectivityLost	警告
18013	該当なし	該当なし
18014	該当なし	該当なし
18015	NicAllLinksDown	クリティカル
18016	NicAllLinksDownRepaired	OK
18017	該当なし	該当なし
169001	該当なし	該当なし
169002	該当なし	該当なし
999927	EnclosureManagerFirmwareMismatch	クリティカル
80321	StorageSystemNotConnected	クリティカル
80323	StorageSystemConnected	OK
80322	StorageSystemNotSupported	警告
6120	LiquidCoolingModuleFailed	クリティカル
6119	LiquidCoolingModuleDegraded	クリティカル
6121	LiquidCoolingModuleRedundancyLost	警告
6122	LiquidCoolingModuleRedundancyRestored	OK
6123	UnsupportedPowerSupplyUnitDetected	クリティカル
6124	UnsupportedPowerSupplyUnitRemoved	OK
140083	DriveSmartError	クリティカル
140084	DriveFailed	クリティカル
140085	DriveWearOut	警告
140082	DriveOk	OK
140086	DriveRemoved	警告
140087	DriveInserted	警告
140096	SsdWearOut	クリティカル

IPMIアラート

#	名前	IPMI SELイベント (Y/N)	IPMI SELイベントの詳細	SNMPのサポート (Y/N)	OID
1	CPU障害	Y	IERR | 訂正不能なマシンチェックの例外がアサートされた | 構成エラーがアサートされた | アサート済み	Y	cpqSeCpuUncorrectableError cpqSeCpuStatusChange
3	メモリECCエラー	Y	訂正不能なECC | アサート済み	Y	cpqHe5CorrMemReplaceMemModule
4	訂正可能なメモリエラー	Y	訂正可能なECC | アサート済み	N	該当なし
5	メモリ障害	Y	メモリデバイスが無効になっている | 構成エラーがアサートされた | アサート済み	Y	cpqHe5CorrMemReplaceMemModule
9	電源装置で障害が発生している	Y	障害が検出された | 電源ACの損失がアサートされた | アサート済み	Y	cpqHe4FltTolPowerSupplyFailed cpqHePwrSupplyError cpqHe4FltTolPowerSupplyACpowerloss cpqHeNoPowerSupplyDetected
10	電源装置が取り外された	Y	存在が検出された | ディアサート済み	Y	cpqHe3FltTolPowerSupplyRemoved
14	ハードディスクの障害	Y	ドライブの障害 | 事前障害がアサートされた | In Failed Arrayがアサートされた | アサート済み	Y	cpqDa7PhyDrvStatusChange
16	ファン障害	Y	OKに移行 | OKから重大でないへの移行がアサートされた | 軽度から回復不能への移行がアサートされた | より深刻から重大でないへの移行がアサートされた | アサート済み	Y	cpqHe3FltTolFanDegraded cpqHe3FltTolFanFailed cpqHe3FltTolFanRedundancyLost cpqHe3FltTolFanInserted
17	ファンの取り外し	N	-	Y	cpqHe3FltTolFanRemoved

iLOアラートメール

iLOアラートメールを使用すると、ホストオペレーティングシステムとは関係なく検出されたアラート条件を、1つ以上のメールアドレスに送信するようにiLOを構成することができます。iLOアラートメールのメッセージには、MLに表示される主要なホストシステムイベントが含まれます。たとえば、ファン障害が発生すると、イベントがIMLに記録され、メールメッセージが詳細とともに構成されたメールアドレスに送信されます。

一部のメールサービスプロバイダーでは、スパム、商用コンテンツ、不要な容量など、問題のあるメールをブロックするためのフィルターやルールが確立されています。これらのツールによって、iLOで生成されたメッセージを受け取れない場合があります。この問題を回避するには、Hewlett Packard EnterpriseではセキュアなSMTP接続（SSL/TLS）を有効にし、構

成されたSMTPサーバーによって認識された送信者のメールアドレスを構成することをお勧めします。

サブトピック

アラートメールを有効にする

アラートメールを無効にする

アラートメールを有効にする

前提条件

- iLOの設定を構成する権限
- この機能をサポートするライセンスがインストールされている。使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
- SMTP認証を有効が有効になっている構成の場合は、メールアカウントのユーザー名とパスワードがSMTPサーバーに表示されます。
- SMTPセキュア接続（SSL/TLS）を有効が有効になっている構成の場合は、SSL/TLSがサーバーで有効になっています。
- パブリックまたはISPのSMTPサーバーを使用する場合、受信者アドレスに使用するメールアドレスが、安全性が低いアプリケーションを許可するように構成されていることを確認します。

手順

1. ナビゲーションツリーで管理をクリックしてから、アラートメールタブをクリックします。
2. iLOアラートメールを有効オプションを有効に設定します。
3. 次の情報を入力します。
   - 受信者のメールアドレス
   - 送信ドメインまたはメールアドレス
   - SMTPポート

     SMTPセキュア接続（SSL/TLS）を有効オプションを使用する場合、Hewlett Packard Enterpriseではこの値を587に設定することをお勧めします。
   - SMTPサーバー
4. セキュアな接続を介してアラートメールメッセージを送信するには、SMTPセキュア接続（SSL/TLS）を有効オプションを有効にします。
5. メールアカウントのユーザー名とパスワードでSMTP接続を認証するには、SMTP認証を有効オプションを有効にします。
6. SMTPセキュア接続（SSL/TLS）を有効およびSMTP認証を有効が有効になっている場合：
   a. SMTPユーザー名ボックスに、構成されているSMTPサーバー上のメールアカウントのユーザー名を入力します。
   b. SMTPパスワードの変更チェックボックスを選択します。
   c. 新しいSMTPパスワードボックスとSMTPパスワードの確認ボックスにメールアカウントのユーザー名のパスワードを入力します。
7. 変更を保存するには、適用をクリックします。
8. （オプション）構成したメールアドレスにテストメッセージを送信するには、テストアラートメールを送信をクリックします。

   このボタンは、アラートメールが有効な場合にのみ使用できます。

テストアラートメールが送信されます。

9. （オプション）テストメッセージを送信した場合は、iLOイベントログで正常に送信されたかどうかを確認します。

サブトピック

アラートメールのオプション

アラートメールのオプション

受信者のメールアドレス

iLOメールアラートを受信する1つ以上の宛先メールアドレス。複数の電子メールアドレスをセミコロンで区切って入力できます。標準メールアドレス形式でアドレスを入力します。受信者のメールアドレスボックスには最大260文字まで入力できます。

パブリックまたはISPのSMTPサーバーを使用する場合、入力するメールアドレスが、安全性が低いアプリケーションを許可するように構成されていることを確認します。

送信ドメインまたはメールアドレス

送信者（送信元）のメールアドレス（最大63文字）。この値は、以下の方法を使用して構成できます。

- iLOホスト名に統合する送信ドメインを入力します。この方法を使用すると、送信者のメールアドレスは<iLO Hostname>@<Sender Domain>になります。
- 内部ネットワークドメインを含むカスタムのメールアドレスを入力します。たとえば、<name>@<internal domain>.comのように入力します。
- パブリックメールサーバーを使用するカスタムメールアドレスを入力します。たとえば、<name>@<email provider>.comのように入力します。

  このアドレスは、構成済みのSMTPサーバーで認識される有効なメールアドレスである必要があります。

SMTPポート

SMTPサーバーが認証済みまたは未認証のSMTP接続に使用するポート。デフォルト値は25です。セキュアな接続のために、Hewlett Packard Enterpriseではポート587を使用することをお勧めします。

SMTPサーバー

SMTPサーバーまたはメール送信エージェントのIPアドレスまたはDNS名。このサーバーは、メール転送エージェントと連携して電子メールを配信します。IPv4アドレス、IPv6アドレス、またはFQDNを入力できます。この文字列は最大63文字です。

SMTPセキュア接続（SSL/TLS）を有効

このオプションを有効にして、セキュアな接続を介してアラートメールメッセージを送信します。メッセージが送信されると、iLOおよび構成済みのSMTPサーバーが共通のSSL/TLS接続を選択するようにネゴシエートします。

iLOは明示的/便宜的TLS SMTPサーバー（STARTTLS SMTPサーバー）のみをサポートします。

この値はデフォルトで有効になっています。

SMTP認証を有効

このオプションを有効にして、セキュアな接続経由で接続した後に構成済みのSMTPサーバーに対して認証します。このオプションを使用するには、SMTPセキュア接続（SSL/TLS）を有効が有効になっているほか、SMTPサーバー上のメールアカウントのユーザー名とパスワードを指定する必要があります。

SMTPユーザー名

構成済みのSMTPサーバー上のアカウントのユーザー名（最大63文字）。SMTP認証を有効が有効になっている場合はこの値が必要です。

この値をクリアするには、SMTP認証を有効オプションを無効にし、このボックス内のテキストを削除してから、適用をクリックします。

SMTPパスワードの変更

このチェックボックスをクリックし、SMTPユーザー名のアカウントのパスワードを入力またはアップデートして確認します。SMTP認証を有効が有効になっている場合はこの値が必要です。入力できる値は63文字までです。

iLO Webインターフェイスからパスワードの値を表示またはコピーすることはできません。

パスワードをクリアするには、SMTP認証を有効オプションを無効にし、パスワードおよびパスワード再入力の値を入力せずに適用をクリックします。

アラートメールを無効にする

前提条件

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

手順

1. ナビゲーションツリーでマネジメントをクリックしてから、アラートメールタブをクリックします。
2. iLOアラートメールを有効オプションを無効に設定します。
3. 変更を保存するには、適用をクリックします。

リモートsyslog

リモートsyslog機能を使用すると、iLOはイベント通知メッセージをsyslogサーバーに送信できます。iLOファームウェアのリモートsyslogには、IMLおよびiLOイベントログが含まれます。

リモートsyslog形式はRFC5242に準拠しています。syslogは、iLOタイムスタンプで始まり、その後にiLOホスト名、サブシステム名（ログ生成元）、およびログテキストが続く必要があります。以下に例を示します。

```
2020-08-26T15:26:43Z  ILO7CE712P2K6  DriveArray  Smart Array - Drive is failed: Port Box 0 Bay 0
ACTION:1. Be sure all cables are connected properly and securely. 2. Be sure all drives are fully
seated. 3 Replace the defective cables, drive, or both.
```

サブトピック

iLOリモートsyslogの有効化

iLOリモートsyslogの無効化

リモートSyslogアラートレベル（Linux）

iLOリモートsyslogの有効化

前提条件

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

手順

1. ナビゲーションツリーでマネジメントをクリックしてから、リモートSyslogタブをクリックします。
2. iLOリモートSyslogを有効オプションを有効に設定します。
3. 次の情報を入力します。
   - リモートSyslogポート
   - リモートSyslogサーバー
4. 変更を保存するには、適用をクリックします。
5. （オプション）構成したSyslogサーバーにテストメッセージを送信するには、テストSyslogを送信をクリックします。

   このボタンは、iLOリモートsyslogが有効な場合のみ使用できます。

サブトピック

リモートsyslogオプション

リモートsyslogオプション

- リモートSyslogポート - syslogサーバーがリスンしているポート番号。このボックスに入力できるポート番号は1つだけです。複数のリモートsyslogサーバーを入力する場合、それらは同じポートを使用する必要があります。デフォルト値は、514です。
- リモートSyslogサーバー - syslogサービスを実行しているサーバーのIPアドレス、FQDN、IPv6名、または省略名。複数のサーバーを入力するには、サーバーのIPアドレス、FQDN、IPv6名、または短い名前をセミコロンで区切ります。リモートSyslogサーバーボックスには最大511文字まで入力できます。

  Linuxシステムでは、システムイベントは「syslog」というツールによって記録されます。iLOシステムの中央ログシステムとして機能するリモートシステムにSyslogサーバーを設定することができます。iLOリモートsyslog機能を有効にした場合、そのログをsyslogサーバーに送信できます。

iLOリモートsyslogの無効化

前提条件

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

手順

1. ナビゲーションツリーでマネジメントをクリックしてから、リモートSyslogタブをクリックします。
2. iLOリモートSyslogを有効オプションを無効に設定します。
3. 変更を保存するには、適用をクリックします。

リモートSyslogアラートレベル（Linux）

iLOの一部のステータス値は、標準のLinux syslogステータス値とは異なります。次の表に、同等の値を示します。

iLOステータス	Linux syslogステータス
クリティカル	クリティカル
注意	警告
修正済み	通知
情報	情報

HPE Compute Ops Management

Compute Ops Managementを使用すると、iLOはGen10以降のサーバーのクラウドベースの管理サービスに接続できます。

Compute Ops Managementは、インフラストラクチャとコンピューティングのワークフローを抽象化およびオーケストレーションする独自のクラウドネイティブアーキテクチャーに基づいて構築されており、複雑なコンピューティング操作をエッジからクラウドにわたる簡素化されたエクスペリエンスに変換して俊敏性を向上させます。HPE GreenLakeを介して、Compute Ops Managementでサーバーを管理できます。詳しくは、https://hpe.com/solutions/compute-ops-managementを参照してください。

Compute Ops Managementへの接続

前提条件

- iLO設定の構成権限。
- 構成されたDNSサーバー。
- Webプロキシを構成する。
- サーバーにシリアル番号、Universally Unique Identifier (UUID) 、および製品IDがあることを確認する

このタスクについて

手順

1. ナビゲーションツリーでマネジメントをクリックしてから、Compute Ops Managementタブをクリックします。

   Compute Ops Managementページが表示されます。

   注記:
   Hewlett-Packard Enterpriseでは、Compute Ops Managementへの接続中にWebプロキシを構成することをお勧めします。Webプロキシ設定は、アクセス設定ページで構成または編集できます。

2. をクリックして、Compute Ops Management設定を編集します。

   COM設定ページが表示されます。

3. トグルボタンを使用してCOMによって管理を有効にします。

   システムがHPE OneViewによって管理されている場合、 COMによって管理を有効にすると、HPE OneViewから切断されます。

4. （オプション）アクティベーションキーを入力します。アクティベーションキーは、HPE GreenLakeのアカウントIDです。**HPE GreenLake**にログインして管理をクリックし、アカウントIDをダブルクリックして選択してから、それをコピーします。アクティベーションキーは英数字である必要があり、最大長は32文字です。

   アクティベーションキーは、 Compute Ops Managementへの接続を開始するために必須ではありません。 Compute Ops Managementが アクティベーションキーなしで接続要求を受け入れる場合、接続ステータスは 接続済みになります。

Compute Ops Managementが アクティベーションキーを必要とする場合、接続ステータスは ActivationKeyRequiredになります。このステータスを受け取ったら、ユーザーは有効な アクティベーションキーで再試行する必要があります。

5. 保存をクリックして、Compute Ops Managementへの接続を開始します。

   接続ラベルは iLOと Compute Ops Management間の接続状態を示します。

   iLOが Compute Ops Managementに接続された後は、接続ステータス（ 成功または 失敗）に関係なく、 COMによって管理が 有効に設定されます。

   リセット中、 Compute Ops Managementへの接続はiLOによって自動的にトリガーされます。ユーザーが Compute Ops Managementを手動で無効にした場合にのみ、 COMによって管理が 無効に設定されます。

Compute Ops Managementの接続状態

このセクションでは、Compute Ops Managementの接続ステータスを示します。

表示される可能性があるステータスの値は、以下のとおりです。

- 無効 - Compute Ops Managementが有効になっていません。
- 進行中 - Compute Ops Managementへの接続が進行中です。
- 接続済み - iLOはCompute Ops Managementに正常に接続されています。
- アクティベーションキーが必要です - iLOはアクティベーションキーなしでCompute Ops Managementに接続しようとしました。要求は拒否され、アクティベーションキーを使用して再試行されます。
- 失敗 - iLOはCompute Ops Managementへの接続に失敗しました。詳しくは、iLO AHSログを参照してください。
- 未接続 - iLOは、ネットワークの中断によりCompute Ops Managementへの接続を失いました。接続を再確立するために、1時間ごとに自動再接続が試行されます。再接続をすぐに試みるには、接続をクリックします。

注記:

- iLOのリセットが発生すると、Compute Ops Managementのステータスが接続済みから無効に変わります。これは予期される動作です。iLOがリセットされてからCompute Ops Managementのステータスが表示されるまで、iLOでは約120秒かかります。
- DNS構成を変更または無効にすると、Webプロキシ構成の値が接続とCompute Ops Managementの接続ステータスに影響します。

ライフサイクル管理機能の使用

サブトピック

Always On Intelligent Provisioning

One-buttonセキュア消去

iLOのバックアップとリストア

Always On Intelligent Provisioning

Always On Intelligent Provisioningは、OSの展開の実行やハードウェア構成の詳細の確認に使用できるWebインターフェイスです。

iLOからのIntelligent Provisioningの起動

前提条件

- リモートコンソール権限
- ホストBIOS構成権限
- Intelligent Provisioningがサーバーにインストールされている。

手順

1. ナビゲーションツリーのライフサイクル管理をクリックします。

   Intelligent Provisioningページが表示されます。

   インストールされているIntelligent Provisioningのバージョンが Intelligent Provisioningページに表示されます。

2. Always Onをクリックして、Intelligent Provisioningを起動します。

   Intelligent Provisioning Webインターフェイスが新しいブラウザーウィンドウで起動します。

   Intelligent Provisioningの使用方法については、Webサイトにある Intelligent Provisioningのドキュメントを参照してください（https://www.hpe.com/info/intelligentprovisioning/docs）。

One-buttonセキュア消去

サーバーを運用廃止するか、または別の用途で準備する場合、One-buttonセキュア消去機能を使用できます。

One-buttonセキュア消去は、NIST Special Publication 800-88 Revision 1のメディアサニタイズのガイドラインに準拠しています。付録では、メディアの最小サニタイズレベルを提示しています。仕様について詳しくは、**メディアサニタイズのガイドライン**のセクション2.5を参照してください。

One-buttonセキュア消去は、ユーザーデータの**パージ**に対するNIST SP 800-88 Revision 1のサニタイズに関する勧告を実装しており、サーバーおよびサポートされたコンポーネントをデフォルトの状態に戻します。この機能は、サーバーの揮発性に関する報告のドキュメントでユーザーが行う多くのタスクを自動化します。

One-buttonセキュア消去アクセス方式

次の製品からOne-buttonセキュア消去プロセスを開始できます。

- iLO6
- Intelligent Provisioning
- iLO RESTful API

iLOからOne-buttonセキュア消去プロセスを開始するための前提条件

手順

1. 自分のiLOユーザーアカウントにすべてのiLOユーザーアカウント権限が割り当てられていることを確認します。
2. この機能をサポートするiLOライセンスをインストールします。

   使用可能なライセンスタイプ、およびサポートされている機能については、Webサイト（https://www.hpe.com/support/ilo-docs）にあるライセンス文書を参照してください。
3. 次の機能が有効になっている場合は、無効にします。
   - サーバー構成ロック

     手順については、UEFIシステムユーティリティユーザーガイドおよびHPE Synergyを参照してください。
   - Smartアレイ暗号化

手順については、**HPE SmartアレイSR Secure Encryptionインストール/ユーザーガイド**の「暗号化構成のクリア」セクションを参照してください。

- Intel VROC暗号化
- 手順については、インテルVirtual RAID on CPUユーザーガイドのセキュリティと暗号化の構成をクリーンアップするセクションを参照してください。

4. HPE Synergyシステムでは、システムに割り当てられているHPE OneViewまたはVirtual Connectプロファイルを削除します。
5. システムメンテナンススイッチのiLOセキュリティ設定の位置がOFFであることを確認します。
6. 消去するストレージドライブで、ネイティブのサニタイズ方式をサポートしています。

   例えば、SATAおよびSASドライブには`SANITIZE`コマンド、NVM Expressドライブには`FORMAT`などです。NIST文書では、上記のデバイスタイプでデータをパージするには上記のコマンドを勧めています。これらのコマンドを使用するほうが、ソフトウェアを使用してストレージドライブ上のデータを上書きするよりも安全です。
7. HPE拡張スキーマでLDAPディレクトリ認証を使用している場合、One-buttonセキュア消去プロセスを開始するために、iLOにログインする別の方法があります。

   サポートされている方法には、ローカルアカウント、Kerberos認証、CACスマートカード、およびスキーマフリーディレクトリアカウントが含まれます。

   HPE拡張スキーマでは、One-buttonセキュア消去プロセスを開始するために必要なユーザー権限をサポートしていません。

iLOからのOne-buttonセキュア消去プロセスの開始

前提条件

ご使用の環境が**iLOからOne-buttonセキュア消去プロセスを開始するための前提条件**を満たしている。

手順

1. 消去しないストレージデバイスを切断またはデタッチします。

   Hewlett Packard Enterpriseでは、データ損失の可能性を低減するため、消去しないドライブを切断またはデタッチすることをお勧めします。この手順には、着脱可能なドライブや、外付けストレージ、共有ストレージが含まれます。

   接続されたストレージデバイスがネイティブのサニタイズ方式をサポートしていない場合、そのストレージデバイスはOne-buttonセキュア消去プロセス中に消去されません。インテグレーテッドマネジメントログ（IML）エントリーにより、デバイスの消去の障害が報告されます。
2. （オプション）SNMP、アラートメール、またはiLO RESTful APIアラートを構成します。

   Hewlett Packard Enterpriseでは、この手順を完了することをお勧めします。

   各コンポーネントが消去されるときにエラーが発生した場合は、各エラーについて、IMLエントリーが記録されます。アラートを構成している場合、通知を受け取ります。IMLは、One-buttonセキュア消去プロセス中に消去されます。IMLが消去されると、セキュア消去レポートテーブルに高レベルのステータス情報が表示されます。

   セキュア消去レポートには、内蔵NANDフラッシュとNVRAMのステータスのみが含まれます。
3. ナビゲーションツリーでライフサイクル管理をクリックし、廃棄タブをクリックします。
4. システムを消去をクリックします。

   iLOが要求を確認するように求めます。

△ **注意:**

この機能は、システムを廃棄する場合、または別の目的で使用する場合にのみ使用してください。このプロセスは、サーバーおよびサポートされるコンポーネントを工場出荷時の状態にリセットします。ストレージ容量によっては、サーバーとコンポーネントのセキュア消去が完了するまでに1日以上かかる場合があります。このプロセスはいったん開始すると、元に戻すことはできません。プロセスが完了するまで、構成の変更やシステムの電源オフに関係するiLOまたはシステムとの対話は避けてください。

5. セキュア消去の意味を理解し、このシステムを廃棄する準備ができましたチェックボックスをオンにして、はい、システムを永久に消去しますをクリックします。

   サーバーが再起動し、One-buttonセキュア消去プロセスが開始します。

   One-buttonセキュア消去の進捗は、すべてのiLO Webインターフェイスページのバナー領域に表示されます。表示される情報には、完了率と推定の残り時間が含まれます。個々のハードウェアまたはソフトウェアコンポーネントの詳細は、セキュア消去ステータステーブルに表示されます。

   One-buttonセキュア消去プロセス中に、構成を変更しないでください。このプロセス中は、iLOによってファームウェアアップデートが妨げられ、iLOがリセットされます。

   One-buttonセキュア消去が完了するとiLOがリセットされ、ネットワーク上で使用できなくなります。

   HPE Synergyコンピュートモジュールでは、プロセスの完了後にiLOのネットワーク設定が再割り当てされることがあり、システムの電源がオンになる場合があります。

6. （オプション）システムを稼働状態に戻します。

7. （オプション）One-buttonセキュア消去レポートを表示、保存、または削除します。

   Hewlett Packard Enterpriseでは、この手順を完了することをお勧めします。

8. （オプション）デバイスが消去プロセスに失敗した場合、またはデバイスがネイティブのサニタイズ方式をサポートしていない場合は、次のいずれかを実行します。

   - これらのデバイスを分離し、他の方式を使用してデータを削除します。
   - 組織のセキュリティポリシーに従ってデバイスを安全に廃棄します。

   Hewlett Packard Enterpriseでは、この手順を完了することをお勧めします。

One-buttonセキュア消去ステータス値

One-buttonセキュア消去プロセスを開始すると、全体の進捗がiLOバナーに表示されます。個々のコンポーネントのステータスは、 セキュア消去ステータステーブルに表示されます。

- アイドル - プロセスは開始されていません。
- 開始 - プロセスは開始されました。
- 進行中 - 消去が進行中です。
- 成功 - プロセスは正常に完了しました。
- エラー - プロセスが完了しましたが、エラーが発生しています。
- 障害 - プロセスは失敗しました。

注記:

セキュア消去ステータステーブル内のiLO設定には、内蔵NANDフラッシュとNVRAMの結果が含まれています。これらのコンポーネントのいずれかで消去の障害が発生すると、iLO設定の全体的な障害になります。

セキュア消去ステータステーブル内のBIOS設定には、UEFI構成ストアとRTC（システム日付時刻）の結果が含まれます。これらのコンポーネントのいずれかで消去の障害が発生すると、BIOS設定の全体的な障害になります。

One-buttonセキュア消去後にシステムを動作状態に戻す

このタスクについて

One-buttonセキュア消去プロセスでシステムが消去された後に、次の手順を使用して操作状態に戻します。

手順

1. iLOネットワーク設定を構成します。
2. Intelligent Provisioningリカバリイメージを使用してIntelligent Provisioningをインストールします。

   詳しくは、Intelligent Provisioningのユーザーガイドを参照してください。
3. オペレーティングシステムをインストールします。
4. オプション：iLOライセンスをインストールします。
5. BIOS設定および環境に適用されるiLO設定を構成します。
6. （オプション）システムリカバリセットを作成します。

One-buttonセキュア消去レポートの表示

前提条件

- サーバーでOne-buttonセキュア消去プロセスが完了している。
- One-buttonセキュア消去プロセスの完了後、iLOがIPアドレスで構成されている。

手順

1. ナビゲーションツリーでライフサイクル管理をクリックし、廃棄タブをクリックします。

   サーバーでOne-buttonセキュア消去プロセスが完了したら、 最新の消去レポートの参照ボタンが使用できます。
2. 最新の消去レポートの参照をクリックします。

   セキュア消去レポートが表示されます。
3. （オプション）テーブルの列でソートするには、列見出しをクリックします。

   ソート順を昇順または降順に変更するには、列見出しをもう一度クリックするか、列見出しの横にある矢印アイコンをクリックします。
4. （オプション） One-buttonセキュア消去レポートを保存します。

   Hewlett Packard Enterpriseでは、今後の参照用に消去レポートのコピーを保存することをお勧めします。
5. （オプション） One-buttonセキュア消去レポートを削除します。

   Hewlett Packard Enterpriseでは、サーバーを廃棄するか、または別の目的で使用する前に、消去レポートを削除することをお勧めします。

One-buttonセキュア消去レポートの詳細

- サーバーシリアル番号 - サーバーのシリアル番号。

- 次によって開始 – One-buttonセキュア消去プロセスを開始したユーザー。

次の情報がデバイスごとにリストされます。

- デバイスタイプ – 消去されたデバイスタイプ。

  影響を受けるデバイスタイプについては、One-buttonセキュア消去の完了後のシステムへの影響を参照してください。

  セキュア消去レポートには、内蔵NANDフラッシュとNVRAMのステータスのみが含まれます。
- 位置 – サーバー内のデバイスの位置。
- シリアル番号 – デバイスのシリアル番号。
- ステータス – デバイスのOne-buttonセキュア消去ステータス。
- 消去タイプ – 消去操作のタイプ。実行された操作について詳しくは、One-buttonセキュア消去のFAQを参照してください。
- 開始時刻 – 特定のデバイスのOne-buttonセキュア消去の開始時刻。
- 終了時間 – 特定のデバイスのOne-buttonセキュア消去の終了時間。

