Hewlett Packard Enterprise

HPE iLO 7ユーザーガイド

部品番号: 30-842B82CC-003-ja-JP
発行: 2025年5月
版数: 1

HPE iLO 7ユーザーガイド

摘要

このガイドは、HPE iLO 7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、iLO 7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: 30-842B82CC-003-ja-JP
発行: 2025年5月
版数: 1

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は、それらに付属する明示的な保証規定によってのみ保証されます。本書が追加の保証を構成するものではありません。本書中の技術的あるいは編集上の誤りや欠落について、Hewlett Packard Enterpriseでは一切責任を負いません。

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から有効な使用許諾を取得する必要があります。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サイトの外部に移動します。Hewlett Packard Enterpriseでは、Hewlett Packard EnterpriseのWebサイト外の情報については管理しておらず、責任を負いかねますのでご了承ください。

商標

Microsoft®、Azure®、Azure Stack®、Azure Stack Hub®、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®およびIntel® Xeon®は、アメリカ合衆国およびその他の国におけるIntel Corporationの商標です。

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。

目次

- ホストの概要の詳細
- ホストヘルスの詳細
- iLO概要の詳細
- 仮想メディアとリモートコンソールの詳細
- 一般情報
- セキュリティダッシュボードの使用
  - セキュリティパラメーターの詳細
    - リスク詳細
    - セキュリティリスク状態の原因
      - セキュリティパラメーターの状態値
- ホスト情報の表示
  - ホストの設定の表示
  - ホスト設定の編集
- iLOセッションの管理
  - セッションリスト詳細
- iLOイベントログ
  - イベントログの表示
    - イベントログの詳細
    - イベントログのアイコン
  - 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
- インテグレーテッドマネジメントログ
  - IMLイベントタイプの例
  - IMLの表示
    - IMLの詳細
    - IMLアイコン
  - IMLログの管理
    - IMLにメンテナンスノートを追加する
    - IMLログの更新
    - IMLログのクリア
    - CSVファイルへのIMLの保存
    - タイムゾーン設定
    - IMLエントリーの修正済みへの変更
- セキュリティログ
  - セキュリティログの表示
    - セキュリティログの詳細
    - セキュリティログアイコン
  - CSVファイルへのセキュリティログの保存
  - セキュリティログのクリア
- Active Health System
  - Active Health Systemのデータ収集
  - Active Health Systemログ
  - Active Health Systemログのダウンロード方法
  - 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

        - ストレージエンクロージャー
        - ドライブ
            - 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
    - 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
            - 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
    - iLOファームウェアとソフトウェアの管理機能
    - インストールされているファームウェアを表示する
        - ファームウェアタイプ
        - ファームウェアの詳細
    - iLOまたはサーバーファームウェアのアップデート
        - 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
    - ファームウェア検証
        - ファームウェア検証設定の構成
            - ファームウェア検証スキャンオプション
            - サービスアクセス設定オプションのアップデート
        - ファームウェアヘルスステータスの表示
            - ファームウェアヘルスステータスの詳細
            - 隔離されたファームウェアの表示
                - 隔離されたファームウェアの詳細
                - 個々の隔離されたファイルの詳細
        - 隔離されたファームウェアのダウンロード
        - 隔離されたファームウェアの削除
        - フルシステムリカバリの開始
        - ファームウェア検証スキャンの実行
    - ソフトウェアの詳細の表示
        - HPEソフトウェアの詳細 製品関連ソフトウェアの詳細
        - 実行中のソフトウェアの詳細
        - インストールされたソフトウェアの詳細
    - メンテナンスウィンドウ
        - メンテナンスウィンドウの表示
            - 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の詳細
        - メンテナンスウィンドウの追加
        - メンテナンスウィンドウの編集
        - メンテナンスウィンドウの削除
    - iLOレポジトリ
        - iLOレポジトリの内容
            - iLOレポジトリの概要およびコンポーネントの詳細の表示
                - iLOレポジトリのストレージの詳細
        - iLOレポジトリからコンポーネントをインストール
            - 時間枠のスケジュール設定

        - Smart Storage Energy Packのリスト
        - 電力監視
        - 高効率モード
    - 電力設定
        - パワーレギュレーターの設定の構成
            - パワーレギュレーターモード
        - 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
        - 消費電力上限の構成
            - 消費電力上限の注意事項
        - マウスとキーボードの持続接続の設定
        - 電力しきい値超過によるSNMPアラート
            - 電力しきい値超過によるSNMPアラートのオプション
    - ファン
        - ファン情報の表示
            - ファン概要の詳細
            - ファンの詳細
            - HPE液冷モジュール情報の表示
                - HPE液冷モジュールのサマリーの詳細
                - HPE液冷モジュールの詳細
                - HPE液体冷却モジュールの漏れステータスをクリアする
            - 温度情報
                - 温度センサーデータの表示
                - 温度センサーの詳細
        - 最小ファン速度の構成
    - 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
    - ネットワーク構成の概要の表示
        - ネットワーク一般情報
        - IPv4概要の詳細
        - IPv6概要の詳細
        - IPv6アドレスリスト
    - 一般的なネットワーク設定

改訂履歴

部品番号	発行日	版	変更の概要
30-842B82CC-003-ja-JP	2025年5月	1	HPE iLO 7 1.13.00リリースアップデート
30-842B82CC-002	2025年3月	1	HPE iLO 7 1.12.00リリースアップデート
30-842B82CC-001	2025年3月	1	HPE iLO 7 1.11.00は、Gen12プラットフォーム用のHPE iLO 7の最初のリリースです。

HPE iLO

HPE iLOは、サポートされている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

HPE iLO 7

HPE iLO 7搭載のHPE ProLiant Compute Gen12は、組み込みのセキュリティプロセッサーによる追加の保護レイヤーを提供します。組み込みのセキュリティプロセッサーは、サーバーハードウェア内に組み込まれた堅牢なセキュリティファウンデーションであるHPE iLO Silicon Root of Trust上に構築され、サーバーの電源投入の瞬間から、ファームウェアとソフトウェアのすべてのレイヤーが安全に読み込まれ、検証されることを保証します。これにより、破られることのない信頼チェーンが提供され、ファームウェア攻撃、未許可アクセス、改ざんからサーバーが保護され、最高レベルのデータ整合性とシステムの信頼性が確保されます。

HPE iLO 7の新機能

- iLO 7 Webインターフェイスのワークフロー指向設計による**顧客エクスペリエンスの向上**：
  - 新しい検索機能によって柔軟なナビゲーションとUIの高速化が実現し、使いやすさが向上しました。
  - 概要メニューからiLOコントロールアイコンにすばやくアクセス。
  - 主要な機能が整理された左側のナビゲーションペイン。
  - ダッシュボードから各機能の詳細を一目で把握できる新しいカードレイアウト。
- **セキュリティプロセッサーの強化** - iLO 7でサポートされるセキュリティプロセッサーは、iLO ASICに組み込まれた独立型のセキュリティシステムです。
- iLOファームウェアはCNSA 2.0署名アルゴリズムを使用します - Leighton-Micali Signature (LMS)。LMS署名スキームはNIST SP800-208標準に準拠し、ファームウェアアップデート時およびセキュアスタート時に真正性を検証します。
- **液冷漏れ検出** - 液体冷却モジュールに漏れがある場合、サーバーの電源がオフになり、iLOは漏れ検出についてIMLに記録します。

- iLO仮想NICを通じた**安全なインバンドアクセス** - 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。iLOはUSBインターフェイスを介してホストシステムに接続します。このとき、iLOはホストシステムのUSB-Enhanced Host Controller Interface (EHCI) に物理的に接続されます。ホストOSはNetwork Control Model (NCM) ドライバーを使用して仮想イーサーネットインターフェイスをエミュレートします。図
- **iLOサービスポート** - Type C USB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。サーバーに物理的にアクセスできる場合は、サービスポートと標準のUSB Type A - Type Cケーブルまたはは USB Type C - Type Cケーブルを使用してホストシステム (Windows/MAC/Linuxラップトップまたはデスクトップ) に接続し、iLO Webインターフェイス、リモートコンソール、iLO RESTful API、またはCLIにアクセスできます。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。

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** - 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。
- **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。
- **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** - スケジュール済みのファームウェア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構成します。
- 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)** - iLO 7には、Redfish API準拠であるiLO RESTful APIが含まれています。
- **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構成します。
- **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、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構成します。iLOは、セキュア標準モード（デフォルト）と、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。Microsoft Active Directoryのログインユーザー向けにTwo-Factor認証を設定することもできます。
- **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。

HPE iLO 7で削除された機能

- HPE iLO連携
- HPE SIM
- HPE Insight Remote Support
- HPE iLOの本番環境セキュリティ状態
- /redfish/v1/Managers/1/SerialInterfaces/1を使用したBitRate: 115200のシリアルインターフェイス構成
- HPE iLOでSSHの標準ポート22番を変更
- WINS構成
- CHIF（ホストOSからBMCチャネル）
- .NET内蔵リモートコンソール（.NET IRC）
- SMASH-CLP
- iLOスクリプティングとコマンドラインツールキット（RIBCL）
- スタンドアロンリモートコンソール（HPLOCONS）

- HPEオンライン構成ユーティリティ（HPONCFG）
- HPE Lights-Out構成ユーティリティ（HPQLOCFG）
- HPEディレクトリ移行ユーティリティ（HPLOMIG）

HPE iLO 7 1.13.00でサポートされない機能

- Always on Intelligent Provisioning
- HPE iLO SSL証明書インポートの自動証明書登録方法

iLOへのアクセス

iLOには、iLO Webインターフェイス、ROMベースの構成ユーティリティ、iLO RESTful API、またはRESTful Interface Toolからアクセスできます。

サブトピック

HPE WebインターフェイスiLO
ROMベースの構成ユーティリティ
iLO RESTful API
RESTfulインターフェイスツール

HPE WebインターフェイスiLO

HPE 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。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。

詳しくは**デモビデオ**をご覧ください。

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iLO 7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。

iLO 7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iLO 7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、アクセスページで構成できます。iLO 7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。

iLO 7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 7構成ユーティリティの順にクリックします。

iLO RESTful API

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、対話型モード、スクリプト可能なモード、および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の構成にどのようなツールを使用しますか。

サブトピック

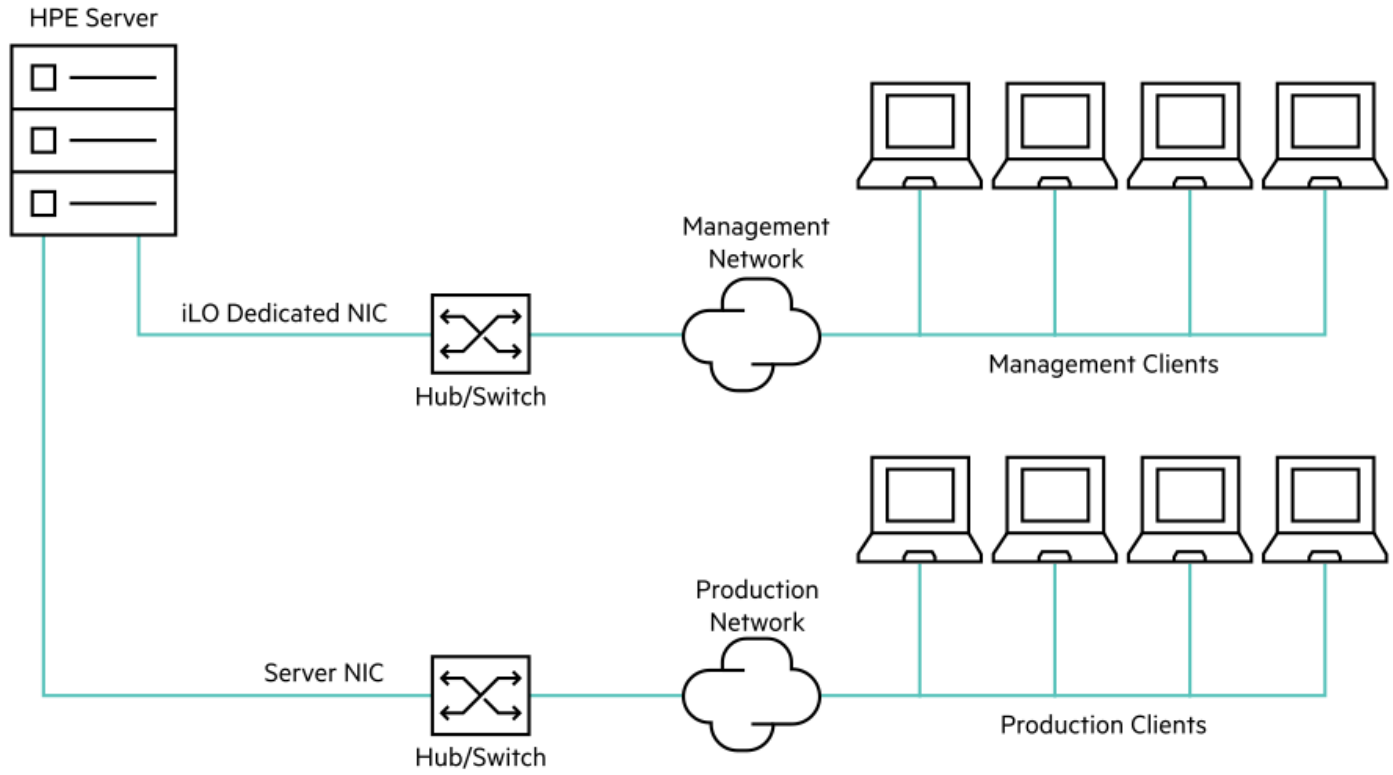
iLOネットワーク接続オプション

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

この構成では、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

この構成では、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。

この構成の使用にはいくつかの欠点があります。

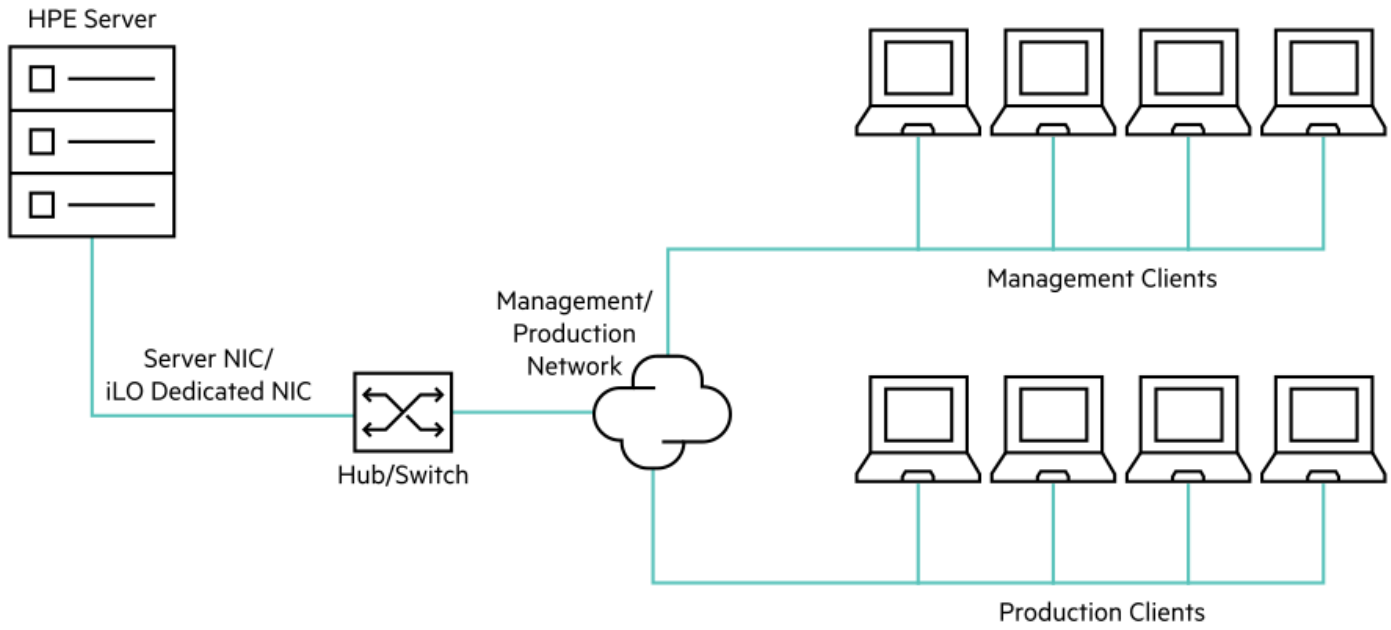
- 共有ネットワーク接続では、トラフィックによって、iLOのパフォーマンスが低下することがあります。
- サーバーの起動時、およびオペレーティングシステムNICドライバーのロードおよびアンロード時に、短時間（2～8

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は要求を再発行します。
- DHCPサーバーは、DNS名前解決を提供するように構成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、iLO 7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。

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またはDNSを使用しない場合は、iLO 7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。

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のユーザーガイドを参照してください。

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アドレスを構成します。
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（iLO 7構成ユーティリティ）を行います。
5. （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。

iLO 7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またはDNS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、iLO 7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（iLO 7構成ユーティリティ）
iLO 7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

静的IPアドレスの構成（iLO 7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 7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。

   iLO 7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。

   iLO 7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。

       iLO 7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。

iLO 7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（iLO 7構成ユーティリティ）
ユーザーアカウントの編集（iLO 7構成ユーティリティ）
ユーザーアカウントの削除（iLO 7構成ユーティリティ）

ユーザーアカウントの追加（iLO 7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 7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、iLO 7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iLO 7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。

   iLO 7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。

ユーザーアカウントの編集（iLO 7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 7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、iLO 7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iLO 7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（iLO 7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 7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iLO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。

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。

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
- **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 Webインターフェイスの使用

サブトピック

サポートされるブラウザー

HPE iLO 7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 iLO 7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またはTLS 1.3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。使用契約条件を承認し、同意しますをクリックしてログインに進みます。
- 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。

3. Microsoft Active Directoryユーザーの場合、ユーザー認証情報の検証に成功すると、Two-Factor認証が有効になっていれば、OTPログイン画面が表示されます。LDAPサーバー上に構成されているメールアドレスで受信したOTPを入力します。

iLO Webインターフェイスを使用してデフォルトのパスワードを回復する

前提条件

- iLOセキュリティオーバーライドスイッチが有効になっている

手順

1. iLOログイン画面からパスワードの回復をクリックします。

   パスワードの回復ウィンドウが表示されます。

2. 署名済みノードIDを入力します。

   署名済みノードIDを複数回使用することはできません。試行に複数回失敗すると、ログイン遅延が発生します。

   署名済みノードIDの生成について詳しくは、iLOトラブルシューティングガイドを参照してください。

3. 新しいパスワードを入力します。

   パスワードの長さは、8～15文字でなければなりません。パスワードの複雑さが有効になっている場合、パスワードには大文字1文字、小文字1文字、数字1文字が含まれている必要があります。

   検証が成功すると、iLOはリセットされ、新しいパスワードが設定されます。リセットした後、デフォルトのユーザー名（Administrator）と新しいパスワードでiLOにログインします。

4. 操作を取り消す場合はキャンセルボタンをクリックします。

5. ✕ をクリックしてパスワードの回復ウィンドウを閉じます。

共有ブラウザーインスタンスとiLO

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。

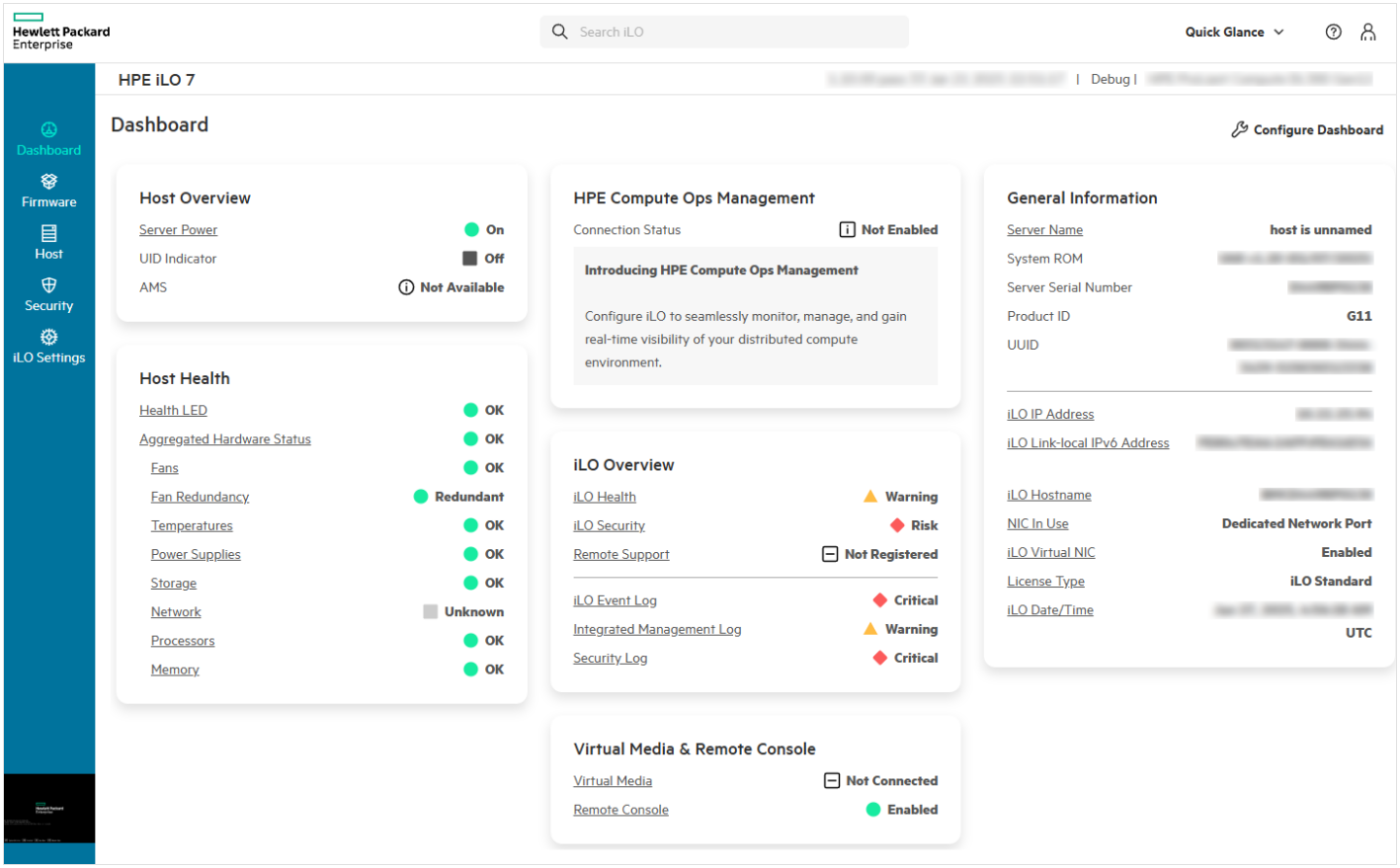
iLOは、同一クライアント上の同じブラウザー内の2つの異なるブラウザーウィンドウから複数のユーザーがログインすることをサポートしません。iLOのWebインターフェイスが別のブラウザーウィンドウまたはタブ（ヘルプファイルなど）を開く場合、このウィンドウは、iLOへの同じ接続とセッションを共有します。