CSVファイルへのOne-buttonセキュア消去レポートの保存

前提条件

- サーバーでOne-buttonセキュア消去プロセスが完了している。
- One-buttonセキュア消去プロセスの完了後、iLOがIPアドレスで構成されている。

このタスクについて

One-buttonセキュア消去機能を使用する場合、Hewlett Packard Enterpriseでは、今後の参照用に消去レポートのコピーを保存することをお勧めします。

手順

1. ナビゲーションツリーでライフサイクル管理をクリックし、廃棄タブをクリックします。
2. 終了ボックスにある  をクリックします。

   CSVアウトプットウィンドウが表示されます。
3. 保存をクリックし、ブラウザーのプロンプトに従ってファイルを保存するか、ファイルを開きます。

One-buttonセキュア消去レポートの削除

前提条件

- iLOの設定を構成する権限
- サーバーでOne-buttonセキュア消去プロセスが完了している。
- One-buttonセキュア消去プロセスの完了後、iLOがIPアドレスで構成されている。
- 後で参照するためにOne-buttonセキュア消去レポートのコピーが必要な場合に、レポートを保存している。

このタスクについて

サーバーを廃棄または再利用する場合、iLO Webインターフェイスで One-buttonセキュア消去レポートを使用可能なままにしたくない場合があります。

Hewlett Packard Enterpriseでは、サーバーを廃棄するか、または別の目的で使用する前に、消去レポートを削除することをお勧めします。

手順

1. ナビゲーションツリーでライフサイクル管理をクリックし、廃棄タブをクリックします。

   サーバーでOne-buttonセキュア消去プロセスが完了したら、 最新の消去レポートの参照ボタンが使用できます。

2. 最新の消去レポートの参照をクリックします。

   セキュア消去レポートが表示されます。

3. 🗑 をクリックします。

   iLOによって、レポートファイルがセキュア消去され、すぐにリセットされます。

   この時点までに作成されたイベントログ、IML、セキュリティログ、および構成設定が、工場出荷時のデフォルト設定にリセットされます。iLOは、起動時に自動リストア操作を試みる場合があります。詳しくは、iLOのバックアップとリストアを参照してください。

One-buttonセキュア消去の完了後のシステムへの影響

One-buttonセキュア消去機能は、システムおよびサポートされたコンポーネントを工場出荷時の状態に戻します。システムを使用するには、再度サーバーをプロビジョニングします。

- 以下のBIOSおよびiLO6設定は消去されるか、工場出荷時デフォルト設定にリセットされます。
  - 工場出荷時に設定されたサーバーID（iLO IDevID）、ユーザー定義のサーバーID （iLO LDevID）、工場出荷時に設定されたTCG準拠のシステムID（System IDevID）は消去されます。
  - プラットフォーム証明書、システムIAK証明書、その他すべての登録済み証明書 （工場出荷時にプリインストールされているUEFIセキュアブート証明書を除く）は消去されます。
  - iLOネットワークやその他の設定は消去され、再構成が必要となります。
  - インストールされたiLOライセンスは削除され、ライセンスのステータスはiLO Standardに戻ります。

    工場でiLO Advancedライセンスが#0D1オプションでプリインストールされている場合、One-buttonセキュア消去プロセスが終了するとライセンスは再インストールされます。このライセンスオプションについて詳しくは、HPE iLOライセンスガイドを参照してください。
  - システムリカバリセットは削除され、再作成が必要となります。
  - iLOのユーザーアカウントが削除されます。プロセスが完了したら、デフォルトの工場出荷時の管理者アカウントとパスワードを使用してログインします。
  - Active Health System、インテグレーテッドマネジメントログ、セキュリティログ、およびiLOイベントログは消去されます。
  - BIOSおよびSmartStorage Redfish APIデータの削除され、次回のブート時に再作成されます。
  - セキュアブートは無効になり、工場出荷時にインストールされている証明書を除き、登録された証明書は削除されます。
  - ブートオプションとユーザーが定義したBIOSのデフォルトは削除されます。
  - TPMまたはBIOSに格納されたパスワード、パスフレーズ、および暗号化キーは削除されます。
  - 日付、時刻、DST、およびタイムゾーンはリセットされます。
  - システムは、BIOSの最新リビジョンがフラッシュされた状態で起動されます。
- Intelligent Provisioningは起動せず、再インストールする必要があります。

工場出荷時の状態に戻されるハードウェアコンポーネント

次のコンポーネントは、One-buttonセキュア消去プロセス中に、工場出荷時の状態に戻されます。

- UEFI構成ストア
- RTC（システムの日付と時刻）
- Trusted Platform Module
- NVRAM

- BIOS設定
- iLO構成設定
- iLOイベントログ
- インテグレーテッドマネジメントログ
- セキュリティログ

- HPE SRコントローラー、MRコントローラー、NSコントローラー、および接続されたストレージドライブ。

  コントローラーについて詳しくは、ILO 6ユーザーガイドの「サポートされるストレージ製品」セクションを参照してください。
- Intel VROC
- ドライブデータ（ネイティブのサニタイズ方式をサポートするドライブの場合）。
  - SATA、SASドライブ（SSDおよびHDD）
  - NVM Express
- 内蔵フラッシュ
  - iLO RESTful APIデータ
  - Active Health System
  - ファームウェアレポジトリ

工場出荷時の状態に戻されないハードウェアコンポーネント

次のコンポーネントはOne-buttonセキュア消去プロセスの影響を受けません。

- USBドライバー
- SDカード
- iLO仮想メディア
- PCIコントローラー上の構成
- SAS HBAおよび接続されたドライブ
- ネイティブのサニタイズ方式をサポートしていないSATA、SAS、およびNVM Expressドライブ。
- FCoE、iSCSIストレージ
- GPGPU
- その他のFPGA、アクセラレータ、キーまたはストレージを持つオフロードエンジン

One-buttonセキュア消去のFAQ

One-buttonセキュア消去はUSBデバイスおよび内部SDカードをパージしますか。

いいえ。One-buttonセキュア消去はUSBデバイスおよび内部SDカードをパージしません。

HDDがパージ機能をサポートしていない場合、 One-buttonセキュア消去はパージを試みますか。

いいえ。One-buttonセキュア消去はパージ機能をサポートしていないドライブをスキップします。

One-buttonセキュア消去はSmartアレイコントローラーをサポートしていますか。

One-buttonセキュア消去ではSRコントローラーとMRコントローラーの両方がサポートされています。

Smartアレイはパージをサポートしていないドライブを消去しますか。

Smartアレイは、パージ操作をサポートしていないドライブをワイプ（あるパターンで上書きする）できます。One-buttonセキュア消去では、Smartアレイでこのセキュリティ保護されていないワイプを実行する必要はありません。Intelligent Provisioningの「システムの消去およびリセット」機能を使用して、このようなドライブのデータ

をワイプします。

One-buttonセキュア消去はバッテリバックアップ式キャッシュを消去しますか。

詳しくは、次の表を参照してください。

One-buttonセキュア消去は消去コマンドをどのように処理しますか。

One-buttonセキュア消去がデータをパージまたは上書きする方法に関する情報については、次の表を参照してください。

One-buttonセキュア消去を起動するために必要な権限は何ですか。

One-buttonセキュア消去を起動するには、すべてのiLO権限が必要です。

One-buttonセキュア消去はシリアル番号とプロダクトIDを削除しますか。

いいえ、これらの項目はOne-buttonセキュア消去によって消去されません。

この処理はどの程度かかりますか。

ハードウェアによって異なります。HDDのサニタイズはSSDよりも時間がかかります。

One-buttonセキュア消去はサポートされたドライブにどのように作用しますか

デバイス	必要な操作	結果
NVRAM	3パス書き込み：0x5a、0xa5、0xff	すべてのバッテリバックアップ式iLO SRAMメモリが上書きされます。
内蔵フラッシュ（NAND）	拡張CSDレジスターのSECURE_REMOVAL_TYPEが物理メモリ消去に設定されているeMMC 5.1（JEDEC 84-B51）セキュア消去コマンド（デバイスでサポートされている場合）。	物理メモリ内のデータが消去されます。
インテルOptane DC PMM	完全消去 + DIMMを上書き	暗号化キーが削除され、すべての物理メモリブロック内のデータ（ユーザーがアクセス可能なデータとスペアブロック内の両方のデータ）がゼロで上書きされます。すべての構成とメタデータを含むPCD領域も上書きされます。
UEFI構成ストア	3パス：チップ消去（0xff）、0x00、チップ消去（0xff）	すべての物理セクターが上書きされます。
RTC	時刻を01-01-2001 00:00:00にリセット	日付、時刻、タイムゾーン、およびDSTがデフォルト設定にリセットされます。
TPM	TPMクリア + NVインデックスをクリア + プラットフォーム対象キーを削除	すべての不揮発性情報を含む、TPMのすべてのデータがクリアされます。

デバイス	必要な操作	結果
HPE SmartアレイSRコントローラー	論理ドライブを削除 + 構成のメタデータをクリア + 工場出荷時設定へのリセット + 物理ドライブのサニタイズ **注記**：One-buttonセキュア消去を開始する前に、Smart Storage Administratorを介して、セキュリティリセット機能を手動で実行する必要があります（Smartアレイセキュア暗号化が有効化されていた場合）。	• セキュリティリセット機能は、リモートキー管理のためにキーマネージャーに保存されているドライブキーを削除します。コントローラーおよびドライブのすべてのシークレット、キー、およびパスワードがクリアされます。この操作は、キーマネージャー上のコントローラーキーを削除しません。 • すべてのアレイ構成、論理ドライブ、およびメタデータが削除されます。すべてのコントローラー設定は工場出荷時の設定にリセットされます。 • フラッシュバックアップはクリアされ、DRAMのライトバックキャッシュ内のデータは電源が取り外されたときに失われます。 接続されたすべてのドライブをサニタイズする必要があります。ドライブ上で必要な操作については、以下を参照してください。
HPE SmartアレイMRコントローラー	論理ドライブを削除 + 構成のメタデータをクリア + 工場出荷時設定へのリセット + 物理ドライブのサニタイズ	• すべてのアレイ構成、論理ドライブ、およびメタデータが削除されます。すべてのコントローラー設定は工場出荷時の設定にリセットされます。暗号化キーがクリアされます。 • フラッシュバックアップはクリアされ、DRAMのライトバックキャッシュ内のデータは電源が取り外されたときに失われます。 接続されたすべてのドライブをサニタイズする必要があります。ドライブ上で必要な操作については、以下を参照してください。
HPE NSブートコントローラー	論理ドライブを削除 + 構成のメタデータをクリア + 工場出荷時設定へのリセット + 物理ドライブのサニタイズ	• すべてのアレイ構成、論理ドライブ、およびメタデータが削除されます。すべてのコントローラー設定は工場出荷時の設定にリセットされます。 接続されたすべてのドライブをサニタイズする必要があります。ドライブ上で必要な操作については、以下を参照してください。
SATA HDD [1]	ATA SANITIZE with CRYPTO SCRAMBLE EXT（サポートされている場合）。	CRYPTO SCRAMBLE EXTコマンドは、ユーザーデータに使用される内部暗号化キーを変更するため、ユーザーデータを元に戻すことはできません。

デバイス	必要な操作	結果
	シングルパスのATA SANITIZE with OVERWRITE EXTオプション	ユーザーがアクセスできない物理セクターを含む、すべての物理セクターがゼロで上書きされます。キャッシュ内のすべての旧データもアクセスできなくなります。
SATA SSD [1]	ATA SANITIZE with CRYPTO SCRAMBLE EXT（サポートされている場合）。	CRYPTO SCRAMBLE EXTコマンドは、ユーザーデータに使用される内部暗号化キーを変更するため、ユーザーデータを元に戻すことはできません。
	シングルパスのATA SANITIZE with BLOCK ERASEオプション	ユーザーがアクセスできない物理メモリブロックを含む、すべての物理メモリブロック内の旧データは元に戻すことができなくなります。キャッシュ内のすべての旧データもアクセスできなくなります。
SAS HDD [2]	シングルパスのSCSI SANITIZE with OVERWRITE EXTオプション	ユーザーがアクセスできない物理セクターを含む、すべての物理セクターが上書きされます。キャッシュ内のすべてのデータもサニタイズされます。
SAS SSD [2]	シングルパスのSCSI SANITIZE with BLOCK ERASEオプション	ユーザーがアクセスできない物理メモリブロックを含む、すべての物理メモリブロックがベンダー固有値に設定されます。キャッシュ内のすべてのデータもサニタイズされます。
NVM Express	NVM Express FORMAT with Secure Erase Setting (SES) = 2（サポートされている場合）。	これは、暗号化キーを削除することで行われる暗号による消去です。
	シングルパスのNVM Express FORMAT with SES = 1	すべてのネームスペースに関連付けられているすべてのデータとメタデータは破棄されます。NVMサブシステムに存在するユーザーのすべての内容は消去されます。

1 これらのドライブは、 HPE Smartアレイ「SR」コントローラーまたはチップセットSATAコントローラーに接続される場合があります。
2 HPE Smartアレイ「SR」コントローラーにのみに接続されたSASドライブがサポートされます。

消去プロセスが失敗するサポート済みデバイス、およびサポートされていないデバイスの消去は安全ではありません。これらのデバイスに機密データが含まれている可能性があります。消去されないデバイスを分離し、他の方法を使用してデータを削除するか、所属する組織のセキュリティポリシーに従ってデバイスを安全に破棄します。

iLOのバックアップとリストア

自動でのバックアップとリストア

iLOの初期化プロセスが終了すると、バッテリ駆動のSRAMメモリデバイスに保存されている構成情報が不揮発性フラッシュメモリ（NAND）にバックアップされます。

SRAMが消去された、またはデータ破壊が検出された場合、 iLOはバックアップファイルから構成情報をリストアしようとします。自動リストア操作はIMLに記録されます。

システムメンテナンススイッチを使用してiLOセキュリティを無効にすると、SRAMデータは自動的にリストアされません。

自動でのバックアップとリストアのプロセスによって作成されたバックアップファイルには、ユーザーはアクセスできません。手動リストア操作を実行するために使用することはできません。

手動でのバックアップとリストア

iLOでは、バッテリ駆動のSRAMメモリデバイスに保存された構成情報の手動リストアがサポートされています。この機能は、バックアップされたシステムと同じハードウェア構成を持つシステムで使用するためのものです。構成を複製して別のiLOシステムに適用するものではありません。

Hewlett Packard Enterpriseでは、リストア操作を実行する理由が生じることは想定されていません。ただし、構成のバックアップを取っておくことで、通常の動作環境にすばやく戻ることができる場合があります。

あらゆるコンピューターシステムと同様に、データをバックアップして障害の影響を最小限に抑えることをお勧めします。Hewlett Packard Enterpriseは、iLOファームウェアをアップデートするたびにバックアップを実行することをお勧めします。

バックアップとリストアのためのiLOファームウェア要件

- iLO 6ファームウェアでは、iLOファームウェアのバージョンが同じシステムや異なるシステムでバックアップおよびリストアのタスクが実行される、バックアップおよびリストア操作がサポートされています。

バックアップとリストアの操作中にリストアされる情報

iLO構成には、電源、ネットワーク、セキュリティ、ライセンスキー、ユーザーデータベースなど、多くのカテゴリが含まれます。ほとんどの構成情報は、バッテリ駆動のSRAMメモリデバイスに保存されており、バックアップとリストアが可能です。

注記:
環境変数をリストアしたときは、リストアした設定を有効にするためにサーバーのリセットが必要です。
たとえば、パフォーマンス設定はリストアされてもサーバーリセットが完了するまで有効になりません。

バックアップとリストアの操作中にリストアされない情報

一部の情報は、バックアップとリストアの操作中にリストアするのに適していません。リストアできない情報はiLO構成には含まれません。その情報はiLOまたはサーバーのシステム状態に関連します。

以下の情報は、バックアップまたはリストアされません。

セキュリティ状態

リストア操作によってiLOのセキュリティ状態を変更することを許可すると、セキュリティの原則が破られ、セキュリティの適用が無効になります。

インテグレーテッドマネジメントログ

バックアップから、リストアが必要になったイベントまでに発生したイベントの情報を保持するため、この情報はリストアされません。

iLOイベントログ

バックアップから、リストアが必要になったイベントまでに発生したイベントの情報を保持するため、この情報はリストアされません。

セキュリティログ

バックアップから、リストアが必要になったイベントまでに発生したセキュリティイベントの情報を保持するため、この情報はリストアされません。

Active Health Systemデータ

バックアップおよびリストアプロセス中に記録された情報を保持するため、この情報はリストアされません。

サーバーの状態情報

- サーバーの電源状態（オン/オフ）
- サーバーのUID LEDの状態
- iLOおよびサーバーのクロック設定

iLO構成を手動でリストアする理由

次のような状況ではiLO構成のリストアが必要になる場合があります。

バッテリの障害または取り外し

さまざまな構成パラメーターがバッテリ駆動のSRAMに保存されています。まれですが、バッテリ障害が発生する場合があります。状況によっては、バッテリの取り外しと交換が必要になる場合があります。構成情報の消失を避けるために、バッテリの交換後にバックアップファイルからiLO構成をリストアします。

デフォルト設定へのリセット

場合によっては、iLOを工場出荷時のデフォルト設定にリセットし、iLO以外の設定を消去することが必要になることがあります。iLOを工場出荷時の設定にリセットすると、iLOの構成は消去されます。iLO構成をすばやく復旧するには、工場出荷時設定へのリセットが完了した後、バックアップファイルから構成をリストアします。

構成の偶発的または不適切な変更

場合によって、iLO構成が不適切に変更され、重要な設定が消失することがあります。iLOを工場出荷時のデフォルト設定に設定したり、ユーザーアカウントを削除したりした場合にこのような状況が発生することがあります。元の構成を回復するには、バックアップファイルから構成をリストアします。

システムボードの交換

ハードウェアの問題に対処するためにシステムボードの交換が必要な場合、この機能を使用してiLO構成を元のシステムボードから新しいシステムボードに転送できます。

ライセンスキーの喪失

ライセンスキーが誤って置き換えられた、またはiLOを工場出荷時のデフォルトの設定にリセットした場合に、インストールするキーがわからないときは、ライセンスキーと他の構成設定をバックアップファイルからリストアできます。

iLO構成のバックアップ

前提条件

- iLOの設定を構成する権限
- iLOは、本番環境または高度なセキュリティのセキュリティ状態を使用するように構成されています。iLOが高いセキュリティ状態を使用するように構成されている場合、構成のバックアップとリストアはサポートされていません。

手順

1. ナビゲーションツリーでライフサイクル管理をクリックし、バックアップとリストアをクリックします。
2. バックアップをクリックします。
3. （オプション）バックアップファイルをパスワード保護するには、バックアップファイルパスワードボックスにパスワードを入力します。

   パスワードは最大32文字です。
4. ダウンロードをクリックします。

   ファイルがダウンロードされ、この動作がイベントログに記録されます。

   ファイル名は、次の形式を使用します。`<サーバーシリアル番号>_<YYYYMMDD>_<HHMM>.bak`.

iLO構成のリストア

前提条件

- iLOの設定を構成する権限
- ユーザーアカウント管理権限
- バックアップファイルが存在する。
- 以前にiLOを工場出荷時のデフォルト設定にリセットした場合は、デフォルトのiLOアカウント認証情報を使用できる。
- 使用するiLOセキュリティ状態が構成されている。

  本番環境または高セキュリティよりも高いセキュリティ状態を構成すると、iLOは工場出荷時のデフォルト設定にリセットされます。これらのセキュリティ状態を構成せずにリストアを実行した場合、リストアされた情報はセキュリティ状態のアップデート時に削除されます。

手順

1. ナビゲーションツリーでライフサイクル管理をクリックし、バックアップとリストアをクリックします。
2. リストアをクリックします。
3. 使用しているブラウザーに応じて参照またはファイルを選択をクリックし、バックアップファイルに移動します。
4. バックアップファイルがパスワードで保護されている場合、パスワードを入力します。
5. アップロードおよびリストアをクリックします。

   iLOが要求を確認するように求めます。
6. リストアをクリックします。

   iLOが再起動され、ブラウザー接続が閉じます。接続が再確立されるまでに、数分かかることがあります。

詳しくは

iLOのバックアップとリストア
iLOのデフォルトのDNS名とユーザーアカウント
iLO暗号化設定

システムボード交換後のiLO構成のリストア

前提条件

- iLOの設定を構成する権限
- ユーザーアカウント管理権限
- バックアップファイルが存在する。
- 以前にiLOを工場出荷時のデフォルト設定にリセットした場合は、デフォルトのiLOアカウント認証情報を使用できる。
- 使用するiLOセキュリティ状態が構成されている。

  本番環境または高セキュリティよりも高いセキュリティ状態を構成すると、iLOは工場出荷時のデフォルト設定にリセットされます。これらのセキュリティ状態を構成せずにリストアを実行した場合、リストアされた情報はセキュリティ状態のアップデート時に削除されます。

このタスクについて

システムボードを交換する場合、交換前のシステムボードから構成をリストアできます。

手順

1. システムボードを交換し、ハードウェアコンポーネントを古いシステムボードから新しいシステムボードに転送します。
2. システムの電源を入れ、すべてのコンポーネントが正常に動作していることを確認します。
3. 新しいシステムボードのデフォルトのユーザー認証情報を使用してiLOにログインします。
4. バックアップファイルから構成をリストアします。

詳しくは

iLOのバックアップとリストア
iLOのデフォルトのDNS名とユーザーアカウント
iLO暗号化設定

iLOと他のソフトウェア製品およびツールとの使用

サブトピック

iLOおよびリモート管理ツール

IPMIサーバー管理

HPE SIMでのiLOの使用

iLOおよびリモート管理ツール

iLOとリモート管理ツールの関連付けは、リモート管理ツールを使用して構成します。手順については、リモート管理ツールのドキュメントを参照してください。

iLOがリモート管理ツールで制御されているとき、iLOのWebインターフェイスには次の拡張機能が含まれます。

- iLOログインページに、以下のようなメッセージが表示されます。

  このシステムは以下によって管理されています：<リモート管理ツール名>。
  iLO内でローカルで変更すると、その変更は、集中管理された設定と同期が取れなくなります。

- <リモート管理ツール名>というページが、iLOナビゲーションツリーに追加されます。

サブトピック

iLOからのリモート管理ツールの起動

リモートマネージャー構成の削除

iLOでのHPE OneViewの使用

ホットフィックスを追加してHPE OneViewカスタムファームウェアバンドルを作成する

iLOからのリモート管理ツールの起動

このタスクについて

iLOがリモート管理ツールで制御されているときは、以下の手順に従ってiLOからリモートマネージャーのユーザーインターフェイスを開きます。

手順

1. ナビゲーションツリーで<リモート管理ツール名>をクリックします。
2. 起動をクリックします。

   リモート管理ツールが、独立したブラウザーウィンドウで起動します。

詳しくは

ログインページからのリモート管理ツールの起動

リモートマネージャー構成の削除

このタスクについて

ネットワークでリモート管理ツールの使用を停止する場合は、ツールとiLO間の関連付けを削除できます。

この機能は、Synergyコンピュートモジュールではサポートされません。

重要:
Hewlett Packard Enterpriseでは、iLOでリモートマネージャーの構成を削除する前に、リモート管理ツールからサーバーを削除することをお勧めします。ネットワーク上で使用中のツールのうち、現在のiLOシステムを含んでいるサーバーを管理しているツールのリモートマネージャー構成を削除しないでください。

手順

1. ナビゲーションツリーで<リモート管理ツール名>をクリックします。
2. このiLOからリモートマネージャー構成を削除しますセクションで、削除ボタンをクリックします。

   管理対象サーバーをリモート管理ツールで管理しなくなった場合のみ先へ進むようiLOが警告します。
3. OKをクリックします。

   <リモート管理ツール名>ページが、iLOのナビゲーションツリーから削除されます。

iLOでのHPE OneViewの使用

HPE OneViewは、iLO管理プロセッサーとやり取りして、サポート対象のサーバーの構成、監視、および管理を行います。また、iLOのリモートコンソールへのシームレスなアクセスを設定します。これにより、HPE OneViewユーザーインターフェイスからiLOリモートコンソールを1回のクリックで起動できるようになります。iLO権限は、アプライアンスアカウントに割り当てられた役割によって決まります。

HPE OneViewは、以下のiLO設定を管理します。

- リモート管理ツール
- SNMP v1トラップ宛先
- SNMP v1読み取りコミュニティ
- SSO証明書 - 信頼された証明書がHPE SSOページに追加されます。
- NTP（タイムサーバー）構成
- ユーザーアカウント - 管理者ユーザーアカウントがiLOに追加されます。
- ファームウェアバージョン - サーバーをHPE OneViewに追加するときに、サポートされているバージョンのiLOファームウェアがまだインストールされていない場合、iLOファームウェアが自動的にアップデートされます。詳しくは、HPE OneViewのサポートマトリックスを参照してください。
- iLO RESTful APIイベントの宛先としてアプライアンスが追加されます。
- リモートサポートの登録

重要:
HPE OneViewをiLO6と使用するときに最高のパフォーマンスを得るために、Hewlett Packard Enterpriseは、iLO Webインターフェイスを使用してこれらの設定を削除したり変更しないことをおすすめします。ファームウェアからデバイス構成を変更すると、デバイス構成がHPE OneViewと同期しなくなる可能性があります。

サブトピック

サーバー署名（Synergyコンピュートモジュールのみ）

サーバー署名（Synergyコンピュートモジュールのみ）

HPE OneViewがSynergyコンピュートモジュールを管理する場合、iLOでは、HPE OneViewが固有のネットワーク設定、仮想識

別子、およびアダプター設定を管理できるサーバーの署名を生成します。

iLOが起動するたびに、サーバーの署名が更新され、適合について検証されます。これには、フレームベイとUUID、HPE OneViewドメインのIPアドレス、サーバーのデバイスの署名などの情報が含まれます。

サーバーが別のフレームまたはベイに移動したり、サーバーをベイに挿入したときにそのハードウェア構成が変わったりした場合は、サーバーの署名が変わります。この変更が発生した場合、HPE OneViewによって構成された設定は消去され、iLOイベントログにイベントのログが記録され、iLO RESTful APIイベントが生成されます。このプロセスによって、アドレスの重複が回避され、HPE OneViewはサーバーが固有のプロファイルを確実に持つことができます。

ほとんどの場合、HPE OneViewは自動的にサーバーを再検出して、構成します。この検出と構成が実行されなかった場合は、HPE OneViewソフトウェアを使用してサーバーを含むフレームを更新します。

サーバーの署名データはiLO Webインターフェイスで表示または編集できませんが、RESTクライアントを使用した読み取りができます。詳しくは、https://www.hpe.com/support/restfulinterface/docsを参照してください。

ホットフィックスを追加してHPE OneViewカスタムファームウェアバンドルを作成する

このタスクについて

ホットフィックスを追加して、ベースラインとして使用するための（およびオプションでSUTインストール用の）HPE OneViewカスタムファームウェアバンドルを作成するには、次の手順に従います。

手順

1. 必要なすべてのアップデートパッケージをローカルシステムにダウンロードします。
2. HPE OneViewメインメニューから、アプライアンスを選択し、次にファームウェアバンドルを選択します。

   サービスパックベースラインパッケージがリストされます。

   注記:

   少なくとも1つのサービスパックベースラインがロードされる必要があります。そうでない場合は、先に進む前に互換性のあるService Pack for ProLiant、HPE Synergyカスタムスマート、またはHPE Synergy Service Packをダウンロードし、HPE OneViewにロードします。
3. ファームウェアバンドルの追加をクリックします。ファームウェアバンドルの追加ダイアログボックスが表示されます。
4. ファームウェアバンドルの追加ダイアログで、参照をクリックし、次にステップ1でダウンロードしたアップデートパッケージの1つを選択します。

   一度に選択できるファイルは1つだけです。ファイルタイプは scexe、 exe、 rpm、 zip、または fwpkgである必要があります。

   注記: HPE Smart Update Manager（SUM）バージョン8.7.0以降は、 fwpkgファイルタイプをサポートしています。2020年10月より前にリリースされたベースラインサービスパックがある場合は、 fwpkg以外のサポートされるファイルタイプを選択します。
5. OKをクリックしてファイルをアップロードします。
6. ファイルがアップロードされた後、署名ファイルがないことを示すエラーがHPE OneViewに表示される場合があります。これは、Gen10アップデートパッケージで予想される動作です。

   不足している署名ファイルをアップロードするには：

   a. エラーメッセージを展開し、**署名ファイルのアップロード**リンクをクリックします。または、メニューからアクションを選択し、次に署名ファイルのアップロードを選択します。署名ファイルのアップロードダイアログボックスが表示されます。

   b. 参照をクリックし、パッケージに含まれていた署名ファイルを選択します。署名ファイルの拡張子は.compsigです。

一部のアップデートパッケージには、複数の署名ファイルが必要です。各署名ファイルを個別にアップロードする必要があります。

c. OKをクリックして署名ファイルをアップロードします。

HPE OneViewが署名ファイルを処理して関連付けるまで待機します。プロセスが完了すると、HPE OneViewはアップデートファイルを検証し、 **ホットフィックス**が正常なステータスであることを示します。

7. ファームウェアバンドルのアクションメニューからカスタムファームウェアバンドルの作成を選択します。カスタムファームウェアバンドルの作成ダイアログボックスが表示されます。
8. カスタムファームウェアバンドルの名前を選択します。カスタムファームウェアバンドルには1つ以上のホットフィックスパッケージが含まれている場合があることに注意してください。
9. カスタムファームウェアバンドルを作成するために1つ以上のホットフィックスパッケージを追加するベースファームウェアバンドルを選択します。
10. ホットフィックスの追加をクリックします。ホットフィックスの追加ダイアログボックスが表示されます。
11. このカスタムファームウェアバンドルに必要なすべてのホットフィックスパッケージを選択します。複数のホットフィックスパッケージを選択できます。
12. 必要なホットフィックスパッケージをすべて選択したら、追加をクリックします。

選択したホットフィックスパッケージが カスタムファームウェアバンドルの作成ダイアログボックスに表示されます。

13. OKをクリックします。カスタムファームウェアバンドルの作成ダイアログが閉じ、HPE OneViewがファームウェアバンドルを作成します。新しいファームウェアバンドルには、ベースファームウェアバンドルとこれまでに追加されたホットフィックスパッケージが含まれます。

カスタムファームウェアバンドルが作成されたら、それを新しい論理エンクロージャーファームウェアベースラインとして選択できます。また、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のファームウェアベースラインとしても使用できます。

14. HPE Smart Update Toolsを使用してオンラインでアップデートをインストールするには：
    - サーバープロファイルのファームウェアベースラインオプションをカスタムベースラインに設定してから、ファームウェアとOSドライバー（Smart Update Toolsを使用）インストール方法を選択します。

これにより、HPE Smart Update Toolsを使用してオペレーティングシステムにドライバーパッケージをインストールできるようになります。

HPE Smart Update Toolsの使用について詳しくは、HPE OneViewオンラインヘルプ、および**Hewlett Packard Enterpriseサポートセンター - Smart Update Manager Software**にあるSUTドキュメントを参照してください。

IPMIサーバー管理

IPMIによるサーバー管理は、サーバーを制御し、監視するための標準的な方法です。iLOファームウェアは、以下を定義するIPMIバージョン2.0仕様に基づくサーバー管理を提供します。

- ファン、温度、パワーサプライなどのシステム情報の監視
- システムのリセットおよび電源オン/オフ操作などのリカバリ機能
- 温度上昇読み取りやファン障害などの異常なイベントのロギング機能
- 障害のあるハードウェアコンポーネントの特定などのインベントリ機能

IPMI通信は、BMCとSMSに依存します。BMCは、SMSとプラットフォーム管理ハードウェアの間のインターフェイスを管理します。iLOファームウェアはBMC機能をエミュレートし、各種業界標準ツールでSMS機能が提供されます。詳しくは、IntelのWebサイト**http://www.intel.com**のIPMI仕様を参照してください。

iLOファームウェアは、SMS通信にKCSインターフェイスまたはオープンインターフェイスを提供します。KCSインターフェイスは、1組のI/Oマップ通信レジスタを提供します。I/OマップSMSインターフェイスのデフォルトシステムベースアドレスは、`0xCA2`で、このシステムアドレスでバイトアラインされています。

KCSインターフェイスは、ローカルシステムで動作するSMSソフトウェアにアクセス可能です。互換性のあるSMSソフトウェアアプリケーションの例は、次のとおりです。

- **IPMIバージョン2.0 Command Test Tool** - ローレベルMS-DOSコマンドラインツールです。KCSインターフェイスを実装したIPMI BMCに、16進数形式のIPMIコマンドを送信できるようにします。このツールはIntelのWebサイトhttp://www.intel.comからダウンロードできます。
- **IPMItool** - IPMIバージョン1.5およびバージョン2.0仕様をサポートするデバイスを管理したり設定するためのユーティリティです。IPMItoolは、Linux環境で使用できます。このツールはIPMItoolのWebサイトhttp://ipmitool.sourceforge.net/index.htmlからダウンロードできます。
- **FreeIPMI** - IPMIバージョン1.5およびバージョン2.0仕様をサポートするデバイスを管理したり設定するためのユーティリティです。FreeIPMIはWebサイトhttp://www.gnu.org/software/freeipmi/からダウンロードできます。
- **IPMIUTIL** - IPMIバージョン1.0、1.5およびバージョン2.0仕様をサポートするデバイスを管理したり設定するためのユーティリティです。IPMIUTILは、次のサイトからダウンロードできます。http://ipmiutil.sourceforge.net/

IPMIインターフェイスに対するBMCをエミュレートする場合に、iLOは、IPMIバージョン2.0仕様にリストされている必須コマンドをすべてサポートします。SMSは、その仕様に記述された方法を使用してBMC内で有効または無効にするIPMI機能を決定する必要があります（たとえば、`Get Device ID`コマンドを使用）。

サーバーのOSが動作中でiLOドライバーが有効な場合は、KCSインターフェイスを介したIPMIのデータ通信量がiLOのパフォーマンスとシステムヘルスに影響を与える可能性があります。KCSインターフェイスを介してIPMIコマンドを実行しないでください。これはIPMIサービスに悪影響を与えることがあります。この制限には、IPMIパラメーター（たとえば、`Set Watchdog Timer`および`Set BMC Global Enabled`）を設定または変更するあらゆるコマンドが含まれています。単にデータを返すIPMIコマンド（たとえば、`Get Device ID`および`Get Sensor Reading`）は、どれでも安全です。

サブトピック

Linux環境でのIPMIツールの高度な使用方法

Linux環境でのIPMIツールの高度な使用方法

LinuxのIPMIツールは、IPMI 2.0 RMCP+プロトコルを使用してiLOファームウェアと安全に通信できます。この機能は、`ipmitool lanplus`プロトコル機能です。

次に例を示します。iLOのイベントログを取得するには、次のコマンドを入力します。

```
ipmitool -I lanplus -H <iLO IPアドレス> -U <ユーザー名> -P <パスワード> sel list
```

出力例：

```
1 | 03/18/2000 | 00:25:37 | Power Supply #0x03 | Presence detected | Deasserted
2 | 03/18/2000 | 02:58:55 | Power Supply #0x03 | Presence detected | Deasserted
3 | 03/18/2000 | 03:03:37 | Power Supply #0x04 | Failure detected | Asserted
4 | 03/18/2000 | 03:07:35 | Power Supply #0x04 | Failure detected | Asserted
```

HPE SIMでのiLOの使用

iLOファームウェアは主なオペレーティング環境でHPE SIMと統合され、標準のWebブラウザーから単一の管理コンソールを提供します。オペレーティングシステムの動作中、HPE SIMを使用することでiLOへの接続を確立することができます。

HPE SIMと統合すると、以下を実現できます。

HPE SIMコンソールへのSNMPトラップの配信サポート

HPE SIMコンソールを構成して、SNMPトラップをポケットベルや電子メールアドレスに転送することができます。

マネジメントプロセッサーのサポート

ネットワーク上のサーバーにインストールされたすべてのiLOデバイスは、HPE SIMではマネジメントプロセッサーとして検出されます。

iLOマネジメントプロセッサーのグループ化

すべてのiLOデバイスを、論理的なグループとしてまとめて1つのページに表示することができます。

Agentless Management

iLOをAgentless Managementと組み合わせると、iLOのWebインターフェイス経由でシステム管理情報にリモートアクセスできます。

SNMP管理のサポート

HPE SIMは、iLO経由でSNMP情報にアクセスできます。

サブトピック

HPE SIMの機能

HPE SIMでは以下を実行できます。

- iLOプロセッサーの識別
- iLOプロセッサーとそのサーバーの関連付け
- iLOプロセッサーとそのサーバー間のリンクの作成
- iLOとサーバーの情報およびステータスの表示
- iLOについて表示する情報の量の制御

以下の項で、これらの機能について説明します。詳しくは、HPE SIMユーザーガイドを参照してください。

HPE SIMでのSSOの確立

手順

1. HPE SIM SSO用にiLOを設定し、HPE SIM信頼済みサーバーを追加します。
2. 前の手順で指定したHPE SIMサーバーにログインし、iLOプロセッサーを検出します。

   検出プロセスが完了したら、iLOに対してSSOが有効になります。

   HPE SIM検出タスクについて詳しくは、HPE SIMユーザーガイドを参照してください。

iLOの識別および関連付け

iLOの識別および関連付け

HPE SIMは、iLOプロセッサーを識別し、iLOとサーバーを関連付けます。iLOがHPE SIMの識別要求に応答するように設定するには、アクセス設定ページで匿名データ設定を有効にします。

サブトピック

HPE SIMでのiLOステータスの表示

HPE SIMでのiLOリンク

HPE SIMのシステムリストでのiLOの表示

詳しくは

iLOアクセス設定の構成

HPE SIMでのiLOステータスの表示

HPE SIMは、iLOデバイスを管理プロセッサーとして識別します。HPE SIMは、すべてのシステムページに管理プロセッサーのステータスを表示します。

iLO管理プロセッサーは、そのホストサーバーと同じ行にアイコンとして表示されます。管理プロセッサーのステータスは、アイコンの色で示されます。

デバイスステータスのリストについては、HPE SIMユーザーガイドを参照してください。

HPE SIMでのiLOリンク

HPE SIMは、管理を簡単にするために、次の位置へのリンクを作成します。

- 任意のシステムリストからiLOおよびホストサーバーへ
- iLOのシステムページからサーバーへ
- サーバーのシステムページからiLOへ

システムリストページには、iLO、サーバー、およびその関係が表示されます。

- iLOのWebインターフェイスを表示するには、ステータスアイコンをクリックします。
- デバイスのシステムページを表示するには、iLOまたはサーバー名をクリックします。

HPE SIMのシステムリストでのiLOの表示

iLO管理プロセッサーをHPE SIMに表示できます。完全な設定権限を持つユーザーは、管理プロセッサーをグループにまとめて、カスタマイズされたシステムの集合を作成し、使用することができます。詳しくは、HPE SIMユーザーガイドを参照してください。

HPE SIMでのSNMPアラートの受信

このタスクについて

HPE SIMでは、SNMPを完全に管理できます。iLOは、HPE SIMへのSNMPトラップ送信をサポートします。ユーザーは、イベントログを表示し、イベントを選択し、アラートについての詳細情報を表示できます。

手順

1. SNMPトラップを送信するようにiLOを有効にするには、以下のようにします。
   a. ナビゲーションツリーの管理をクリックします。
   b. SNMP設定およびSNMPアラートを構成します。

      SNMPアラートの送信先ボックスに、HPE SIMコンピューターのIPアドレスを入力します。
2. HPE SIMでiLOを検出するには、HPE SIMの管理対象デバイスとしてiLOを設定します。

   この構成により、iLO上のNICインターフェイスが専用の管理ポートとして機能するようになり、管理トラフィックはリモートのホストサーバーのNICインターフェイスから分離されます。手順については、HPE SIMユーザーガイドを参照してください。

   主要な、クリアされていないイベントについて、iLOトラップがすべてのイベントに表示されます。イベントについて詳しくは、イベントタイプをクリックしてください。

詳しくは

SNMPアラートの送信先の追加

iLOとHPE SIMのHTTPポート一致要件

HPE SIMは、デフォルトのWebサーバー非SSLポート（ポート80）で、HTTPセッションを開始してiLOを確認するように設定されています。ポート番号を変更する場合は、iLOとHPE SIMの両方で変更する必要があります。

- iLOでポートを変更するには、アクセス設定ページでWebサーバー非SSLポート値をアップデートします。
- HPE SIMでポート番号を変更するには、ポートを、HPE SIMのインストールディレクトリの`config\identification\additionalWsDisc.props`ファイルに追加します。

  ポートエントリーは1行でなければならず、最初にポート番号を指定し、以後の他のすべての項目は（大文字を含めて）次の例と同じです。次の例は、ポート55000でiLOを検出するための正しいエントリーを示しています。

  55000=iLO 6, ,true,false,com.hp.mx.core.tools.identification.mgmtproc.MgmtProcessorParser

詳しくは

iLOアクセス設定の構成

HPE SIMでのiLOライセンス情報の確認

HPE SIMは、iLO管理プロセッサーのライセンスステータスを表示します。この情報を使用すると、どのiLOデバイスに、また何台のiLOデバイスにライセンスがインストールされているかを確認できます。

ライセンス情報を表示するには、展開 > ライセンスマネージャーを選択します。

データが最新であることを確認するには、管理プロセッサーに対してシステム識別タスクを実行します。詳しくは、HPE SIMユーザーガイドを参照してください。

Kerberos認証とディレクトリサービスの設定

サブトピック

iLOでのKerberos認証

ディレクトリ統合の利点

iLOで使用するディレクトリ構成の選択

スキーマフリーディレクトリ認証

HPE拡張スキーマディレクトリ認証

ディレクトリサービスによるユーザーログイン

一度に複数のiLOシステムを構成するためのツール

ProLiant管理プロセッサー用のディレクトリサポート（HPLOMIG）

HPLOMIGによるディレクトリ認証の設定

ディレクトリサービススキーマ

iLOでのKerberos認証

Kerberosのサポートにより、ユーザーはユーザー名とパスワードを入力する代わりに、ログインページのZeroサインインボタンをクリックして、iLOにログインすることができます。正常にログインするには、クライアントワークステーションがドメインにログインし、ユーザーが、iLOが設定されているディレクトリグループのメンバーでなければなりません。ワークステーションがドメインにログインしていない場合でも、ユーザーは、Kerberos UPNとドメインパスワードを使用してiLOにログインできます。

システム管理者はユーザーサインオンの前にiLOとドメイン間の信頼関係を確立するため、（Two-Factor認証を含む）任意の形式の認証がサポートされます。Two-Factor認証をサポートするようにユーザーアカウントを設定する方法については、サーバーオペレーティングシステムのドキュメントを参照してください。

サブトピック

Kerberos認証の設定

Kerberos認証用のiLOホスト名とドメイン名の構成

ドメインコントローラーでのKerberosサポートの準備

Windows環境でのiLO用キータブファイルの生成

ご使用の環境がKerberos認証の時刻要件を満たしていることの確認

サポートされるブラウザーでのシングルサインオンの設定

Kerberos認証の設定

手順

1. iLOホスト名およびドメイン名を設定します。
2. iLOライセンスをインストールしてKerberos認証を有効にします。
3. ドメインコントローラーでKerberosサポートを準備します。
4. Kerberosキータブファイルを生成します。
5. ご使用の環境がKerberos認証の時刻要件を満たしていることを確認します。
6. iLOでKerberosパラメーターを設定します。
7. iLOディレクトリグループを設定します。
8. サポートされるブラウザーでシングルサインオンを設定します

Kerberos認証用のiLOホスト名とドメイン名の構成

このタスクについて

使用したいドメイン名またはDNSサーバーがDHCPサーバーによって提供されない場合は、次の手順を使用します。

手順

1. ナビゲーションツリーでiLO専用ネットワークポートをクリックします。
2. IPv4タブをクリックします。
3. 次のチェックボックスの選択を解除して、送信をクリックします。
   - DHCPv4のドメイン名の使用
   - DHCPv4のDNSサーバーの使用
4. IPv6タブをクリックします。
5. 次のチェックボックスの選択を解除して、送信をクリックします。
   - DHCPv6のドメイン名の使用
   - DHCPv6のDNSサーバーの使用
6. 全般タブをクリックします。
7. （オプション）iLOサブシステム名（ホスト名）をアップデートします。
8. ドメイン名をアップデートします。
9. 送信をクリックします。
10. iLOを再起動するには、リセットをクリックします。

サブトピック

Kerberos認証のiLOホスト名とドメイン名の要件

詳しくは

iLOホスト名の設定
iLOホスト名とドメイン名の制限
Kerberos認証のiLOホスト名とドメイン名の要件

Kerberos認証のiLOホスト名とドメイン名の要件

- ドメイン名 - iLOドメイン名の値は、通常大文字に変換されたドメイン名であるKerberosレルム名と一致している必要があります。たとえば、親ドメイン名が`somedomain.net`である場合、Kerberosレルム名は、`SOMEDOMAIN.NET`になります。
- iLOサブシステム名（ホスト名） - 設定されたiLOホスト名は、キータブファイルを生成するときに使用するiLOホスト名と同じでなければなりません。iLOホスト名は大文字小文字が区別されます。

ドメインコントローラーでのKerberosサポートの準備

このタスクについて

Windows Server環境で、Kerberosサポートはドメインコントローラーに含まれ、Kerberosレルム名は通常、大文字に変換されたドメイン名になります。

手順

1. iLOシステムごとにドメインディレクトリにコンピューターアカウントを作成して有効にします。
2. Active Directoryユーザーとコンピュータースナップインでユーザーアカウントを作成します。例：
   - iLOホスト名：`myilo`
   - 親ドメイン名：`somedomain.net`
   - iLOドメイン名（完全修飾）：`myilo.somedomain.net`
3. iLOへのログインが許可されている各ユーザーについて、ドメインディレクトリにユーザーアカウントが存在していることを確認します。
4. ドメインディレクトリにユニバーサルおよびグローバルユーザーグループを作成します。

   iLOで権限を設定するには、ドメインディレクトリにセキュリティグループを作成する必要があります。iLOにログインするユーザーには、そのユーザーがメンバーとなっているすべてのグループの一切の権限が付与されます。権限の設定には、グローバルユーザーグループおよびユニバーサルユーザーグループのみを使用できます。ドメインローカルグループは、サポートされていません。

Windows環境でのiLO用キータブファイルの生成

手順

1. `Ktpass.exe`ツールを使用して、キータブファイルを生成し、共有秘密を設定します。
2. （オプション）`Setspn`コマンドを使用して、Kerberos SPNをiLOシステム用SPNを表示します。
3. （オプション）`Setspn -L <iLO name>`コマンドを使用して、iLOシステム用SPNを表示します。

   `HTTP/myilo.somedomain.net`サービスが表示されることを確認します。

サブトピック

Ktpass

Setspn

詳しくは

Ktpass
Setspn

Ktpass

構文

`Ktpass [options]`

説明

`Ktpass`は、Kerberos認証用のサービスプリンシパル名と暗号化されたパスワードのペアが含まれているキータブファイルと呼ばれるバイナリファイルを生成します。

パラメーター

`+rndPass`

ランダムパスワードを指定します。

-ptype KRB5_NT_SRV_HST

プリンシパルタイプ。ホストサービスインスタンス（KRB5_NT_SRV_HST）タイプを使用します。

-princ <principal name>

大文字と小文字が区別されるプリンシパル名を指定します。たとえば、`HTTP/myilo.somedomain.net@SOMEDOMAIN.net`などです。

- サービスタイプは大文字を使用する必要があります（`HTTP`）。
- iLOホスト名は小文字を使用する必要があります（`myilo.somedomain.net`）。
- レルム名は大文字を使用する必要があります（`@SOMEDOMAIN.NET`）。

-mapuser <user account>

プリンシパル名をiLOシステムドメインアカウントにマップします。

-out <file name>

`.keytab`ファイルのファイル名を指定します。

-crypto <encryption>

`.keytab`ファイルに生成されるキーの暗号化を指定します。

iLOで、高度なセキュリティ、FIPS、またはCNSAセキュリティ状態を使用するように構成されている場合、AES Kerberosキータイプを使用する必要があります。

kvno

キーバージョン番号を上書きします。

> **重要:**
> このパラメーターは使用しないでください。このオプションを使用すると、キータブファイルの`kvno`とActive Directoryの`kvno`が同期しなくなります。

コマンド例

```
Ktpass +rndPass -ptype KRB5_NT_SRV_HST -princ
HTTP/myilo.somedomain.net@SOMEDOMAIN.NET -mapuser myilo$@somedomain.net
-out myilo.keytab
```

出力例

```
Targeting domain controller: domaincontroller.example.net
Using legacy password setting method
Successfully mapped HTTP/iloname.example.net to iloname.
WARNING: pType and account type do not match. This might cause problems.
Key created.
Output keytab to myilo.keytab:
Keytab version: 0x502
keysize 69 HTTP/iloname.example.net@EXAMPLE.NET ptype 3
(KRB5 _NT_SRV_HST) vno 3 etype 0x17 (RC4-HMAC) keylength 16
(0x5a5c7c18ae23559acc2 9d95e0524bf23)
```

`Ktpass`コマンドでは、UPNを設定できないことに関するメッセージが表示される場合があります。この結果は、iLOがユーザーではなくサービスであるため、問題ありません。コンピューターオブジェクトで、パスワード変更を確認するように求められる場合があります。ウィンドウを閉じ、キータブファイルの作成を続行するには、OKをクリックします。

Setspn

構文

`Setspn [options]`

説明

`Setspn`コマンドは、SPNを表示、修正、および削除します。

パラメーター

`-A <SPN>`

追加するSPNを指定します。

`-L`

システムの現在のSPNを一覧表示します。

コマンド例

```
SetSPN -A HTTP/myilo.somedomain.net myilo
```

SPNコンポーネントでは大文字と小文字が区別されます。プライマリ（サービスタイプ）は、たとえば`HTTP`のように大文字でなければなりません。インスタンス（iLOホスト名）は、たとえば`myilo.somedomain.net`のように小文字でなければなりません。

`SetSPN`コマンドでは、UPNを設定できないことに関するメッセージが表示される場合があります。この結果は、iLOがユーザーではなくサービスであるため、問題ありません。コンピューターオブジェクトで、パスワード変更を確認するように求められる場合があります。OKをクリックしてウィンドウを閉じ、キータブファイルの作成を続行します。

ご使用の環境がKerberos認証の時刻要件を満たしていることの確認

このタスクについて

Kerberos認証が正常に機能するには、iLOプロセッサー、KDC、およびクライアントワークステーションの間で日付と時刻が同期している必要があります。サーバーでiLOの日付および時刻を設定するか、iLO内でSNTP機能を有効にしてネットワークから日付および時刻を取得してください。

手順

以下の日付と時間が互いに5分以内で設定されていることを確認します。

- iLOの日付と時刻の設定
- Webブラウザーを実行するクライアント
- 認証を実行するサーバー

サポートされるブラウザーでのシングルサインオンの設定

ユーザーがiLOにログインするには、権限が割り当てられたグループのメンバーになっている必要があります。Windowsクライアントの場合、ワークステーションのロックまたはロック解除によって、iLOへのログインに使用される認証情報が更新されます。HomeバージョンのWindowsオペレーティングシステムは、Kerberosログインをサポートしていません。

iLOに関してActive Directoryが適切に設定されており、Kerberosログインに関してiLOが適切に設定されている場合には、このセクションの手順によって、ログインが有効になります。

サブトピック

Mozilla Firefoxでのシングルサインオンの有効化

Google Chromeでのシングルサインオン

Microsoft Edgeでのシングルサインオンの有効化

シングルサインオン（Zeroサインイン）設定の確認

名前によるログインが動作していることの確認

詳しくは

サポートされているブラウザー

Mozilla Firefoxでのシングルサインオンの有効化

手順

1. ブラウザーの場所ツールバーに
   `about:config`
   と入力して、ドメインの設定ページを開きます。

   Firefoxには次のメッセージが表示されます。

   `動作保証対象外になります!`
2. 危険性を承知の上で使用するボタンをクリックします。
3. 検索ボックスに
   `network.negotiate`
   と入力します。
4. `network.negotiate-auth.trusted-uris`をダブルクリックします。
5. iLOのDNSドメイン名を入力し（たとえば、`example.net`）、OKをクリックします。
6. シングルサインオンの設定を確認します。

Google Chromeでのシングルサインオン

Google Chromeでは設定は必要ありません。

Microsoft Edgeでのシングルサインオンの有効化

このタスクについて

Microsoft Edgeでは設定は必要ありません。

シングルサインオン（Zeroサインイン）設定の確認

手順

1. iLOログインページ（例：`http://iloname.example.net`）に移動します。
2. Zeroサインインボタンをクリックします。

名前によるログインが動作していることの確認

手順

1. iLOログインページに移動します。
2. Kerberos UPN形式のユーザー名（例：`user@EXAMPLE.NET`）を入力します。
3. 関連付けられているドメインパスワードを入力します。
4. ログイン をクリックします。

ディレクトリ統合の利点

- **スケーラビリティ** – ディレクトリサービスを利用して、数千台のiLOプロセッサー上で数千のユーザーをサポートできます。
- **セキュリティ** – ディレクトリサービスから強力なユーザーパスワードポリシーが継承されます。ポリシーには、ユーザーパスワードの複雑度、ローテーション頻度、有効期限などがあります。
- **ユーザーの責任** – 環境によっては、ユーザーがiLOアカウントを共有することがあり、その場合、操作を実行したユーザーの特定が困難になります。
- **ロールベースの管理**（HPE拡張スキーマ） – ロール（たとえば、事務処理、ホストのリモート制御、完全な制御）を作成して、ユーザーやユーザーグループに関連付けることができます。1つのロールで変更が行われると、その変更は、そのロールに関連付けられたすべてのユーザーおよびiLOデバイスに適用されます。
- **集中管理**（HPE拡張スキーマ） – MMCなどオペレーティングシステム固有の管理ツールを使用して、iLOユーザーを管理できます。
- **緊急性** – ディレクトリでの1つの変更が、関連付けられたiLOプロセッサーにただちに公開されます。この機能により、このプロセスをスクリプト化する必要がなくなります。
- **認証情報の簡素化** – ディレクトリでは、iLO用の新しい認証情報を記録せずに、既存のユーザーアカウントとパスワードを使用できます。
- **柔軟性**（HPE拡張スキーマ） – 企業の環境に合わせて、1台のiLOプロセッサーについて1ユーザーを対象に1つのロールを作成することも、複数のiLOプロセッサーについて複数のユーザーを対象に1つのロールを作成することも、ロールを組み合わせて使用することもできます。HPE拡張スキーマ構成では、アクセスを特定の時間だけに制限したり、特定のIPアドレス範囲に制限したりすることができます。
- **互換性** – iLOディレクトリ統合は、Active DirectoryおよびOpenLDAPをサポートします。
- **規格** – iLOディレクトリサポートは、安全なディレクトリアクセスに関するLDAP 2.0規格に基づいています。iLOのKerberosサポートはLDAP v3に基づいています。

iLOで使用するディレクトリ構成の選択

ディレクトリに対してiLOを構成する前に、スキーマフリー構成オプションかHPE拡張スキーマ構成オプションかを選択します。

以下の質問について検討します。

1. **使用するディレクトリにスキーマ拡張を適用できますか。**
   - **「はい」の場合** – 質問2に進みます。
   - **「いいえ」の場合** – Active Directoryを使用しており、お客様の会社のポリシーにより拡張を適用できません。

「いいえ」の場合 – OpenLDAPを使用しています。HPE拡張スキーマは、現時点ではOpenLDAPでサポートされていません。

「いいえ」の場合 – お使いの環境には、HPE拡張スキーマとのディレクトリ統合は適しません。

グループベースのスキーマフリーディレクトリ統合を使用します。試用版のサーバーをインストールして、HPE拡張スキーマ構成とのディレクトリ統合の利点を検討してみるとよいでしょう。

2. **スケーラブルな設定を使用していますか。**

次の質問に回答すると、設定がスケーラブルかどうかがわかります。

- ディレクトリユーザーのグループの権限を変更する可能性がありますか。
- iLOの変更を定期的にスクリプト化するつもりですか。
- iLO権限の制御に6つ以上のグループを使用しますか。

これらの質問に対する答えに応じて、次のオプションから選択します。

- **「いいえ」の場合** – スキーマフリーディレクトリ統合のインスタンスをインストールして、この方式がお使いのポリシーおよび手順の要件に合っているかどうかを検討してみましょう。必要に応じて、後で、HPE拡張スキーマ構成を展開できます。
- **「はい」の場合** – HPE拡張スキーマ構成を使用します。

詳しくは

スキーマフリーディレクトリ認証
HPE拡張スキーマディレクトリ認証

スキーマフリーディレクトリ認証

スキーマフリーディレクトリ認証を使用すると、ユーザーおよびグループがディレクトリに存在し、グループ権限がiLOの設定に存在します。iLOはディレクトリログイン証明書を使用してディレクトリ内のユーザーオブジェクトを読み取り、ユーザーグループのメンバーシップを取得します。これらのグループは、iLOのグループ構成と比較されます。ディレクトリユーザーアカウントが、構成されているiLOディレクトリグループのメンバーとして確認されると、iLOのログインに成功します。

スキーマフリーディレクトリ統合の利点

- ディレクトリスキーマを拡張する必要がありません。
- ディレクトリ内のユーザーについては、設定はほとんど必要ありません。設定が存在しない場合、ディレクトリは既存のユーザーおよびグループメンバーシップを使用してiLOにアクセスします。たとえば、User1というドメイン管理者がいるとすると、このドメイン管理者のセキュリティグループのDNをiLOにコピーして、フル権限を与えます。すると、User1はiLOにアクセスできるようになります。

スキーマフリーディレクトリ統合の欠点

グループ権限は、各iLOシステムで管理されます。この欠点は、グループ権限がほとんど変更されないため最小限に抑えられ、グループのメンバーシップを変更するタスクは、各iLOシステムでなく、ディレクトリで管理されます。Hewlett Packard Enterpriseは、同時に複数のiLOシステムを構成できるツールを提供しています。

構成オプション

スキーマフリーのセットアップオプションは、ディレクトリ用の設定にどの方法を用いても同じです。最も柔軟でないログイン、より柔軟なログイン、または非常に柔軟なログインのディレクトリ設定を構成できます。

- **最も柔軟でないログイン** – この構成を使用すると、完全DNとパスワードを入力してiLOにログインできます。iLOが認識するグループのメンバーでなければなりません。

  この構成を使用するには、次の設定を入力します。

  - ディレクトリサーバーのDNS名またはIPアドレスとLDAPポート。通常、SSL接続用のLDAPポートは、636です。

- 少なくとも1つのグループのDN。このグループは、セキュリティグループ（例：Active Directoryの場合は`CN=Administrators,CN=Builtin,DC=EXAMPLE,DC=COM`、OpenLDAPの場合は`UID=username,ou=People,dc=hpe,dc=com`）、または目的のiLOユーザーがグループメンバーであれば、別のどのグループでもかまいません。

- **より柔軟なログイン** - この構成を使用すると、ログイン名とパスワードを入力してiLOにログインできます。iLOが認識するグループのメンバーでなければなりません。ログイン時に、ログイン名とユーザーコンテキストが結合されて、ユーザーDNになります。

  この構成を使用するには、最も柔軟でないログインの設定と少なくとも1つのディレクトリユーザーコンテキストを入力します。

  たとえば、ユーザーが`JOHN.SMITH`としてログインし、ユーザーコンテキスト`CN=USERS,DC=EXAMPLE,DC=COM`が構成されている場合は、iLOで `CN=JOHN.SMITH,CN=USERS,DC=EXAMPLE,DC=COM`というDNが使用されます。

- **非常に柔軟なログイン** - この構成を使用すると、完全なDNとパスワード、ディレクトリに表示される名前、NetBIOS形式（domain/login_name）、または電子メール形式（login_name@domain）を使用してiLOにログインできます。

  この構成を使用するには、IPアドレスの代わりにディレクトリのDNS名を入力して、iLOにディレクトリサーバーアドレスを構成します。DNS名は、iLOおよびクライアントシステムの両方から、IPアドレスに解決できなければなりません。

サブトピック

ディレクトリ統合の設定（スキーマフリー構成）

スキーマフリーディレクトリ統合を使用するための前提条件

ディレクトリ統合の設定（スキーマフリー構成）

手順

1. ご使用の環境がスキーマフリーのディレクトリ統合を使用するための前提条件を満たしていることを確認します。
2. iLOスキーマフリーディレクトリのパラメーターを設定します。
3. ディレクトリグループを設定します。

スキーマフリーディレクトリ統合を使用するための前提条件

手順

1. Active DirectoryおよびDNSをインストールします。
2. ルートCAをインストールして、SSLを有効にします。

   iLOは、安全なSSL接続でのみ、ディレクトリと通信します。

   Active Directoryでの証明書サービスの使用について詳しくは、Microsoftのドキュメントを参照してください。
3. 少なくとも1人のユーザーのディレクトリDNとそのユーザーが含まれているセキュリティグループのDNが、使用可能であることを確認します。この情報は、ディレクトリのセットアップを検証するために使用されます。
4. ディレクトリサービス認証を有効にするiLOライセンスをインストールします。
5. iLOネットワーク設定のIPv4またはIPv6のページで、正しいDNSサーバーが指定されていることを確認します。

HPE拡張スキーマディレクトリ認証

HPE拡張スキーマディレクトリ認証オプションを使用すると、以下のことを行うことができます。

- 統合されたスケーラブルな共有ユーザーデータベースからユーザーを認証します。
- ディレクトリサービスを使用して、ユーザーの権限を制御（権限付与）します。
- ディレクトリサービスでは、iLO管理プロセッサーおよびiLOユーザーのグループレベルの管理にロールを使用します。

HPE拡張スキーマディレクトリ統合の利点

- グループが各iLO上ではなく、ディレクトリ内で維持管理されます。
- 柔軟なアクセス制御 – アクセスを特定の時間だけに制限したり、特定のIPアドレス範囲に制限したりすることができます。

サブトピック

ディレクトリサービスのサポート

iLOソフトウェアは、Microsoft Active Directoryユーザーとコンピュータースナップイン内で動作するように設計されており、ユーザーは、ディレクトリ経由でユーザーアカウントを管理できます。

iLOは、HPE拡張スキーマ構成でMicrosoft Active Directoryをサポートします。

ディレクトリ統合の設定（HPE拡張スキーマ構成）

手順

計画

1. 以下の内容を確認してください。
   - ディレクトリ対応リモート管理（HPE拡張スキーマ構成）
   - ディレクトリサービススキーマ

インストール

2. 次のように操作します。
   a. ご使用の環境がActive DirectoryとHPE拡張スキーマを構成するための前提条件を満たしていることを確認します。
   b. ディレクトリサービス認証を有効にするiLOライセンスをインストールします。

c. ProLiantマネジメントプロセッサー用のディレクトリサポートパッケージをダウンロードし、ご使用の環境に必要なユーティリティをインストールします。

Schema Extender、スナップイン、およびProLiantマネジメントプロセッサー用のディレクトリサポートユーティリティをインストールすることができます。

d. スキーマエクステンダーを使用してスキーマを拡張します。

アップデート

3. iLOのWebインターフェイスで、管理プロセッサーオブジェクトのディレクトリサーバー設定とDNを設定します。

このステップは、ProLiant管理プロセッサーのディレクトリサポートソフトウェアを使用して実行することもできます。

ロールとオブジェクトの管理

4. HPE Active Directoryスナップインを使用して、デバイスオブジェクトとロールオブジェクトを設定します。

a. マネジメントデバイスオブジェクトとロールオブジェクトを作成します。

b. 必要に応じて、ロールオブジェクトに権限を割り当て、役割を管理デバイスオブジェクトと関連付けます。

c. ユーザーをロールオブジェクトに追加します。

例外の取り扱い

5. 複雑なロール関連付けについては、ディレクトリスクリプティングユーティリティの使用を検討してください。

iLOユーティリティは、単一のロールで簡単に使用できます。ディレクトリに複数の役割を作成することを計画している場合は、`LDIFDE`またはVBScriptユーティリティのようなディレクトリスクリプティングユーティリティを使用することができます。これらのユーティリティは複雑なロールの関係を作成します。

詳しくは

Active DirectoryとHPE拡張スキーマの構成（構成例）

HPE拡張スキーマ構成でActive Directoryを設定するための前提条件

手順

1. Active DirectoryおよびDNSをインストールします。
2. ルートCAをインストールして、SSLを有効にします。

iLOは、安全なSSL接続でのみ、ディレクトリと通信します。

Active Directoryでの証明書サービスの使用について詳しくは、Microsoftのドキュメントを参照してください。

iLOには、ディレクトリサービスと通信するためにセキュリティ保護された接続が必要です。この接続には、Microsoft CAをインストールする必要があります。詳しくは、Microsoft Knowledge BaseのArticle ID番号321051を参照してください。サードパーティの証明機関がSSL経由でLDAPを有効にする方法

3. .NET Frameworkのバージョン3.5以降がインストールされていることを確認します。

iLO LDAPコンポーネントはこのソフトウェアを必要とします。

Windows Server Core環境ではLDAPコンポーネントを使用できません。

4. 次のMicrosoft Knowledge Baseの記事を参照してください。299687 MSO1-036: LDAP over SSLの機能によりパスワードの変更が可能になる

iLOディレクトリサポートソフトウェアのインストール

手順

1. ProLiantマネジメントプロセッサー用のディレクトリサポートパッケージをWebサイトhttps://www.hpe.com/support/ilo6からダウンロードします。
2. .NET Framework 3.5以降をターゲットサーバーにインストールします。

   .NET Framework 3.5以降は、ProLiantマネジメントプロセッサーソフトウェア用のディレクトリサポートをインストールするために使用します。
3. ダウンロードしたEXEファイルをダブルクリックします。
4. 次へをクリックします。
5. I accept the terms of the license agreement をクリックし、次へ をクリックします。
6. ディレクトリサポートウィンドウで、スキーマエクステンダーをクリックし、スキーマエクステンダーソフトウェアをインストールします。
   a. スキーマエクステンダーセットアップウィザードウィンドウで、次へをクリックします。
   b. ライセンス契約ウィンドウで、同意するを選択し、次へをクリックします。
   c. インストール先フォルダの選択ウィンドウで、インストールディレクトリとユーザー設定を選択し、次へをクリックします。
   d. インストール要求を確認するメッセージが表示されたら、次へをクリックします。

      インストールの完了ウィンドウが開きます。
   e. 閉じるをクリックします。
7. コンソールのスナップインをインストールするには、MMCコンソールが閉じられていることを確認してから、Snap-ins (x86)またはSnap-ins (x64)をクリックします。
   a. スナップインセットアップウィザードウィンドウで、次へをクリックします。
   b. ライセンス契約ウィンドウで、同意するを選択し、次へをクリックします。
   c. 情報ウィンドウで詳細を読んで、次へをクリックします。
   d. インストール要求を確認するメッセージが表示されたら、次へをクリックします。

      インストールの完了ウィンドウが開きます。
   e. 閉じるをクリックします。

   スナップインのインストール後、iLOオブジェクトとiLOロールをディレクトリ内で作成できます。ディレクトリオブジェクトの管理に使用される各コンピューターにスナップインをインストールします。詳しくは、ディレクトリサービスオブジェクトを参照してください。
8. ProLiant管理プロセッサー用のディレクトリサポートソフトウェアをインストールするには、ProLiantマネジメントプロセッサー用のディレクトリサポートをクリックします。
   a. ようこそウィンドウで、次へをクリックします。
   b. ライセンス契約ウィンドウで、同意するを選択し、次へをクリックします。
   c. インストール先フォルダの選択ウィンドウで、インストールディレクトリとユーザー設定を選択し、次へをクリックします。
   d. インストール要求を確認するメッセージが表示されたら、次へをクリックします。

      インストールの完了ウィンドウが開きます。
   e. 閉じるをクリックします。

サブトピック

ProLiant管理プロセッサー用のディレクトリサポートのインストールオプション

詳しくは

ProLiant管理プロセッサー用のディレクトリサポート (HPLOMIG)
Schema Extenderの実行
HPE Active Directoryスナップインによって追加される管理オプション

ProLiant管理プロセッサー用のディレクトリサポートのインストールオプション

- Schema Extender - Schema Extenderとバンドルされている`.xml`ファイルには、ディレクトリに追加されるスキーマが格納されます。通常、これらのファイルのうち1つに、サポートされているすべてのディレクトリサービスに共通のコアスキーマが格納されます。他のファイルには、製品固有のスキーマが格納されます。スキーマインストーラーには、.NET Frameworkが必要です。
  Windows Server Coreをホストするドメインコントローラー上でスキーマインストーラーを実行することはできません。セキュリティおよびパフォーマンス上の理由から、Windows Server Coreは、GUIを使用しません。スキーマインストーラーを使用するには、ドメインコントローラーにGUIをインストールするか、より古いバージョンのWindowsをホストするドメインコントローラーを使用する必要があります。
- Snap-ins (x86)またはSnap-ins (x64) - マネジメントスナップインインストーラーは、Microsoft Active Directory Users and Computersディレクトリまたは Novell ConsoleOneディレクトリで、iLOオブジェクトを管理するためのスナップインをインストールします。

  iLOスナップインは、iLOディレクトリを作成する際に次のタスクを実行するために使用されます。

  - iLOオブジェクトとロールオブジェクトを作成して管理する
  - iLOオブジェクトとロールオブジェクトとの関連を作成する
- ProLiant管理プロセッサー用のディレクトリサポート - このユーティリティでは、iLOでのKerberos認証およびディレクトリサービスを設定できます。

  `HPLOMIG.exe`ファイル、必要なDLL、ライセンス契約、およびその他のファイルが、`C:\Program Files (x86)\Hewlett Packard Enterprise\Directories Support for ProLiant Management Processors`ディレクトリにインストールされます。別のディレクトリを選択することもできます。インストーラーが、スタートメニューにProLiant管理プロセッサー用のディレクトリサポートへのショートカットを作成します。
  インストールユーティリティは、.NET Frameworkがインストールされていないことを検出すると、エラーメッセージを表示して終了します。

Schema Extenderの実行

手順

1. WindowsのスタートメニューからManagement Devices Schema Extenderを起動します。
2. Lights Out Managementが選択されていることを確認してから、次へを選択します。
3. Preparationウィンドウの情報を読んでから、次へを選択します。
4. Schema Previewウィンドウで次へをクリックします。
5. Setupウィンドウで、
   - ディレクトリサーバーの種類、名前、およびポートを入力します。
   - ディレクトリログイン情報とSSLの設定

   Resultsウィンドウには、スキーマを拡張できたかどうかや変更された属性など、インストールの結果が表示されます。

サブトピック

Schema Extenderで必要な情報

Schema Extenderで必要な情報

ディレクトリサーバー

- タイプ - ディレクトリサーバーのタイプ。
- 名前 - ディレクトリサーバーの名前。
- ポート - LDAP通信に使用するポート。

ディレクトリログイン

- ログイン名 - ディレクトリにログインするユーザーの名前。

  スキーマの拡張を完了するためにディレクトリユーザーの名前とパスワードが必要である場合があります。

  認証情報を入力するときに、`Administrator`ログインをドメイン名とともに使用する必要があります（例：`Administrator@domain.com`または`domain\Administrator`）。
  Active Directoryでスキーマを拡張するには、ユーザーが認証されているスキーマ管理者でなければなりません。また、スキーマが書き込み禁止であってはなりません。さらに、そのディレクトリがツリー内でFSMOロールオーナでなければなりません。インストーラーは、ターゲットディレクトリサーバーをフォレストのFSMOスキーママスターにしようとします。
- パスワード - ディレクトリにログインするためのパスワード。
- Use SSL for this Session - 使用する安全な認証の形式を設定します。このオプションを選択すると、SSL経由でのディレクトリ認証が使用されます。このオプションを選択せず、Active Directoryを選択すると、Windows認証が使用されます。

ディレクトリサービスオブジェクト

ディレクトリベースの管理で大切なことの1つは、ディレクトリサービス内の管理対象デバイスを正しく仮想化することです。この仮想化によって、管理者は、ディレクトリサービス内の管理対象デバイスとユーザーまたはグループとを関連付けることができます。iLOのユーザー管理では、ディレクトリサービス内に以下の基本オブジェクトが必要です。

- Lights-Out Managementオブジェクト
- Roleオブジェクト
- Userオブジェクト

各オブジェクトは、ディレクトリベースの管理に必要なデバイス、ユーザー、関連を意味します。

スナップインのインストール後、iLOオブジェクトとiLOロールを、ディレクトリ内で作成できます。次のタスクは、Active Directory Users and Computersツールを使用して行います。

- iLOオブジェクトとロールオブジェクトの作成
- ロールオブジェクトへのユーザーの追加
- ロールオブジェクトの権限と制限の設定

詳しくは

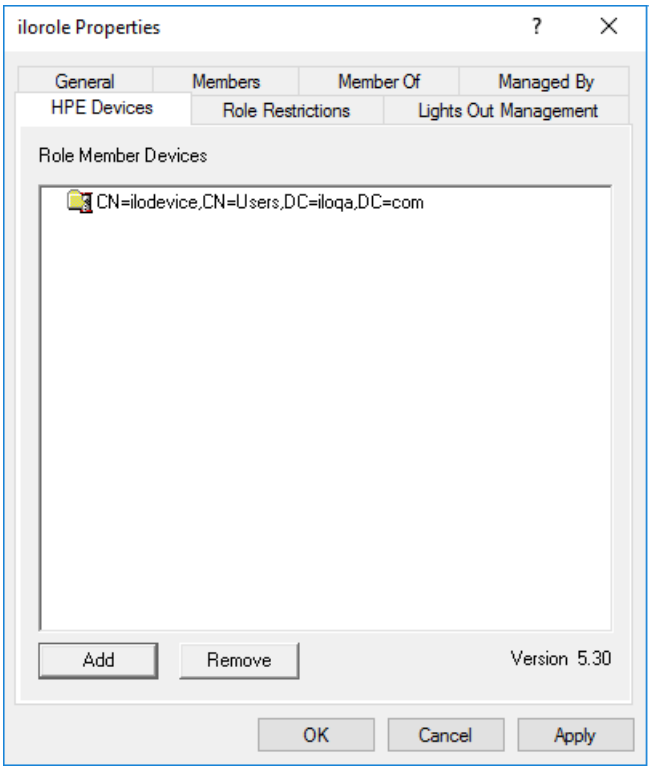
Active DirectoryとHPE拡張スキーマの構成（構成例）
HPE Active Directoryスナップインによって追加される管理オプション
ディレクトリ対応リモート管理（HPE拡張スキーマ構成）

組織構造に基づいたロール
ロールアクセス制限の適用方法
ユーザーアクセス制限
ロールアクセス制限

HPE Active Directoryスナップインによって追加される管理オプション

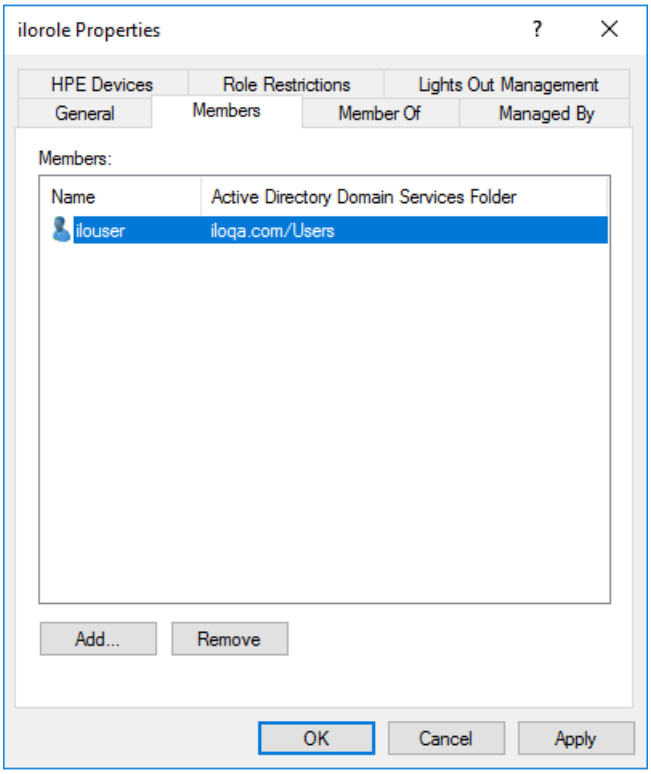
Hewlett Packard Enterpriseスナップインをインストールした後、Active Directoryユーザーとコンピューターで次の管理オプションが使用できるようになります。

Devicesタブ



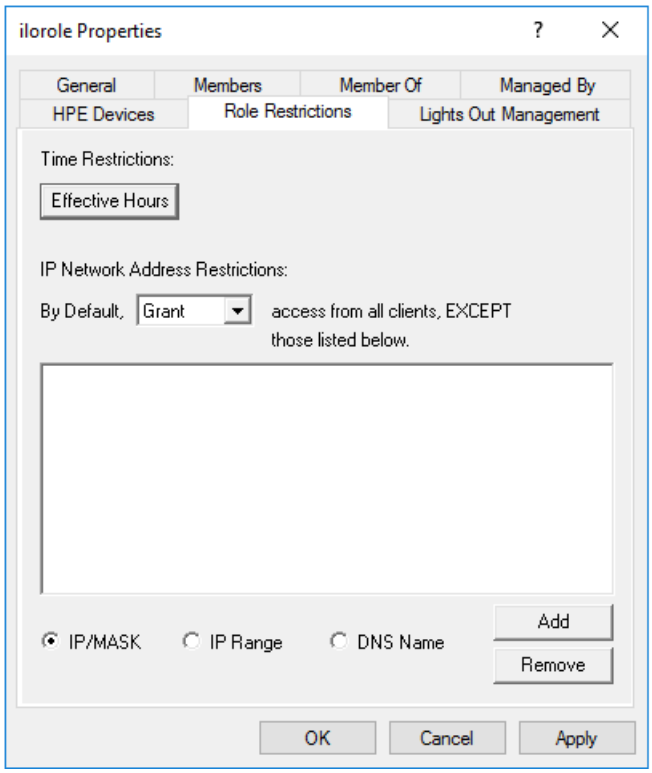
このタブでは、ロール内で管理するHewlett Packard Enterpriseデバイスを追加できます。Addをクリックすると、デバイスにアクセスして、そのデバイスをメンバーデバイスのリストに追加することができます。既存のデバイスを選択して、Removeをクリックすると、そのデバイスは有効なメンバーのデバイスリストから削除されます。

Membersタブ



ユーザーオブジェクトが作成された後、このタブを使用してロール内でユーザーを管理できます。Addをクリックすると、追加するユーザーにアクセスできます。既存ユーザーを強調表示して、Removeをクリックすると、そのユーザーは有効なメンバーのリストから削除されます。

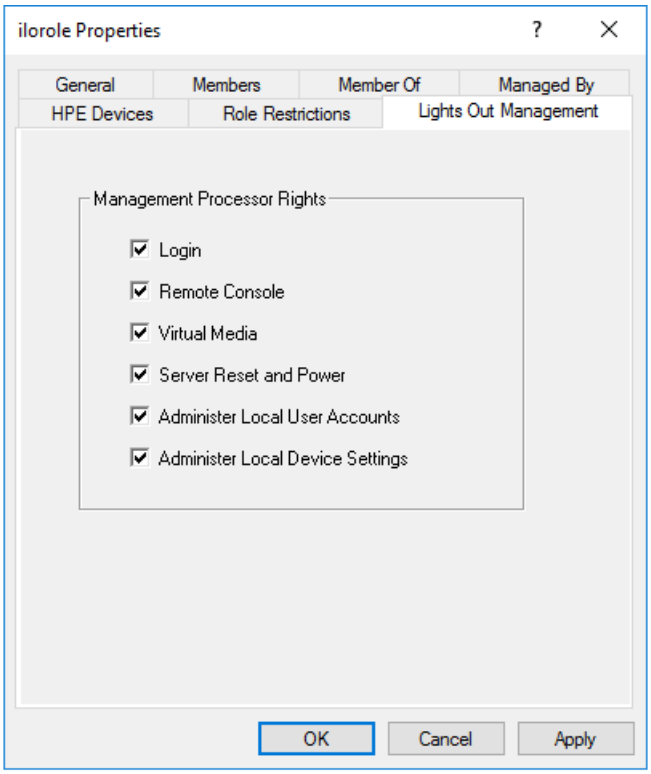
Role Restrictionsタブ



このタブでは、以下のタイプのロールの制限を設定できます。

- Time restrictions – Effective Hoursをクリックして、曜日ごとにログオンできる時間を30分単位で選択します。1つの四角形を変更するには、クリックして変更できます。複数の四角形のボックスをまとめて変更するには、マウスボタンを押したまま、ボックス上でカーソルをドラッグして、マウスボタンを離してください。デフォルトでは、常時アクセスできるように設定されています。
- IP/マスク、IP範囲、およびDNS名を含むIPネットワークアドレス制限。

Lights Out Managementタブ



ロールを作成した後で、このタブを使用してロールの権限を選択できます。ユーザーオブジェクトおよびグループオブジェクトをロールのメンバーにすることにより、ユーザーまたはユーザーグループにロールが付与する権限を与えることができます。

iLOに対するユーザー権限は、そのユーザーがメンバーとして所属し、そのiLOが管理対象デバイスとなっているすべてのロールによって割り当てられたすべての権限の和とみなされます。Active Directory内で、iLOで使用するために、ディレクトリオブジェクトを作成して設定するの例では、あるユーザーが`remoteAdmins`ロールと`remoteMonitors`ロールの両方に所属する場合、`remoteAdmins`ロールがすべての権限を持っているため、そのユーザーは使用できるすべての権限を持つことになります。