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。

HPE iLO Webインターフェイスの概要

HPE iLO 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。

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制御をすべてのページから使用できます。それぞれの機能設定を概要メニューから表示したり、それらに移動したりできます。

サーバー名

ホストOSによって定義されたサーバー名。

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。

iLO日付/時刻

iLOサブシステムの内蔵クロック。

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。

ヘルスLEDアイコン

システムの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。表示される値は、OK、警告、およびクリティカルです

iLOヘルスアイコン

iLO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、警告、およびクリティカルです

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、リスク無視、およびリスクありです

ヘルプ

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。

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。

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。
- 環境設定オプションを使用して、タイムゾーン、電源ユニット、温度単位、ブラウザーにiLOセッションキーを保存して、頻繁なログインを減らしますでのユーザー初期設定を行います。

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。

詳細については、リモートコンソールセクションを参照してください。

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。

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。

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。

iLO情報およびログの表示

サブトピック

ホストの概要の詳細

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。

電源制御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、iLO Webインターフェイスの上部にある概要オプションの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。

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。

AMSについてこれ以上の情報を得ることはできません。

表示される値は、OKまたは利用不可です。

ホストヘルスの詳細

ヘルスLED

システムのLEDステータス。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、警告、およびクリティカルです。LEDステータスは概要メニューからも確認できます。

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。

集約されたハードウェアステータス

ハードウェアの集約された動作ステータス。表示可能なステータスは、OK、警告、およびクリティカルです

ハードウェアページに移動するには集約されたハードウェアステータスリンクをクリックします。

ファン

サーバーファンのヘルスステータス。表示可能な値は、OK、警告、およびクリティカルです

温度と冷却ページに移動するには、ファンリンクをクリックします。

ファンの冗長性

サーバーファンの冗長性ファクター。表示可能な値は、冗長化、非冗長化、冗長化の障害、および不明です。

温度と冷却ページに移動するには、ファンリンクをクリックします。

温度

サーバー温度センサーのヘルスステータス。表示される値は、OK、警告、およびクリティカルです

温度と冷却ページに移動するには、ファンリンクをクリックします。

電源装置

電源装置のステータス。表示される値は、OK、警告、およびクリティカルです

電源ページに移動するには、電源装置リンクをクリックします。

電源装置の冗長性

電源の冗長性ファクター。表示可能な値は、冗長化、非冗長化、冗長化の障害、および不明です

電源ページに移動するには、電源装置の冗長性リンクをクリックします。

ストレージ

ストレージのヘルスステータス。表示される値は、OK、警告、およびクリティカルです。

ストレージページに移動するには、ストレージリンクをクリックします。

ネットワーク

サーバーのネットワークステータス。表示される値は、OK、警告、およびクリティカルです。

ネットワークページに移動するには、ネットワークリンクをクリックします。

プロセッサー

サーバーのプロセッサーステータス。表示される値は、OK、警告、およびクリティカルです

プロセッサーページに移動するには、プロセッサーリンクをクリックします。

メモリ

サーバーのメモリステータス。表示される値は、OK、警告、およびクリティカルです。

メモリページに移動するには、メモリリンクをクリックします。

iLO概要の詳細

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。表示される値は、OK、警告、およびクリティカルです。

トラブルシューティング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、リスク無視、およびリスクありです。

セキュリティパラメーター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。

リモートサポート

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。

リモートサポートページに移動するには、リモートサポートリンクをクリック。

iLOイベントログ

iLOファームウェアが記録した重要なイベントレコードを表示します。

iLOイベントログページに移動するには、iLOイベントログリンクをクリックします。

インテグレーテッドマネジメントログ

IML（インテグレーテッドマネジメントログ）は、サーバーで発生した履歴イベントの記録です。

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インテグレーテッドマネジメントログリンクをクリックします。

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。

セキュリティログページに移動するには、セキュリティログリンクをクリックします。

仮想メディアとリモートコンソールの詳細

仮想メディア

iLO仮想メディアは、ネットワーク上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。

仮想メディアとブートオプションページに移動するには、仮想メディアリンクをクリックします。

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。

リモートコンソール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。

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。

一般情報

サーバー名

ホストOSによって定義されたサーバー名。

ホスト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。

システムROM

アクティブなシステムROMのバージョンとアクティブなシステムROMの日付。

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。

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。

iLO IPアドレス

iLOサブシステムのネットワークIPアドレス。

iLO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。

IPv4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。

iLO共有ネットワークポート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使用中のNIC

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。

iLO専用ネットワークポートページに移動するには、iLO使用中のNICリンクをクリックします。

iLO仮想NIC

iLO仮想NICのステータス。

指定できる値は、有効および無効です。

この機能を構成できるアクセス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

iLOライセンスタイプを表示します。

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日付/時刻

iLOサブシステムの内蔵クロック。

時刻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。

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

セキュリティページの概要セクションには、システムの全体的なセキュリティステータスとセキュリティ状態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

左側のナビゲーションペインでセキュリティをクリックします。

セキュリティページが表示されます。
概要セクションで、全体的なセキュリティステータスおよびセキュリティ状態の詳細を確認します。

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。

  セキュリティ機能がリスクステータスで表示されている場合、詳細については、画面上の情報を参照してください。詳細情報には、リスクと推奨される解決策についての情報が含まれています。
- 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ます。

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。

- セキュリティ状態を変更した後、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。

セキュリティ状態

- セキュア標準
- FIPS
- CNSA
- Synergyセキュリティモード

サブトピック

セキュリティパラメーターの詳細

セキュリティパラメーターの詳細

セキュリティパラメーターは、監視対象のセキュリティ機能の名前です。

セキュリティリスク状態の原因について詳しくは、セキュリティリスク状態の原因を参照してください。

セキュリティ機能のリスク無視オプションを構成できます。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、概要セクション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。

このステータスは、セキュリティページの概要セクションとiLOのコントロールにも表示されます。

機能を無視しても、セキュリティページの概要セクションに表示されているステータス値は変わりません。

iLO Webインターフェイスで構成できる機能については、このページ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。

サブトピック

リスク詳細
セキュリティリスク状態の原因

リスク詳細

セキュリティ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。

> **注記**
> iLOは、システムに電源がない場合でもシャーシ侵入を検出します。最初の侵入のタイムスタンプがIMLに記録されます。

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、ユーザー管理ページでこの機能を有効にすることを推奨します。

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。

ユーザー管理ページでこの機能を有効にすることができます。

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。

SNMPv1リクエスト

SNMPv1リクエストが有効になっています。この構成は、iLOでのSNMPv1リクエストの受信を許可します。SNMPv1リクエストを有効にすると、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。

アクセスページでこの機能を有効にできます。

サブトピック

セキュリティパラメーターの状態値

セキュリティパラメーターの状態値

指定可能なセキュリティパラメーターの状態値は、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。

ホスト情報の表示

サブトピック

ホストの設定の表示

サーバー名

ホストOSによって定義されたサーバー名。

サーバーのFQDN/IPアドレス

サーバーのIPアドレスまたはドメイン名。

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。

表示される値は、以下のとおりです。

- 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。

指定できる値は、有効および無効です

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。

ホスト設定の編集

手順

1. 左側のナビゲーションペインでホストをクリックします。

   ホストページが表示されます。

2. （ホスト設定定セクション）をクリックします。

   ホスト設定ウィンドウが表示されます。

3. 以下の設定を編集できます。
   - サーバー名
   - サーバーのFQDN/IPアドレス
4. 変更を保存するには、アップデートをクリックします。
5. 操作を取り消す場合はキャンセルボタンをクリックします。
6. をクリックしてウィンドウを閉じます。

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. 左側のナビゲーションペインでiLO設定をクリックし、ユーザー管理をクリックします。

   ユーザー管理ページが表示されます。

2. セッションをクリックします。

   セッションページが表示され、iLOセッションに関する情報が表示されます。

3. （オプション）セッションを削除するには、その横にあるチェックボックスをクリックし、 をクリックします。

   iLOは、選択したセッションの削除を確認するプロンプトを表示します。

4. はい、削除しますをクリックします。

サブトピック

セッションリスト詳細

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およびセッションリスト（*セッションのリストと 詳細*）テーブルに表示されます。

- 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。
- ログイン時刻 – iLOセッションが開始した日時。
- 最終アクティブ日 – iLOがセッションで最後にアクティブだった日時。
- 期限切れ – 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（例えば、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、VNICなど）。

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. 左側のナビゲーションペインでiLO設定をクリックし、トラブルシューティングをクリックします。

   トラブルシューティングページが表示されます。
2. iLOイベントログをクリックします。

   iLOイベントログページが表示され、iLOイベントログの詳細が表示されます。
3. （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。
4. （オプション）イベントを検索するには、日付、イベントID、または説明テキストを検索ボックスに入力します。
5. （オプション）イベントリストを更新するには、アクション > ログをリフレッシュ をクリックします。
6. ログフィルターにアクセスするには、 をクリックします。

フィルターウィンドウが表示されます。

- 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。
- 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。
- 最終アップデート日でフィルタリングするには、最終アップデートリストで値を選択します。

7. 表示されるイベントの日付と時刻を変更するには、アクションをクリックして時刻メニューで値を選択します。以下から選択します。
   - iLOタイムゾーン – iLOのサブシステムの時間を表示します。
   - ユーザーのローカルタイムゾーン – 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。
   - UTC（協定世界時）– UTC時刻をISO 8601形式で表示します。
8. フィルターを保存するにはフィルターの適用をクリックします。
9. リセットフィルターをクリックすると、フィルターはデフォルト値に戻ります。
10. ✕ をクリックしてフィルターウィンドウを閉じます。

サブトピック

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下に表示されます。

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。

CSVファイルへのイベントログの保存

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、トラブルシューティングをクリックします。

   トラブルシューティングページが表示されます。

2. iLOイベントログをクリックします。

   iLOイベントログページが表示されます

3. アクション > CSVのダウンロードをクリックします。

   csvファイルがダウンロードされます。

4. （オプション）特定のイベントのcsvファイルをダウンロードするには、イベントの横にあるチェックボックスをオンにして、アクション > CSVのダウンロードをクリックします。

   選択したイベントのcsvファイルがダウンロードされます。

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. 左側のナビゲーションペインでiLO設定をクリックし、トラブルシューティングをクリックします。

   トラブルシューティングページが表示されます。

2. iLOイベントログをクリックします。

   iLOイベントログページが表示されます

3. アクション > ログを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。

4. 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。システムROMとiLOドライバーがイベントを生成します。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。予防措置はサービスの中断を回避するのに役立ちます。

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. 左側のナビゲーションペインでホストをクリックしてインテグレーテッドマネジメントログをクリックするか、左側のナビゲーションペインでiLO設定をクリックしてトラブルシューティング > インテグレーテッドマネジメントログをクリックします。

   インテグレーテッドマネジメントログページが表示されます。

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）イベントを検索するには、日付、イベントID、または説明テキストを 検索ボックスに入力します。
4. （オプション）ログフィルターにアクセスするには、 をクリックします。

   フィルターウィンドウが表示されます。

   - 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。
   - 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。

- 最終アップデート日でフィルタリングするには、最終アップデートリストで値を選択します。

5. フィルターを保存するにはフィルターの適用をクリックします。
6. リセットフィルターをクリックすると、フィルターはデフォルト値に戻ります。
7. ✕ をクリックしてフィルターウィンドウを閉じます。

サブトピック

IMLの詳細
IMLアイコン

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下に表示されます。

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。

- **Repairable events** – Webインターフェイスの左側の最初の列には、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、ステータスがクリティカルまたは注意のイベントを選択するために使用されます。また、他のすべてのイベントステータスについては、チェックボックスを選択してCSVをダウンロードします。
- 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。例えば、ハードウェア、ファームウェア、構成などです。

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ログの管理

アクションメニューから以下のタスクを実行できます。

- IMLにメンテナンスノートを追加する
- ログをリフレッシュ
- ログをクリア
- CSVのダウンロード
- タイムゾーン
- IMLエントリーの修正済みへの変更

サブトピック

IMLにメンテナンスノートを追加する
IMLログの更新
IMLログのクリア
CSVファイルへのIMLの保存
タイムゾーン設定
IMLエントリーの修正済みへの変更

IMLにメンテナンスノートを追加する

前提条件

iLOの設定を構成する権限

このタスクについて

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. 左側のナビゲーションペインでホストをクリックしてインテグレーテッドマネジメントログをクリックするか、左側のナビゲーションペインでiLO設定をクリックしてトラブルシューティング > インテグレーテッドマネジメントログをクリックします。

   インテグレーテッドマネジメントログページが表示されます。

2. アクションをクリックして、＋ メンテナンスノートの追加をクリックします。

   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。

   情報ログエントリーがIMLに追加されます。

IMLログの更新

前提条件

iLOの設定を構成する権限

手順

1. 左側のナビゲーションペインでホストをクリックしてインテグレーテッドマネジメントログをクリックするか、左側のナビゲーションペインでiLO設定をクリックしてトラブルシューティング＞インテグレーテッドマネジメントログをクリックします。

   インテグレーテッドマネジメントログページが表示されます。

2. アクション＞ ログをリフレッシュ をクリックします。

   ログが更新されます。

IMLログのクリア

前提条件

iLOの設定を構成する権限

手順

1. 左側のナビゲーションペインでホストをクリックしてインテグレーテッドマネジメントログをクリックするか、左側のナビゲーションペインでiLO設定をクリックしてトラブルシューティング＞インテグレーテッドマネジメントログをクリックします。

   インテグレーテッドマネジメントログページが表示されます。

2. アクション＞ ログを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。

   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。

CSVファイルへのIMLの保存

手順

1. 左側のナビゲーションペインでホストをクリックしてインテグレーテッドマネジメントログをクリックするか、左側の

ナビゲーションペインでiLO設定をクリックしてトラブルシューティング > インテグレーテッドマネジメントログをクリックします。

インテグレーテッドマネジメントログページが表示されます。

2. アクション > CSVのダウンロードをクリックします。

csv ファイルがダウンロードされます。

3. （オプション）特定のイベントの csv ファイルをダウンロードするには、イベントの横にあるチェックボックスをオンにして、アクション > CSVのダウンロードをクリックします。

選択したイベントの csv ファイルがダウンロードされます。

タイムゾーン設定

手順

1. 左側のナビゲーションペインでホストをクリックしてインテグレーテッドマネジメントログをクリックするか、左側のナビゲーションペインでiLO設定をクリックしてトラブルシューティング > インテグレーテッドマネジメントログをクリックします。

インテグレーテッドマネジメントログページが表示されます。

2. アクションをクリックして、希望するタイムゾーンのオプションをクリックします。

- iLOタイムゾーン – iLOのサブシステム時間を表示します。
- ユーザーのローカルタイムゾーン – 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。
- UTC（協定世界時）–UTC時刻をISO 8601形式で表示します。

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。

手順

1. 問題を調べて修正します。
2. 左側のナビゲーションペインでホストをクリックしてインテグレーテッドマネジメントログをクリックするか、左側のナビゲーションペインでiLO設定をクリックしてトラブルシューティング > インテグレーテッドマネジメントログをクリックします。

インテグレーテッドマネジメントログページが表示されます。

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。

4. 修正済みとしてマークをクリックします。

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。

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。

サブトピック

セキュリティログの表示
CSVファイルへのセキュリティログの保存
セキュリティログのクリア

セキュリティログの表示

手順

1. 左側のナビゲーションペインでセキュリティをクリックしてセキュリティログをクリックするか、左側のナビゲーションペインでiLO設定をクリックしてトラブルシューティング > セキュリティログをクリックします。

   セキュリティログページが表示され、ログの詳細が表示されます。

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）イベントを検索するには、日付、イベントID、または説明テキストを 検索ボックスに入力します。
4. （オプション）イベントリストを更新するには、アクション > ログをリフレッシュ をクリックします。
5. ログフィルターにアクセスするには、 をクリックします。

   フィルターウィンドウが表示されます。

   - 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。
   - 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。
   - 最終アップデート日でフィルタリングするには、最終アップデートリストで値を選択します。

6. 表示されるイベントの日付と時刻を変更するには、アクションをクリックして時刻メニューで値を選択します。以下から選択します。

   - iLOタイムゾーン – iLOのサブシステムの時間を表示します。
   - ユーザーのローカルタイムゾーン – 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。
   - UTC（協定世界時）– UTC時刻をISO 8601形式で表示します。

7. フィルターを保存するにはフィルターの適用をクリックします。
8. リセットフィルターをクリックすると、フィルターはデフォルト値に戻ります。
9. をクリックしてフィルターウィンドウを閉じます。

サブトピック

セキュリティログの詳細
セキュリティログアイコン

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下に表示されます。

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。

CSVファイルへのセキュリティログの保存

手順

1. 左側のナビゲーションペインでセキュリティをクリックしてセキュリティログをクリックするか、左側のナビゲーションペインでiLO設定をクリックしてトラブルシューティング > セキュリティログをクリックします。

   セキュリティログページが表示されます。

2. アクション > CSVのダウンロードをクリックします。

   csvファイルがシステムのダウンロードフォルダーにダウンロードされます。

3. （オプション）特定のイベントのcsvファイルをダウンロードするには、イベントの横にあるチェックボックスをオンにして、アクション > CSVのダウンロードをクリックします。

   選択したイベントのcsvファイルがシステムのダウンロードフォルダーにダウンロードされます。

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. 左側のナビゲーションペインでセキュリティをクリックしてセキュリティログをクリックするか、左側のナビゲーションペインでiLO設定をクリックしてトラブルシューティング > セキュリティログをクリックします。

   セキュリティログページが表示されます。

2. アクション > ⃠ ログを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。

   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。

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（例えば、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ログをダウンロードする場合、オプションで連絡先情報を追加できます。Active Health Systemデータを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、プライバシーに関する声明（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。

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。
- **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。

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

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、トラブルシューティングをクリックします。

   トラブルシューティングページが表示されます。

2. Active Health Systemログをクリックします。

Active Health Systemログページが表示されます。

3. タイプで日付範囲の場合を選択します。
4. 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。
5. （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。
6. ダウンロードをクリックします。
7. ファイルを保存します。
8. 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。

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. 左側のナビゲーションペインでiLO設定をクリックし、トラブルシューティングをクリックします。

   トラブルシューティングページが表示されます。
2. Active Health Systemログをクリックします。

   Active Health Systemログページが表示されます。
3. タイプでログ全体を選択します。

4. （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。
5. ダウンロードをクリックします。
6. ファイルを保存します。
7. 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。

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ログページでログを有効が設定されている。

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. 左側のナビゲーションペインでiLO設定をクリックし、トラブルシューティングをクリックします。

   トラブルシューティングページが表示されます。
2. Active Health Systemログをクリックします。

   Active Health Systemログページが表示されます。
3. ログを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. 操作を取り消す場合はキャンセルボタンをクリックします。
6. ✕ をクリックしてウィンドウを閉じます。
7. ログをクリアした後、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、データ一式が確実にログに記録されます。
8. 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。

Active Health Systemログの無効化

このタスクについて

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、トラブルシューティングをクリックします。

   トラブルシューティングページが表示されます。

2. Active Health Systemログをクリックします。

   Active Health Systemログページが表示されます。

3. ログの無効化をクリックします。

4. 要求を確認するメッセージが表示されたら、はい、無効にしますをクリックします。

   ログが無効になります。

5. 操作を取り消す場合はキャンセルボタンをクリックします。

6. ✕ をクリックしてウィンドウを閉じます。

iLOとシステム診断の使用

このタスクについて

サブトピック

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。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. 左側のナビゲーションペインでiLO設定をクリックし、トラブルシューティングをクリックします。

   トラブルシューティングページが表示されます。
   iLOセルフテスト結果セクションにはセルフテストの結果が表示されます。

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。

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。

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。
- 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。
- 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。
- **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。例えば、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

iLOをリセットオプションを使用します。

iLO 7構成ユーティリティ

UEFIシステムユーティリティのiLO 7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

IPMI

詳しくは、HPE iLO 7 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

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。例えば、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を使用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。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、アップロードは停止します。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。

手順

1. 左側のナビゲーションペインでiLO設定をクリックしてトラブルシューティングをクリックするか、クイックアクションメニューからiLOをリセットをクリックします。

2. トラブルシューティングページを経由してナビゲートする場合、システム診断 > iLOをリセットをクリックします。

   iLOをリセットウィンドウが表示されます。

   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て要求を確認します。

   iLOがリセットされ、ブラウザー接続が閉じます。

iLOのiLO 7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 7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。

   iLO 7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iLO 7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。

システム診断

システム診断セクションには、サーバーでサポートされている機能が表示されます。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。

> **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

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. （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。

3. 左側のナビゲーションペインでiLO設定をクリックし、トラブルシューティングをクリックします。

   トラブルシューティングページが表示されます。

4. システム診断 > システムデフォルト設定のリストアをクリックします。

   システムデフォルト設定のリストアウィンドウが表示されます。
   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。

   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システム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. 左側のナビゲーションペインでiLO設定をクリックし、トラブルシューティングをクリックします。

   トラブルシューティングページが表示されます。

2. システム診断 > システムインテリジェント診断モードをクリックします。

iLOが要求を確認するように求めます。

3. はい、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。

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. 左側のナビゲーションペインでiLO設定をクリックし、トラブルシューティングをクリックします。

   トラブルシューティングページが表示されます。

3. システム診断_>_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。

4. 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PCIe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. 左側のナビゲーションペインでiLO設定をクリックし、トラブルシューティングをクリックします。

   トラブルシューティングページが表示されます。

2. システム診断 > システムセーフモードをクリックします。

   iLOが要求を確認するように求めます。

3. はい、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。

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. 左側のナビゲーションペインでiLO設定をクリックし、トラブルシューティングをクリックします。

   トラブルシューティングページが表示されます。

2. システム診断 > 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。

   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。

3. 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。

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. 左側のナビゲーションペインでiLO設定をクリックし、トラブルシューティングをクリックします。

   トラブルシューティングページが表示されます。

2. システム診断 > UEFIシリアルデバッグメッセージをクリックします。

3. 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。

Webインターフェイスを使用したiLOプロセッサーのリセット

前提条件

iLOの設定を構成する権限

このタスクについて

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。例えば、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を使用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。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、アップロードは停止します。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。

手順

1. 左側のナビゲーションペインでiLO設定をクリックしてトラブルシューティングをクリックするか、クイックアクションメニューからiLOをリセットをクリックします。

2. トラブルシューティングページを経由してナビゲートする場合、システム診断 > iLOをリセットをクリックします。

   iLOをリセットウィンドウが表示されます。

   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て要求を確認します。

   iLOがリセットされ、ブラウザー接続が閉じます。

ホストプロセッサーモジュールによるデータセンターセキュアコントロールモジュールのバインド

前提条件

- リカバリセット権限を持つ管理者。
- 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

このオプションを使用して、データセンターセキュアコントロールモジュール（DC-SCM）をホストプロセッサーモジュール（HPM）にバインドします。このオプションは、モジュラーハードウェアシステム（MHS）でのみ使用でき、モノボードでは使用できません。これは、インテグレーテッドマネジメントログにHPM認証失敗ログが表示される場合に、現場から返却されたボードを対象としています。

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、トラブルシューティングをクリックします。

   トラブルシューティングページが表示されます。

2. システム診断 > DC-SCMをHPMにバインドをクリックします。

   DC-SCMをHPMにバインドウィンドウが表示されます。

3. バインドの完了後ただちにAUX電源再投入を自動的に実行しますをクリックして、バインドが完了したらAUX電源再投入を実行します。

4. はい、続行しますをクリックして要求を確認します。

   DC-SCMとHPMのバインドが正常に完了しました。

5. （オプション）最新の変更を表示するには、AUXサイクルをクリックします。

   確認ダイアログボックスが表示されます。

6. はい、続行しますをクリックします。

   iLOがリセットを開始します。リセット後、iLOに再度ログインしてインテグレーテッドマネジメントログにアクセスし、バインディングが成功したかどうかを確認します。

   バインドが失敗した場合は、この手順を繰り返します。バインドが失敗した場合は、AHSログをダウンロードして**HPEサポート**にお問い合わせください。

全般的なシステム情報の表示

サブトピック

プロセッサーとGPUの情報の表示
メモリ情報の表示
ネットワークアダプター

デバイスインベントリの表示
ストレージの詳細の表示

プロセッサーとGPUの情報の表示

このタスクについて

プロセッサーページは、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。

サポートされているサーバーのGPU情報も表示されます。

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

左側のナビゲーションペインでホストをクリックし、ハードウェア＞プロセッサーをクリックします。

プロセッサーページが表示されます。

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。
- 状態 – プロセッサーの現在の状態。
- ヘルス – 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。

サーバーの電源が切れている場合、このページのシステムヘルス情報は、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。

手順

1. 左側のナビゲーションペインでホストをクリックし、ハードウェア＞メモリをクリックします。

メモリページが表示されます。
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

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。

メモリタイプ

メモリのタイプ

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、OS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。

状態

現在の物理メモリの状態。表示される値は、存在しないおよび有効です。

ヘルス

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）

サブトピック

メモリ詳細ペイン（物理メモリ）

メモリ詳細ペイン（物理メモリ）

製造元

メモリモジュールの製造元。

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。

誤り訂正

メモリモジュールが使用する誤り訂正のタイプ。

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）。

ネットワークアダプター

このタスクについて

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。

サブトピック

ネットワークの詳細の表示

ネットワークの詳細の表示

手順

1. 左側のナビゲーションペインでホストをクリックし、ハードウェアをクリックします。

   ハードウェアページが表示されます。

2. ネットワーク をクリックします。

   ネットワークページが表示され、使用可能なネットワークアダプターの詳細が表示されます。

3. ネットワークアダプターをクリックします。

   ネットワークアダプターページが表示され、次の情報が表示されます。

   - 概要
   - ポート
   - デバイス機能
   - イーサーネットインターフェイス
   - メトリック

サブトピック

ネットワーク詳細オプション

ネットワーク詳細オプション

概要

概要セクションには以下の情報が表示されます。

- 状態 – アダプターの状態
- ヘルス – アダプターの稼働状態
- ロケーション – システムボード上のアダプターの位置
- 部品番号 – NICの部品番号
- 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
- モデル – NICのモデル
- 製造元 – NICの製造元

- シリアル番号 – NICのシリアル番号
- デバイス機能の数 – ネットワークに接続されたデバイス機能の数
- ポート数 – ネットワークに接続されているポートの数

すべてのプロパティを表示をクリックすると、コントローラーの詳細を含むアダプターの詳細情報が表示されます。

> **注記**
> ネットワークアダプターで分岐が有効になっている場合、ネットワークページにはネットワークアダプターの状態、ヘルス、ロケーションが表示されません。アダプターの状態、ヘルス、ロケーションの情報は、デバイスインベントリおよびファームウェアインベントリページで確認してください。

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

イーサーネットの場合：

- ポート – ポートの名前
- LLDP有効 – このポートのLLDPを有効または無効にする
- MACアドレス – ポートのMACアドレス
- リンク状態 – ポートのリンク状態
- リンクステータス – ポートのリンクステータス
- 状態 – ポートの状態
- ヘルス – ポートの稼働状態

ファイバーチャネルの場合：

- ポート – ポートの名前
- EEE有効 – このポートのEEEを有効または無効にする
- ワールドワイド名 – ポートのワールドワイド名
- ファブリック名 – ポートのファブリック名
- リンク状態 – ポートのリンク状態
- リンクステータス – ポートのリンクステータス
- 状態 – ポートの状態
- ヘルス – ポートの稼働状態

ポートをクリックすると、対応するポートの詳細ペインが表示されます。

デバイス機能

デバイス機能に応じて、次の詳細が表示されます。

イーサーネット、iSCSI、FCoEの場合：

- ID – デバイス機能名
- 状態 – デバイス機能の状態
- ヘルス – デバイス機能の稼働状態
- デバイス技術 – デバイス機能の構成された能力
- 関連ポート – デバイス機能の関連ポート
- MACアドレス – デバイス機能MACアドレス

- ブートモード – デバイス機能のブートモード

ファイバーチャネルの場合：

- ID – デバイス機能名
- 状態 – デバイス機能の状態
- ヘルス – デバイス機能の稼働状態
- デバイス技術 – デバイス機能の構成された能力
- 関連ポート – デバイス機能の関連ポート
- ワールドワイドノード名 – デバイス機能のワールドワイドノード名

  デバイス技術にInfinibandが構成されている場合、ノードGUIDが表示されます。
- ブートモード – デバイス機能のブートモード

デバイス機能をクリックすると、対応するデバイス詳細ペインが表示されます。

イーサーネットインターフェイス

イーサーネットに関する以下の詳細が表示されます。

- 名前 – インターフェイスの名前
- 状態 – インターフェイスの状態
- ヘルス – インターフェイスの稼働状態
- IPv4アドレス – システムNIC（内蔵および直立型）の場合、サーバーのIPアドレス（使用できる場合）。
- IPv6アドレス – システムNIC（内蔵および直立型）の場合、サーバーのIPアドレス（使用できる場合）。
- リンクステータス – インターフェイスのリンクステータス
- MACアドレス – インターフェイスのMACアドレス
- チーム/ブリッジ – ポートがNICチーミング用に設定されている場合、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設定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。

イーサネットインターフェイスをクリックすると、対応するイーサネットインターフェイスの詳細ペインが表示されます。

注記

iLOでは、MCTP PLDM RDEベースのネットワークアダプター用のネットワークアダプターポートに割り当てられたIPv4アドレス、IPv6アドレス、およびチーム/ブリッジの詳細が表示されません。

メトリック

ネットワークアダプターメトリックには、ネットワークアダプターの使用状況と正常性の統計が表示されます。

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、例えば、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。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。

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。

ホストまたはiLOの再起動後、デバイスインベントリを表示するにはRedfish DeviceDiscoveryが`vMainDeviceDiscoveryComplete`状態に到達する必要があります。

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. 左側のナビゲーションペインでホストをクリックし、ハードウェアをクリックします。

   ハードウェアページが表示されます。

2. デバイスインベントリをクリックします。

   デバイスインベントリページが表示されます。

3. （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。

4. （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。

5. （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

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。

  OCPスロットにネットワークまたはストレージアダプターが取り付けられている場合、iLOではOCPデバイスの位置の詳細がOCP Slot AおよびOCP Slot Bのように表示されますが、デバイスでは位置情報の詳細が`Slot <番号>`のように表示されます。

- 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。

- 製品バージョン – デバイスの製品バージョン。

  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。
- 状態 - デバイスの状態。

  存在しない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、ストレージページのドキュメントを参照してください。
- ヘルス - デバイスの稼働状態。

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。

- SKU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。

  > **注記**
  > ネットワークコントローラーのデバイスインベントリページのSKU番号は、ネットワークページのSKU番号と一致しない場合があります。

- 部品番号 - 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。
- 関数（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関数。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のインスタンスは、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。

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。

UEFIシステムユーティリティを使用したPCIe MCTPオプションの構成について詳しくは、**HPE Computeサーバー用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。

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。
- MCTP検出が無効になっている場合、HPE Compute Ops Managementによって開始されたファームウェアのアップデートは

  失敗します。
- 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. 左側のナビゲーションペインでホストをクリックし、ハードウェアをクリックします。

   ハードウェアページが表示されます。
2. デバイスインベントリをクリックします。

   デバイスインベントリページが表示されます。
3. 検出設定をクリックします。

   検出設定ウィンドウが表示されます。
4. 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。
5. 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。
6. 変更を保存するには、アップデートをクリックします。
7. 設定を工場出荷時の状態にリセットするには、MCTP工場出荷時リセットをクリックします。

   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。
8. 操作を取り消す場合はキャンセルボタンをクリックします。
9. ✕ をクリックして検出設定を閉じます

MCTP工場出荷時リセットの開始

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. 左側のナビゲーションペインでホストをクリックし、ハードウェアをクリックします。

   ハードウェアページが表示されます。

2. デバイスインベントリをクリックします。

   デバイスインベントリページが表示されます。

3. 検出設定をクリックします。

   検出設定ウィンドウが表示されます。

4. 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。

5. アップデートをクリックします。

   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。

ストレージの詳細の表示

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。

ホストまたはiLOの再起動後、デバイスインベントリを表示するにはRedfish DeviceDiscoveryが`vMainDeviceDiscoveryComplete`状態に到達する必要があります。

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、左側のナビゲーションペインでホストをクリックしてネットワークをクリックします。

手順

1. 左側のナビゲーションペインでホストをクリックし、ハードウェアをクリックします。

   ハードウェアページが表示されます。

2. ハードウェアページのストレージをクリックします。

   ストレージページが表示されます。

3. （オプション）コンポーネントの詳細を表示するには、エンティティテーブルから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。

注記

言語翻訳機能は、詳細ペインには適用されません。

4. （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、トグルボタンを使用します。

   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。

   LEDステータスをオンまたはオフに変更できます。

5. （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

ストレージの詳細

ストレージページには、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。

サポート対象のストレージコンポーネント

ストレージページには、以下のストレージコンポーネントに関するエンティティ、回数、およびヘルスサマリーの情報が表示されます。

- ストレージコントローラー、ボリューム、ストレージエンクロージャー、ドライブ、スイッチ、ポート。

  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。

  次の直接接続ストレージタイプがサポートされています。SATA、NVMe、およびRDE対応デバイス。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。

注記

直接接続NVMeまたはEDSSFドライブは、ドライブの下にのみ表示されます。

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 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
- Intel VROC 9.0
- M.2 SSD対応キット
- デュアル8 GB MicroSD EM USBキット（Windowsのみ）
- NVMeドライブ
- NS204i-uブートコントローラー
- NS204i-dブートコントローラー

サブトピック

ステータスの値と定義

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。

ストレージコントローラー

ストレージ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。

- 名前
- 位置 – サーバー内のコントローラーの位置。
- 状態 – 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。
- ヘルス
- ファームウェアバージョン
- 暗号化モード
- エンクロージャー
- ボリューム
- ドライブ

コントローラー名をクリックすると、詳細ペインが表示されます。また、メトリックおよびボリュームの詳細が表示されます。

エンクロージャーシャーシ

エンクロージャーシャーシセクションには、各エンクロージャーに関する次の情報が表示されます。

- 位置
- ステータス
- ドライブ
- 合計ポート数

エンクロージャーを選択すると、関連付けられたドライブ、スイッチ、およびポートが表示されます。

スイッチ

スイッチセクションには、各スイッチに関する次の情報が表示されます。

- モデル
- ステータス
- ファームウェアバージョン

ポート

ポートセクションには、各ポートについて次の情報が表示されます。

- ポート番号
- 位置
- ステータス

- 現在の速度
- アクティブ幅

> **注記**
> ドライブバックプレーンの命名規則に記載されているレーンあたりの最大リンク速度（GT/s）は、ポートに表示される現在の速度または最大速度とは異なります。

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
- RAIDのタイプ
- ドライブ
- 交換用部品

ボリュームは、事前に構成しないと、このページに表示されません。

ボリュームを選択すると、詳細ペインが開き、詳細情報が表示されます。また、関連するドライブが表示されます。

ストレージエンクロージャー

ストレージ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。エンクロージャー情報は、エンクロージャーの詳細を共有するコントローラーの機能に基づいて利用できます。

- 名前
- 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。
- タイプ
- スイッチ

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、詳細ペインが開き、詳細情報が表示されます。また、関連するドライブが表示されます。

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。

- 名前
- 状態
- ヘルス

- 容量（バイト）
- 永続的な名前
- 永続的な名前の形式
- EUI
- モデル
- プロトコル
- シリアル番号
- メディアタイプ
- 予測されるメディアの残りの寿命（%）
- ロケーションタイプ
- 位置

ドライブを選択すると、詳細ペインが開き、詳細情報が表示されます。

詳細ペインには、選択したドライブに関する次の詳細も表示されます。

- ロケーションインジケーターアクティブ – LEDのステータス（オンまたはオフ）。トグルボタンを使用してLEDステータスを変更します。この機能は、NVMeとSATAドライブでのみ使用できます。
- LED切り替え – 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）。
- 強制電源オン – 電源オンまたは電源オフボタンを使用して、NVMeのドライブ電源を制御できます。
- マルチパス
- 偽
- ドライブの形状
- ファームウェアバージョン
- 障害予告
- ステータスインジケーター
- ホットスペアタイプ
- 暗号化機能
- 暗号化ステータス
- 書き込みキャッシュ有効
- 対応速度（Gbs）
- ネゴシエート済み速度（Gbs）
- スロット対応プロトコル

サブトピック

ドライブの電源の管理

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
- iLO

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、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. 左側のナビゲーションペインでホストをクリックし、ハードウェアをクリックします。

   ハードウェアページが表示されます。

2. ストレージをクリックします。

   ストレージページが表示されます。

3. ドライブをクリックします

   ドライブページが表示されます。

4. ドライブを選択します。

   詳細ペインが開きます。

5. 電源オンまたは電源オフボタンをクリックします。

6. 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

- 強制電源オン – すぐにドライブの電源を入れます。
- 強制電源オフ – 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

ファームウェアアップデート
iLOファームウェアとソフトウェアの管理機能
インストールされているファームウェアを表示する
iLOまたはサーバーファームウェアのアップデート

ファームウェアアップデート

ファームウェアアップデートでは、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、仮想NICドライバーが必要です。詳しくは、ホスト上でのiLOの使用を参照してください

iLOが、セキュア標準、FIPS、またはCNSAのセキュリティ状態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。

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

オンラインROMフラッシュコンポーネント

1. ファームウェアパッケージをフラッシュするには、RESEFUL Interface Tool（iLORest）v. 6.x.0以降をダウンロードしてください。
2. ファームウェアパッケージと、対応するjson（利用可能な場合）を同じ場所にダウンロードします

   例：

   `ilorest flashfwpkg <ファイル名.fwpkg>--url<iLO 7 IPアドレス>-u<iLO 7ユーザー名>-p<iLO 7パスワード>`

   または

ローカルホストOSの例：

`ilorest flashfwpkd<ファイル名.fwpkg>-u<iLO 7ユーザー名>-p<iLO 7パスワード>`

ファームウェアパッケージは、Smart Update Manager v 12.0.0以降でもインストールできます。

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。

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。

iLOファームウェアとソフトウェアの管理機能

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。
- 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。
- 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します。
  - 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。

インストールされているファームウェアを表示する

手順

1. 左側のナビゲーションペインでファームウェアをクリックし、ファームウェアインベントリをクリックします。

   ファームウェアインベントリページが表示され、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**
> 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必要があります。

2. （オプション）ファームウェアリストを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）ファームウェアを検索するには、ファームウェア名の横にある列見出しの検索テキストボックス内にファームウェア名を入力します。

サブトピック

ファームウェアタイプ

ファームウェアインベントリページに表示されるファームウェアタイプは、サーバーまたはシャーシのモデルおよび構成によって変化します。

ファームウェアインベントリページに表示されるファームウェアタイプは、サーバーのモデルおよび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の一部は、次のとおりです。

- ストレージおよびネットワークコントローラー
- さまざまなプログラマブルロジックデバイス
- ドライブファームウェア
- TPMまたはTMファームウェア
- 電源装置ファームウェア

ファームウェアの詳細

ファームウェアリストページには、リストされた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。

iLOまたはサーバー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アップデートし、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、同様にiLOレポジトリに保存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. 左側のナビゲーションペインでファームウェアをクリックしてファームウェアインベントリ＞ファームウェアのアップデートをクリックするか、クイックアクションメニューからファームウェア＞ファームウェアのアップデートをクリックします。

   ファームウェアのアップデートオプションが表示されない場合は、ファームウェアページの右上隅にある省略記号アイコンをクリックします。

   ファームウェアのアップデートウィンドウが表示されます。
3. 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。
4. 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、ローカルファイルフィールド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フィールドに、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有効にするには、（ファームウェア設定オプション）をクリックします。

      ファームウェア設定ポップアップウィンドウが表示されます。設定はファームウェア設定ウィンドウで編集できます。

      オプションについて詳しくは、ファームウェア設定ページのヘルプを参照してください。
5. （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。
6. （オプション）手順6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。

リカバリセットをアップデート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、同様に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。

7. 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。

8. アップデートプロセスを開始するには、アップデートをクリックします。

   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。

9. 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。

10. 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。

11. 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。

12. （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、ファームウェアインベントリページでファームウェアバージョンを確認します。

    ダッシュボードで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。

13. 操作を取り消す場合はキャンセルボタンをクリックします。

14. ✕ をクリックしてファームウェアのアップデートウィンドウを閉じます。

サブトピック

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

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
- 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、ファームウェア設定でサードパーティ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。

ファームウェア検証

ファームウェア検証機能では、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）

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。

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。

サブトピック

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. 左側のナビゲーションペインでファームウェアをクリックし、ファームウェア検証をクリックします。

   ファームウェア検証ページが表示されます。

2. 設定をクリックします。

   スキャン設定ウィンドウが表示されます。

3. 整合性障害のアクションを選択します。
4. 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。

5. 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。
6. アップデートをクリックして設定を保存します。
7. 操作を取り消す場合はキャンセルボタンをクリックします。
8. ✕ をクリックしてスキャン設定ウィンドウを閉じます。

サブトピック

ファームウェア検証スキャンオプション

- 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。

    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’の権限が必要ですに設定されている場合、BIOS/iLO/CPLDの自動リカバリは失敗します。これは予期される動作です。リカバリセット権限を持つユーザーとしてログインした後、手動でリカバリを実行する必要があります。
- スキャン間隔（日数）- バックグランドスキャン頻度（日数）を設定します。有効な値は1～365です。
- 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。

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。

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

左側のナビゲーションペインでファームウェアをクリックし、ファームウェア検証をクリックします。

ファームウェア検証ページが表示されます。
ファームウェアステータスの詳細がページに表示されます。

サブトピック

ファームウェアヘルスステータスの詳細
隔離されたファームウェアの表示

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、未装着が表示されます。

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

左側のナビゲーションペインでファームウェアをクリックし、ファームウェア検証をクリックします。

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`（隔離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。

サブトピック

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。
- サイズ-無効なファイルサイズ。

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レポジトリの隔離エリアにファイルが保存されている場合、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. 左側のナビゲーションペインでファームウェアをクリックし、ファームウェア検証をクリックします。