使用できる権限は、次のとおりです。

- Login – 関連付けられたデバイスにユーザーがログインできるかどうかを制御します。
- Remote Console – ユーザーがiLOリモートコンソールにアクセスできるようにします。
- Virtual Media – ユーザーがiLO仮想メディア機能にアクセスできるようにします。
- Server Reset and Power – ユーザーがiLO仮想電源ボタンを使用できるようにします。
- Administer Local User Accounts – ユーザーがユーザーアカウントを管理できるようにします。ユーザーは、自身および他のユーザーのアカウント設定の変更、ユーザーの追加と削除を行うことができます。
- Administer Local Device Settings – ユーザーがiLO管理プロセッサーを設定できるようにします。

注記:
システムリカバリ、ホストNIC、ホストストレージ、およびホストBIOS権限は、Schema Extenderで使用できません。

サブトピック

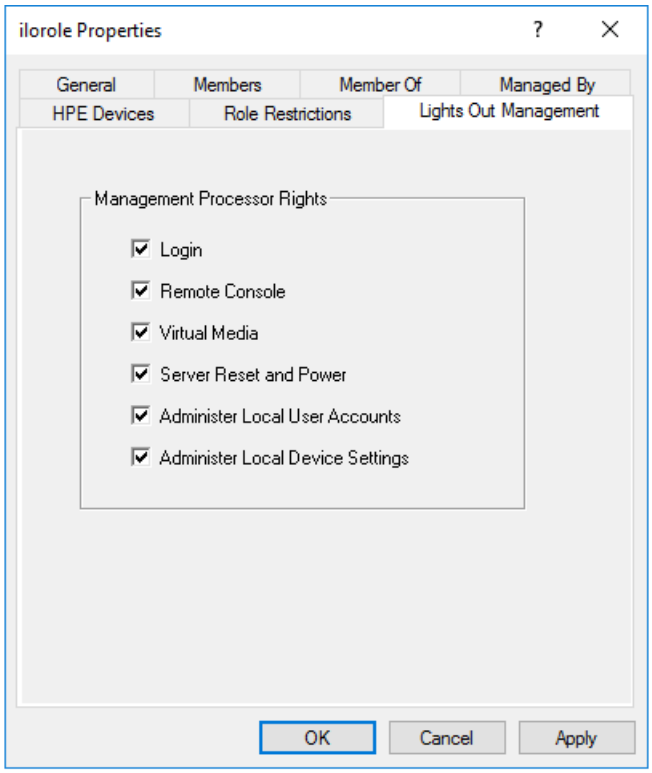
クライアントIPアドレスまたはDNS名の制限の設定

クライアントIPアドレスまたはDNS名の制限の設定

手順

1. Role Restrictionsタブ上のBy Defaultリストで、指定したIPアドレスを除くすべてのアドレス、IPアドレス範囲、およびDNS名からのアクセスを、許可するか取り消すかを選択します。
2. 次の制限タイプのいずれかを選択し、追加をクリックします。
   - DNS Name - 単一のDNS名またはサブドメインベースでアクセスを制限できます。入力は、`host.company.com`または`*.domain.company.com`という形式で行います。
   - IP/MASK - IPアドレスまたはネットワークマスクを入力できます。
   - IP Range - IPアドレス範囲 を入力できます。
3. 制限の設定ウィンドウで必要な情報を入力して、OKをクリックします。

   次の例では、New IP/Mask Restrictionウィンドウを示します。



4. OKをクリックします。

   変更が保存されると、iLORole Propertiesダイアログボックスが閉じます。

ディレクトリ対応リモート管理（HPE拡張スキーマ構成）

ディレクトリ対応リモート管理により、以下の作業を実行できます。

Lights-Out Managementオブジェクトの作成

ディレクトリサービスを使用してユーザーの認証や権限付与を行うデバイスごとに、そのデバイスを表すLOMデバイスオブジェクトを1つ作成する必要があります。Hewlett Packard Enterpriseスナップインを使用してLOMオブジェクトを作成することができます。

Hewlett Packard Enterpriseは、LOMデバイスオブジェクトに意味のある名前を付けることをおすすめします。たとえば、デバイスのネットワークアドレス、DNS名、ホストサーバー名、シリアル番号などを使用できます。

Lights-Outマネジメントデバイスの設定

ユーザーの認証や権限付与にディレクトリサービスを使用するすべてのLOMデバイスは、適切なディレクトリ設定を使用して設定する必要があります。一般に、各デバイスを、適切なディレクトリサーバーアドレス、LOMオブジェクトDN、およびユーザーコンテキストを使用して設定します。サーバーアドレスは、ローカルディレクトリサーバーのIP

アドレスまたはDNS名です。冗長性を高くするために、マルチホストDNS名を使用できます。

サブトピック

組織構造に基づいたロール

組織内の管理者は、下級管理者が上級管理者から独立して権限を割り当てなければならない階層体制に属している場合があります。このような場合、上級管理者によって割り当てられる権限を表すロールを1つ作成するとともに、下級管理者が独自のロールを作成して管理することを許可すると便利です。

既存のグループの使用

多くの組織では、ユーザーや管理者をグループ分けしています。多くの場合、既存のグループを使用し、そのグループを1つまたは複数のLOMロールオブジェクトに関連付けると便利です。デバイスがロールオブジェクトに関連付けられている場合、管理者は、グループのメンバーを追加または削除することによって、そのロールに関連付けられたLights-Outデバイスへのアクセスを制御します。

Microsoft Active Directoryを使用する場合は、あるグループを別のグループ内に配置できます（つまり、入れ子型のグループを使用できます）。ロールオブジェクトはグループとみなされ、他のグループを直接含むことができます。既存の入れ子型グループを直接ロールに追加し、適切な権限と制限を割り当ててください。新しいユーザーを、既存のグループまたはロールのいずれかに追加できます。

トラスティまたはディレクトリ権限割り当てを使用してロールのメンバーシップを拡張する場合、ユーザーは、LOMデバイスを表すLOMオブジェクトを読み出すことができる必要があります。一部の環境では、正常なユーザー認証を行うために、ロールのトラスティが、オブジェクトの読み出すトラスティでもある必要があります。

複数のロールの使用

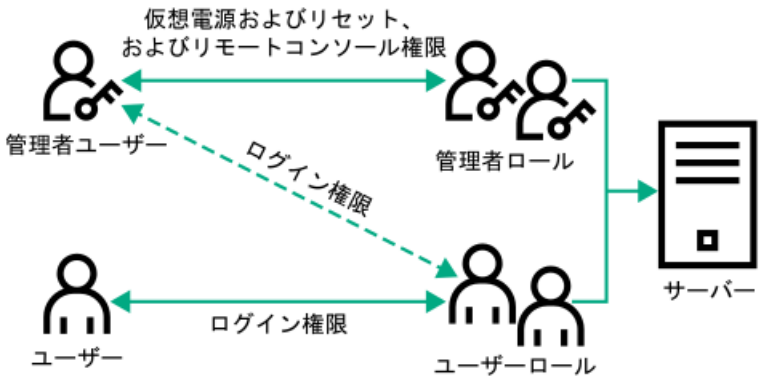
ほとんどのデプロイメントでは、同じユーザーが、同じデバイスを管理する複数のロールに入っている必要はありません。ただし、これらの構成は、複雑な権限関係を構築する際には便利です。ユーザーが複数のロールの関係を構築すると、そのユーザーには、該当する各ロールによって割り当てられるすべての権限が付与されます。ロールは、権限を付与することしかできず、権限を取り消すことはできません。あるロールがユーザーに権限を付与する場合、そのユーザーは、その権限を付与しない別のロールに入っていても、その権限を持ちます。

一般に、ディレクトリ管理者は、最小の数の権限が割り当てられたベースロールを作成し、追加のロールを作成して権限を追加します。これらの追加権限は、特定の状況で、またはベースロールユーザーの特定のサブセットに追加されます。

たとえば、組織は、LOMデバイスまたはホストサーバーの管理者とLOMデバイスのユーザーという2つのタイプのユーザーを持つことがあります。この状況では、管理者のロールとユーザーのロールという2つのロールを作成することが有効です。両方のロールにはいくつかの同じデバイスが含まれますが、これらのロールは異なる権限を付与します。より小さなロールに包括的な権限を割り当てて、LOM管理者をそのロールと管理者ロールに入れると便利な場合があります。

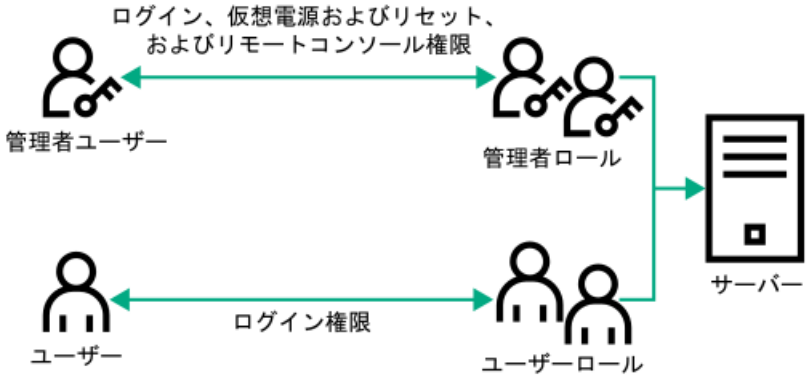
複数の（重複する）ロールには、管理者ユーザーがユーザーロールからログイン権限を取得し、管理者ロールから高度な権限が割り当てられる例を示します。

図 1. 複数の（重複する）ロール



重複するロールを使用しない場合は、複数の（独立した）ロールに示すように、ログイン、仮想電源およびリセット、およびリモートコンソール権限を管理者ロールに割り当て、ログイン権限をユーザーロールに割り当てることがあります。

図 2. 複数の（独立した）ロール

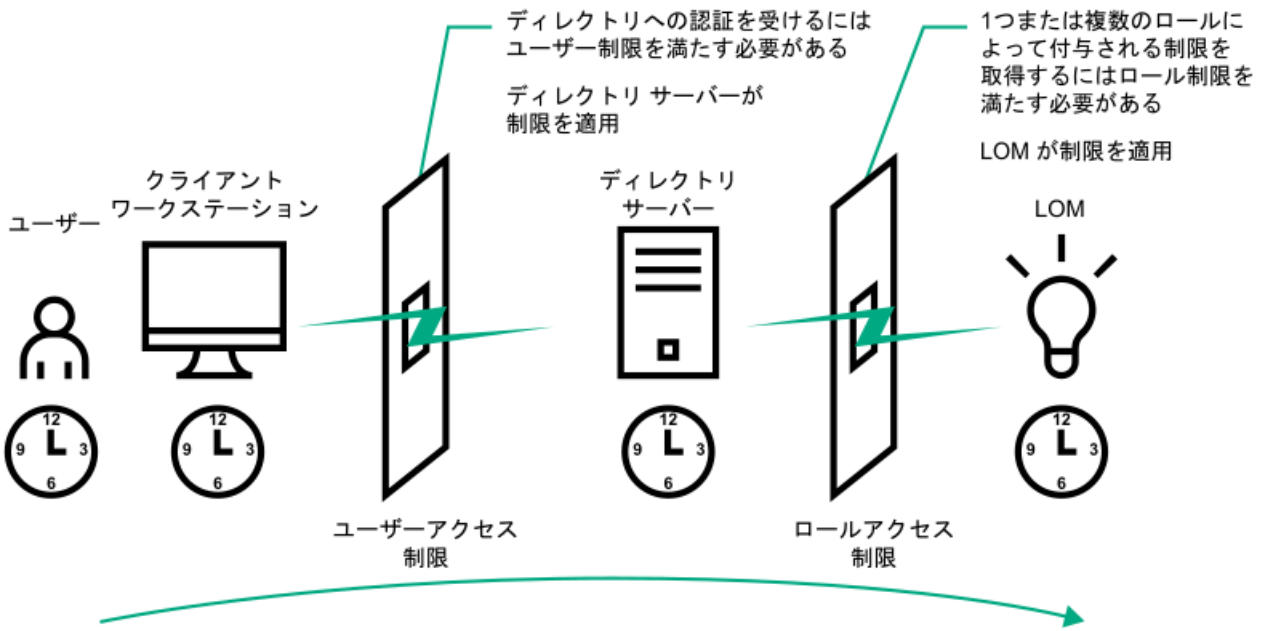


ロールアクセス制限の適用方法

ディレクトリユーザーによるLOMデバイスへのアクセスは、2段階の制限によって限定することができます。

- ユーザーアクセス制限は、ディレクトリへの認証を受けるためのユーザーアクセスを限定します。
- ロールアクセス制限は、1つまたは複数のロールでの指定に基づいてLOM権限を受けることができる認証済みユーザーの機能を限定します。

図 1. ディレクトリのログイン制限



ユーザーアクセス制限

アドレス制限

管理者は、ディレクトリユーザーアカウントにネットワークアドレス制限を設定できます。ディレクトリサーバーには、これらの制限が適用されます。

LDAPクライアント（LOMデバイスへのユーザーのログインなど）へのアドレス制限の適用について詳しくは、ディレクトリサービスのドキュメントを参照してください。

ディレクトリのユーザーに設定したネットワークアドレス制限は、ディレクトリユーザーがプロキシサーバー経由でログインする場合は、予期したとおりに適用されない場合があります。ユーザーがディレクトリユーザーとしてLOMデバイスにログインする場合は、LOMデバイスが、そのユーザーとしてのディレクトリへの認証を試みます。つまり、ユーザーアカウントに設定されたアドレス制限が、LOMデバイスへのアクセス時に適用されます。プロキシサーバーが使用される場合は、認証が試みられるネットワークアドレスがクライアントワークステーションのものではなく、LOMデバイスのものになります。

IPv4アドレス範囲制限

IPアドレス範囲制限によって、管理者は、アクセスを許可または拒否するネットワークアドレスを指定することができます。

アドレス範囲は、一般に、「最小-最大」範囲フォーマットで指定します。アドレス範囲を指定して、単一のアドレスのアクセスを許可または拒否することもできます。「最小-最大」IPアドレス範囲内のアドレスには、IPアドレス制限が適用されます。

IPv4アドレスおよびサブネットマスク制限

IPアドレスおよびサブネットマスク制限によって、管理者は、アクセスを許可または拒否するアドレスの範囲を指定することができます。

このフォーマットは、IPアドレス範囲制限に似ていますが、ご使用のネットワーク環境によっては特有のものになる場合があります。IPアドレスおよびサブネットマスク範囲は、一般に、同じ論理ネットワーク上のアドレスを特定するサブネットアドレスおよびアドレスビットマスクによって指定します。

2進数演算で、クライアントマシンのアドレスのビットにサブネットマスクのビットを加えたものが制限にあるサブネットアドレスと一致する場合、クライアントは制限を満たします。

DNSベース制限

DNSベース制限では、ネットワークネームサービスを使用して、クライアントIPアドレスに割り当てられたマシン名を検出することによって、クライアントマシンの論理名を調べます。DNS制限には、正常に動作しているネームサーバーが必要です。ネームサービスがダウンしていたり、利用できなかったりすると、DNS制限が満たされず、クライアントマシンは制限

を満たすことができなくなります。

DNSベース制限を使用すると、特定マシン名や、共通のドメインサフィックスを共有するマシンへのアクセスを制限できます。たとえば、**www.example.com**というDNS制限は、**www.example.com**というドメイン名が割り当てられているホストによって満たされ、***.example.com**というDNS制限は、**example**社が提供元になっているすべてのマシンによって満たされます。

マルチホームホストを使用している場合があるので、DNS制限では、あいまいさが発生する可能性があります。DNS制限は、必ずしも単一のシステムに一対一で適用されるわけではありません。

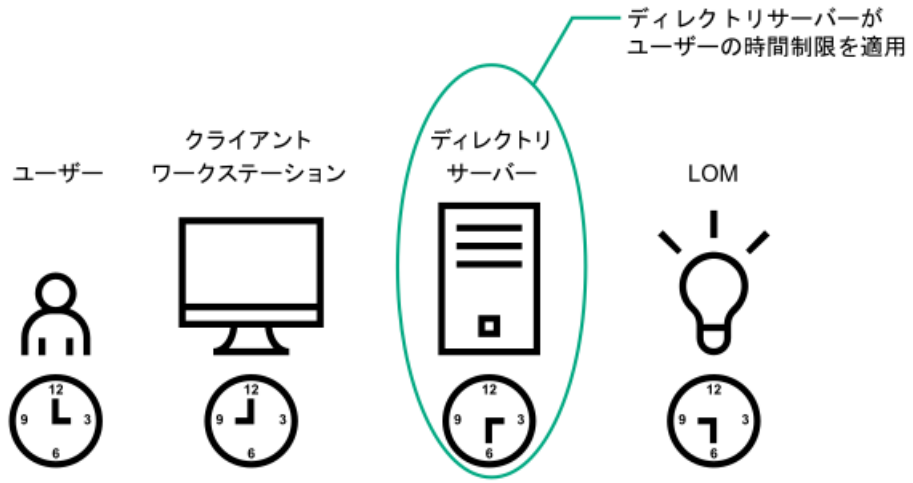
DNSベース制限を使用すると、セキュリティが複雑になる場合があります。ネームサービスプロトコルは、安全ではありません。ネットワークにアクセスできる悪意を持ったユーザーは、誰でも、不正なDNSサーバーをネットワークに配置して偽のアドレス制限基準を作成することができます。DNSベースのアドレス制限を実装している場合は、組織的なセキュリティポリシーを考慮に入れてください。

ユーザーの時間制限

時間制限によって、ディレクトリへのユーザーのログイン（認証）が限定されます。通常、時間制限は、ディレクトリサーバーの時間を使用して適用されます。ディレクトリサーバーが異なるタイムゾーンにある場合または異なるタイムゾーンにあるレプリカサーバーにアクセスしている場合は、管理対象オブジェクトからのタイムゾーン情報を使用して相対的な時間を調整することができます。

ディレクトリサーバーは、ユーザーの時間制限を確認しますが、判定方法は、タイムゾーンの変化や認証メカニズムによって複雑になる場合があります。

図 1. ユーザーの時間制限



ロールアクセス制限

制限によって、管理者は、ロールの範囲を限定することができます。ロールは、ロールの制限を満たすユーザーだけに権限を付与します。制限付きロールを使用することによって、ユーザーに、時間帯やクライアントのネットワークアドレスによって変化する動的権限を付与することができます。

ディレクトリが有効な場合、iLOシステムへアクセス可能かどうかは、該当するiLOオブジェクトを含むロールオブジェクトへの読み取りアクセス権が、ユーザーにあるかどうかによって決まります。このユーザーには、ロールオブジェクトで許可されているメンバーも含まれますが、そのメンバーに限定されません。継承可能な権限を親から伝達できるようにロールを設定すると、読み出し権限を持つ親のメンバーもiLOにアクセスできます。

アクセス制御リストを表示するには、Active Directory Users and Computersに移動し、ロールオブジェクトのプロパティページを開き、セキュリティタブをクリックします。セキュリティタブを表示するには、MMCでAdvanced Viewを有効にする必要があります。

ロールベースの時間制限

管理者は、LOMロールに時間制限を設定することができます。ユーザーには、そのユーザーがロールのメンバーであり、そのロールの時間制限を満たしている場合にのみ、そのロールに示されているLOMデバイスについて、指定された権限が付与されます。

ロールベースの時間制限は、LOMデバイスで時間が設定されている場合にのみ、機能します。LOMデバイスは、ローカルホストの時間に従って、時間制限を適用します。LOMデバイスの時計が設定されていない場合、ロールに対して時間制限が指定

されていない限り、ロールベースの時間制限は適用されません。時間は、通常、ホストの起動時に設定されます。

時間設定は、SNTPを設定することで維持できます。SNTPによって、LOMデバイスでうるう年を補正することや、ホストとの時間のずれを最小限に抑えることができます。予定外の停電やLOMファームウェアのフラッシュなどのイベントによって、LOMデバイスの時計が設定されないことがあります。また、LOMデバイスがファームウェアをフラッシュする時間の設定を保持するために、ホストの時間は正確でなければなりません。

ロールベースのアドレス制限

LOMファームウェアでは、クライアントのIPネットワークアドレスに基づいてロールベースのアドレス制限が適用されます。ロールのアドレス制限が満たされる場合、そのロールによって付与される権利が適用されます。

ファイアウォールの外からのアクセスやネットワークプロキシ経由のアクセスが試みられる場合、アドレス制限は、管理が困難になる場合があります。これらの方式のアクセスが可能な場合、クライアントの見かけ上のネットワークアドレスが変更されることがあるので、アドレス制限の予期しない適用が発生する場合があります。

複数の制限およびロール

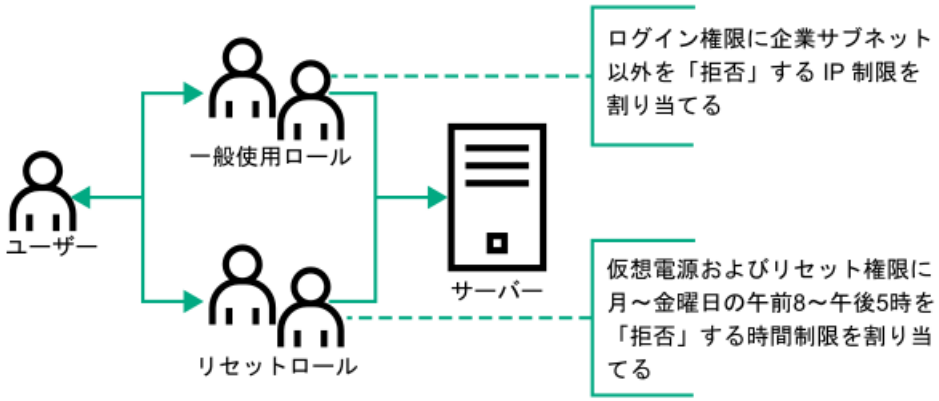
権限の適用される状況が限定されるように1つまたは複数のロールを制限したい場合には、多数のロールを作成すると非常に便利です。他のロールが、異なる権限を異なる制限で付与します。複数の制限とロールを使用すると、管理者は、任意の複雑な権限関係を最小限のロールで作成できます。

たとえば、組織が、LOM管理者について、「企業ネットワーク内からLOMデバイスを使用できるが通常の業務時間外にはサーバーのリセットしかできない」というセキュリティポリシーを設定しているとします。

ディレクトリ管理者は、2つのロールを作成してこの状況に対応しようと考えるかもしれませんが、この場合には特別の注意が必要です。必要なサーバーリセット権限を付与するロールを作成し、このロールを業務時間外に制限すると、管理者が企業ネットワークの外からサーバーをリセットできるようになる場合があり、多くの場合セキュリティポリシーに反します。

制限およびロールの作成では、セキュリティポリシーで、一般的な使用を企業サブネット内のクライアントに制限しており、サーバーリセット操作を業務時間外に制限していることを示しています。

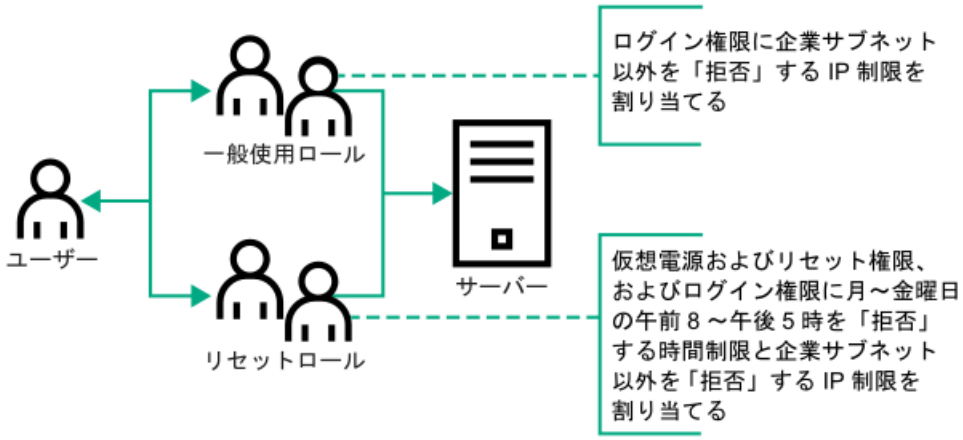
図 1. 制限およびロールの作成



また、ディレクトリ管理者は、ログイン権限を付与するロールを作成し、このロールを企業ネットワークに制限した後、サーバーリセット権限だけを付与する別のロールを作成し、これを業務時間外に制限しようと考えるかもしれません。この設定では管理が簡単になりますが、継続的な管理によって企業ネットワーク外部のアドレスからのユーザーにログイン権限を付与する別のロールが作成される場合があるため、危険性が増します。サーバーリセットロールに属するLOM管理者がロールの時間制限を満たす場合、このロールは意図せずに、このLOM管理者にどこからでもサーバーをリセットできる権限を付与する可能性があります。

制限およびロールの作成に示されている設定は、企業のセキュリティ要件を満たしています。ただし、ログイン権限を付与する別のロールを追加することによって、間違って、業務時間外に企業サブネットの外からサーバーをリセットする権限を付与する可能性があります。リセットロールと一般使用ロールの制限で示すように、リセットロールと一般使用ロールを制限することによって、より管理しやすいソリューションを実現できます。

図 2. リセットロールと一般使用ロールの制限



Active DirectoryとHPE拡張スキーマの構成（構成例）

このタスクについて

この手順では、HPE拡張スキーマを使用してActive Directoryを構成する方法の例を示します。

手順

1. ご使用の環境がHPE Active Directoryと拡張スキーマを構成するための前提条件を満たしていることを確認します。
2. ディレクトリサービス認証を有効にするiLOライセンスをインストールします。
3. iLOディレクトリサポートソフトウェアをインストールします。
4. Schema Extenderを使用してスキーマを拡張します。
5. デバイスオブジェクトとロールオブジェクトを設定します。
6. iLOにログインし、ディレクトリページで、ディレクトリ設定を入力します。
7. iLOネットワーク設定のIPv4またはIPv6のページで、正しいDNSサーバーが指定されていることを確認します。

サブトピック

Active Directory内で、iLOで使用するために、ディレクトリオブジェクトを作成して設定する

iLOの構成およびLights-Out Managementオブジェクトとの関連付け

Active Directory内で、iLOで使用するために、ディレクトリオブジェクトを作成して設定する

このタスクについて

次の例は、ドメイン**testdomain.local**があるエンタープライズディレクトリでロールとHewlett Packard Enterpriseデバイスをセットアップする方法を示します。このドメインは、2つの組織単位（**Roles**および**iLOs**）で構成されます。このセクションの手順は、Hewlett Packard Enterprise Active Directory Users and Computersスナップインを使用して完了します。

手順

1. iLOs組織単位を作成し、LOMオブジェクトを追加します。
2. Roles組織単位を作成し、ロールオブジェクトを追加します。

3. ロールに権限を割り当て、ロールをユーザーおよびデバイスと関連付けます。

サブトピック

iLOs組織ユニットの作成およびLOMオブジェクトの追加

Roles組織ユニットの作成およびロールオブジェクトの追加

ロールへの権限の割り当てとロールのユーザーおよびデバイスへの関連付け

詳しくは

HPE Active Directoryスナップインによって追加される管理オプション
ディレクトリサービスオブジェクト

iLOs組織ユニットの作成およびLOMオブジェクトの追加

手順

1. ドメインによって管理されるiLOデバイスを含む、iLOsという組織単位を作成します。
2. testdomain.localドメイン内にある組織単位iLOsを右クリックして、New HPE Objectを選択します。
3. 新しいオブジェクトの作成ダイアログボックスで、デバイスを選択します。
4. Nameボックスに該当する名前を入力します。

   この例では、iLOデバイスのDNSホスト名**rib-email-server**がLights-Out Managementオブジェクト名として使用されます。
5. OKをクリックします。

Roles組織ユニットの作成およびロールオブジェクトの追加

手順

1. Rolesという組織単位を作成します。
2. Roles組織単位を右クリックし、New HPE Objectを選択します。
3. 新しい管理オブジェクトの作成ダイアログボックスで、役割を選択します。
4. Nameボックスに該当する名前を入力します。

   この例では、ロールには、リモートサーバーの管理を行うことのできる信頼されるユーザーを所属させるので、**remoteAdmins**と名付けます。
5. OKをクリックします。
6. 手順を繰り返して、リモートサーバーの監視を行う**remoteMonitors**という名前のロールを作成します。

ロールへの権限の割り当てとロールのユーザーおよびデバイスへの関連付け

手順

1. testdomain.localドメインのRoles組織単位のremoteAdminsロールを右クリックして、Propertiesを選択します。
2. remoteAdmins Propertiesダイアログボックスで、HPE Devicesタブをクリックし、Addをクリックします。

3. Select Usersダイアログボックスで、testdomain.local/iLOsフォルダーに作成したLights-Out Managementオブジェクト**rib-email-server**を入力します。
4. OKをクリックして、Applyをクリックします。
5. Membersタブをクリックし、Addボタンを使用してユーザーを追加します。
6. OKをクリックして、Applyをクリックします。

   これで、デバイスとユーザーが関連付けられます。
7. Lights Out Managementタブをクリックします。

   ロールに所属するすべてのユーザーとグループが、ロールによって管理されるすべてのiLOデバイス上でロールに割り当てられた権限を所有します。
8. 各権限の横のチェックボックスを選択して、適用をクリックします。

   この例では、remoteAdminsロール内のユーザーにiLOの機能へのフルアクセス権限が付与されます。
9. OKをクリックします。
10. remoteMonitorsロールを編集するには、手順を繰り返します。
    a. HPE Devicesタブのリストに、rib-email-serverデバイスを追加します。
    b. MembersタブのremoteMonitorsロールにユーザーを追加します。
    c. Lights Out Managementタブで、Login権限を選択します。

       この権限を設定すると、remoteMonitorsロールのメンバーは、サーバーステータスへのアクセスの認証を受けることができ、サーバーステータスを表示できます。

iLOの構成およびLights-Out Managementオブジェクトとの関連付け

手順

ディレクトリページで、次のような設定を入力します。

```
LOM Object Distinguished Name = cn=rib-email-server,ou=ILOs,dc=testdomain,dc=local Directory User Context 1 = cn=Users,dc=testdomain,dc=local
```

詳しくは

iLOにおけるHPE拡張スキーマディレクトリ設定の構成

ディレクトリサービスによるユーザーログイン

iLOログインページのLogin Nameボックスでは、ディレクトリユーザーとローカルユーザーを受け入れます。

ログイン名の最大長は、ローカルユーザーの場合が39文字、ディレクトリユーザーの場合が127文字です。

LDAPユーザーログインの最大パスワード長は63です。

（ブレードサーバー上の）診断ポート経由で接続すると、Zeroサインインおよびディレクトリユーザーログインがサポートされず、ローカルアカウントを使用する必要があります。

ディレクトリユーザー

次の形式がサポートされています。

- LDAP完全識別名（Active DirectoryとOpenLDAP）

  例：`CN=John Smith,CN=Users,DC=HPE,DC=COM`、または`@HPE.com`

ログイン名の短い形式は、アクセスしようとしているドメインをディレクトリに通知しません。ドメイン名を入力するか、またはアカウントのLDAP DNを使用します。

- `ドメイン\ユーザー名` 形式（Active Directory）

  例：`HPE\jsmith`

- `ユーザー名@ドメイン` 形式（Active Directory）
  例：`jsmith@hpe.com`

  @検索可能形式を使用して指定されるディレクトリユーザーは、3つの検索可能コンテキストのいずれかに配置できます。このコンテキストは、ディレクトリページで構成します。

- ユーザー名形式（Active Directory）

  例：John Smith

  ユーザー名形式を使用して指定されるディレクトリユーザーは、3つの検索可能コンテキストのいずれかに配置できます。このコンテキストは、ディレクトリページで構成します。

ローカルユーザー

iLOローカルユーザーアカウントのログイン名を入力します。

一度に複数のiLOシステムを構成するためのツール

Kerberos認証およびディレクトリサービスに多数のLOMオブジェクトを構成すると時間がかかります。次のユーティリティを使用すると、一度に複数のLOMオブジェクトを構成できます。

ProLiant管理プロセッサー用のディレクトリサポート

このソフトウェアには、多数の管理プロセッサーを使用したKerberos認証およびディレクトリサービスを構成する段階的なアプローチを提供するGUIが含まれています。Hewlett Packard Enterpriseは、複数の管理プロセッサーを構成するときに、このツールを使用することをおすすめします。

従来のインポートユーティリティ

LDIFDEやNDS Import/Export Wizardなどのツールを熟知している管理者は、これらのユーティリティを使用して、LOMデバイスディレクトリオブジェクトをインポートまたは作成できます。管理者はデバイスを手動で構成する必要がありますが、いつでもこの構成を行うことができます。プログラマチックインターフェイスまたはスクリプティングインターフェイスを使用して、LOMデバイスオブジェクトをユーザーオブジェクトや他のオブジェクトと同じように作成できます。LOMオブジェクトを作成する際の属性や属性データフォーマットについては、ディレクトリサービススキーマを参照してください。

詳しくは

ProLiant管理プロセッサー用のディレクトリサポート（HPLOMIG）
HPLOMIGによるディレクトリ認証の設定
ディレクトリサービススキーマ

ProLiant管理プロセッサー用のディレクトリサポート（HPLOMIG）

HPLOMIGは、iLOプロセッサーをディレクトリによる管理に簡単に移行したいお客様向けです。このソフトウェアは、管理プロセッサーがディレクトリサービスをサポートするために必要な手順の一部を自動化します。

HPLOMIGは、次のWebサイトで入手できます。**https://www.hpe.com/support/ilo6**

オペレーティングシステムのサポート

HPLOMIGは、Microsoft Windowsで動作し、Microsoft .NET Frameworkバージョン3.5以降を必要とします。次のオペレーティングシステムがサポートされています。

- Microsoft Windows Server 2019

- Microsoft Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

要件

拡張セキュリティ機能（FIPS、CNSA、または高セキュリティセキュリティ状態など）をHPLOMIGを使用してiLOシステムで構成できるようになっている場合、HPLOMIGクライアントは以下の要件を満たす必要があります。

- Windows .NET Framework v4.5がインストールされている。
- オペレーティングシステムでTLS v1.1またはv1.2がサポートされている。

HPLOMIGを使用する場合のOSおよびWindows .NET Frameworkの要件を次の表に示します。

オペレーティングシステム	Windows .NET Framework	iLOで本番環境セキュリティ状態が有効になっているHPLOMIG。	iLOで高セキュリティ、FIPS、またはCNSAセキュリティ状態が有効になっているHPLOMIG。
Windows Server 2008[1]	4.0またはそれ以前	サポート	未サポート
	4.5	サポート	未サポート
Windows 7 Windows Server 2008 R2	4.0またはそれ以前	サポート	未サポート
	4.5	サポート	サポート
Windows 8 Windows 8.1 Windows 10 Windows Server 2012 Windows Server 2012 R2 Microsoft Windows Server 2016 Microsoft Windows Server 2019	4.0またはそれ以前	サポート	未サポート
	4.5	サポート	サポート

1 NET Frameworkバージョン4.5がインストールされている場合でも、Windows Server 2008では、TLS v1.1またはv1.2はサポートされません。

HPLOMIGによるディレクトリ認証の設定

手順

1. ネットワーク内のiLOマネジメントプロセッサーを検出します。
2. （オプション）マネジメントプロセッサーでiLOファームウェアをアップデートします。
3. ディレクトリ構成設定を指定します。
4. ご使用の構成に固有の手順を完了します。
   a. マネジメントプロセッサーに名前を付けます（HPE拡張スキーマのみ）
   b. ディレクトリを構成します（HPE拡張スキーマのみ）
   c. デフォルトスキーマを使用するようにマネジメントプロセッサーを設定します（スキーマフリーのみ）
5. iLOとディレクトリの間の通信を設定します。
6. LDAP CA証明書をインポートします。
7. （オプション）iLOディレクトリテストを実行します。

サブトピック

マネジメントプロセッサーの検出

（オプション）管理プロセッサーのファームウェアのアップグレード（HPLOMIG）

ディレクトリ構成オプションの選択

マネジメントプロセッサーの命名（HPE拡張スキーマのみ）

HPE拡張スキーマを選択したときのディレクトリの設定

管理プロセッサーの設定（スキーマフリー構成のみ）

ディレクトリ用のマネジメントプロセッサーのセットアップ

LDAP CA証明書のインポート

（オプション）HPLOMIGを使用したディレクトリテストの実行

マネジメントプロセッサーの検出

手順

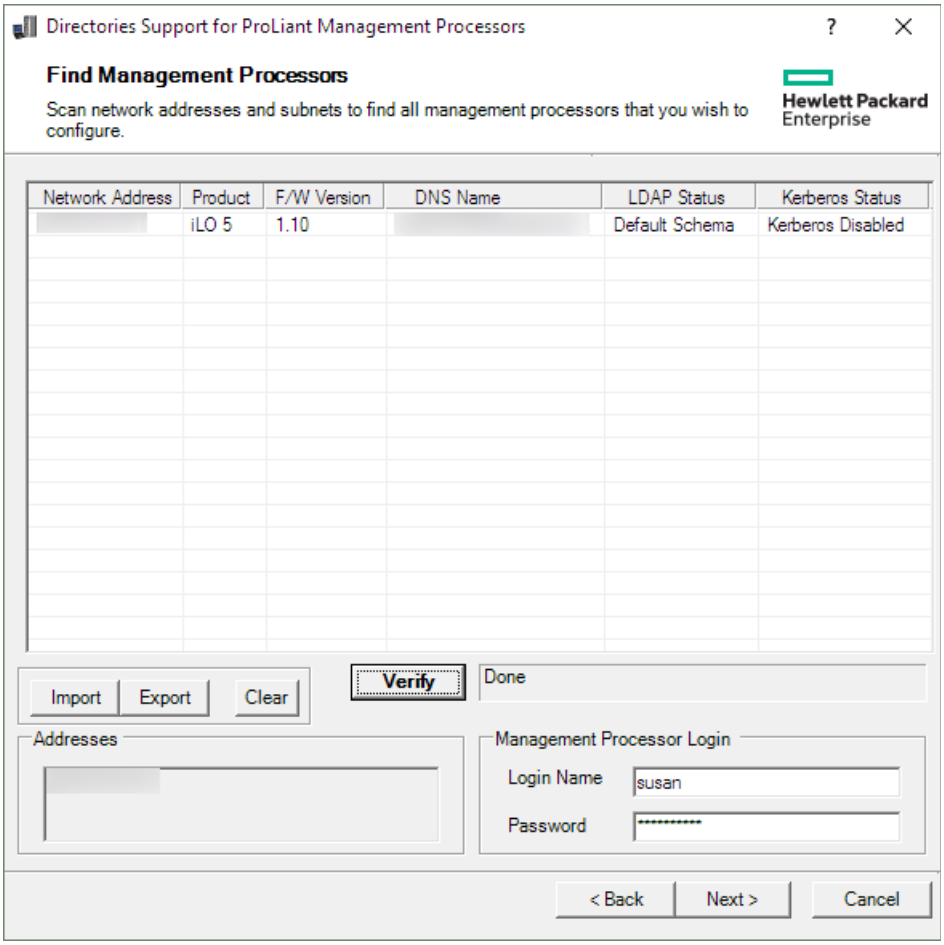
1. スタート > すべてのプログラム > Hewlett-Packard Enterprise > ProLiantマネジメントプロセッサー用のディレクトリサポートの順に選択します。
2. ようこそページで、Nextをクリックします。
3. Find Management Processorsウィンドウで、Addressesボックスに、マネジメントプロセッサーの検索条件を入力します。

   ヒント:
   また、Importをクリックしてからファイルを選択して、ファイルからマネジメントプロセッサーのリストを入力することもできます。

4. iLOのLogin NameとPasswordを入力して、Findをクリックします。

検出時に次へやBackをクリックするかユーティリティを終了すると、現在のネットワークアドレスでの作業は完了しますが、次のネットワークアドレスでの作業はキャンセルされます。

検索が完了すると、マネジメントプロセッサーが表示され、FindボタンがVerifyに変化します。



サブトピック

HPLOMIG管理プロセッサーの検索条件

HPLOMIGマネジメントプロセッサーのインポートリストの要件

HPLOMIG管理プロセッサーの検索条件

DNS名、IPアドレス、またはIPアドレスワイルドカードを使用して管理プロセッサーを検索することができます。

Addressesボックスに値を入力する場合、以下のルールが適用されます。

- DNS名、IPアドレス、およびIPアドレスワイルドカードは、セミコロンまたはカンマのいずれかで区切る必要があり、区切り文字として両方を使用することはできません。
- IPアドレスワイルドカードでは、3番目と4番目のオクテットフィールドでアスタリスク（*）文字を使用します。たとえば、`16.100.*.*`というIPアドレスは有効ですが、`16.*.*.*`というIPアドレスは無効です。
- ハイフンを使用して範囲を指定することができます。たとえば、`192.168.0.2-10`は有効な範囲です。ハイフンは、一番右のオクテットフィールドでのみ使用できます。
- Findをクリックすると、HPLOMIGは、pingとポート443（デフォルトSSLポート）への接続を開始します。この動作の目的は、ターゲットネットワークアドレスが管理プロセッサーであるかどうかを判定することです。pingに対するデバイスからの応答がなく、ポート443に適切に接続できなかった場合、ユーティリティは、ターゲットが管理プロセッサーではないと判定します。

HPLOMIGマネジメントプロセッサーのインポートリストの要件

各行に1つのマネジメントプロセッサーを記載した単純なテキストファイルをインポートできます。

セミコロンで区切られた、サポートされる各列は次のとおりです。

- Network Address
- Product
- F/W Version
- DNS Name
- TPM Status
- User Name
- Password
- LDAP Status
- Kerberos Status
- License Type
- FIPS Status

例えば、テキストファイルのある行に次の情報が含まれる場合があります。

```
16.100.225.20;iLO;1.10;ILOTPILOT2210;Not Present;user;password;Default
Schema;Kerberos Disabled;iLO Advanced;Enabled
```

ユーザー名とパスワードを（セキュリティ上の理由で）ファイル内に含めることができない場合は、それらの列を空白にして、セミコロンだけを入れてください。

（オプション）管理プロセッサーのファームウェアのアップグレード（HPLOMIG）

前提条件

管理プロセッサーのファームウェアのバイナリイメージは、HPLOMIGを実行しているシステムからアクセスできる必要があります。これらのバイナリイメージは**https://www.hpe.com/support/ilo6**からダウンロードできます。

このタスクについて

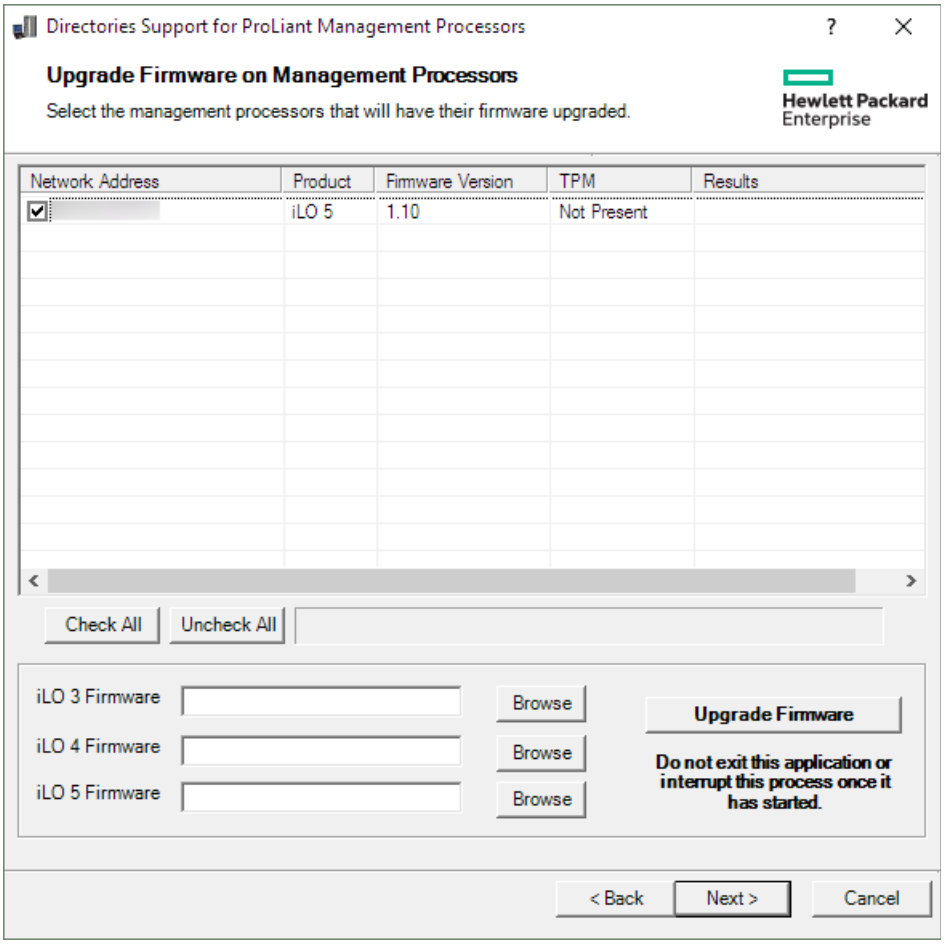
Find Management Processorsウィンドウの次へをクリックしたら、次のタスクは、必要に応じてiLOファームウェアをアップデートすることです。選択した管理プロセッサーの数によっては、アップグレードプロセスに長い時間がかかる場合があります。単一の管理プロセッサーのファームウェアアップグレードは、約5分で完了します。

重要:

Hewlett Packard Enterpriseは、本番環境ネットワークでHPLOMIGを実行する前に、テスト環境でアップグレードプロセスをテストし、結果を確認することをおすすめします。管理プロセッサーへのファームウェアイメージの不完全な転送によって、管理プロセッサーをローカルで再プログラミングしなければならなくなる場合があります。

手順

1. Upgrade Firmware on Management Processorsウィンドウがまだ開いていない場合は移動します。



2. アップグレードするマネジメントプロセッサーを選択します。
3. 選択した管理プロセッサーごとに、参照をクリックし、ファームウェアイメージファイルを選択します。また、手動でファームウェアイメージのパスを入力することもできます。
4. ファームウェアのアップグレードをクリックします。

   ファームウェアアップグレードプロセス時は、すべてのボタンが非アクティブになり、操作できません。

   選択したマネジメントプロセッサーがアップグレードされます。HPLOMIGを使用すると、数百の管理プロセッサーをアップグレードできますが、同時にアップグレードできるのは最大25の管理プロセッサーです。このプロセス時には、大量のネットワーク動作が発生します。

   アップグレードに失敗すると、Results欄にメッセージが表示され、ユーティリティは、選択された他の管理プロセッサーのアップグレードを継続します。
5. アップグレードが完了したら、Nextをクリックします。

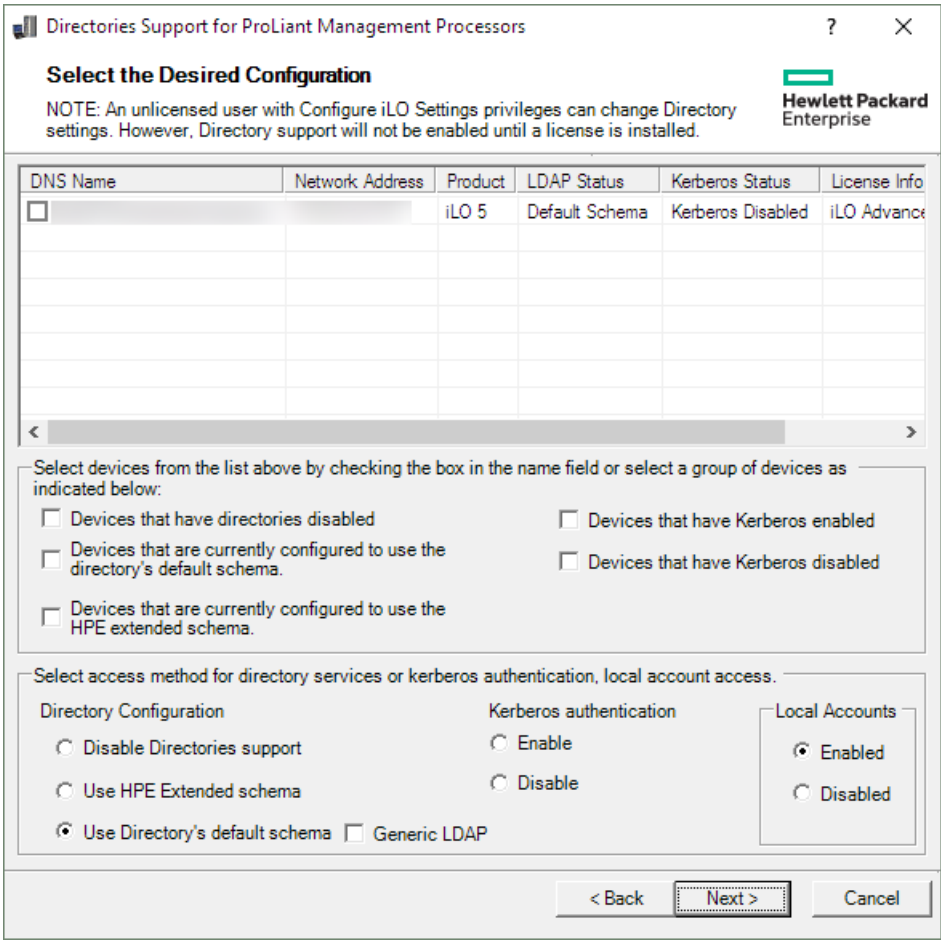
ディレクトリ構成オプションの選択

このタスクについて

Upgrade Firmware on Management Processorsウィンドウで次へをクリックした後の次のタスクは、構成する管理プロセッサーの選択と有効にするディレクトリオプションの指定です。

手順

1. Select the Desired Configurationウィンドウに移動します（開いていない場合）。



2. 構成するiLO管理プロセッサーを選択します。
3. （オプション）選択フィルターを使用して、Kerberos認証またはディレクトリサービス用にすでに構成されているiLO管理プロセッサーを除外します。Kerberos認証とディレクトリサービスが無効になっている管理プロセッサーを除外することもできます。
4. Directory Configuration、Kerberos authentication、およびLocal accountsセクションで、ディレクトリ、Kerberos、およびローカルアカウントの設定を選択します。
5. 次へをクリックします。

   このページでの選択によって、次へをクリックしたときに表示されるウィンドウが決まります。
6. スキーマフリー構成を選択した場合は、管理プロセッサーの設定（スキーマフリー構成のみ）に進みます。HPE拡張スキーマ構成を選択した場合は、マネジメントプロセッサーの命名（HPE拡張スキーマのみ）を続行します。

サブトピック

管理プロセッサーの選択方法

ディレクトリアクセス方法および設定

管理プロセッサーの選択方法

次の方法で構成するiLO管理プロセッサーを選択します。

- 構成するリスト内の各管理プロセッサーの横のチェックボックスをクリックします。
- 特定のステータスに一致するiLO管理プロセッサーを選択するには、次のいずれかのフィルターの横にあるチェックボックスをクリックします。

- Devices that have directories disabled
- Devices that are currently configured to use the directory’s default schema
- Devices that are currently configured to use the HPE Extended Schema
- Devices that have Kerberos enabled
- Devices that have Kerberos disabled

ディレクトリアクセス方法および設定

- Disable Directories support – 選択したシステムでディレクトリサポートを無効にします。
- Use HPE Extended Schema – 選択したシステムのディレクトリでHPE拡張スキーマを使用します。
- Use Directory’s default schema – 選択したシステムでスキーマフリーディレクトリを使用します。
- Generic LDAP – 選択したシステムでOpenLDAPがサポートするBIND方式を使用します。
- Kerberos authentication – 選択したシステムでKerberos認証を有効または無効にします。
- Local Accounts – 選択したシステムでローカルユーザーアカウントを有効または無効にします。

マネジメントプロセッサーの命名（HPE拡張スキーマのみ）

このタスクについて

Select the Desired Configurationウィンドウの次へをクリックしたら、次のタスクはディレクトリ内のiLO管理デバイスオブジェクトに名前を付けることです。

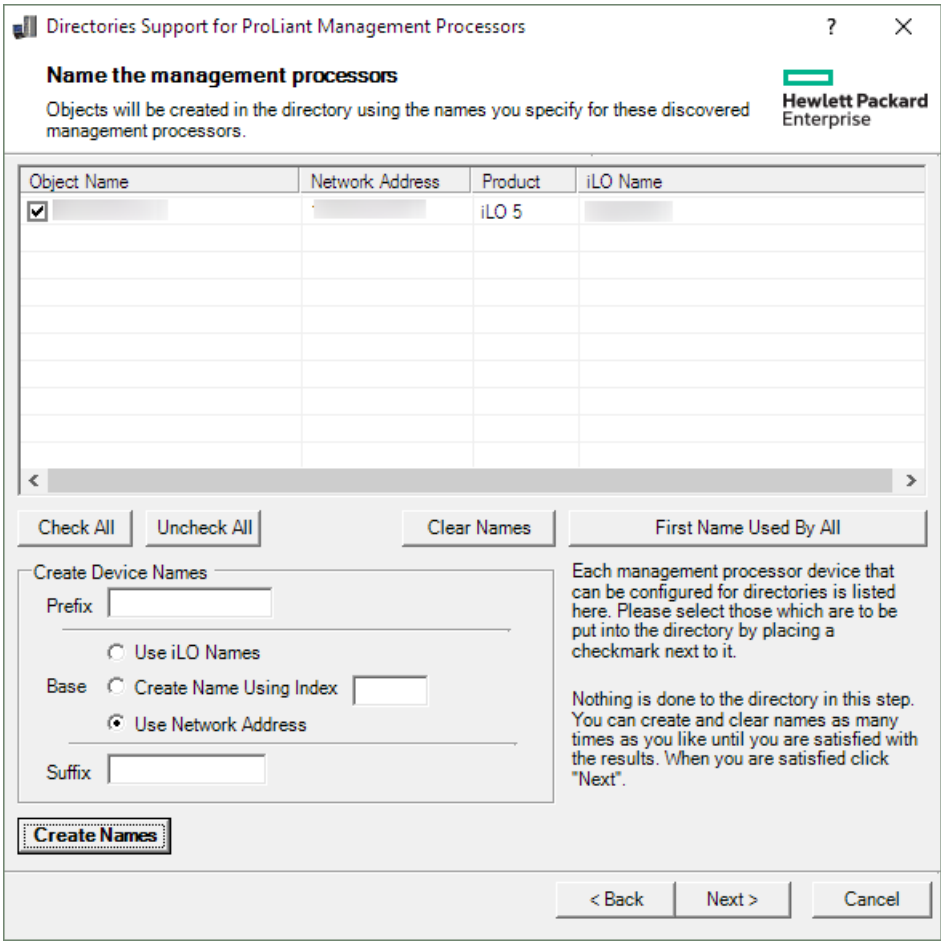
以下の1つまたは複数のコンポーネントを使用して名前を作成できます。

- ネットワークアドレス
- DNS名
- インデックス
- 名前の手動作成
- すべてにプレフィクスを追加
- すべてにサフィックスを追加

マネジメントプロセッサーに名前を付けるには、Object Name列をクリックして名前を入力するか、以下の手順に従ってください。

手順

1. Use iLO Names、Create Name Using Index、またはUse Network Addressを選択します。
2. （オプション）すべての名前の先頭または末尾に追加するテキストを入力します。
3. Create Namesをクリックします。