   ファームウェア検証ページが表示されます。

2. 隔離セクションで、ダウンロードしたいファイルを選択し、アクション＞ファームウェアをダウンロードをクリック

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。

手順

1. 左側のナビゲーションペインでファームウェアをクリックし、ファームウェア検証をクリックします。

   ファームウェア検証ページが表示されます。

2. 隔離セクションで、削除したいファイルを選択し、アクション > ファームウェア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。

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。
- サポートされる管理ツール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. 左側のナビゲーションペインでファームウェアをクリックし、ファームウェア検証をクリックします。

   ファームウェア検証ページが表示されます。

2. リカバリイベントを送信をクリックします。
3. 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。）

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. 左側のナビゲーションペインでファームウェアをクリックし、ファームウェア検証をクリックします。

   ファームウェア検証ページが表示されます。
2. ファームウェア検証ページでスキャンを実行をクリックします。

   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。

   注記

   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。

ソフトウェアの詳細の表示

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、構成され、実行されている必要があります。

手順

1. 左側のナビゲーションペインでホストをクリックし、ソフトウェアをクリックします。

   ソフトウェアページが表示されます。

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。

サブトピック

HPEソフトウェアの詳細 製品関連ソフトウェアの詳細
実行中のソフトウェアの詳細
インストールされたソフトウェアの詳細

HPEソフトウェアの詳細 製品関連ソフトウェアの詳細

ソフトウェアインベントリテーブルでは、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。

このセクションでは、管理対象サーバー上のすべての製品関連ソフトウェアを一覧表示します。

- 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 – インストールされているソフトウェアの説明。
- 製造者 – ソフトウェア製造元の名前。

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ページ上。
- タスクをインストールキューに追加するとき。

サブトピック

メンテナンスウィンドウの表示

手順

1. 左側のナビゲーションペインでファーム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。

   メンテナンスウィンドウが表示されます。

2. （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。

サブトピック

メンテナンスウィンドウの詳細

メンテナンスウィンドウページに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。

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. 左側のナビゲーションペインでファームウェアをクリックし、メンテナンスウィンドウ > 新しいウィンドウの追加をクリックします。

   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。

2. 名前ボックスに名前を入力します。
3. 説明ボックスに説明を入力します。
4. 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. （オプション） を開始および終了ボックスでクリックします。

      カレンダーが表示されます。

      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。

5. 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。

6. 操作を取り消す場合はキャンセルボタンをクリックします。
7. ✕ をクリックしてメンテナンスウィンドウの追加を閉じます。

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. 左側のナビゲーションペインでファーム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。

   メンテナンスウィンドウが表示されます。

2. 省略記号アイコンをクリックし、編集するメンテナンスウィンドウの横にある編集をクリックします。

   メンテナンスウィンドウの編集が表示されます。

3. 必要な変更をアップデートし、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。

4. ✕ をクリックしてメンテナンスウィンドウの編集を閉じます。

メンテナンスウィンドウの削除

前提条件

手順

1. 左側のナビゲーションペインでファーム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。

   メンテナンスウィンドウが表示されます。

2. 省略記号アイコンをクリックし、編集するメンテナンスウィンドウの横にある削除をクリックします。

   確認ウィンドウが表示されます。

3. はい、削除しますをクリックして、メンテナンスウィンドウを削除します。

   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。

4. （オプション）すべてのメンテナンスウィンドウと関連タスクを削除する場合、すべてを削除をクリックします。

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、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。

サブトピック

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
- ロック済み/未ロック

サブトピック

iLOレポジトリの概要およびコンポーネントの詳細の表示

手順

1. 左側のナビゲーションペインでファームウェアをクリックし、iLOレポジトリをクリックします。
2. （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。

サブトピック

iLOレポジトリのストレージの詳細

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レポジトリからコンポーネントをインストール

前提条件

iLO設定の構成権限

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、ファームウェア＞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、次の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. 左側のナビゲーションペインでファーム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にある省略記号アイコンをクリックし、インストールキューをクリックします。

   インストールコンポーネントポップアップウィンドウが開き、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。

  新しいメンテナンスウィンドウを追加するには、新しいメンテナンスウィンドウを追加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。

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。

4. 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。

サブトピック

時間枠のスケジュール設定

時間枠のスケジュール設定

前提条件

iLOの設定を構成する権限

このタスクについて

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. （開始ボックス内）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. （終了ボックス内）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

アップロードオプションを使用して、iLOレポジトリにコンポーネントを追加できます。

手順

1. 左側のナビゲーションペインでファームウェアをクリックし、iLOレポジトリを選択します。

   iLOレポジトリページが表示されます。

2. 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、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にある省略記号アイコンをクリックして、アップロードをクリックします。

   iLOiLOにアップロードウィンドウが表示されます。

3. 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。
4. 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。
5. 複数のファイルで指定されたファームウェアコンポーネントの場合のみ：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オンにします。
6. 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。
7. （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。

8. 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。

9. 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。

10. ✕ をクリックして、iLO iLOにアップロードメンテナンスウィンドウを閉じます。
11. 操作を取り消す場合はキャンセルボタンをクリックします。

サブトピック

iLOレポジトリの個々のコンポーネントの詳細
iLOレポジトリからコンポーネントを削除する

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。

iLOレポジトリからコンポーネントを削除する

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. 左側のナビゲーションペインでファームウェアをクリックし、iLOレポジトリを選択します。
2. 削除したいコンポーネントの横にある省略記号アイコンをクリックし、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。

4. (オプション) すべてのコンポーネントを削除するには、すべてを削除をクリックします。プロンプトが表示されたらメッセージを確認します。

すべてのコンポーネントが削除されます。

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。

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。

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。

サブトピック

インストールセットを表示する

手順

1. 左側のナビゲーションペインでファームウェアをクリックし、インストールセットをクリックします。
2. （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。

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。

Intel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。

  詳しくは、Webサイト（**https://www.hpe.com/support/ilo-docs**）にあるiLOユーザーガイドを参照してください。

- 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。

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。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. 左側のナビゲーションペインでファームウェアをクリックし、インストールセットをクリックします。

   インストールセットページが表示されます。

2. インストールするコンポーネントの横にある省略記号アイコンをクリックし、インストールをクリックします。

   コンポーネントのインストールウィンドウが表示されます。

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、新しいメンテナンスウィンドウを追加リンク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ドロップダウン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. （オプション）TPMオーバーライドの確認を選択します
6. 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。
7. 操作を取り消す場合はキャンセルボタンをクリックします。
8. ✕をクリックしてコンポーネントのインストールウィンドウを閉じます。

サブトピック

時間枠のスケジュール設定
インストールセットの削除

時間枠のスケジュール設定

前提条件

iLOの設定を構成する権限

このタスクについて

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. （開始ボックス内）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. （終了ボックス内）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の削除

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. 左側のナビゲーションペインでファームウェアをクリックし、インストールセットをクリックします。
2. 削除したいインストールセットの横にある削除をクリックします。

   すべてのインストールセットを削除する場合は、すべてを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、削除しますをクリックします。

   インストールセットが削除されます。
4. 操作を取り消す場合はキャンセルボタンをクリックします。

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。

> **注記**
> インストールセットに追加できるコンポーネントの最大数は35です。

- iLOインストールキューオプションを使用します。
- インストールキューページのキューに追加オプションを使用します。
- iLOレポジトリページのコンポーネントのインストールオプションを使用します。
- SUMを使用します。

サブトピック

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. 左側のナビゲーションペインでファームウェアをクリックし、インストールキューをクリックします。

   インストールキューページが表示されます。
2. （オプション）コンポーネントに関する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

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 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。

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。例えば、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。

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. 左側のナビゲーションペインでファームウェアをクリックしてインストールキュー＞キューに追加を選択するか、クイックアクションからファームウェア＞キューに追加をクリックします ＋

   キューに追加オプションが表示されない場合は、ファームウェアページの画面右上の省略記号アイコンをクリックしてください。

   インストールキューに追加ウィンドウが表示されます。
   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。
   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。
2. タスク名ボックスにタスク名（最大64文字）を入力します。
3. 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。
4. 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。
5. （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。

6. （オプション）キューの先頭に追加を選択して、タスクをインストールキューの先頭に移動します。
7. （オプション）手順3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. 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

時間枠のスケジュール設定
インストールキューに追加できるコマンド

時間枠のスケジュール設定

前提条件

iLOの設定を構成する権限

このタスクについて

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. （開始ボックス内）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. （終了ボックス内）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

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。

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. 左側のナビゲーションペインでファームウェアをクリックし、インストールキューをクリックします。
2. 編集対象のタスクの横にある編集をクリックします。

   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/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. 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。

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. 左側のナビゲーションペインでファームウェアをクリックし、インストールキューをクリックします。
2. 削除したいコンポーネントの横にある削除をクリックします。

   すべてのコンポーネントを削除する場合は、すべてを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。

Synergyサーバーでは、統合リモートコンソールは常に有効です。

ProLiant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。

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終了したら、ログアウトして終了します。
- 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。
- リモートコンソール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。

サブトピック

リモートコンソールの詳細の表示
リモートコンソールの取得
リモートコンソールのコンピューターロック設定の構成
リモートコンソールのホットキー
HTML5 IRCの起動

リモートコンソールの詳細の表示

手順

1. 左側のナビゲーションペインでダッシュボードまたはホストをクリックし、リモートコンソールをクリックします。

   リモートコンソールページが表示されます。
   概要セクションにリモートコンソールのステータスおよびリモートコンソールサムネイルステータスが表示されます。
   セキュリティ設定は、セキュリティセクションに表示されます。

2. （概要セクション）をクリックします。

   概要ウィンドウが表示されます。

3. 必要な設定を編集した後、アップデートをクリックします。
4. 操作を取り消す場合はキャンセルボタンをクリックします。
5. をクリックして概要ウィンドウを閉じます。

サブトピック

リモートコンソールの詳細

リモートコンソールの詳細

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にアクセスできません。

リモートコンソールサムネイル

リモートコンソールサムネイルのステータス（有効または無効）。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ステータスがリモートコンソール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. 左側のナビゲーションペインでホストをクリックし、リモートコンソールをクリックします。

   リモートコンソールコンソールページが表示されます。

2. HTML5コンソールの起動をクリックします。

   リモートコンソールが新しいウィンドウで起動します。
   別のユーザーがリモートコンソールで作業している場合、iLOは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を通知します。

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。

リモートコンソールのコンピューターロック設定の構成

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. 左側のナビゲーションペインでダッシュボードまたはホストをクリックし、リモートコンソールをクリックします。

   リモートコンソールページが表示されます。

2. （セキュリティセクション）をクリックします。

   セキュリティウィンドウが表示されます。

3. 以下のリモートコンソールコンピューターロックの設定から選択します。

Windows、カスタム、または無効

4. 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。
5. （オプション）IRCはiLOの信頼済みの証明書を要求しますを選択します。
6. 変更を保存するには、アップデートをクリックします。
7. 操作を取り消す場合はキャンセルボタンをクリックします。
8. ✕ をクリックしてセキュリティウィンドウを閉じます。

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、例えば、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OS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OS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を設定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. 左側のナビゲーションペインでダッシュボードまたはホストをクリックし、リモートコンソールをクリックします。

   リモートコンソールページが表示されます。

2. （ホットキーセクション）をクリックします。

   ホットキーウィンドウが表示されます。

3. 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。

4. アップデートをクリックします。

   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。

5. 操作を取り消す場合はキャンセルボタンをクリックします。

6. ✕ をクリックしてホットキーウィンドウを閉じます。

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

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

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. 左側のナビゲーションペインでダッシュボードまたはホストをクリックし、リモートコンソールをクリックします。

   リモートコンソールページが表示されます。

2. （ホットキーセクション）をクリックします。

   ホットキーをリセットウィンドウが表示されます。

3. リセットの確認をクリックします。

   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。

4. 操作を取り消す場合はキャンセルボタンをクリックします。

5. をクリックしてホットキーをリセットウィンドウを閉じます。

HTML5 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ホストページで有効になっている。

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. 左側のナビゲーションペインでホストをクリックし、リモートコンソールをクリックします。

   リモートコンソールページが表示されます。

2. HTML5コンソールの起動をクリックします。

   新しいウィンドウにコンソールが表示されます。

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。例えば、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 7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

- NCMドライバー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、Windowsでドライバーの詳細を調べることでサポートを確認できます。詳しくは、仮想NICのIPの構成 - Windows OSを参照してください。

  Windows 2022の場合は、最新のOS更新プログラムを使用してください。更新プログラムは2024-6Bより新しいか、バージョン25398.950以降である必要があります。このためのNCMドライバーが含まれる累積更新プログラムは`KB5039236`です。

  Linuxホストでは、次の方法を使用して仮想NIC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_ncm.ko`を探します。

    ```
    find /lib/modules/$(uname -r) *.ko* | grep cdc_ncm
    ```

  - 次のコマンドを入力して、`cdc_ncm`がロードされているかどうか確認します。

    ```
    lsmod | grep cdc_ncm
    ```

- ホストサーバーOSが仮想NICをサポートしている。
- サポートされているVMware ESXiのバージョンはESXi 8.0 U3 P05以降です。
- 仮想NIC機能がアクセス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。

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、iLO 7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 2025
- Microsoft Windows Server 2022 - 25398.950より新しいバージョンはパッチ`KB5039236`または`2024-6B`で入手できます。
- Red Hat Enterprise Linux 9.4 Server
- Red Hat Enterprise Linux 9.6 Server
- SUSE Linux Enterprise Server 15 SP6
- SUSE Linux Enterprise Server 15 SP7
- VMWare ESXi 8.0 U3 P05
- VMware ESXi 9.0

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. 左側のナビゲーションペインでiLO設定をクリックし、アクセスをクリックします。

      アクセスページが表示されます。
   b. 他のインターフェイスセクションで仮想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. （他のインターフェイスの隣）をクリックします。

      他のインターフェイスウィンドウが開きます。
   b. 仮想NICチェックボックスを選択します。

      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. 設定のアップデートが完了している場合は、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。
   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は、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のIPアドレスの構成 - RHELコマンド
   - 仮想NICのIPアドレスの構成 - SLESコマンド

4. ホストOS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. 以下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、`ipaddr`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のIPアドレスの構成 - RHELコマンド

このタスクについて

仮想NICデバイスのIPアドレスを取得するには、`nmcli`コマンドを実行します。

例：

```
[root@localhost ~]# nmcli device status
DEVICE      TYPE     STATE                CONNECTION
ens14f3     ethernet  connected             Profile 1
enp63s0f4u5  ethernet  connected            enp63s0f4u5
lo          loopback  connected (externally)  lo
ens14f0     ethernet  disconnected          --
ens14f1     ethernet  disconnected          --
ens14f2     ethernet  disconnected          --
```

`nmcli`コマンドを使用して、DHCPを使用するように仮想NICデバイスを構成することもできます。

手順

1. すべてのネットワークデバイスを一覧表示するには、`nmcli device status`コマンドを実行します。
2. 2番目のインターフェイス用の新しいネットワーク接続を追加するには、`sudo nmcli connection add type ethernet ifname <2番目のネットワークインターフェイスの 名前>`コマンドを実行します。
3. DHCPを使用するように新しい接続を変更するには、`sudo nmcli connection modify <2番目のネットワークインター`

フェイスの名前> ipv4.method auto コマンドを実行します。

4. 新しい接続を有効にするには、sudo nmcli connection up <2番目の ネットワークインターフェイスの名前>コマンドを実行します。
5. 新しく追加されたインターフェイスを確認するには、ip addr show <2番目のネットワーク インターフェイスの名前>コマンドを実行します。

仮想NICのIPアドレスの構成 – SLESコマンド

このタスクについて

仮想NICのIPが構成されているかどうかを確認するには、wicked コマンドを実行します。

例：

```
SLES15-PROD2:~ # wicked ifstatus allusb0
usb0           up
     link:     #6, state up, mtu 1500
     type:     ethernet, hwaddr fa:4b:7f:fc:bc:02
     config:   compat:suse:/etc/sysconfig/network/ifcfg-usb0
     leases:   ipv4 dhcp granted
     leases:   ipv6 dhcp requesting
     addr:     ipv4 16.1.15.2/30 [dhcp]
```

wicked コマンドを使用して、DHCPを使用するように仮想NICデバイスを構成するには、次の手順を実行します。

手順

1. usb0ネットワークデバイスが構成されているかどうかを確認するには、wicked ifstatus usb0 コマンドを実行します。
2. 構成ファイルを編集または作成して、DHCPを使用するように仮想NICを設定するには、vi /etc/sysconfig/network/ifcfg-usb0 コマンドを実行します。

   例：

   ```
   vi /etc/sysconfig/network/ifcfg-usb0
   ### 以下の内容でファイルを保存
   BOOTPROTO=dhcp
   STARTMODE=auto
   ONBOOT=yes
   ###
   ```

3. 新しい接続を有効にするには、wicked ifreload usb0 コマンドを実行します。
4. 新しく追加されたインターフェイスを確認するには、wicked ifstatus usb0 コマンドを実行します。

Windowsでのドライバー状態の表示

このタスクについて

NCMドライバーは、Windows 2025ではデフォルトで使用できます。Windows 2022の場合は、必ず最新のパッチ（パッチKB5039236または2024-6Bで入手可能な25398.950より新しいバージョン）をインストールしてください。

手順

1. Windowsのバージョンを表示するには、スタートメニューからシステム設定をクリックし、バージョン情報をクリック

します。

OSバージョンの詳細が表示されます。

2. 仮想NICデバイスがNCMドライバー用に使用可能かどうかを確認するには、デバイスマネージャーを起動します
3. デバイスマネージャーウィンドウから、ネットワークアダプター_>_UsbNCM Host Deviceのプロパティを選択します。

   UsbNCM Host Deviceのプロパティウィンドウが表示されます。

仮想NICのIPの構成 - Windows OS

手順

1. Windowsのコントロールパネルを開きます。
2. ネットワークとインターネットをクリックします。

   ネットワークとインターネットウィンドウが表示されます。
3. ネットワークと共有センターをクリックします。

   ネットワークと共有センターウィンドウが表示されます。
4. 左側のナビゲーションペインでアダプターの設定の変更をクリックします。

   ネットワーク接続ウィンドウが表示されます。
5. 仮想NICアダプター - UsbNcm Host Deviceを選択します。
6. 右クリックメニューのプロパティをクリックします。
7. インターネットプロトコルバージョン4 (TCP/IPv4) をクリックします。

   インターネットプロトコルバージョン4 (TCP/IPv4) のプロパティウィンドウが表示されます。
8. IPアドレスを自動的に取得するとDNSサーバーを自動的に取得するを選択します。
9. OKをクリックします。

   仮想NICのIPが構成されます。

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。

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 -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。

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。

iLO仮想メディアの使用

サブトピック

仮想メディアオペレーティングシステムの詳細

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。

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。

オペレーティングシステムに関する注意事項：ディスケット

Windows Server 2022以降

Windowsのインストール中にディスケット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、仮想ディスケットが強制的にドライブAとして表示されます。

Red Hat Enterprise LinuxおよびSUSE Linux Enterprise Server

Linuxは、USBディスケットとキードライブの使用をサポートしています。

オペレーティングシステムに関する注意事項：CD/DVD-ROM

Windows

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

CD/DVD-ROMは、Linux GUIでは自動的にマウントされます。

Linuxディストリビューションによっては、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、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（例えば、`/dev/cdrom1`）でアクセスできます。

オペレーティングシステムに関する注意事項：仮想フォルダー

- **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とブートオプション

ホスト > 仮想メディアとブートオプションページで仮想メディア機能が有効になっている場合、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、接続、切断する。詳細は、ローカルメディアのセクションを参照してください。
- URLベースのメディアから表示、接続、切断、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HTTPS形式のURLを使用できます。詳細は、URLベースのメディアのセクションを参照してください。
- ブートオプションとサーバーブート順序の詳細を表示または変更します。詳細については、ブートオプションおよびサーバーブート順序セクションを参照してください。

サブトピック

仮想メディアの有効化または無効化
仮想メディアに関する留意事項
接続されているローカルメディアの表示
サーバーブート順序

仮想メディアの有効化または無効化

手順

1. 左側のナビゲーションペインでホストをクリックします。

   ホストページが表示されます。

2. 仮想メディアとブートオプションをクリックします。

   仮想メディアとブートオプションページが表示されます。

3. （概要セクション）をクリックします。

   概要ウィンドウが表示されます。

4. 仮想メディアチェックボックスをチェックして、仮想メディアを有効または無効にします。

5. アップデートをクリックして設定を保存します。

6. 操作を取り消す場合はキャンセルボタンをクリックします。

7. をクリックしてウィンドウを閉じます。

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。

  - 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。
- Hewlett Packard Enterpriseでは、スクリプト方式仮想メディアの機能が正しく動作するために、次のことを推奨します。
  - Webサーバーは、`.iso`および`.img`ファイルのメディアタイプをオクテットストリームとして設定します。iLOは、要求されたコンテンツがWebサーバーからバイナリデータとして送信されることを期待します。
  - Webサーバーは、クライアント要求ヘッダー内のHTTP範囲をサポートし、それに応じて応答します。

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。

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
- 仮想メディアとブートオプションページで仮想メディア機能が有効になっている。

手順

1. 左側のナビゲーションペインでホストをクリックします。

   ホストページが表示されます。

2. 仮想メディアとブートオプションをクリックします。

   仮想メディアとブートオプションページが表示されます。
   このページには、接続されているローカルメディアの詳細が表示されます。

サブトピック

ローカル仮想メディアデバイスの切断
URLベースのメディアの接続

ローカル仮想メディアデバイスの切断

前提条件

- 仮想メディア権限
- 仮想メディアとブートオプションページで仮想メディア機能が有効になっている。

手順

1. 左側のナビゲーションペインでホストをクリックします。

   ホストページが表示されます。

2. 仮想メディアとブートオプションをクリックします。

   仮想メディアとブートオプションページが表示されます。

3. 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切断ボタンをクリックします。

URLベースのメディアの接続

前提条件

- 仮想メディア権限
- 仮想メディアとブートオプションページで仮想メディア機能が有効になっている。

このタスクについて

仮想メディアとブートオプションページからURLベースのメディアを接続できます。仮想メディアとブートオプションページは、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。

URLベースのメディアの使用について詳しくは、iLOユーザーガイドを参照してください。

手順

1. 左側のナビゲーションペインでホストをクリックします。

   ホストページが表示されます。

2. 仮想メディアとブートオプションをクリックします。

仮想メディアとブートオプションページが表示されます。

3. 仮想フロッピーまたは仮想CD/DVD-ROMセクションの横にある接続をクリックします。
4. 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。
5. 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。

   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。
6. 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無効になっています。
7. 接続をクリックします。
8. （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。
9. 操作を取り消す場合はキャンセルボタンをクリックします。
10. ✕ をクリックしてウィンドウを閉じます

サブトピック

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切断

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
- 仮想メディアとブートオプションページで仮想メディア機能が有効になっている。

手順

1. 左側のナビゲーションペインでホストをクリックします。

   ホストページが表示されます。
2. 仮想メディアとブートオプションをクリックします。

   仮想メディアとブートオプションページが表示されます。
   このページでは、接続されたメディアを確認できます。

URLベースの仮想メディアデバイスの切断

前提条件

- 仮想メディア権限
- 仮想メディアとブートオプションページで仮想メディア機能が有効になっている。

手順

1. 左側のナビゲーションペインでホストをクリックします。

   ホストページが表示されます。

2. 仮想メディアとブートオプションをクリックします。

   仮想メディアとブートオプションページが表示されます。

3. 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。

サーバーブート順序

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。

サブトピック

サーバーブート順序の構成
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構成
ワンタイムブートステータスの変更

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. 左側のナビゲーションペインでホストをクリックし、仮想メディアとブートオプションをクリックします。
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。
3. アップデートをクリックします。

   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。

> **注記**
> POST中はブート順序をアップデートできません。

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. 左側のナビゲーションペインでホストをクリックし、仮想メディアとブートオプションをクリックします

   仮想メディアとブートオプションページが表示されます。
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。
3. 操作を取り消す場合はキャンセルボタンをクリックします。
4. ✕ をクリックしてウィンドウを閉じます。

サーバーブートモードの構成

前提条件

- iLOの設定を構成する権限

このタスクについて

手順

1. 左側のナビゲーションペインでホストをクリックします。

   ホストページが表示されます。
2. 仮想メディアとブートオプションをクリックします。

   仮想メディアとブートオプションページが表示されます。
3. ✎ （サーバーブート順序セクションの横）をクリックします。

   サーバーブート順序ウィンドウが表示されます。
4. ドロップダウンから必要なオプションを選択します。
5. 変更を保存するには、アップデートをクリックします。
6. 操作を取り消す場合はキャンセルボタンをクリックします。
7. ✕ をクリックして編集ウィンドウを閉じます。
8. サーバーをリセットします。

> ✎ **注記**
> POST中はブート順序をアップデートできません。

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

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. 左側のナビゲーションペインでホストをクリックし、仮想メディアとブートオプションをクリックします

   仮想メディアとブートオプションページが表示されます。

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ターゲットオプションを選択：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. アップデートをクリックします。

   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。

5. 操作を取り消す場合はキャンセルボタンをクリックします。
6. ✕ をクリックしてウィンドウを閉じます。

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。
- 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ターゲット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。

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。.imgおよび.isoファイルのMIMEタイプを`application/octet-stream`に構成する必要があります。詳しくは、Webサーバーのドキュメントを参照してください。

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

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

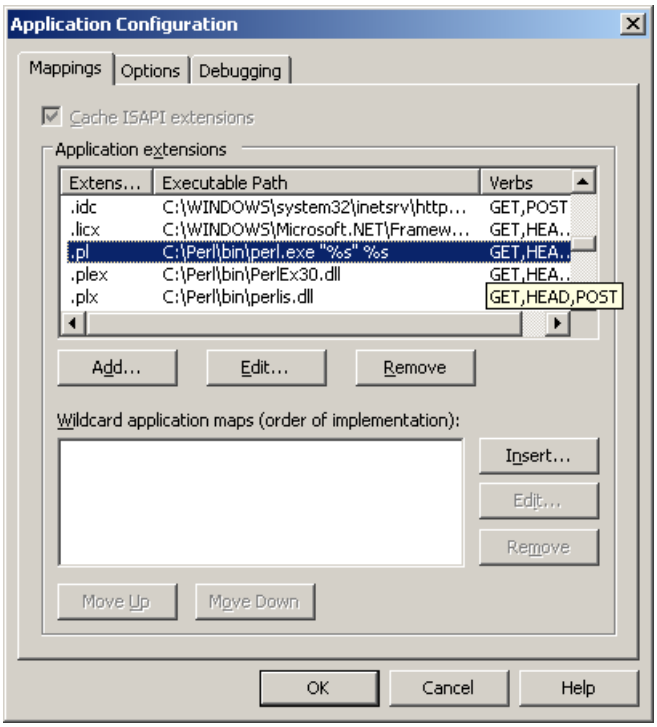
1. Perl（たとえば、ActivePerl）をインストールします。
2. 必要に応じて、仮想メディアヘルパーアプリケーションをカスタマイズします。
3. 仮想メディアヘルパースクリプトのWebサイトにディレクトリを作成し、そのディレクトリにスクリプトをコピーします。

   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。

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。HTTPS。
- 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 7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

iLO 7を搭載したGen12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。

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。

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、セカンダリ電源装置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。セカンダリ電源装置が省電力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。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、電源装置がより効率的で

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電源装置の最大電力出力の70%を超える電力を使用すると、セカンダリ電源装置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電源装置の60%未満の容量に低下すると、セカンダリ電源装置が省電力モードに戻ります。HEMを使用すると、プライマリ電源装置とセカンダリ電源装置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。

HEMを構成するには、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。

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。

電力割当て

Synergy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。

サーバー電力の管理

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

電源制御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。サーバーの電源状態は、オン、オフのいずれかになります。

手順

1. 左側のナビゲーションでホストをクリックします。

   ホストページが表示されます。

2. 電源をクリックします。

   電源ページが表示されます。

3. 電源がオンになると、次のオプションが表示されます。

   - 正常なシャットダウン
   - 強制電源オフ
   - 電源再投入
   - リセット

   強制電源オフ、リセット、および電源再投入のオプションは、サーバーの電源がオフになっている場合は使用できません。

   確認ウィンドウが表示されます。

4. 操作を続行するには要求を確認します。
5. 操作を取り消す場合はキャンセルボタンをクリックします。
6. ✕ をクリックして確認ウィンドウを閉じます。

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

- 正常なシャットダウン – 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。

- 強制電源オフ – 物理的な電源ボタンを5秒間押し続けてから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、キーを短く押すまたは長く押すか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。またCPUおよびI/Oリソースはリセットされます。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。
- 電源再投入 – ただちにサーバーの電源をオフにします。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. 左側のナビゲーションペインでホストをクリックし、電源制御をクリックします。

   電源制御ページが表示されます。

2. をクリックして、システム電源リストア設定を変更します。

   システム電源リストア設定ウィンドウが表示されます。

3. 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。

4. 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。

5. アップデートをクリックして設定を保存します。
6. 操作を取り消す場合はキャンセルボタンをクリックします。
7. をクリックしてウィンドウを閉じます。

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。

電力情報の表示

手順

1. 左側のナビゲーションペインでホストをクリックし、ハードウェアをクリックします。

   ハードウェアページが表示されます。

2. ハードウェアページの電源をクリックします。

   電源ページが表示されます。
   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。

サブトピック

サーバー電力使用量の表示
電源装置概要の詳細
電源装置のリスト

Power Discovery Services iPDU概要
電力読み取り値
パワーマイクロコントローラー
バッテリバックアップユニットの詳細
Smart Storage Energy Packのリスト
電力監視
高効率モード

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。

このタスクについて

電力グラフは、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。安全な電源オフまたは強制電源オフアクションを使用してもデータは消去されません。

手順

1. 左側のナビゲーションペインでホストをクリックし、ハードウェア＞電源をクリックします。

   電源ページが表示されます。

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、以下の凡例を選択またはクリアします。

   - 消費電力上限
   - 最大
   - 平均値
   - 合計ファン（推定）
   - 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、関連する凡例は表示されません。

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。

   - ページデータの自動更新を開始するには、自動更新トグルボタンをクリックします。

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。

   この値を設定した場合、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。

サブトピック

電力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

以下の凡例を使用して、電力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、関連する凡例は表示されません。

- 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。
- 合計ファン（推定）- サーバー内のすべてのファンの推定されるファン電力測定値の合計値。実際のファン電力測定値は、推定される測定値と異なる場合があります。
- 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。

電源ステータスの詳細

電源ステータステーブルには、以下の情報が表示されます。

- 消費電力 – サーバーが消費する電力。
- パワーレギュレーターモード – 設定されているパワーレギュレーターモード。
- 入力電圧 – サーバーに指定された入力電圧。

電源メトリックの詳細

電源メトリックテーブルには、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。
- 非冗長化 - 電源装置の少なくとも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。
- 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

値には、以下のものがあります。

- 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。

サブトピック

システムドメイン/システムドメイン1

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ドメイン1

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）。

注記
複数のGPUドメインをサポートするサーバーでは、個々のGPUドメインの冗長性に関する概要情報が表示されます。

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、ProLiant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。
- 状態 - 電源装置が搭載されているかどうかを示します。表示される値は、有効、無効、利用不可オフラインです。
- ヘルス - 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、警告、およびクリティカル）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

- 不一致 - 不一致の電源が存在するかどうか。値として"Yes"または"No"を指定できます。
- 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。
- 電力消費 - 各電源装置の電力消費量（W）。
- 容量 - 電源装置の容量（W）。
- ファームウェアバージョン - 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。

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。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。

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。

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の構成

前提条件

- iLOの構成
- 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://-WWWDOC-）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. 左側のナビゲーションペインでホストをクリックし、ハードウェアをクリックします。

   ハードウェアページが表示されます。

2. 電源をクリックします。

   電源ページが表示されます。

3. 設定をクリックします。

   電力設定ページが表示されます。

4. （パワーレギュレーターセクション）をクリックします。

   パワーレギュレーターウィンドウが表示されます。

5. パワーレギュレーターモードを選択します。

   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システムのみ
- OSコントロールモード - Intelシステムのみ

6. アップデートをクリックします。

   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。

   > **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システムでアップデートをクリックすると、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コントロールモードに変更した場合、またはOSコントロール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。

7. 再起動が必要である場合は、サーバーを再起動します。
8. ✕ をクリックしてパワーレギュレーターウィンドウを閉じます。
9. 操作を取り消す場合はキャンセルボタンをクリックします。

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。

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. 左側のナビゲーションペインでホストをクリックし、ハードウェア＞電源をクリックします。

   電源ページが表示されます。

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. アップデートをクリックします。

   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/quickspecs）でサーバー仕様をご覧ください。

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. 左側のナビゲーションペインでホストをクリックし、ハードウェアをクリックします。

   ハードウェアページが表示されます。

2. 電源をクリックします。

   電源ページが表示されます。

3. 設定をクリックします。

   電力設定ページが表示されます。

4. 編集をクリックします。

   編集ページが表示されます。

5. 消費電力上限を有効チェックボックスを選択します。

6. 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。

7. （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。

8. アップデートをクリックします。

   変更が正常に終了したことがiLOによって通知されます。

9. ✕ をクリックして編集ウィンドウを閉じます。

10. 操作を取り消す場合はキャンセルボタンをクリックします。

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、Insight Control電力管理を使用して設定/変更されます。
- 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

  ご使用のサーバーがサポートしている電力管理機能については、https://www.hpe.com/info/quickspecsにあるサーバーの仕様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。

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設定を有効または無効にすることができます。

手順

1. 左側のナビゲーションペインでホストをクリックし、ハードウェアをクリックします。

   ハードウェアページが表示されます。
2. 電源をクリックします。

   電源ページが表示されます。
3. 設定をクリックします。

   電力設定ページが表示されます。
4. その他の設定セクションで、マウス、キーボードの持続接続を構成します。

   設定が変更されたことがiLOによって通知されます。

電力しきい値超過によるSNMPアラート

このタスクについて

手順

1. 左側のナビゲーションペインでホストをクリックし、ハードウェアをクリックします。

   ハードウェアページが表示されます。
2. 電源をクリックします。

   電源ページが表示されます。
3. 設定をクリックします。

   電力設定ページが表示されます。
4. （電力しきい値超過によるSNMPアラートセクション）をクリックします。

   電力しきい値超過によるSNMPアラートウィンドウが表示されます。

5. 警告トリガーで次のいずれかのオプションを選択します。
   - 警告無効
   - ピーク電力消費
   - 平均電力消費
6. （ピーク電力消費または平均電力消費の場合のみ）警告しきい値（ワット）の値を設定します。
7. （ピーク電力消費または平均電力消費の場合のみ）持続時間（分）の値を設定します。
8. 構成を保存するには、アップデートをクリックします。
9. 操作を取り消す場合はキャンセルボタンをクリックします。
10. ✕ をクリックしてウィンドウを閉じます。

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。

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。

サブトピック

ファン情報の表示
最小ファン速度の構成

ファン情報の表示

このタスクについて

ファン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. 左側のナビゲーションペインでホストをクリックし、ハードウェア > 温度と冷却をクリックします。

   温度と冷却ページが表示されます。
   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。

サブトピック

ファン概要の詳細
ファンの詳細
HPE液冷モジュール情報の表示
温度情報

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。

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。
- 状態 - ファンの現在の状態。
- ヘルス - ファンのヘルスステータス。
- 速度 - ファン速度（%）。

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

1. 左側のナビゲーションペインでホストをクリックし、ハードウェアをクリックします。

   ハードウェアページが表示されます。

2. 温度と冷却をクリックします。

   温度と冷却ページが表示されます。

サブトピック

HPE液冷モジュールのサマリーの詳細
HPE液冷モジュールの詳細
HPE液体冷却モジュールの漏れステータスをクリアする

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。

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。
- 状態 – 冷却ポンプの状態。
- ヘルス - 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液体冷却モジュールの漏れステータスをクリアする

このタスクについて

液体冷却モジュールに漏れがある場合、サーバーの電源がオフになり、iLOは漏れ検出についてIMLに記録します。Hewlett Packard EnterpriseではAC電源を取り外すことをお勧めします。漏れが修理されたら、AC電源を復旧し、iLO RESTful APIまたはiLO Webインターフェイスを使用して、漏れステータスをクリアします。

> **注意**
> ボード上の液体をクリーニングおよびモジュールを交換（必要な場合）せずに、漏れのステータスをクリアすると、サーバーが損傷する可能性があります。

手順

1. 左側のナビゲーションペインでホストをクリックし、ハードウェア＞温度と冷却をクリックします。

   温度と冷却ページが表示されます。

2. 冷却ポンプセクションで、クリアをクリックします。

   確認ダイアログボックスが表示されます。

3. はい、クリアしますをクリックします。

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

温度センサーデータの表示
温度センサーの詳細

温度センサーデータの表示

手順

1. 左側のナビゲーションペインでホストをクリックし、ハードウェア＞温度と冷却をクリックします

   温度と冷却ページが表示されます。

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、 ＞ または ⌄ 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。

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。
- 座標 - 温度センサーのxおよびy座標。
- 状態 - センサーの現在の状態。表示される値は、有効および存在しないです
- ヘルス - 温度状態。
- 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。
- 注意 - 注意の警告に対する温度しきい値。
- クリティカル - クリティカルの警告に対する温度しきい値。

  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、iLOはCPUパッケージの温度も報告します。

iLOには通常、CPU温度が40～70℃で表示されます。パッケージ温度が上昇すると、iLOには対応するCPU温度の上昇が表示されます。しかし、例えば負荷が低いためにCPUが長時間アイドル状態になった場合、iLOでは温度が40℃未満の場合でも、CPU温度が40℃として表示されます。これは想定された動作です。

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. 左側のナビゲーションペインでホストをクリックし、ハードウェア＞温度と冷却をクリックします

   温度と冷却ページが表示されます。
   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. 設定をクリックします。

   ファン設定ページが表示されます。

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（%）を入力します。

4. 変更を保存するには、アップデートをクリックします。

5. 操作を取り消す場合はキャンセルボタンをクリックします。

6. ✕ をクリックしてファン設定ウィンドウを閉じます。

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. 左側のナビゲーションペインでホストをクリックし、ハードウェア＞温度と冷却をクリックします

   温度と冷却ページが表示されます。
   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. 設定をクリックします。

   ファン設定ページが表示されます。

3. 温度構成値を選択します。

4. アップデートをクリックします。

   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。

温度構成オプション

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。

冷却

プロセッサーに適切な冷却を提供します。

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。

スムーズな冷却

スムーズなファン応答を提供し、ファン速度の変動を低減します。

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.SetUserTem
   pThreshold/",
   "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。

   rawpost *filename*.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

パフォーマンス監視

パフォーマンス管理機能は、Intelプラットフォームにのみ適用されます。

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。

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。

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。

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。

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。

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。

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

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POSTのとき、次のメッセージが表示されます。

サーバー上のMCTP検出が無効です。MCTP検出を有効にして、このページの情報を表示または編集します。

サーバーが電源オフのとき、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. 左側のナビゲーションペインでホストをクリックし、パフォーマンスをクリックします。

パフォーマンスページが表示されます。

2. センサーのドロップダウンから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）自動更新トグルボタンを使用して、グラフを更新します。

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、ドロップダウンから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

自動更新トグルボタンを使用して、グラフを更新します。

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電力の上限しきい値がサポートされます。

手順

1. 左側のナビゲーションペインでホストをクリックし、パフォーマンスをクリックします。

   パフォーマンスページが表示されます。
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. （アラート設定セクション）をクリックします。
4. しきい値設定と滞留時間を入力し、アップデートをクリックします

   アラートを無効にするには、滞留時間を0に設定します。
5. 操作を取り消す場合はキャンセルボタンをクリックします。
6. をクリックしてウィンドウを閉じます。

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

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。

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。

例えば、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。

この機能は、サポートされているサーバーで使用できます。

サブトピック

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

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. 左側のナビゲーションペインでホストをクリックし、パフォーマンスをクリックします。

   パフォーマンスページが表示されます。
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。

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。

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. 左側のナビゲーションペインでホストをクリックし、パフォーマンスをクリックします。

   パフォーマンスページが表示されます。
2. ドロップダウンリストから値を選択します。

   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、編集をクリックします。
5. 必要に応じて、チューニングオプションを変更し、アップデートをクリックします。

   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。

   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。
6. 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

パフォーマンスチューニングの設定

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コントロールモード

> **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

ネットワーク設定にアクセスするために、iLO専用ネットワークポートページまたはiLO共有ネットワークポートページでアクティブなNICを選択できます。

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

1. 左側のナビゲーションペインでiLO設定をクリックし、iLOネットワークポートをクリックします。

   iLOネットワークポートページが表示されます。次のセクションでネットワーク設定を表示できます。

   - 一般情報
   - IPv4設定
   - IPv6設定
   - SNTP設定

2. ネットワーク構成に応じて、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。

   選択内容に応じて、iLO専用ネットワークポートページまたはiLO共有ネットワークポートページに、構成されたネットワークの詳細が表示されます。

サブトピック

ネットワーク一般情報

一般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。
- 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。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。
- 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接続は、最大100 Mbpsの速度で動作できます。

  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。
- 現在のデュプレックス – 全二重または半二重。
- 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。
- 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。
- 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。

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。

一般的なネットワーク設定

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一般情報ページを使用して、iLOホスト名とNIC設定を構成します。

サブトピック

iLOホスト名の設定
NIC設定

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. 左側のナビゲーションペインでiLO設定をクリックし、iLOネットワークポートをクリックします。

   iLOネットワークポートページが表示されます。

2. 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。

   選択内容に応じて、iLO専用ネットワークポートページまたはiLO共有ネットワークポートページが表示されます。

3. （一般情報セクション）をクリックします。

一般情報ウィンドウが表示されます。

4. 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。

   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。

5. 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。

6. 変更を保存するには、アップデートをクリックします。

   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. 操作を取り消す場合はキャンセルボタンをクリックします。

8. ✕ をクリックして編集ウィンドウを閉じます。

9. （オプション）IPv4またはIPv6の各セクションで、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

iLOホスト名とドメイン名の制限

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** – この問題を回避するために、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名でiLOプロセッサーが接続できていることを確認する
  - 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名をフラッシュする。
- 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。

詳しくは、iLOのユーザーガイドを参照してください。

NIC設定

一般情報セクションの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。

サブトピック

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。

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. 左側のナビゲーションペインでiLO設定をクリックし、iLOネットワークポートをクリックします。

   iLOネットワークポートページが表示されます。
3. 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。

   選択内容に応じて、iLO専用ネットワークポートページまたはiLO共有ネットワークポートページが表示されます。
4. （一般情報セクション）をクリックします。

   一般情報ウィンドウが表示されます。
5. 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。
6. リンク設定を選択します。
7. 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。
8. 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。

   1～4096の値を入力します。
9. 変更を保存するには、アップデートをクリックします。

   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セクションまたはiLO共有ネットワークポートセクションに表示されます。
10. （オプション）IPv4またはIPv6の各セクションで、その他のネットワーク設定を構成します。

11. 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

専用ネットワークポートの全般設定

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 - OCP Slot Aまたは共有ネットワークポート - OCP Slot Bに接続します。
2. 左側のナビゲーションペインでiLO設定をクリックし、iLOネットワークポートをクリックします。

   iLOネットワークポートページが表示されます。
3. iLO共有ネットワークポートをクリックします。

iLO共有ネットワークポートページが表示されます。

4. （一般情報セクション）をクリックします。

   一般情報ウィンドウが表示されます。

5. 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。
6. 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。
7. ポートメニューから値を選択します。
8. 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。
9. 仮想LAN機能を有効にした場合は、VLANタグを入力します。
10. 変更を保存するには、アップデートをクリックします。