生成された名前がObject Name欄に表示されます。この時点では、名前は、ディレクトリやマネジメントプロセッサーに書き込まれていません。名前は、次のProLiantマネジメントプロセッサー用のディレクトリサポートウィンドウが表示されるまで保存されます。

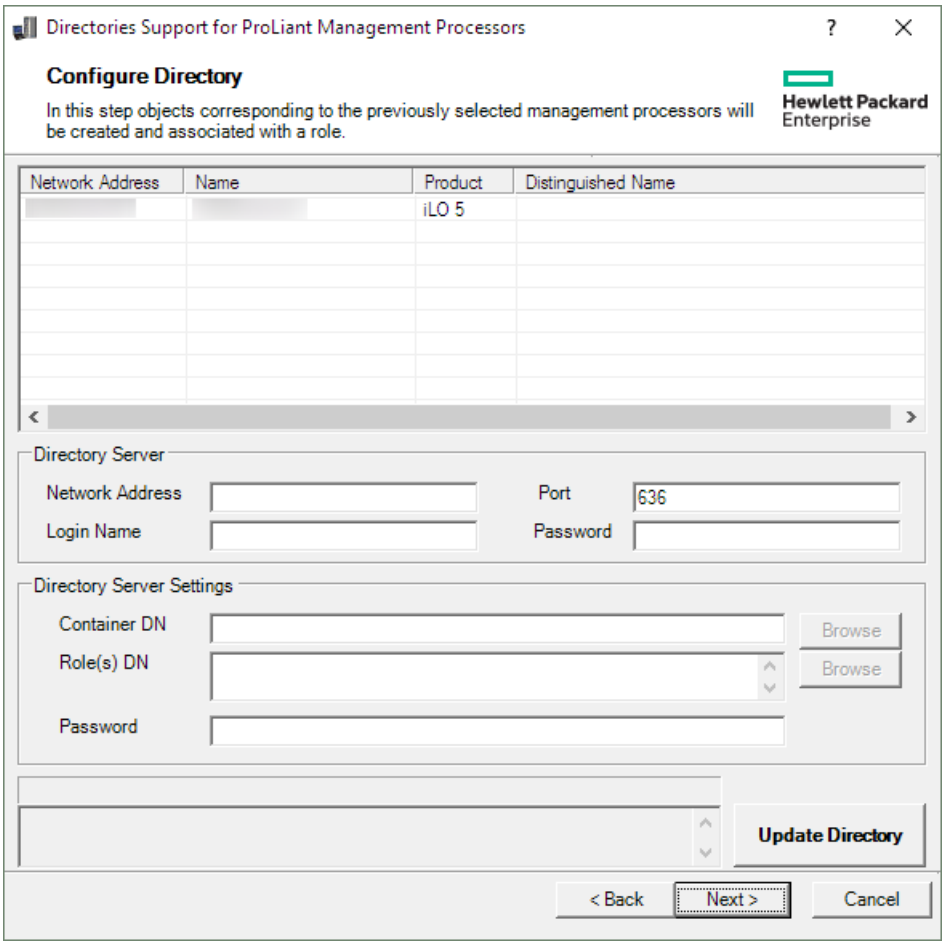
4. （オプション）名前を変更するには、Clear Namesをクリックしてマネジメントプロセッサーの名前を修正します。
5. 名前が正しい場合は、 Nextをクリックします。

   Configure Directoryウィンドウが開きます。 HPE拡張スキーマを選択したときのディレクトリの設定に進みます。

HPE拡張スキーマを選択したときのディレクトリの設定

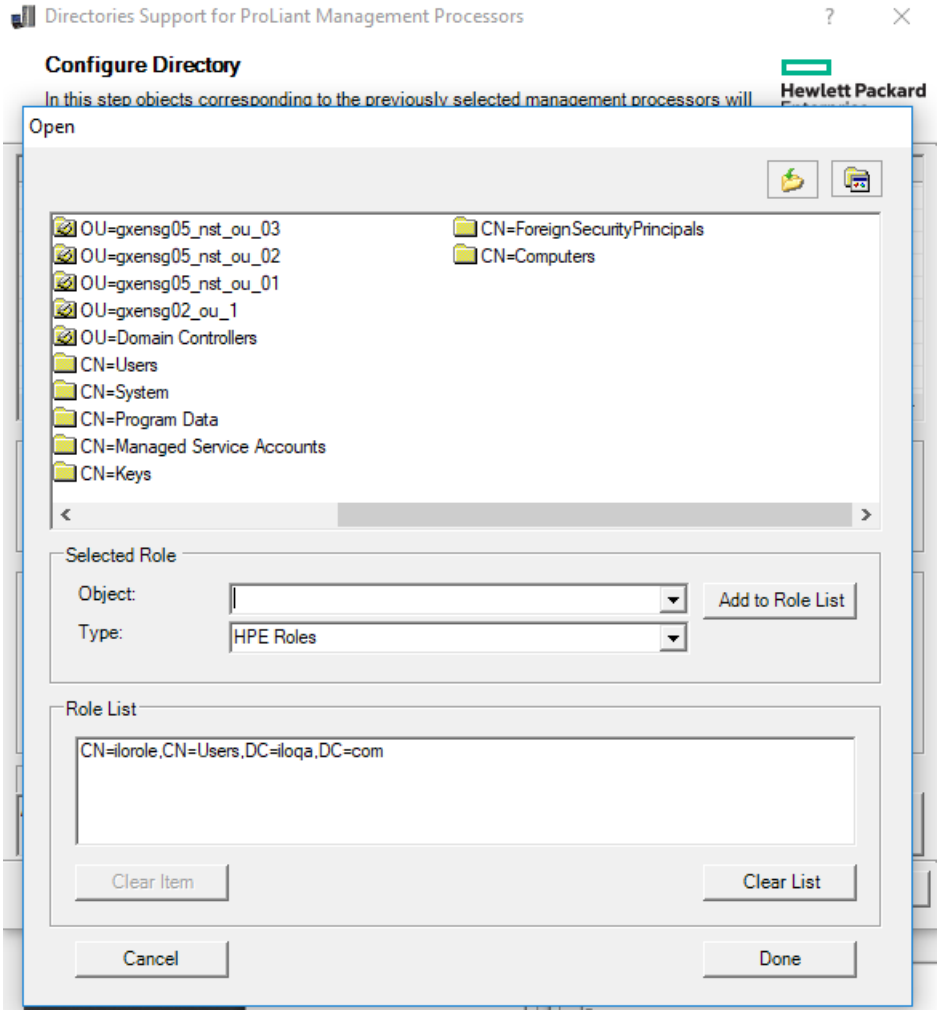
このタスクについて

Name the management processorsウィンドウでNextをクリックした後、Configure Directoryウィンドウでは、検出された各マネジメントプロセッサー用のデバイスオブジェクトを作成し、新しいデバイスオブジェクトを定義済みのロールに関連付けることができます。例えば、ディレクトリは、ユーザーを、特定のデバイスオブジェクトに対するいくつかの権限を持つロール（管理者など）のメンバーとして定義します。

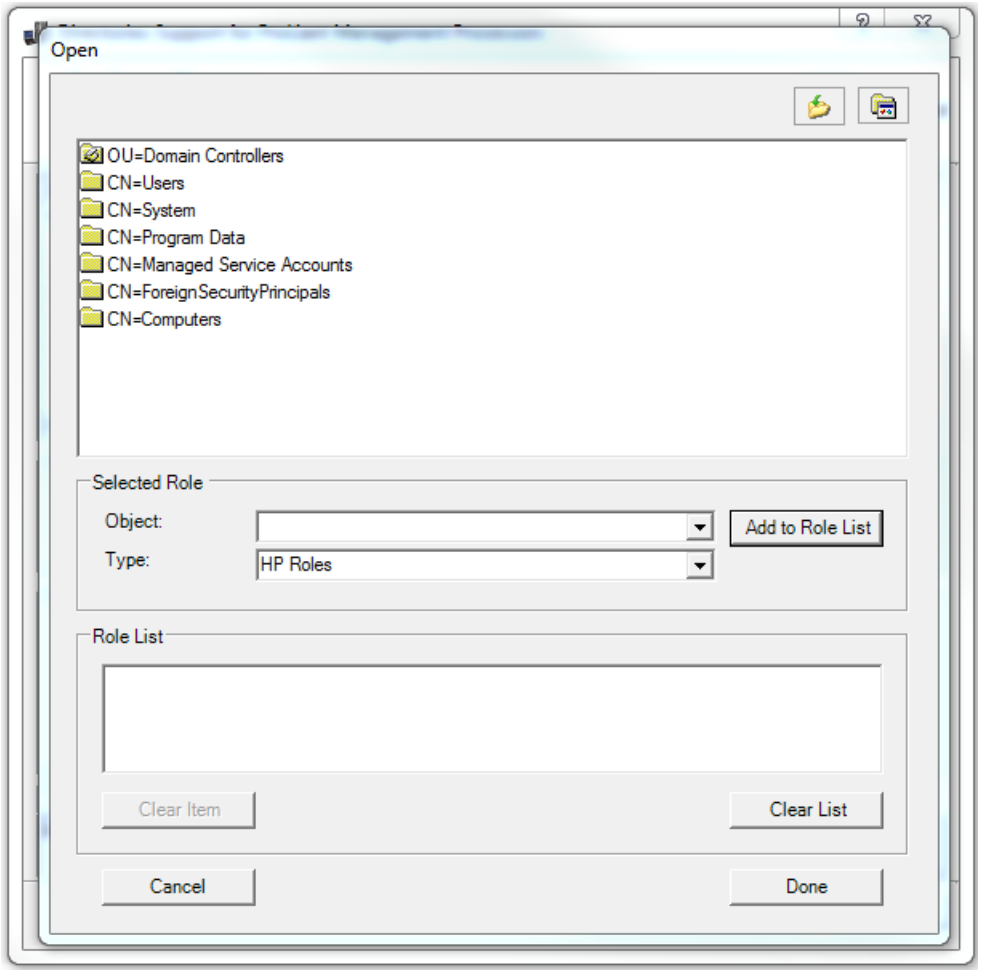


手順

1. Directory Serverセクションで、指定されたディレクトリサーバーのNetwork Address、Login Name、およびPasswordを入力します。
2. Container DNの値を入力するか、Browseをクリックしてコンテナーを選択します。



3. Role(s) DNの値を入力するか、Browseをクリックしてロール DNを選択します。

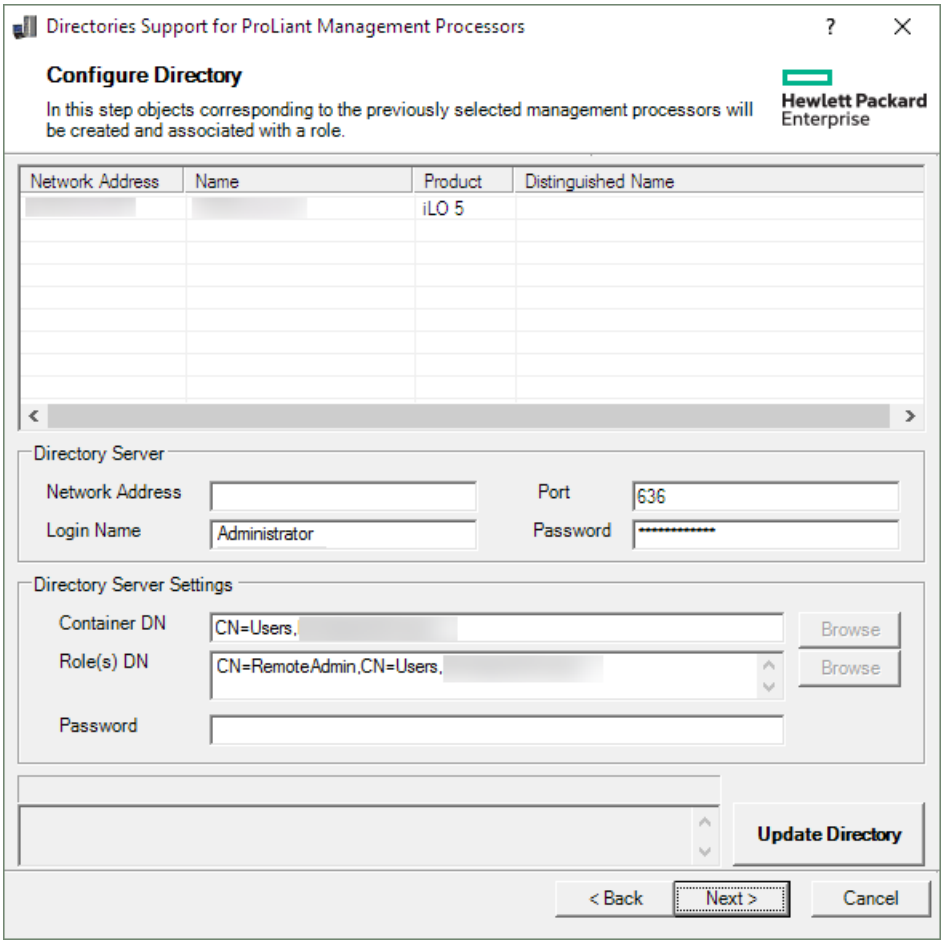


4. Update Directoryをクリックします。

   HPLOMIGは、ディレクトリに接続し、マネジメントプロセッサーオブジェクトを作成して、それらを選択されたロールに追加します。

5. デバイスオブジェクトがロールに関連付けられたら、Nextをクリックします。

   入力した値は、Configure Directoryウィンドウに表示されます。



6. 次へをクリックします。

   Set up Management Processors for Directoriesウィンドウが開きます。

7. ディレクトリ用のマネジメントプロセッサーのセットアップに進みます。

サブトピック

Configure Directoryウィンドウのオプション

Configure Directoryウィンドウのオプション

Configure Directoryウィンドウには以下のボックスがあります。

- Network Address - ディレクトリサーバーのネットワークアドレス（有効なDNS名またはIPアドレス）です。
- Port - ディレクトリへのSSLポートです。デフォルトポートは636です。マネジメントプロセッサーは、SSLを使用してのみディレクトリと通信できます。
- Login NameおよびPassword - ディレクトリへのドメイン管理者アクセスを持つアカウントのログイン名とパスワードを入力します。
- Container DN - ネットワークアドレス、ポート、およびログイン情報を入力したら、Browseをクリックして、コンテナーDNを検索できます。コンテナーとは、マイグレーションユーティリティがディレクトリ内のマネジメントプロセッサーオブジェクトを作成する場所です。
- Role(s) DN - ネットワークアドレス、ポート、およびログイン情報を入力したら、Browseをクリックして、ロールDNを検索できます。ロールとは、デバイスオブジェクトに関連付けられるロールが存在する場所です。ロールは、このユーティリティの実行前に作成する必要があります。

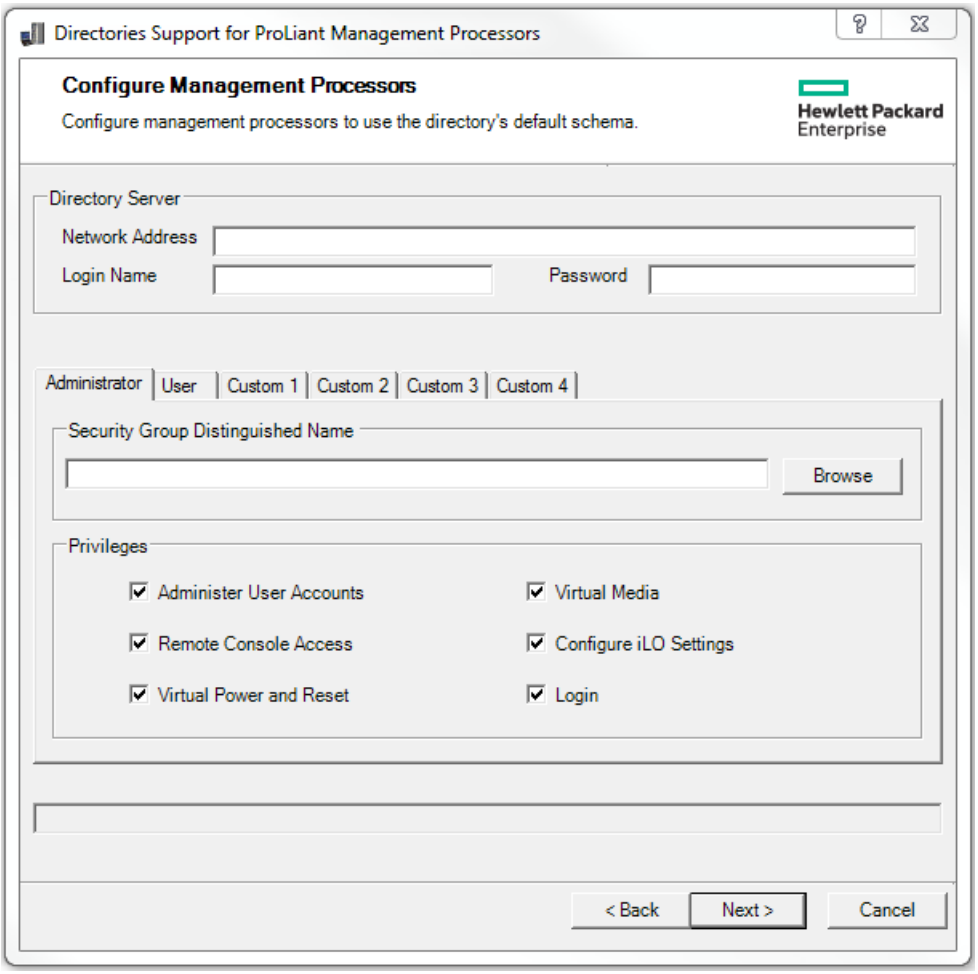
管理プロセッサーの設定（スキーマフリー構成のみ）

このタスクについて

Select the Desired Configurationウィンドウで Nextをクリックした後、次のタスクは、選択したマネジメントプロセッサーをデフォルトのディレクトリスキーマを使用するように設定することです。

手順

1. Configure Management Processorsウィンドウがまだ開いていない場合は、そのウィンドウに移動します。



2. ディレクトリサーバー設定を入力します。
3. セキュリティグループDNを入力します。
4. セキュリティグループと関連付けるiLO権限を選択します。
5. 次へをクリックします。

   Set up Management Processors for Directoriesウィンドウが開きます。
6. ディレクトリ用のマネジメントプロセッサーのセットアップに進みます。

サブトピック

管理プロセッサー設定

管理プロセッサー設定

- Network Address – ディレクトリサーバーのネットワークアドレス（有効なDNS名またはIPアドレス）です。
- Login NameおよびPassword – ディレクトリへのドメイン管理者アクセスを持つアカウントのログイン名（DN）とパスワードを入力します。
- Security Group Distinguished Name – 共通の権限を持つ一連のiLOユーザーを含むディレクトリ内のグループのDNです。ディレクトリ名、ログイン名、およびパスワードが正しい場合は、Browseをクリックしてグループにアクセスし、選択することができます。
- Privileges – 選択されたグループに関連付けられたiLO権限です。ユーザーがグループのメンバーである場合は、ログイン権限が暗黙に設定されています。

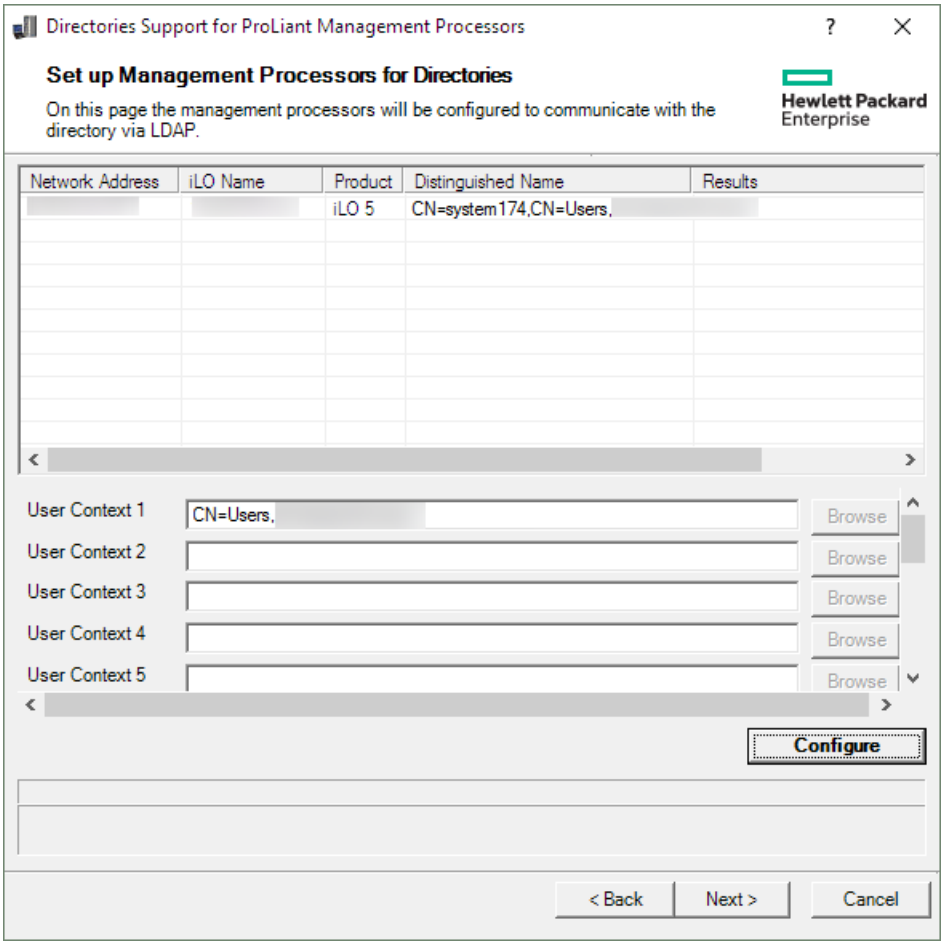
ディレクトリ用のマネジメントプロセッサーのセットアップ

このタスクについて

Configure DirectoryまたはConfigure Management Processorsウィンドウで Nextをクリックした後の次の手順は、ディレクトリと通信するマネジメントプロセッサーのセットアップです。

手順

1. Set up Management Processors for Directoriesウィンドウがまだ開いていない場合は、そのウィンドウに移動します。
2. ユーザーコンテキストを定義します。



ユーザーコンテキストは、iLOにログインするユーザーのLDAP構造内の位置を定義します。User Contextボックス組織単位のDNを入力するか、Browseをクリックしてユーザーコンテキストを選択することができます。

最大15個のユーザーコンテキストがサポートされています。

3. 構成をクリックします。
4. プロセスが完了したら、Nextをクリックします。

   LDAP CA Certificate Importウィンドウが開きます。
5. LDAP CA証明書のインポートに進みます。

詳しくは

ディレクトリユーザーコンテキスト

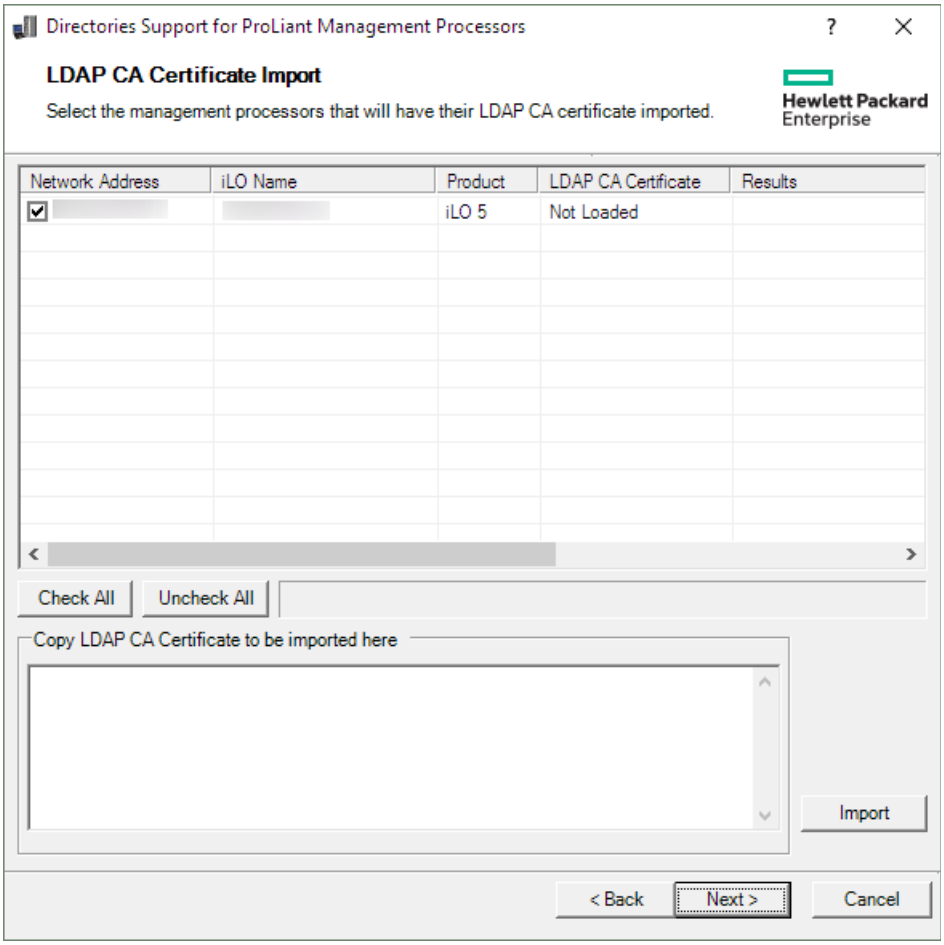
LDAP CA証明書のインポート

このタスクについて

Set up Management Processors for Directoriesで次へをクリックしたら、次の手順はLDAP CA証明書をインポートすることです。

手順

1. LDAP CA Certificate Importウィンドウがまだ開いていなければ、移動します。



2. 証明書をインポートする対象のiLOシステムを選択します。
3. テキストボックスに証明書を貼り付け、インポートをクリックします。
4. 証明書のインポートが完了したら、次へをクリックします。