    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ページまたはiLO共有ネットワークポートページに表示されます。

11. （オプション）IPv4またはIPv6の各セクションで、その他のネットワーク設定を構成します。
12. 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。

    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 - OCP Slot Aまたは共有ネットワークポート - OCP Slot B経由で転送されるようになります。

サブトピック

共有ネットワークポートの全般設定

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に独立した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 Slot A - 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OCP Slot B - 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/quickspecs

サブトピック

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OS NICドライバーのロードおよびアンロード時に、短い時間（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、最大100 Mbpsの速度で動作できます。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、iLO 7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/quickspecs**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. 左側のナビゲーションペインでiLO設定をクリックし、iLOネットワークポートをクリックします。

   iLOネットワークポートページが表示されます。
2. ネットワーク構成に応じて、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。

   選択内容に応じて、iLO専用ネットワークポートページまたはiLO共有ネットワークポートページが表示されます。
3. IPv4セクションをクリックします。

   IPv4ページが表示されます。
4. ✎ を次のセクションでクリックして、設定を構成します。

- DHCPv4構成
- DNS構成
- 静的経路構成
- 開始時にゲートウェイにping

静的IPv4設定は、静的IPv4アドレス構成セクションに表示されます。

5. 必要な変更を加えた後、アップデートをクリックします。

   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. 操作を取り消す場合はキャンセルボタンをクリックします。
7. ✕ をクリックして編集ウィンドウを閉じます。
8. （オプション）全般またはIPv6の各セクションで、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。

サブトピック

DHCPv4構成設定
静的IPv4アドレス構成設定
IPv4 DNS構成設定
IPv4の静的経路構成設定
その他のIPv4設定

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ボックス、静的経路 #2ボックス、および静的経路 #3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。

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。iLO 7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。例えば、iLO 7 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 Address

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を使用しない場合は、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. 左側のナビゲーションペインでiLO設定をクリックし、iLOネットワークポートをクリックします。

   iLOネットワークポートページが表示されます。

2. ネットワーク構成に応じて、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。

   選択内容に応じて、iLO専用ネットワークポートページまたはiLO共有ネットワークポートページが表示されます。

3. IPv6セクションをクリックします。

   IPv6ページが表示されます。

4. を次のセクションでクリックして、設定を構成します。

   - DHCPv6構成
   - グローバルIPv6構成
   - DNS構成
   - 静的IPv6アドレス構成
   - 静的経路構成

5. 必要な変更を加えた後、アップデートをクリックします。

   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. 操作を取り消す場合はキャンセルボタンをクリックします。

7. をクリックして編集ウィンドウを閉じます。

8. （オプション）全般またはIPv4の各セクションで、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。

サブトピック

DHCPv6構成設定
グローバルIPv6構成設定
IPv6 DNS構成設定

静的IPv6アドレス構成設定
IPv6の静的経路構成設定
IPv6をサポートしているiLOの機能

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。

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を構成する場合、名前リゾルバーから受信したアドレスの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。

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。

iLO SNTP設定の構成

前提条件

iLOの設定を構成する権限

- 管理ネットワーク上で1台以上のNTPサーバーが利用可能である。
- DHCPv4が提供するNTPサービス構成を使用する場合、IPv4ページで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ページでDHCPv6ステートレスモードが有効になっている。

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、iLOネットワークポートをクリックします。

   iLOネットワークポートページが表示されます。

2. SNTPセクションをクリックします。
3. 次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. iLOタイムゾーン情報はDHCPサーバーから自動的に取得されません。タイムゾーンリストからタイムゾーンを手動で選択します。
5. 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。
6. 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。

7. 変更を保存するには、アップデートをクリックします。

   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ページまたはiLO共有ネットワークポートページに表示されます。

8. 操作を取り消す場合はキャンセルボタンをクリックします。
9. ✕ をクリックして編集ウィンドウを閉じます。
10. （オプション）全般、IPv4、IPv6、SNTPの各ページで、その他のネットワーク設定を構成します。
11. 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

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#PRODABR#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。

  HPE OneView for Synergyサーバーをntp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）を使用するように設定してください。

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。

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。

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。

iLOと連携し、サポートされるアプリケーションにサービスアカウントが必要な場合は、ユーザーアカウントを追加して、このアカウントをサービスアカウントとして指定できます。また、サポートされるアプリケーションまたはiLO RESTful APIを使用して、サービスアカウントを追加することもできます。

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

アプリケーションアカウント

アプリケーションアカウントはiLOのサービスアカウントで、iLOとの間で安全に認証および通信するためにホストアプリケーションによって使用されます。iLOと連携し、サポートされるアプリケーションにアプリケーションアカウントが必要な場合は、ホストOSアプリケーションからアプリケーションアカウントを作成できます。アプリケーションアカウントを使用して作成されたセッションは、仮想NIC上のインバンドチャネルを通じてのみ機能します。

アプリケーションアカウントを作成するにはiLOユーザーアカウント管理権限が必要です。アカウント権限について詳しくは、アカウント権限セクションを参照してください。

アプリケーションアカウントは、iLO Webインターフェイスを使用して表示および削除できます。Hewlett Packard Enterpriseでは、アプリケーションアカウントをホストアプリケーションのCLIコマンドから削除することをお勧めします。

アプリケーションアカウントはHPEアプリケーションでのみ使用できます。

サブトピック

アプリケーションアカウントの詳細の表示

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、ユーザー管理をクリックします。

   ユーザー管理ページが表示されます。

2. ユーザーをクリックします。

   ユーザーページが表示されます。
   アプリケーションアカウントセクションには、アプリケーションアカウントごとのアプリケーション名およびアプリケーションID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。

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。

ユーザー（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。

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、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設定の構成 - 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 Webインターフェイス
  - iLO RESTful API

  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

  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。

  （アプリケーションアカウントのみ）アプリケーションアカウントを作成するにはユーザーアカウント管理権限が必要で

すが、アプリケーションアカウントには、アカウントの作成に使用されたユーザーアカウントの権限のみが付与されます。

- 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管理者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。

  リカバリセット権限を持つユーザーアカウントがなく、この権限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、リカバリセット権限を持つデフォルトの管理者アカウントが作成されます。

次の権限は、UEFIシステムユーティリティのiLO 7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

ユーザー管理設定

手順

1. 左ナビゲーションペインでiLO 設定をクリックし、ユーザー管理をクリックします。

   ユーザー管理ページが表示されます。次のページに移動できます。

2. （設定セクションの横）をクリックします。

   設定ウィンドウが表示されます。

3. 必要な変更を加えた後、アップデートをクリックします。
4. 操作を取り消す場合はキャンセルボタンをクリックします。
5. をクリックして設定ウィンドウを閉じます。

サブトピック

アカウントサービスのアクセス設定オプション

アカウントサービスのアクセス設定オプション

ユーザー管理の設定ページでは、以下の設定を構成できます。

遅延の前の認証エラー

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。例えば、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を作成または編集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。

アイドル接続タイムアウト（分）

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、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。
有効な値は15、30、60、120分、またはInfinite（無期限）です。

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。オペレーターレベルを満たさない権限の任意の組み合わせは、IPMIユーザーです。

- オペレーター - オペレーターは、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。

  IPMIオペレーター権限については、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。管理者レベルを満たさないオペレーター以上の権限の任意の組み合わせは、IPMIユーザーです。

- 管理者 - 管理者は、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管理者権限については、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. 左ナビゲーションペインでiLO設定をクリックし、ユーザー管理をクリックします。

   ユーザー管理ページが表示されます。

2. ユーザーをクリックします。

   ユーザーページが表示されます。
   ローカルユーザーテーブルは、各ローカルユーザーのログイン名、ユーザー名、ステータス、役割、CAC/スマートカード証明書指紋、およびSSH公開鍵を表示します。

   サービスアカウントが構成されている場合、サービスアカウントテーブルでは各サービスアカウントのログイン名、ユーザー名、ステータス、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。

   アプリケーションアカウントが構成されている場合、アプリケーションアカウントテーブルでは、サービスアカウントごとのアプリケーション名およびアプリケーションIDが表示されます。アプリケーション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。

ユーザーアカウントの管理

アクションメニューから以下のタスクを実行できます。

- ユーザーの編集
- CAC/スマートカード証明書のインポート
- 新しいSSHキーの認証
- ユーザーを無効
- ユーザーの削除
- CAC/スマートカード証明書を削除
- SSHキーを削除

ユーザーアカウントの有効化

前提条件

ユーザーアカウント管理権限

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、ユーザー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. ユーザーをクリックします

   ユーザーページが表示されます

3. 有効にするユーザーアカウントを選択し、アクション＞ユーザーを有効をクリックします。

   ユーザーを有効ウィンドウが表示されます。

4. 要求を確認するメッセージが表示されたら、はい、有効にしますをクリックします。

   iLOは、選択したアカウントが有効になったことを通知します。

5. 操作を取り消す場合はキャンセルボタンをクリックします。

6. ✕ をクリックしてユーザーを有効ウィンドウを閉じます。

ユーザーアカウントの無効化

前提条件

ユーザーアカウント管理権限

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、ユーザー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. ユーザーをクリックします

   ユーザーページが表示されます

3. 無効にするユーザーアカウントを選択し、アクション＞ユーザーを無効をクリックします。

   ユーザーを無効ウィンドウが表示されます。

4. 要求を確認するメッセージが表示されたら、はい、無効にしますをクリックします。

   iLOは、選択したアカウントが無効になったことを通知します。

5. 操作を取り消す場合はキャンセルボタンをクリックします。

6. ✕ をクリックしてユーザーを無効ウィンドウを閉じます。

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. 左側のナビゲーションペインでiLO設定をクリックし、ユーザー管理をクリックします。

   ユーザー管理ページが表示されます。

2. ユーザーをクリックします

   ユーザーページが表示されます。

3. ユーザー＞ ✚ 追加をクリックします。

   ユーザーウィンドウが表示されます。

4. 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

5. （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。

6. 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。

7. (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。

8. 新しいユーザーを保存するには、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。

9. 操作を取り消す場合はキャンセルボタンをクリックします。

10. ✕ をクリックしてユーザーを追加ウィンドウを閉じます。

サブトピック

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

iLOユーザーアカウントオプション

- 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。ユーザー名は最長で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。
- 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。
- 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。

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）。
- ユーザーアカウントのパスワードの最低文字数は、ユーザー管理 > 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。

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. 左側のナビゲーションペインでiLO設定をクリックし、ユーザー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. ユーザーをクリックします。

   ユーザーページが表示されます。

3. ユーザーアカウントを選択して、アクション > ユーザーの編集を選択します。

   ユーザーの編集ウィンドウが表示されます。

4. 必要に応じて、以下の値をアップデートします。

   - ユーザー名
   - ログイン名

5. 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、新しい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。

6. （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。

7. ユーザーアカウントの変更を保存するには、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。

8. 操作を取り消す場合はキャンセルボタンをクリックします。

9. ✕ をクリックしてユーザーの編集ウィンドウを閉じます。

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. 左側のナビゲーションペインでiLO設定をクリックし、ユーザー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. ユーザーをクリックします

   ユーザーページが表示されます。

3. 無効にするユーザーアカウントを選択し、アクション > ユーザーの削除をクリックします。

ユーザーの削除ウィンドウが表示されます。

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ることを通知します。

5. 操作を取り消す場合はキャンセルボタンをクリックします。

6. ✕ をクリックしてユーザーの削除ウィンドウを閉じます。

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。

サブトピック

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（例えば、CN=Group1, OU=Managed Groups, DC=domain, DC=extension）。

  短縮されたDNもサポートされます（例えば、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。

- 役割（セキュリティID）- グループのメンバーの役割。

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設定の構成 - 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、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. 左側のナビゲーションペインでiLO設定をクリックし、ユーザー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. ディレクトリグループをクリックします

   ディレクトリグループページが表示されます。
   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、および役割が表示されます。

ディレクトリグループの追加

前提条件

- ユーザーアカウント管理権限

- 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. 左側のナビゲーションペインでiLO設定をクリックし、ユーザー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. ディレクトリグループをクリックします

   ディレクトリグループページが表示されます。

3. ディレクトリグループ＞＋追加をクリックします。

   ディレクトリグループの追加ウィンドウが表示されます。

4. 次の詳細情報を指定してください。
   - グループDN
   - グループSID（Kerberos認証およびActive Directory統合のみ）
   - 役割
5. 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
6. 新しいディレクトリグループを保存するには、アップデートをクリックします。
7. ✕をクリックしてディレクトリグループの追加ウィンドウを閉じます。

ディレクトリグループの編集

前提条件

- ユーザーアカウント管理権限
- 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. 左側のナビゲーションペインでiLO設定をクリックし、ユーザー管理をクリックします。

   ユーザー管理ページが表示されます。

2. ディレクトリグループをクリックします

   ディレクトリグループページが表示されます。

3. ディレクトリグループセクションでグループを選択し、アクション > 編集をクリックします。

   ディレクトリグループの編集ウィンドウが表示されます。

4. 次の詳細情報を指定してください。
   - グループDN
   - グループSID（Kerberos認証およびActive Directory統合のみ）

5. 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

6. ディレクトリグループの変更を保存するには、アップデートをクリックします。
7. ✕ をクリックしてディレクトリグループの編集ウィンドウを閉じます。

ディレクトリグループの削除

前提条件

- ユーザーアカウント管理権限
- 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. 左側のナビゲーションペインでiLO設定をクリックし、ユーザー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. ディレクトリグループをクリックします

ディレクトリグループページが表示されます。

3. ディレクトリグループセクションでグループを選択し、アクション＞削除をクリックします。

   ディレクトリグループを削除ウィンドウが表示されます。

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。

5. グループが削除されたことがiLOによって通知されます。

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 7ライセンスガイドを参照してください。

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、ライセンスをクリックします。

   ライセンスページが表示されます。

2. ライセンスのインストールをクリックします。

   ライセンスのインストールウィンドウが表示されます。

3. アクティブ化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。

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。

   これで、ライセンスキーは有効になります。

サブトピック

iLO Webインターフェイスでのインストール済みライセンスの表示

iLO Webインターフェイスでのインストール済みライセンスの表示

手順

左側のナビゲーションペインでiLOiLO設定をクリックし、ライセンスをクリックします。

ライセンスページが表示されます。
このページから現在のライセンスのステータスを表示したり、ライセンスをインストールしたりすることができます。

サブトピック

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HPE Compute Ops Managementに自動的に付属します
- 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。
- ライセンスキーをなくした場合、HPE iLO 7ライセンスガイドに記載されている、なくなったライセンスキーに対する手順に従います。
- 以下については、https://www.hpe.com/support/ilo-docsのHPE iLO 7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。
- ライセンスキーの購入、登録、および取得については、次のWebサイトを参照してください。https://www.hpe.com/support/ilo-docs

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。
- マイHPEソフトウェアセンターを通じたソフトウェアアップデートへのアクセス。
- マイHPEソフトウェアセンターを通じて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。
- 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

iLO 7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

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。

キーマネージャーサーバーの構成

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。
- iLOの設定を構成する権限
- 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. 左側のナビゲーションペインでセキュリティをクリックし、リモートキーマネージャーをクリックします。

   リモートキーマネージャーページが表示されます。
2. （サーバーセクション）をクリックします。

   サーバーウィンドウが開きます。
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. アップデートをクリックします。

   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

- 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
- 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. 左側のナビゲーションペインでセキュリティをクリックし、リモートキーマネージャーをクリックします。

   リモートキーマネージャーページが表示されます。

2. （構成セクション）をクリックします。

   構成ウィンドウが表示されます。

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. アップデートをクリックします。

   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。

       このパスワードはRESTful API PATCHコマンドを使用して変更することもできます。

       `"/redfish/v1/Managers/1/SecurityService/ESKM/"`

       新しいパスワードを作成するときは、次のルールが適用されます。

       - 過去6回のパスワードは使用できません
       - パスワードの最小文字数は8文字、最大文字数は16文字です
       - パスワードは小文字、大文字、数字、特殊文字の組み合わせにする必要があります
     - 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>という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、リモートキーマネージャーページのインポート済み証明書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. 左側のナビゲーションペインでセキュリティをクリックし、リモートキーマネージャーをクリックします。

   リモートキーマネージャーページが表示されます。

2. 接続テストをクリックします。

   テスト結果は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. 左側のナビゲーションペインでセキュリティをクリックし、リモートキーマネージャーをクリックします。

   リモートキーマネージャーページが表示されます。

2. イベントセクションにスクロールします。

   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. 左側のナビゲーションペインでセキュリティをクリックし、リモートキーマネージャーをクリックします。

   リモートキーマネージャーページが表示されます。

2. イベントログ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。

3. はい、削除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勧めします。

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。

サブトピック

言語パックのインストール

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 <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. 次のいずれかの手順を使用してファームウェアのアップデートページに移動します。
   - 左側のナビゲーションペインでファームウェアをクリックし、クイックアクションメニューからファームウェアのアップデートをクリックします。

     または
   - 左側のナビゲーションペインでファームウェアをクリックし、ファームウェアインベントリ＞ファームウェアのアップデートをクリックします
     または
   - 左側のナビゲーションペインでiLO設定をクリックし、言語をクリックします。言語ページで、言語パックのインストールリンクをクリックし、ファームウェアインベントリ＞ファームウェアのアップデートページに移動します。

   ファームウェアのアップデートオプションが表示されない場合は、ファームウェアページの右上隅にある省略記号アイコンをクリックします。
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. アップデートをクリックします。

   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。

言語パックの選択

このタスクについて

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、言語をクリックします。

   言語ページが表示されます。

2. インストールされた言語リストから必要な言語をクリックして、言語パックを選択します。

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

この手順を使用して、デフォルトの言語を構成します。

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、言語をクリックします。

   言語ページが表示されます。

2. 言語ページで既定の言語を設定をクリックします。

   iLOデフォルト言語ウィンドウが表示されます。

3. 言語ドロップダウンから値を選択します。

   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。

4. アップデートをクリックします。

   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。

5. 操作を取り消す場合はキャンセルボタンをクリックします。

6. ✕ をクリックして既定の言語を設定ウィンドウを閉じます。

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. 左側のナビゲーションペインでiLO設定をクリックし、言語をクリックします。

   言語ページが表示されます。

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。

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. 左側のナビゲーションペインでiLO設定をクリックし、言語をクリックします。

   言語ページが表示されます。

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。

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**
> 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。

Smart Update Manager（SUM）では、HPE ProLiant RL3xx Gen 11プラットフォームをサポートしていません。

手順

1. サポートされるHPE Service Pack for HPE ProLiant、HPE Synergy Service Pack、またはHPE 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

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。

  ユーザー管理 > 設定ページでこのタスクを実行できます。

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。

  iLO設定のアクセスページでこのタスクを実行できます。
- 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。

  ホストタブのリモートコンソール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ページにある、リモートコンソールコンピューターロック設定を構成します。
- UEFIシステムユーティリティでiLO 7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。

  iLO設定のアクセスページでこのタスクを実行できます。
- UEFIシステムユーティリティでROMベースの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。

  iLO設定のアクセス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。

  iLO設定のアクセス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。
- 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 。

  ファームウェア＞ファームウェア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できる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、セキュリティのSSL証明書ページとホストのリモートコンソールページで完了できます。

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。

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構成します。

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。

CAC Smartcard

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構成します。

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。

ディレクトリとLDAP

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。

暗号化とセキュリティ

iLOのセキュリティ状態をデフォルト値（セキュア標準）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

表 1. iLOの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	
IPMI over KCS	有効	
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トラップポート	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 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	

その他の発信ポート

セキュリティ管理者は、**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こくことが必要な場合があります。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
DNS解決	53	UDP
SSDPマルチキャスト	1900	UDP
DHCPv4	67、68	UDP
DHCPv6	547	UDP
NTP	123	UDP
Kerberos KDCサーバーポート	88	TCP、UDP
ディレクトリサーバーLDAP SSLポート	636	TCP
アラートメールSMTPポート	25	TCP
リモートSyslogポート	514	UDP
キーマネージャーのポート	9000	TCP
リモートサポートのポート	7906	TCP

iLOでサポートされていないポート

iLOは、**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（Secure 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。

iLOは認証のためにSPDM仕様v1.0、v1.0.1、v1.1、およびv1.2をサポートします。いずれのSPDMバージョンもサポートしていないデバイスの場合、iLOはSPDM障害のセキュリティログイベントをログに記録します。

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

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。

ポリシー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

ポリシー設定の構成グローバルコンポーネントの完全性の有効化

ポリシー設定の構成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
- SPDMをサポートするUBM

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、ポリシーをクリックします。

   ポリシーページが表示されます。

2. （セキュリティセクション）をクリックします。

   セキュリティウィンドウが表示されます。

3. （全般セクション）をクリックします。

   全般ウィンドウが表示されます。

4. 必要な変更を加えた後、アップデートをクリックします。
5. 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。
6. コンポーネントの完全性ポリシーを選択します。
7. 構成を保存するには、アップデートをクリックします。
8. 操作を取り消す場合はキャンセルボタンをクリックします。
9. をクリックしてセキュリティウィンドウを閉じます。

サブトピック

ポリシー設定オプション

ポリシー設定オプション

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。

> **注記**
> コンポーネントの完全性ポリシーは、MHSベースシステムのホストプロセッサーモジュールにも適用されます。

一般的な設定

ポリシーページで以下の設定を有効または無効にすることもできます。

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": "1.11.00",
"ManagerType": "iLO 7",
"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の匿名呼び出しでは、次の情報が除外されます。`ManagerFirmwareVersion`、`ManagerType`、`Status`。

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 7トラブルシューティングガイドを参照してください。

サーバーヘルスサマリー画面について詳しくは、iLO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。

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。コンポーネントの完全性ポリシーは、MHSベースシステムのホストプロセッサーモジュールにも適用されます。

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 IDevIDPCA）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 IDevIDPCA
- iLO LDevID

サブトピック

iLO LDevID
iLO IDevIDPCA

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。Hewlett Packard Enterpriseでは、iLO IDevIDのプライバシーを確保するために、常にLDevIDを使用することをお勧めします。

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
インポートされたLDevID証明書の表示
インポートされたLDevID証明書の削除
LDevID証明書の置き換え

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。

iLO IDevIDPCA

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 IDevIDPCAと呼ばれます。HPEサーバーは、802.1X認証用のIDevIDPCA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 IDevIDPCAは生涯有効であり、不変です。

サブトピック

iLO IDevIDPCAの機能

iLO IDevIDPCAの機能

iLO IDevIDPCA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 IDevIDPCA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/BMCIDevIDPCA/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 LDevID、iLO HPE LDevID、iLO LAK、System LDevID、およびSystem LAKは、One-buttonセキュア消去後に削除されます。iLO IDevIDPCA、iLO IAK、システムIDEVID、およびシステムIAK証明書は、One-buttonセキュア消去後には削除されません。

Hewlett Packard Enterpriseでは、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 LDevID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 LDevID、iLO HPE LDevID、iLO LAK、システムIDevID、システムIAK、システムLDevID、およびシステムLAKは無効になりますが、iLO IDevIDPCAとiLO IAKは証明書内のPCAシリアル番号を使用するため有効になります。新しいボードで無効なIDは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、iLO HPE LDevID、iLO LAK、システムIDevID、システムIAK、システムLDevID、およびシステムLAK）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、以前にバックアップしたiLO IDevIDPCAおよびLDevIDをリストアするか、または新しい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、HPE iLO IDevIDPCAとHPE iLO LDevIDが、IEEE 802.1X認証のためのサーバーIDになります。

802.1X認証

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 iLO 7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サポートします。工場出荷時にプロビジョニングされたサーバーIDであるIDevIDを使用して、HPEサーバーは、無人自律操作用に、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 IDevIDPCA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 LDevIDがない場合、iLO 7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。

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/iLO IDevIDPCA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（例えば、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）。

> **注記**
> 工場で一度にプロビジョニングされる証明書は、iLO IDevIDまたはiLOIDevIDPCAのいずれか1つだけです。

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
iLO機能の無効化
SSHクライアントによるiLOログイン
時間設定の構成

iLOアクセス設定の構成

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機能の無効化セクションを参照してください。

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、アクセスをクリックします。

   アクセスページが表示されます。

2. （アップデートするアクセス設定カテゴリの横にある）をクリックします。

   以下から選択します。

   - IPMI/DCMI over LAN
   - IPMI/DCMI over LANポート
   - IPMI over KCS
   - 仮想シリアルポートログover CLI
   - ダウンロード可能な仮想シリアルポートログ
   - 検出
   - 通知間隔
   - IPv6マルチキャストスコープ
   - 存続時間（TTL）
   - SNMP
   - SNMPリクエストポート
   - SNMPトラップポート
   - セキュアシェル（SSH）
   - セキュアシェル（SSH）ポート
   - Webプロキシ
   - Webプロキシサーバー
   - Webプロキシ ポート
   - Webプロキシユーザー名
   - iLO ROMベースセットアップユーティリティ
   - iLOのWebインターフェイス
   - 仮想NIC

   > **注記**
   > アクセスページではリモートコンソールおよび仮想メディア状態のみ表示できます。リモートコンソールまたは仮想メディアリンクをクリックしてそれぞれのページに移動し、設定を編集します。

   編集ウィンドウが表示されます。

3. 必要に応じて設定をアップデートし、アップデートをクリックします。

   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。例えば、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。

例えば、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. 操作を取り消す場合はキャンセルボタンをクリックします。
5. ✕ をクリックして編集ウィンドウを閉じます。
6. 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。
7. 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。

サブトピック

アクセス設定オプション

アクセス設定オプション

アクセス設定ページでは、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。

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。

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。

IPMI over KCS

IPMI over Keyboard Controller Style (KCS) を使用すると、ホストOS内からコンピューターシステムを管理し、操作を監視できます。

IPMI over KCSオプションを使用して、KCSインターフェイスを有効または無効にすることができます。

この設定は、デフォルトで有効になっています。

新しいバージョンにアップグレードするとき、IPMI over KCSのデフォルト値は以前の構成設定に基づいて保存されます。

KCSインターフェイスを有効または無効にするコマンド

揮発性構成

コマンドの構文--0x06 command: 0x41(get)/0x40(set) interface : 0x0F(KCS) conf:0x82(enable)/0x80(disable) 0x00
KCSインターフェイスを有効にするには、#> ipmitool -I lanplus -H <IPアドレス> -U <ユーザー 名> -P <パスワード> raw 0x06 0x40 0x0F 0x82 0x00 コマンドを実行します。
KCSインターフェイスのステータスを確認するには、#> ipmitool -I lanplus -H <IPアドレス> -U <ユーザー名> -P <パスワード> raw 0x06 0x41 0x0F 0x80 コマンドを実行します。
応答データ：02 04

02 -- KCSが有効であることを示します

04 -- 管理者権限を示します

KCSインターフェイスを無効にするには、 #> ipmitool -I lanplus -H <IPアドレス> -U <ユーザー 名> -P <パスワード> raw 0x06 0x40 0x0F 0x80 0x00 コマンドを実行します。

不揮発性構成

コマンドの構文--0x06 command: 0x41(get)/0x40(set) interface : 0x0F(KCS) conf:0x42(enable)/0x40(disable) 0x00
KCSインターフェイスを有効にするには、#> ipmitool -I lanplus -H <IPアドレス> -U <ユーザー名> -P <パスワード> raw 0x06 0x40 0x0F 0x42 0x00 コマンドを実行します。
KCSインターフェイスのステータスを確認するには、#> ipmitool -I lanplus -H <IPアドレス> -U <ユーザー名> -P <パスワード> raw 0x06 0x41 0x0F 0x40 コマンドを実行します。
応答データ：02 04

02 -- KCSが有効であることを示します

04 -- 管理者権限を示します

KCSインターフェイスを無効にするには、 #> ipmitool -I lanplus -H <IPアドレス> -U <ユーザー 名> -P <パスワード> raw 0x06 0x40 0x0F 0x40 0x00 コマンドを実行します。

注記

- 揮発性構成では、KCSインターフェイスの有効化または無効化はIPMIツールを介してのみ可能です。
- 揮発性構成を変更しても、不揮発性構成には影響しません。
- 不揮発性構成では、Redfish、iLO Webインターフェイス、またはIPMIツールを通じてKCSインターフェイスの有効化または無効化が可能です。
- 不揮発性構成の変更は、揮発性構成にも影響します。

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、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

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://-WWWDOC-）にあるライセンス文書を参照してください。

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。

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。

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。

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。

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。

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。

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。

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。

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アドレスを指定します。

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プロキシユーザー名を指定します。

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。

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。
- 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。iLO 7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。

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機能をもう一度有効にするには、UEFIシステムユーティリティを使用します。

   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

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を使用してiLO機能を再度有効にできます。

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。

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。

時間設定の構成

前提条件

- SNTP構成が設定されていません

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、時刻をクリックします。

   または、ダッシュボードページのiLO日付/時刻リンクをクリックして時刻ページに移動できます。

   時刻ページが表示されます。

   > **注記**
   > SNTPが構成されていない場合、デフォルトで時刻のソースはローカルに設定されます。
   > SNTPが構成されている場合、時刻のソースはネットワークに設定されます。

2. （概要セクション）をクリックします。

   概要ウィンドウが表示されます。

3. （日付ボックス内）をクリックします。

   カレンダーが表示されます。

4. 日付を選択します。
5. iLO時刻ボックスで時刻を選択します。
6. タイムゾーンドロップダウンから必要なタイムゾーンを選択します。
7. 変更を保存するには、アップデートをクリックします。
8. 操作を取り消す場合はキャンセルボタンをクリックします。
9. をクリックして概要ウィンドウを閉じます。
10. iLO日付/時刻の構成が終了したら、iLOをリセットします。

    接続が再確立されるまでに、数分かかることがあります。

SNTPオプションを使用して時刻を設定するには、iLO SNTP設定の構成を参照してください。

サブトピック

時間設定オプション

時間設定オプション

時刻のソース

時刻のソースをネットワークまたはローカルのどちらかで表示します。

iLO 時刻

設定されているiLO時刻を表示します。

ユーザー設定による時刻表示

環境設定で設定されているタイムゾーン設定を表示します。

タイムゾーン

設定されているタイムゾーンを表示します

iLOサービスポート

サービスポートは、サーバーの前面にある、**iLO**のラベルが付けられているUSBポートです。

お使いのサーバー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/quickspecs**）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OSはアクセスできません。
- 標準のUSB Type A - Type CケーブルまたはUSB Type C - Type Cケーブルを使用してホストシステム（Windows/MAC/Linuxラップトップまたはデスクトップ）を接続し、次のものにアクセスします。
  - iLOのWebインターフェイス
  - リモートコンソール
  - iLO RESTful API
  - CLI

> **注記**
> サーバーOSを搭載したホストシステムをサービスポートに接続することはサポートされていません。

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。

サブトピック

サポートされていないUSBポート
iLOサービスポート経由でのActive Health Systemログのダウンロード
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

サポートされていないUSBポート

- USB Type CからUSB Type Aへのアダプターはサポートされていません。
- USB Type CからRJ45へのアダプターはサポートされていません。

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。

サブトピック

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

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

iLOサービスポートを通して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 Type A - Type CケーブルまたはType C - Type Cケーブルを使用して、クライアントをサービスポートに接続します。サポートされるUSBケーブルの長さは最大1mです。

   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。

サブトピック

Windows 10でのドライバー選択

Windows 10でのドライバー選択

前提条件

- iLOサービスポートおよびUSB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。

このタスクについて

Windows 10ホストを使用してiLOネットワークにアクセスしている場合は、サーバーごとに以下の手順に従います。これは一度限りの構成です。

手順

1. デバイスマネージャーを開きます。
2. その他のデバイスに移動します。
3. CDC NCMを選択します。
4. 右クリックメニューからドライバーのアップデートを選択します。

   ドライバーのアップデートウィンドウが開きます。

5. コンピューターを参照してドライバーを検索をクリックし、コンピューター上の使用可能なドライバーの一覧から選択しますを選択します。

6. ネットワーク アダプターを選択します。

   このハードウェアのためにインストールするデバイスドライバーを選択してくださいウィンドウが表示されます。

7. 製造元の一覧でMicrosoftを選択します。

8. モデルの一覧でUsbNcm Host Deviceを選択します。

   確認ウィンドウが表示されます。はいをクリックして確認します。設定が保存され、Windowsはドライバーがアップデートされたことを通知します。

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. 左側のナビゲーションペインでセキュリティをクリックします

   iLOサービスポートページが表示されます。

2. （iLOサービスポートセクションの横にある）をクリックします。

   iLOサービスポートウィンドウが表示されます。

3. 以下の設定を構成します。
   - iLOサービスポート
   - 大容量ストレージ - USBフラッシュドライブ
   - 大容量ストレージ - 認証が必要
   - ネットワーク - USBイーサーネットアダプター

4. アップデートをクリックします。

   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。

サブトピック

iLOサービスポートオプション

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。

- 大容量ストレージ - 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。

- 大容量ストレージ – 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。
- ネットワーク – USBイーサーネットアダプター – USBケーブル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/exFAT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。

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。
- 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。

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**https://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

このタスクについて

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
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ビットまたは4,096ビットの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. 左側のナビゲーションペインでiLO設定をクリックし、ユーザー管理をクリックします。

   ユーザー管理ページが表示されます。

5. ユーザーをクリックします。

   ユーザーページが表示されます

6. 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。

7. アクションドロップダウンリストから新しいSSHキーの認証をクリックします。
8. PEMでエンコードされた公開キーを公開キーボックスに貼り付けます。
9. インポートをクリックします。

ユーザーページのSSHホストキーセクションには、ユーザーアカウントに関連付けられたSSH公開キーが表示されます。

10. 操作を取り消す場合はキャンセルボタンをクリックします。
11. ✕ をクリックしてウィンドウを閉じます。

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ビットの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. アクセスページでセキュアシェル（SSH）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。

iLOからSSHキーを削除すると、SSHクライアントはiLOに対し、対応する秘密キーを使用して認証することができません。

手順

1. 左ナビゲーションペインでiLO設定をクリックし、ユーザー管理をクリックします。

ユーザー管理ページが表示されます。

2. ユーザーをクリックします

   ユーザーページが表示されます。
   ローカルユーザーセクションには、SSHキーが構成されたユーザーアカウントが表示されます。

3. SSHキーを削除する必要があ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。

4. アクションドロップダウンリストからSSHキーを削除を選択します。

   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。

   選択したSSHキーがiLOから削除されます。

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. 左側のナビゲーションペインでiLO設定をクリックし、ユーザー管理をクリックします。

   ユーザー管理ページが表示されます。SSHホストキーがページに表示されます。

2. キーをクリップボードにコピーをクリックします。

   SSHキーがコピーされます。

3. （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。

4. （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
w011agB5xY6B3pjP/qaeFJb29sGqPwoaXps6g5t/YFhxIQ8is8N+LnfuTzMtQDj74rfq6pcXGnXq+ErmbkcfHn
AdSMveT6rXPM1U+Je1B9VOVS23fUL7mfoshLnSHrJJtP7XkZ1rKf1QPKCChWLfpdmTprsaJrxDrwCNxX4+pPh
UXqHYLTlvPA8xsqaPxPZfHxZWTZrCp
```

5. 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. 左側のナビゲーションペインでiLO設定をクリックし、ユーザー管理をクリックします。

   ユーザー管理ページが表示されます。

2. ユーザーをクリックします

   ユーザーページが表示されます。
   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。

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

これらの形式の例については、iLOユーザーガイドを参照してください。

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。
- 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。
- 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 ----
```

```
Comment: "rsa-key-20250307"
AAAAB3NzaC1yc2EAAAADAQABAAABAQCMobxxIAk0i313m4/U69BxRwSrSPZBy545
ArQBMYw+VI0kKFH9XgMwC5TN6RL+b6T1c6bg+YuUrruqgk06Q6GJy7mvfOobcsGb
9ABvjoekIKnidRZj6uE4zPtPwkK1tQtNhkdMOPuPDdLbz7PIQAAVkOX9zsZShp21
8Q/5cN+AyvItZNgbnkeSklJh8VdGaqFbHx25W4qHpYI4C52YFMt+dhkjeUGiS6LQ
NmQSuDqPGwI5fbO/Dt/Ei9dJrBtkarI1CUlmjwM+0f3MiPWyyGYMyVrG2cqq7JMP
KY9aIsiU0cpicYmn+FlOh3Rh06pybaF6nIs/v5qXc6ws4d5a0yeB
---- END SSH2 PUBLIC KEY ----
```