   ディレクトリテストウィンドウが開きます。

5. （オプション）HPLOMIGを使用したディレクトリテストの実行に進みます。

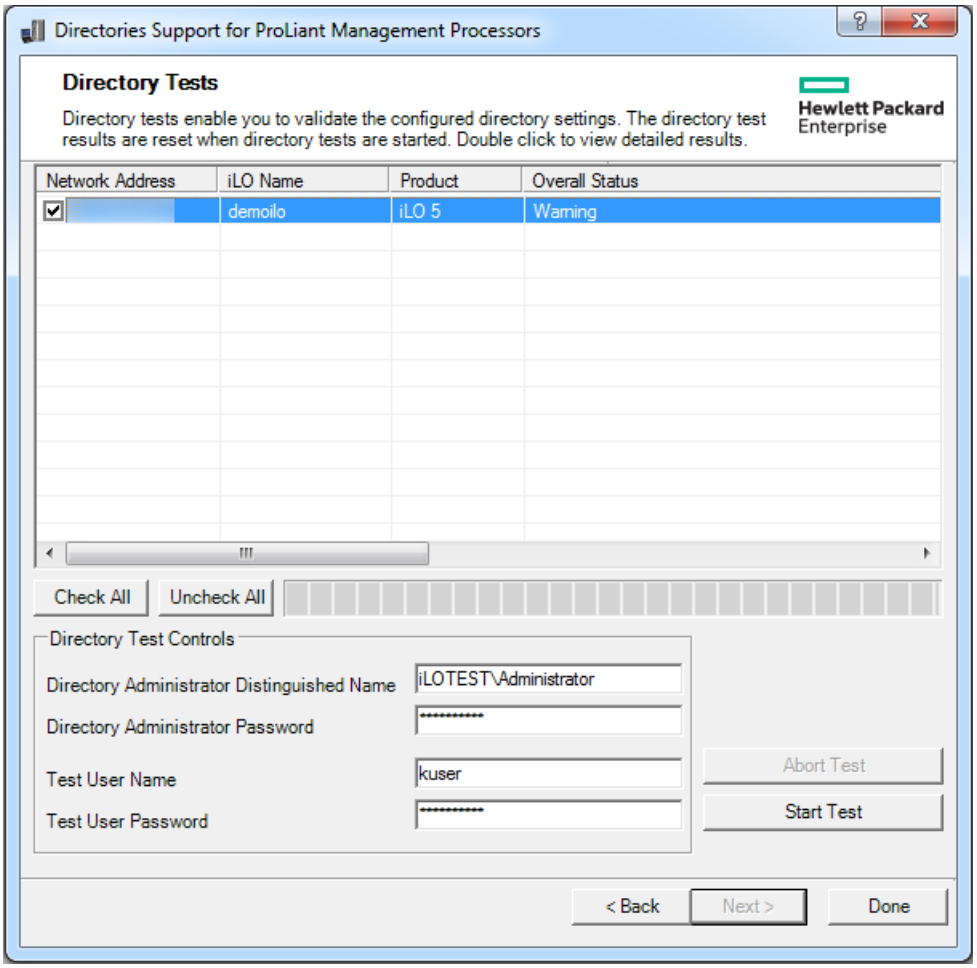
（オプション）HPLOMIGを使用したディレクトリテストの実行

このタスクについて

LDAP CA Certificate Importで次へをクリックした後の次の手順は、ディレクトリ構成のテストです。

手順

1. ディレクトリテストウィンドウに移動します（開いていない場合）。



2. ディレクトリ設定をテストします。
   a. 1つまたは複数のiLOシステムを選択します。
   b. ディレクトリテスト制御セクションで、以下を入力します。
      - ディレクトリ管理者識別名およびディレクトリ管理者パスワード - iLOオブジェクト、ロール、および検索コンテキストについてディレクトリを検索します。このユーザーは、ディレクトリ読み取り権限を持っている必要があります。

        Hewlett Packard Enterpriseでは、ディレクトリ内にiLOオブジェクトを作成する際に使用するものと同じ識別名とパスワードを使用することをおすすめします。これらの識別情報は、iLOに保存されるものではなく、iLOオブジェクトとユーザー検索コンテキストを確認するために使用されます。

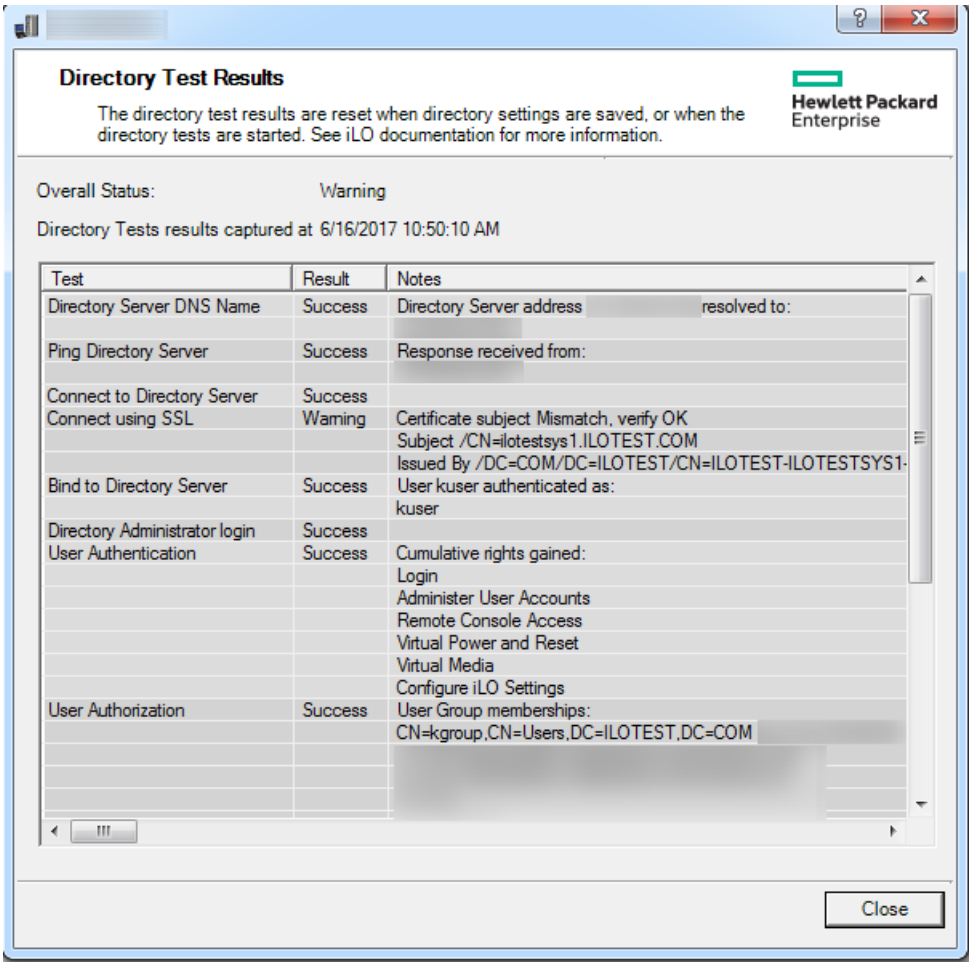
      - テストユーザー名およびテストユーザーパスワード - iLOへのログインとアクセス権をテストします。ユーザー検索コンテキストを適用できるため、ユーザー名は完全修飾である必要はありません。このユーザーは、このiLOのロールに関連付けられている必要があります。

通常、このアカウントは、テスト対象のiLOプロセッサーへのアクセスに利用します。これはディレクトリ管理者アカウントでも構いませんが、スーパーユーザーアカウントではテストでユーザー認証を検証できません。iLOには、これらの認証情報が保存されません。

c. テストの開始をクリックします。

複数のテストがバックグラウンドで開始します。最初のテストでは、サーバーとのSSL接続を確立し、ユーザー権限を評価して、ネットワーク経由でのディレクトリユーザーに対するネットワークPingが実行されます。

3. 個々のテスト結果を表示するには、iLOシステムをダブルクリックします。



詳しくは、ディレクトリテストの実行を参照してください。

4. 完了をクリックします。

ディレクトリサービススキーマ

ディレクトリサービススキーマでは、Hewlett Packard Enterprise Lights-Outマネジメント権限付与データをディレクトリサービスに保存するために使用されるクラスおよび属性について説明します。

サブトピック

HPE ManagementコアLDAP OIDクラスおよび属性

コアクラスの定義

コア属性の定義

Lights-Out Management固有のLDAP OIDクラスおよび属性

HPE ManagementコアLDAP OIDクラスおよび属性

スキーマのセットアッププロセスでスキーマに加える変更には、次の変更が含まれます。

- コアクラス
- コア属性

コアクラス

クラス名	割り当てられるOID
hpqTarget	1.3.6.1.4.1.232.1001.1.1.1.1
hpqRole	1.3.6.1.4.1.232.1001.1.1.1.2
hpqPolicy	1.3.6.1.4.1.232.1001.1.1.1.3

コア属性

属性名	割り当てられるOID
hpqPolicyDN	1.3.6.1.4.1.232.1001.1.1.2.1
hpqRoleMembership	1.3.6.1.4.1.232.1001.1.1.2.2
hpqTargetMembership	1.3.6.1.4.1.232.1001.1.1.2.3
hpqRoleIPRestrictionDefault	1.3.6.1.4.1.232.1001.1.1.2.4
hpqRoleIPRestrictions	1.3.6.1.4.1.232.1001.1.1.2.5
hpqRoleTimeRestriction	1.3.6.1.4.1.232.1001.1.1.2.6

コアクラスの定義

以下の表に、Hewlett Packard Enterprise Managementコアクラスの定義を示します。

hpqTarget

OID	1.3.6.1.4.1.232.1001.1.1.1.1
説明	このクラスは、ターゲットオブジェクトを定義し、ディレクトリ対応管理を使用するHewlett Packard Enterprise製品の基礎を提供します。
クラスのタイプ	Structural
スーパークラス	user
属性	hpqPolicyDN - 1.3.6.1.4.1.232.1001.1.1.2.1 hpqRoleMembership - 1.3.6.1.4.1.232.1001.1.1.2.2
注意事項	なし

hpqRole

OID	1.3.6.1.4.1.232.1001.1.1.1.2
説明	このクラスは、ロールオブジェクトを定義し、ディレクトリ対応管理を使用するHewlett Packard Enterprise製品の基礎を提供します。
クラスのタイプ	Structural
スーパークラス	group
属性	hpqRoleIPRestrictions - 1.3.6.1.4.1.232.1001.1.1.2.5 hpqRoleIPRestrictionDefault - 1.3.6.1.4.1.232.1001.1.1.2.4 hpqRoleTimeRestriction - 1.3.6.1.4.1.232.1001.1.1.2.6 hpqTargetMembership - 1.3.6.1.4.1.232.1001.1.1.2.3
注意事項	なし

hpqPolicy

OID	1.3.6.1.4.1.232.1001.1.1.1.3
説明	このクラスは、ポリシーオブジェクトを定義し、ディレクトリ対応管理を使用するHewlett Packard Enterprise製品の基礎を提供します。
クラスのタイプ	Structural
スーパークラス	top
属性	hpqPolicyDN - 1.3.6.1.4.1.232.1001.1.1.2.1
注意事項	なし

コア属性の定義

以下の表に、HPE Managementコアクラス属性の定義を示します。

hpqPolicyDN

OID	1.3.6.1.4.1.232.1001.1.1.2.1
説明	このターゲットの一般設定を制御するポリシーの識別名です。
構文	識別名 - 1.3.6.1.4.1.1466.115.121.1.12
オプション	単一値
注意事項	なし

hpqRoleMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.2
説明	このオブジェクトに所属するhpqRoleオブジェクトのリストを提供します。
構文	識別名 - 1.3.6.1.4.1.1466.115.121.1.12
オプション	複数値
注意事項	なし

hpqTargetMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.3
説明	このオブジェクトに所属するhpqTargetオブジェクトのリストを提供します。
構文	識別名 - 1.3.6.1.4.1.1466.115.121.1.12
オプション	複数値
注意事項	なし

hpqRoleIPRestrictionDefault

OID	1.3.6.1.4.1.232.1001.1.1.2.4
説明	IPネットワークアドレス制限のもとでの権限の制限を部分的に指定する未指定クライアントによるアクセスを表すBoolean値。
構文	Boolean値 - 1.3.6.1.4.1.1466.115.121.1.7
オプション	単一値
注意事項	この属性が`TRUE`の場合、IP制限が通常のネットワーククライアントに適用されます。この属性が`FALSE`の場合、IP制限が通常のネットワーククライアントに適用されません。

hpqRoleIPRestrictions

OID	1.3.6.1.4.1.232.1001.1.1.2.5
説明	IPネットワークアドレス制限のもとでの権限の制限を部分的に指定するIPアドレス、DNS名、ドメイン、アドレス範囲、およびサブネットのリストを提供します。
構文	オクテット文字列 - 1.3.6.1.4.1.1466.115.121.1.40
オプション	複数値
注意事項	この属性は、ロールオブジェクトについてのみ使用されます。 アドレスが一致し、一般アクセスが拒否される場合、IP制限は適用されます。アドレスが一致し、一般アクセスが許可される場合、IP制限が適用されません。 値には、IDバイトの後にネットワークアドレスを指定する（タイプ別の数の）バイトを続けたものを使用します。 • IPサブネットの場合、IDバイトは<0x01>で、その後にネットワーク順のIPネットワークアドレスとネットワーク順のIPネットワークサブネットマスクを続けます。たとえば、127.0.0.1/255.0.0.0というIPサブネットの場合は、<0x01 0x7F 0x00 0x00 0x01 0xFF 0x00 0x00 0x00>となります。IP範囲の場合、IDバイトは<0x02>で、その後に下限のIPアドレスと上限のIPアドレスを続けます。両方とも範囲に含まれ、ネットワーク順に指定します。たとえば、10.0.0.1～10.0.10.255というIP範囲の場合は、<0x02 0x0A 0x00 0x00 0x01 0x0A 0x00 0x0A 0xFF>となります。 • DNS名またはドメインの場合、IDバイトは<0x03>で、その後にASCIIエンコードのDNS名を続けます。DNS名には、指定された文字列で終了するすべての名前と一致させるために、先頭に*（ASCIIコードでは0x2A）を付けることができます。たとえば、DNSドメイン*.acme.comは、<0x03 0x2A 0x2E 0x61 0x63 0x6D 0x65 0x2E 0x63 0x6F 0x6D>となります。一般アクセスが許可されます。

hpqRoleTimeRestriction

OID	1.3.6.1.4.1.232.1001.1.1.2.6
説明	時間制限のもとでの権限の制限を指定する1週間の時間枠（30分単位）です。
構文	オクテット文字列 {42}-1.3.6.1.4.1.1466.115.121.1.40
オプション	単一値
注意事項	この属性は、ロールオブジェクトについてのみ使用されます。 デバイスがある場所の現在の現地時間に対応するビットが1の場合には、時間制限が適用され、ビットが0の場合には、時間制限が適用されません。 • 最初のバイトの最下位ビットは、日曜日の午前0時から午前0時30分に対応します。 • 最下位ビットよりも上位のビットおよび後続のバイトは、日曜日の午前0時30分以降の、1週間を30分ごとに区切った時間枠に、順番に対応します。 • 42番目のバイトの最上位ビット（8番目）は、土曜日の午後11時30分から日曜日の午前0時に対応します。

Lights-Out Management固有のLDAP OIDクラスおよび属性

以下のスキーマ属性およびクラスは、Hewlett Packard Enterprise Managementコアクラスおよび属性で定義される属性およびクラスに依存する場合があります。

表 1. Lights-Out Managementクラス

クラス名	割り当てられるOID
hpqLOMv100	1.3.6.1.4.1.232.1001.1.8.1.1

Lights-Out Management属性

クラス名	割り当てられるOID
hpqLOMRightLogin	1.3.6.1.4.1.232.1001.1.8.2.3
hpqLOMRightRemoteConsole	1.3.6.1.4.1.232.1001.1.8.2.4
hpqLOMRightVirtualMedia	1.3.6.1.4.1.232.1001.1.8.2.6
hpqLOMRightServerReset	1.3.6.1.4.1.232.1001.1.8.2.5
hpqLOMRightLocalUserAdmin	1.3.6.1.4.1.232.1001.1.8.2.2
hpqLOMRightConfigureSettings	1.3.6.1.4.1.232.1001.1.8.2.1

Lights-Out Managementクラスの定義

以下の表に、Lights-Out Managementコアクラスの定義を示します。

表 1. hpqLOMv100

OID	1.3.6.1.4.1.232.1001.1.8.1.1
説明	このクラスは、HPE Lights-Out Management製品で使用される権限と設定を定義します。
クラスのタイプ	Auxiliary
スーパークラス	なし
属性	hpqLOMRightConfigureSettings - 1.3.6.1.4.1.232.1001.1.8.2.1 hpqLOMRightLocalUserAdmin - 1.3.6.1.4.1.232.1001.1.8.2.2 hpqLOMRightLogin - 1.3.6.1.4.1.232.1001.1.8.2.3 hpqLOMRightRemoteConsole - 1.3.6.1.4.1.232.1001.1.8.2.4 hpqLOMRightServerReset - 1.3.6.1.4.1.232.1001.1.8.2.5 hpqLOMRightVirtualMedia - 1.3.6.1.4.1.232.1001.1.8.2.6
注意事項	なし

Lights-Out Management属性の定義

以下の表に、Lights-Out Managementコアクラス属性の定義を示します。

hpqLOMRightLogin

OID	1.3.6.1.4.1.232.1001.1.8.2.3
説明	Lights-Out Management製品のログイン権限です。
構文	Boolean値 - 1.3.6.1.4.1.1466.115.121.1.7
オプション	単一値
注意事項	この属性は、ロールオブジェクトについてのみ有効です。`TRUE`の場合は、ロールのメンバーに権限が付与されます。

hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.4
説明	Lights-Out Management製品のリモートコンソール権限です。この属性は、ロールオブジェクトについてのみ有効です。
構文	Boolean値 - 1.3.6.1.4.1.1466.115.121.1.7
オプション	単一値
注意事項	この属性は、ロールオブジェクトについてのみ使用されます。値が`TRUE`の場合は、ロールのメンバーに権限が付与されます。

hpqLOMRightVirtualMedia

OID	1.3.6.1.4.1.232.1001.1.8.2.6
説明	Lights-Out Management製品の仮想メディア権限です。
構文	Boolean値 - 1.3.6.1.4.1.1466.115.121.1.7
オプション	単一値
注意事項	この属性は、ロールオブジェクトについてのみ使用されます。値が`TRUE`の場合は、ロールのメンバーに権限が付与されます。

hpqLOMRightServerReset

OID	1.3.6.1.4.1.232.1001.1.8.2.5
説明	Lights-Out Management製品のリモートサーバーリセットおよび電源ボタン権限です。
構文	Boolean値 - 1.3.6.1.4.1.1466.115.121.1.7
オプション	単一値
注意事項	この属性は、ロールオブジェクトについてのみ使用されます。値が`TRUE`の場合は、ロールのメンバーに権限が付与されます。

hpqLOMRightLocalUserAdmin

OID	1.3.6.1.4.1.232.1001.1.8.2.2
説明	Lights-Out Management製品のローカルユーザーデータベース管理権限です。
構文	Boolean値 - 1.3.6.1.4.1.1466.115.121.1.7
オプション	単一値
注意事項	この属性は、ロールオブジェクトについてのみ使用されます。値が`TRUE`の場合は、ロールのメンバーに権限が付与されます。

hpqLOMRightConfigureSettings

OID	1.3.6.1.4.1.232.1001.1.8.2.1
説明	Lights-Out Management製品のデバイス設定権限です。
構文	Boolean値 - 1.3.6.1.4.1.1466.115.121.1.7
オプション	単一値
注意事項	この属性は、ロールオブジェクトについてのみ使用されます。値が`TRUE`の場合は、ロールのメンバーに権限が付与されます。

iLOの工場出荷時設定へのリセット

場合によっては、iLOを工場出荷時のデフォルト設定にリセットする必要があることがあります。たとえば、FIPSのセキュリティ状態を無効にすると、iLOを工場出荷時設定にリセットする必要があります。

工場出荷時設定へのリセット方法

- iLO6構成ユーティリティ - この機能にはUEFIシステムユーティリティからアクセスします。
- iLO RESTful API - 詳しくは、次のWebサイトを参照してください。https://www.hpe.com/support/restfulinterface/docs
- コマンドラインとスクリプティングツール - 手順については、HPE iLO 6スクリプティング/コマンドラインガイドを参照してください。

サブトピック

iLOの工場出荷時デフォルト設定へのリセット（iLO6構成ユーティリティ）

詳しくは

iLOの工場出荷時デフォルト設定へのリセット（iLO6構成ユーティリティ）

iLOの工場出荷時デフォルト設定へのリセット（iLO6構成ユーティリティ）

このタスクについて

> △ **注意:**
> iLOを工場出荷時のデフォルト設定にリセットすると、iLOのユーザーおよびライセンスデータ、構成設定、およびログを含むすべての設定が消去されます。サーバーに工場でインストールされたライセンスキーがある場合、このライセンスキーは保持されます。
>
> この手順によりログ内のすべてのデータが消去されるため、リセットに関するイベントはiLOイベントログおよびインテグレーテッドマネジメントログに記録されません。

手順

1. （オプション）サーバーにリモートアクセスする場合、iLOリモートコンソールセッションを開始します。
2. サーバーを再起動するかまたは電源を入れます。
3. サーバーのPOST画面でF9キーを押します。

   UEFIシステムユーティリティが起動します。
4. システムユーティリティ画面で、システム構成、iLO 6構成ユーティリティの順にクリックします。
5. 工場出荷時のデフォルトにセットメニューではいを選択します。

   iLO6構成ユーティリティに、要求の確認を求めるメッセージが表示されます。
6. OKをクリックします。
7. iLOが工場出荷時のデフォルト設定にリセットされます。iLOをリモートで管理している場合は、リモートコンソールセッションが自動的に終了します。次にシステムを再起動するまでiLO6構成ユーティリティに再びアクセスすることはできません。
8. ブートプロセスを再開します。
   a. （オプション）iLOをリモート管理している場合は、iLOのリセットが完了するのを待ってから、iLOリモートコンソールを起動します。

      以前のセッションのiLO6構成ユーティリティ画面がまだ開いています。
   b. メインメニューが表示されるまでEscキーを押します。
   c. システムを終了して再起動をクリックします。
   d. 要求の確認を求めるメッセージが表示されたら、OKをクリックして画面を終了し、ブートプロセスを再開します。
9. （オプション）リセット後にデフォルトのiLOアカウント情報を使用して、iLOにログインします。
10. サーバーのオペレーティングシステムを再起動します。

    工場出荷時のデフォルト設定へのリセット中に、SMBIOSレコードはクリアされます。メモリおよびネットワーク情報は、サーバーOSの再起動が完了するまでiLO Webインターフェイスに表示されません。

    パフォーマンス管理のプロセッサージッターコントロール最適化機能は、サーバーOSの再起動が完了するまで使用できません。

Webサイト

iLO

https://www.hpe.com/jp/servers/ilo

iLO 6のドキュメント

https://www.hpe.com/support/ilo6

iLOの役立つリンクとリソース

https://www.hpe.com/support/ilo-resource-ref-en

HPE iLOの無料オンライントレーニング

https://www.hpe.com/ww/iloBundle

HPE ProLiantのトレーニング

https://www.hpe.com/ww/learnproliant

UEFIシステムユーティリティ

https://www.hpe.com/info/ProLiantUEFI/docs

SUM

https://www.hpe.com/info/sum-docs

SPP

https://www.hpe.com/info/spp/documentation

Intelligent Provisioning

https://www.hpe.com/info/intelligentprovisioning/docs

iLO RESTful APIおよびRESTfulインターフェイスツール

https://www.hpe.com/support/restfulinterface/docs

リモートサポート

https://www.hpe.com/info/insightremotesupport/docs

HPE InfoSight for Servers

https://www.hpe.com/servers/infosight

iLO Amplifier Pack

https://www.hpe.com/servers/iloamplifierpack

HPE OneView

https://www.hpe.com/info/oneview/docs

HPE SIM

https://www.hpe.com/info/insightmanagement/sim/docs

サポートと他のリソース

サブトピック

Hewlett Packard Enterpriseサポートへのアクセス

アップデートへのアクセス

Hewlett Packard Enterpriseサポートへのアクセス

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

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

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

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

ご用意いただく情報

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

アップデートへのアクセス

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

  Hewlett Packard Enterpriseサポートセンター

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

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

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

  マイ HPEソフトウェアセンター

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

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

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

- お客様のエンタイトルメントを表示およびアップデートするには、または契約と標準保証をお客様のプロファイルにリンクするには、Hewlett Packard Enterpriseサポートセンター—More Information on Access to Support Materialsページをご覧ください。

  https://www.hpe.com/support/AccessToSupportMaterials

> **重要:**
> Hewlett Packard Enterpriseサポートセンターからアップデートにアクセスするには、製品エンタイトルメントが必要な場合があります。関連するエンタイトルメントでHPE Passportをセットアップしておく必要があります。

リモートサポート（HPE通報サービス）

リモートサポートは、保証またはサポート契約の一部としてサポートデバイスでご利用いただけます。優れたイベント診断、Hewlett Packard Enterpriseへのハードウェアイベント通知の自動かつ安全な送信を提供します。また、お使いの製品のサービスレベルに基づいて高速かつ正確な解決方法を開始します。Hewlett Packard Enterpriseでは、ご使用のデバイスをリモートサポートに登録することを強くお勧めします。

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

HPE通報サービス

http://www.hpe.com/jp/hpalert

HPE Pointnext Tech Care

https://www.hpe.com/jp/ja/services/tech-care

HPE Complete Care

https://www.hpe.com/jp/ja/services/complete-care

カスタマーセルフリペア（CSR）

Hewlett Packard Enterpriseカスタマーセルフリペア（CSR）プログラムでは、ご使用の製品をお客様ご自身で修理することができます。CSR部品を交換する必要がある場合、お客様のご都合のよいときに交換できるよう直接配送されます。一部の部品はCSRの対象になりません。Hewlett Packard Enterpriseの正規保守代理店が、CSRによって修理可能かどうかを判断します。

CSRについて詳しくは、お近くの正規保守代理店にお問い合わせください。

保証情報

ご使用の製品の保証情報を確認するには、以下のリンクを参照してください。

HPE ProLiantとIA-32サーバーおよびオプション

https://www.hpe.com/support/ProLiantServers-Warranties

HPE EnterpriseおよびCloudlineサーバー

https://www.hpe.com/support/EnterpriseServers-Warranties

HPEストレージ製品

https://www.hpe.com/support/Storage-Warranties

HPEネットワーク製品

https://www.hpe.com/support/Networking-Warranties

規定に関する情報

安全、環境、および規定に関する情報については、Hewlett Packard Enterpriseサポートセンターからサーバー、ストレージ、電源、ネットワーク、およびラック製品の安全と準拠に関する情報を参照してください。

https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts

規定に関する追加情報

Hewlett Packard Enterpriseは、REACH（欧州議会と欧州理事会の規則EC No 1907/2006）のような法的な要求事項に準拠する必要に応じて、弊社製品の含有化学物質に関する情報をお客様に提供することに全力で取り組んでいます。この製品の含有化学物質情報レポートは、次を参照してください。

https://www.hpe.com/info/reach

RoHS、REACHを含むHewlett Packard Enterprise製品の環境と安全に関する情報と準拠のデータについては、次を参照してください。

https://www.hpe.com/info/ecodata

社内プログラム、製品のリサイクル、エネルギー効率などのHewlett Packard Enterpriseの環境に関する情報については、次を参照してください。

https://www.hpe.com/info/environment

ドキュメントに関するご意見、ご指摘

Hewlett Packard Enterpriseでは、お客様により良いドキュメントを提供するように努めています。ドキュメントの改善に役立てるために、Hewlett Packard Enterpriseサポートセンターポータル（https://www.hpe.com/support/hpesc）にあるフィードバックボタンとアイコン（開いているドキュメントの下部にあります）から、エラー、提案、またはコメントを送信いただけます。すべてのドキュメント情報は、プロセスによってキャプチャーされます。