OpenSSHキー形式

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCMobxxIAk0i313m4/U69BxRwSrSPZBy545ArQBMYw+VI0
kKFH9XgMwC5TN6RL+b6T1c6bg+YuUrruqgk06Q6GJy7mvfOobcsGb9ABvjoekIKnidRZj6uE4zP
tPwkK1tQtNhkdMOPuPDdLbz7PIQAAVkOX9zsZShp218Q/5cN+AyvItZNgbnkeSklJh8VdGaqFbH
x25W4qHpYI4C52YFMt+dhkjeUGiS6LQNmQSuDqPGwI5fbO/Dt/Ei9dJrBtkarI1CUlmjwM+0f3M
iPWyyGYMyVrG2cqq7JMPKY9aIsiU0cpicYmn+FlOh3Rh06pybaF6nIs/v5qXc6ws4d5a0yeB
rsa-key-20250307
```

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。ユーザー管理 > ユーザー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。

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構成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、構成されたグループ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。例えば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。

サブトピック

CACスマートカード認証設定の構成
CAC Smartcard認証用の信頼済み証明書の管理

CACスマートカード認証設定の構成

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. 左側のナビゲーションペインでセキュリティをクリックし、認証をクリックします。

   認証ページが表示されます。

2. CAC/Smartcardをクリックします

   CAC/Smartcardページが表示されます。

3. 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。

4. CAC/Smartcardページの設定で以下の設定を行います。

   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。

5. （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。

   - FIPSセキュリティ状態 - この設定は暗号化とセキュリティページで構成できます。

6. （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。

7. アップデートをクリックして、CAC/Smartcard > 設定ページで変更を保存します。

   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。

8. 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。

9. （オプション）証明書失効リスト(CRL) をインポートします。

10. （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、CAC/Smartcard > 設定のOCSP URLフィールドにHTTPS URLを入力して、アップデートをクリックします。

11. 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）。

サブトピック

CACスマートカード認証設定
新しいローカルユーザー証明書の承認
ローカルユーザー証明書の削除
認定された証明書の表示

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。例えば、`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。例えば、`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。例えば、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。例えば、`rfc822Name:testuser@domain.com`の場合、ユーザー名は`testuser@domain.com`となります。

OCSP URL

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。

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。

新しいローカルユーザー証明書の承認

前提条件

- ユーザーアカウント管理権限
- 証明書が埋め込まれたスマートカードまたはその他の共通アクセスカード（CAC）を所持していること。

  証明書は設定されているiLOセキュリティ状態に準拠していなければならない。
- CAC Smartcard認証がCAC/Smartcardページの設定セクションで有効である。
- 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. 左側のナビゲーションペインでiLO設定をクリックし、ユーザー管理をクリックします。

   ユーザー管理ページが表示されます。
2. ユーザーをクリックします。

   ユーザーページが表示され、ローカルユーザーアカウントの詳細がローカルユーザーテーブルに表示されます。
3. ログイン名の横にあるチェックボックスをクリックして、ユーザーアカウントを選択します。
4. アクションCAC/スマートカード証明書のインポートをクリックします。

CAC/スマートカード証明書のインポートウィンドウが表示されます。

5. 選択したユーザーアカウントの証明書をPEMにエンコードされたBase64形式で証明書ボックスに貼り付けます。
6. 証明書をインポートするには、インポートをクリックします。
7. 操作を取り消す場合はキャンセルボタンをクリックします。
8. ✕ をクリックして、CAC/スマートカード証明書のインポートウィンドウを閉じます。

ローカルユーザー証明書の削除

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。
- 証明書が関連付けられた1つまたは複数のローカルユーザーアカウントがシステムに存在する。

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、ユーザー管理をクリックします。

   ユーザー管理ページが表示されます。

2. ユーザーをクリックします。

   ユーザーページが表示され、ローカルユーザーアカウントの詳細がローカルユーザーテーブルに表示されます。

3. ログイン名の横にあるチェックボックスをクリックして、ユーザーアカウントを選択します。
4. アクションCAC/スマートカード証明書を削除をクリックします。

   確認ウィンドウが表示されます。

5. はい、削除しますをクリックして削除を確認します。

   証明書が削除され、証明書が削除されましたのメッセージが表示されます。

6. 操作を取り消す場合はキャンセルボタンをクリックします。
7. ✕ をクリックして、CAC/スマートカード証明書を削除ウィンドウを閉じます。

認定された証明書の表示

手順

1. 左ナビゲーションペインでiLO 設定をクリックし、ユーザー管理をクリックします。

   ユーザー管理ページが表示されます。

2. ユーザーをクリックします。

   ユーザーページが表示され、各ユーザーアカウントに関連付けられた証明書指紋がローカルユーザーテーブルに表示されます。
   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。

CAC Smartcard認証用の信頼済み証明書の管理

サブトピック

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
- 信頼済みCA証明書を取得している。
- 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。
- 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。
- iLOは最大3つのCAC CA証明書をサポートし、サポートされる最大サイズはDER形式で6 KB、PEM形式で8 KBです。

手順

1. 左側のナビゲーションペインでセキュリティをクリックし、認証をクリックします。

   認証ページが表示されます。

2. CAC/Smartcardをクリックします

   CAC/Smartcardページが表示されます。

3. インポートをクリックします。

   信頼できるCA証明書をインポートウィンドウが表示されます。

4. 信頼できるCA証明書を証明書テキストボックスに貼り付けます。

5. インポートをクリックします。

   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。

6. 操作を取り消す場合はキャンセルボタンをクリックします。

7. ✕ をクリックして信頼できるCA証明書をインポートウィンドウを閉じます。

信頼できる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. 左側のナビゲーションペインでセキュリティをクリックし、認証をクリックします。

   認証ページが表示されます。

2. CAC/Smartcardをクリックします

   CAC/Smartcardページが表示されます。

3. 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。

4. 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。

5. 🗑 をクリックします。

   確認ウィンドウが表示され、iLOが要求を確認するように求めます。

6. 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。

7. 操作を取り消す場合はキャンセルボタンをクリックします。

8. ✕ をクリックして確認ウィンドウを閉じます。

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. ナビゲーションペインでセキュリティをクリックし、認証をクリックします。

   認証ページが表示されます。

2. CAC/Smartcardをクリックします。

   CAC/Smartcardページが表示されます。

3. 証明書失効リスト(CRL) セクションのインポートをクリックします。

   CRLのインポートウィンドウが表示されます。

4. CRLのインポートボックスにHTTPS 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。

5. インポートをクリックします。

   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. 左側のナビゲーションペインでセキュリティをクリックし、認証をクリックします。

   認証ページが表示されます。

2. CAC/Smartcardをクリックします

   CAC/Smartcardページが表示されます。

3. 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。

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。

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

SSL証明書情報の表示

手順

左側のナビゲーションペインでセキュリティをクリックし、SSL証明書をクリックします。

SSL証明書ページが表示されます。
このページから現在の認証の詳細を表示し、SSL証明書を設定することができます。

サブトピック

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。

- 有効開始日 - 証明書の有効期限の開始日。
- 有効期限 - 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、信頼済み証明書の場合はCAによって生成されます。

信頼済みのSSL証明書

手順

1. 左側のナビゲーションペインでセキュリティをクリックし、SSL証明書をクリックします。

   SSL証明書ページが表示されます。

2. 証明書を構成をクリックします。

   証明書を構成ページが表示されます。

3. 次のいずれかのオプションを選択します。

   - CSRの生成 - 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）を作成するには、このオプションを使用します。
   - SSL証明書および秘密キーのインポート - 信頼済みのSSL証明書および対応する秘密キー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。

     CSRを生成してSSL証明書をインポートする方法について詳しくは、CSRの生成およびSSL証明書のインポート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。

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. 左側のナビゲーションペインでセキュリティをクリックし、SSL証明書をクリックします。

   SSL証明書ページが表示されます。

2. （証明書情報セクション）をクリックします。

   確認ウィンドウが表示されます。

   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、削除してリセット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。

5. 操作を取り消す場合はキャンセルボタンをクリックします。

6. をクリックしてウィンドウを閉じます。

CSRの生成およびSSL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。

iLOは、DER形式で最大3 KB（PEM形式で約4 KB）までのWebサーバー証明書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。

サブトピック

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. 左側のナビゲーションペインでセキュリティをクリックし、SSL証明書をクリックします。

   SSL証明書ページが表示されます。
2. 証明書を構成をクリックします。

   SSL証明書ウィンドウが表示されます。
3. CSRの生成を選択します。
4. 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）
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**
   > 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。
6. CSRの生成をクリックします。

   SSL証明書ウィンドウが閉じます。CSRが生成されていることを通知するメッセージが表示されます。

   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。
7. 数分後（最大10分）、CSRがSSL証明書ページの証明書署名要求セクションに表示されます。
8. をクリックしてCSRテキストをコピーします。

9. 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。
10. 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。
11. 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。

サブトピック

CSR入力の詳細
証明書署名要求

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。
- 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。
- 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。

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. 左側のナビゲーションペインでセキュリティをクリックし、SSL証明書をクリックします。

   SSL証明書ページが表示されます。

2. 証明書のインポートをクリックします。

   SSL証明書のインポートウィンドウが表示されます。

3. SSL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。

4. 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。

5. 操作を取り消す場合はキャンセルボタンをクリックします。

6. ✕ をクリックしてSSL証明書のインポートウィンドウを閉じます。

SSL証明書および秘密キーのインポート

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、信頼できるSSL証明書とそれに対応する秘密キーをインポートできます。

証明書と秘密キーの合計サイズは20 KB以下になります。

証明書と秘密キーの両方がPEM形式であり、証明書がSSLサーバー証明書として使用できることを確認してください。

> **注記**
> CNSAセキュリティ状態では384ビットのECDSAキーのみが許可され、他のセキュリティ状態では最大2048ビットのRSAキーが許可されます。

手順

1. 左側のナビゲーションペインでセキュリティをクリックし、SSL証明書をクリックします。

   SSL証明書ページが表示されます。

2. 証明書を構成を選択します。

   証明書を構成ウィンドウが表示されます。

3. ストラテジの選択オプションでSSL証明書および秘密キーのインポートを選択します。

4. SSL証明書および秘密キーのインポートウィンドウで、ボックスに証明書と秘密キーを貼り付けて、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、証明書と秘密キーをインポートしてからリセットします。

SSL証明書の再生成

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。

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. 左側のナビゲーションペインでセキュリティをクリックし、SSL証明書をクリックします。

   SSL証明書ページが表示されます。

2. Regenerateをクリックします。

   ポップアップウィンドウが表示されます。

3. ストラテジの選択オプションではCSRの生成がデフォルトで選択されています。
4. CAからの信頼済み証明書の取得セクションの手順4～7に従ってください。
5. 操作を取り消す場合はキャンセルボタンをクリックします。
6. ✕ をクリックしてポップアップウィンドウを閉じます。

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。Microsoft Active Directoryのログインユーザー向けにTwo-Factor認証を設定することもできます。

Two-Factor認証が有効になっている場合、Active Directoryユーザーに対してREST API経由での基本認証はサポートされません。`Unauthorized login attempt`というHTTP 401エラーが表示されます。

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。

ディレクトリ統合を構成するときは、iLOでスキーマフリーオプションを使用します。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

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。

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. 左側のナビゲーションペインでセキュリティをクリックし、認証をクリックします。

   認証ページが表示されます。

2. ディレクトリとLDAPをクリックします。

   ディレクトリとLDAPページが表示されます。

3. をKerberos設定セクションでクリックします。

   Kerberos設定ウィンドウが表示されます。

4. Kerberos KDCサーバーアドレスを入力します。
5. Kerberos KDCサーバーポートを入力します。
6. Kerberosレルムの名前を入力します。
7. 必要なキータブファイルの場所をキータブファイルロケーションボックスに設定します。
8. `Kerberosキータブ`ファイルを追加するには、ブラウズまたはファイルを（ブラウザーによって異なります）ドラッグしてローカルファイルボックスをクリックし、画面の指示に従います。

9. アップデートをクリックします。
10. 操作を取り消す場合はキャンセルボタンをクリックします。
11. ✕ をクリックしてKerberos設定ウィンドウを閉じます。

サブトピック

Kerberos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. 左側のナビゲーションペインでセキュリティをクリックし、認証をクリックします。

   認証ページが表示されます。

2. ディレクトリとLDAPをクリックします。

   ディレクトリとLDAPページが表示されます。

3. ✎（認証オプションの横にある）を選択します。

   認証オプションウィンドウが表示されます。

4. LDAPディレクトリ認証メニューでHPEディレクトリのデフォルトスキーマを使用を選択します。
5. 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。
6. CAC/Smartcard認証が有効な構成の場合、✎（ディレクトリサーバー設定の横にある）をクリックします。

   ディレクトリサーバー設定ウィンドウが表示されます。

7. 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、かつTwo-Factor認証が無効になっている場合のみ使用

可能です。

8. 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。
9. 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。
10. 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。
11. Add User Contextをクリックします。

    ディレクトリユーザーコンテキストテキストボックスがディレクトリサーバー設定ウィンドウ追加されます。
12. (オプション) Add User Contextをクリックしてディレクトリユーザーコンテキストをさらに追加します。
13. 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。
14. アップデートをクリックして設定を保存します。
15. (オプション) 新しいCA証明書をインポートします。
    a. ディレクトリサーバーCA証明書セクションで上矢印をクリックします。

       CA証明書のインポートウィンドウが表示されます。
    b. Base64でエンコードされたX.509証明書データをCA証明書ウィンドウに貼り付けてインポートをクリックします。
16. ディレクトリサーバーとiLO間の通信をテストするには、ディレクトリテストセクションの接続テストをクリックします。

> **注記**
> LDAPユーザー名と識別名 (DN) に使用できる特殊文字については、次の表を参照してください。特殊文字の組み合わせを含む属性値はサポートされていません。

ユーザー名	識別名
+	+
–	–
<	<
>	>
,	,
;	;
″	″
#	#
/	/
	¥
	)
	(

サブトピック

スキーマフリーディレクトリの設定

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。

- 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。

- サーバーの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。

  Add User Contextをクリックして、ディレクトリサーバー設定ウィンドウにディレクトリユーザーコンテキストボックスを追加します。

- ディレクトリサーバーCA証明書 - 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。

- CRLチェック - iLOが、LDAPサーバー証明書を証明書失効リストに照らし合わせてチェックするかどうかを指定します。

  iLOは、CAC/Smartcardページでインポートした証明書失効リストを使用します。LDAPサーバー証明書からの証明書失効リストはチェックしません。

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. 左側のナビゲーションペインでセキュリティをクリックし、認証をクリックします。

   認証ページが表示されます。

2. ディレクトリとLDAPをクリックします。

   ディレクトリとLDAPページが表示されます。

3. （認証オプションの横にある）を選択します。

   認証オプションウィンドウが表示されます。

4. 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。
5. 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。
6. CAC/Smartcard認証が有効な構成の場合、（ディレクトリサーバー設定の横にある）をクリックします。

   ディレクトリサーバー設定ウィンドウが表示されます。

7. 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、かつTwo-Factor認証が無効になっている場合のみ使用可能です。

8. このiLOインスタンスの位置をiLOオブジェクト識別名ボックスのディレクトリツリー内に入力します。
9. 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。
10. 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。
11. Add User Contextをクリックします。

    ディレクトリユーザーコンテキストテキストボックスがディレクトリサーバー設定ウィンドウ追加されます。

12. （オプション）Add User Contextをクリックしてディレクトリユーザーコンテキストをさらに追加します。
13. 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。
14. アップデートをクリックして設定を保存します。
15. （オプション）新しいCA証明書をインポートします。
    a. ディレクトリサーバーCA証明書セクションで上矢印をクリックします。

       CA証明書のインポートウィンドウが表示されます。

    b. Base64でエンコードされたX.509証明書データをCA証明書ウィンドウに貼り付けてインポートをクリックします。
16. 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。
17. 設定の適用をクリックします。
18. 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

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。以下に例を示します。

  ```
  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、接続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. 左側のナビゲーションペインでセキュリティをクリックし、認証をクリックします。

   認証ページが表示されます。

2. ディレクトリとLDAPをクリックします。

   ディレクトリとLDAPページが表示されます。ディレクトリサーバーCA証明書セクションには、使用可能な証明書がリストされます。

3. （削除したい証明書の横にある）をクリックします

   プロンプトが表示されたら削除を確認します。
   証明書が削除されることが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。

iLOでのTwo-Factor認証の有効化

前提条件

- iLO設定_>_アラートとログ_>_メール設定ページでTwo-Factor認証のSMTPを有効オプションが有効になっている。
- 汎用LDAPが無効になっていること。
- 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. 左側のナビゲーションペインでセキュリティをクリックし、認証をクリックします。

   認証ページが表示されます。
2. ディレクトリとLDAPをクリックします

   ディレクトリとLDAPページが表示されます。
3. （認証オプションセクション）をクリックします。

   認証オプションウィンドウが開きます。
4. Two-Factor認証チェックボックスをオンにします。
5. 変更を保存するには、アップデートをクリックします。
6. 操作を取り消す場合はキャンセルボタンをクリックします。
7. をクリックして認証オプションウィンドウを閉じます。

iLOでのTwo-Factor認証の無効化

前提条件

- 汎用LDAPが無効になっていること。

手順

1. 左側のナビゲーションペインでセキュリティをクリックし、認証をクリックします。

   認証ページが表示されます。
2. ディレクトリとLDAPをクリックします

   ディレクトリとLDAPページが表示されます。
3. （認証オプションセクション）をクリックします。

   認証オプションウィンドウが開きます。
4. Two-Factor認証チェックボックスをクリアします。
5. 変更を保存するには、アップデートをクリックします。
6. 操作を取り消す場合はキャンセルボタンをクリックします。
7. をクリックして認証オプションウィンドウを閉じます。

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. 左側のナビゲーションペインでセキュリティをクリックし、認証をクリックします。

   認証ページが表示されます。

2. ディレクトリとLDAPをクリックします。

   ディレクトリとLDAPページが表示されます。

3. ディレクトリテストセクションで接続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。

   ディレクトリテスト制御ウィンドウが表示されます。

4. 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. 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。

6. 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。

7. 操作を取り消す場合はキャンセルボタンをクリックします。

8. ✕ をクリックしてディレクトリテスト制御ウィンドウを閉じます。

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更新するには、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暗号化の設定

すべてのGen12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。

暗号化とセキュリティページには、現在のセキュリティ設定とiLOセキュリティ状態の概要が表示されます。

暗号化とセキュリティページの概要セクションには、次の現在の設定が表示されます。

- 現在ネゴシエートされた暗号 - 現在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。

暗号化とセキュリティページのiLOのセキュリティ状態セクションには、iLOのセキュリティ状態が一覧表示されます。各セキュリティ状態を展開すると、セキュリティ状態に関する画面上の情報が表示されます。

サブトピック

iLOセキュリティ状態
セキュリティ状態のアップデート

iLOセキュリティ状態

セキュア標準

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

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
- 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。
- TLS 1.2およびTLS 1.3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。

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 140-3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

  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
- 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。
- TLS 1.2およびTLS 1.3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。

CNSA

CNSAセキュリティ状態は、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ファームウェアはCNSA 2.0署名アルゴリズムを使用します - Leighton-Micali Signature (LMS)。
- LMS署名されていないファームウェアは、CNSAモードでフラッシュしたりレポジトリにアップロードしたりすることはできません。
- 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およびTLS 1.3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。

  例：

  - 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
  - Remote Support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。

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。

注記
iLOがセキュア標準、FIPS、またはCNSAのセキュリティ状態に構成されている場合は、システムメンテナンススイッチがオンであってもログイン資格情報が必要です。

Synergyセキュリティモード

Composer 2で使用される特別なセキュリティ状態。このモードを使用するデバイスのセキュリティ状態は変更できません。

サブトピック

CNSAモードを使用するときのiLOへの接続

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、TLS 1.3、またはその両方、およびAES暗号をサポートするよう構成します。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。

iLO RESTful API

TLS 1.2、TLS 1.3、またはその両方、および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る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。iLO 7 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（例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、iLO RESTful APIまたはBMC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。

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、iLO RESTful APIまたはiLO 7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。

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。

FIPSまたはセキュア標準

- aes256-ctr、aes256-gcm@openssh.com
- diffie-hellman-group-exchange-sha256、ecdh-sha2-nistp384
- hmac-sha2-256
- ssh-ed25519、rsa-sha2-512、rsa-sha2-256

CNSA

- aes256-gcm@openssh.com
- ecdh-sha2-nistp384
- hmac-sha2-256
- ecdsa-sha2-nistp384、rsa-sha2-512

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

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コマンドへの接続など、すべてのiLO SSL接続に適用されます。

サポートされている暗号の次の一覧は、以下を含むすべてのiLO SSL接続に適用されます。

- LDAPサーバーへの接続
- 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

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。

セキュア標準

これらのセキュリティ状態にはTLS 1.2またはTLS 1.3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AEAD MAC（ECDHE-RSA-AES128-GCM-SHA256）による128ビットAES-GCM
- AEAD MAC（TLS_AES_256_GCM_SHA384）によるTLS1.3 256ビットAES_GCM
- AEAD MAC（TLS_AES_128_GCM_SHA256）によるTLS1.3 128ビットAES_GCM

FIPS

これらのセキュリティ状態にはTLS 1.2またはTLS 1.3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、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
- AEAD MAC（TLS_AES_256_GCM_SHA384）によるTLS1.3 256ビットAES_GCM
- AEAD MAC（TLS_AES_128_GCM_SHA256）によるTLS1.3 128ビットAES_GCM

CNSA

このセキュリティ状態にはTLS 1.2またはTLS 1.3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
- AEAD MAC（TLS_AES_256_GCM_SHA384）によるTLS1.3 256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
- AEAD MAC（TLS_AES_256_GCM_SHA384）によるTLS1.3 256ビットAES_GCM

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。

FIPSまたはセキュア標準

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

セキュリティ状態のアップデート

すべてのGen12サーバーに付属しているHPE iLO Standardによって、お客様は次の2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3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ります。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脅威を制限するためにクローズされます。

次のセキュリティ状態を利用できます。

- セキュア標準
- FIPS
- CNSA

サブトピック

FIPSおよびCNSAセキュリティ状態を有効にする
セキュア標準の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

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）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. 左側のナビゲーションペインでセキュリティをクリックし、暗号化とセキュリティをクリックします。

   暗号化とセキュリティページが表示されます。
3. セキュリティ状態のアップデートをクリックします。

   概要ウィンドウが表示されます。
4. セキュリティ状態メニューでFIPSを選択して、アップデー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。

   > **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. 左側のナビゲーションペインでセキュリティをクリックし、暗号化とセキュリティをクリックします。

      暗号化とセキュリティページが表示されます。
   c. セキュリティ状態のアップデートをクリックします。

      概要ウィンドウが表示されます。
   d. セキュリティ状態メニューでCNSAを選択して、アップデー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。
   e. 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。
   f. 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証明書（手動インポートでインストールされたもの）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。

9. （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。
10. （オプション）構成をリストアした場合は、アクセスページで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。

11. （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。

セキュア標準の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. ナビゲーションペインでセキュリティをクリックし、暗号化とセキュリティをクリックします。

   暗号化とセキュリティページが表示されます。

3. セキュリティ状態のアップデートをクリックします。

   概要ウィンドウが表示されます。

4. セキュリティ状態メニューでセキュリティ状態のアップデートを選択します。
5. アップデートをクリックします。

   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. ✕ をクリックしてウィンドウを閉じます。
7. 操作を取り消す場合はキャンセルボタンをクリックします。
8. 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。

9. 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。

10. アクセス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。

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。iLOは、3 KBまでのサイズのSSO証明書をサポートしています。

サブトピック

HPE SSO用のiLOの設定
直接DNS名のインポート
信頼済みの証明書とレコードの削除

HPE SSO用のiLOの設定

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

手順

1. 左側のナビゲーションペインでセキュリティをクリックし、認証をクリックします。

   認証ページが表示されます。

2. HPE SSOをクリックします。

   HPE SSOページが表示されます。

3. （シングルサインオン設定）をクリックします。

   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。

   シングルサインオン設定ウィンドウが表示されます。

4. 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。
5. 適用をクリックします。
6. 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。

7. （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。

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。

8. 操作を取り消す場合はキャンセルボタンをクリックします。
9. ✕ をクリックしてシングルサインオン設定ウィンドウを閉じます。

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
信頼済み証明書の追加

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. 左側のナビゲーションペインでセキュリティをクリックし、認証をクリックします。

   認証ページが表示されます。

2. HPE SSOをクリックします。

3. 信頼済み証明書および記録を管理セクションでインポートをクリックします。

   信頼済みの証明書のインポートウィンドウが表示されます。

4. 次のいずれかの方法を使用して、信頼済み証明書を追加します。

   - **URLからのインポート** - 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、インポートをクリックします。

     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。

   - **DNS名から直接インポート** - DNS名またはIPアドレスをDNS名またはIPアドレスセクションのテキストボックスに入力してから、インポートをクリックします。

   - **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、インポートをクリックします。

サブトピック

信頼済みの証明書とレコードの表示

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

1. 左側のナビゲーションペインでセキュリティをクリックし、認証タブをクリックします。

   認証ページが表示されます。

2. HPE SSOをクリックして、信頼済み証明書とレコードを表示します。

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）。

直接DNS名のインポート

前提条件

iLOの設定を構成する権限

手順

1. 左側のナビゲーションペインでセキュリティをクリックし、認証をクリックします。

   認証ページが表示されます。

2. HPE SSOをクリックします。

   HPE SSOが表示されます。

3. 信頼済み証明書および記録を管理セクションでインポートをクリックします。

   信頼済みの証明書のインポートウィンドウが開きます。

4. タイプ値にDNS名から直接インポートを選択します。
5. DNS名から直接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）、アップデートをクリックします。
6. 操作を取り消す場合はキャンセルボタンをクリックします。
7. ✕ をクリックしてウィンドウを閉じます。

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. 左側のナビゲーションペインでセキュリティをクリックし、認証をクリックします。

認証ページが表示されます。

2. HPE SSOをクリックします。

   HPE SSOページが表示されます。

3. 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。

4. 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。

5. 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表示

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

左側のナビゲーションペイン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。

ログインセキュリティバナーページが表示されます。
セキュリティメッセージは、ログイン画面にセキュリティバナーを表示が有効の場合に表示されます。

サブトピック

ログインセキュリティバナーの構成

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

手順

1. 左側のナビゲーションペイン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。

   ログインセキュリティバナーページが表示されます。

2. ログインセキュリティバナーの設定をクリックします。

   ログインセキュリティバナーの設定ページが表示されます。

3. ログイン画面にセキュリティバナーを表示チェックボックスをオンにします。

4. (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。

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.
```

5. アップデートをクリックします。

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。

モジュラーハードウェアシステムでのホストプロセッサーモジュール認証

モジュラーハードウェアシステム（MHS）の場合、iLOは、起動のたびにホストプロセッサーモジュール（HPM）の完全性を検証します。HPM認証が失敗した場合、iLOはインテグレーテッドマネジメントログを記録し、システムはコンポーネントの完全性ポリシーの構成に従って起動します。

iLOマネジメント設定の構成

サブトピック

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。
- iLO 7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で、ダッシュボードページ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が表示されません。
  - 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

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：iLO Webインターフェイス

手順

左側のナビゲーションペインでダッシュボードをクリックします。

AMSはホストの概要セクションにリストされます。

表示される値は、以下のとおりです。

- 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 8.x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

iLO 7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`
   - `agentXSocket /var/agentx/master`
   - `agentXPerms 777 777`
   - `rocommunity <community string>`
   - `trapsink 127.0.0.1 <community string>`
2. 次のコマンドを使用して`snmpd`を再起動します。

   ```
   systemctl restart snmpd
   ```
3. System Management Assistantを有効にします。
   - **SUSE Linux Enterprise ServerおよびRed Hat Enterprise Linux** – 次のコマンドを入力します。
     - `systemctl enable smad_rev`
     - `systemctl start smad_rev`
4. 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** – 次のコマンドを入力します。
     - `systemctl enable amsd_rev`
     - `systemctl start amsd_rev`
5. 必要に応じ、他のサブエージェントを有効にして起動します。
   - **SUSE Linux Enterprise ServerおよびRed Hat Enterprise Linux** – 次のコマンドを入力して、他のリバースモードのサブエージェントを起動します。
     - `systemctl start cpqIde_rev`
     - `systemctl start cpqScsi_rev`
     - `systemctl start mr_cpqScsi_rev`
     - `systemctl start cpqFca_rev`

SNMPv1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. 左側のナビゲーションペインでiLO設定をクリックし、アラートとログをクリックします。

アラートとログページが表示されます。

2. SNMP設定をクリックします。

   SNMP設定ページが表示されます。

3. （SNMPv1設定セクション）をクリックします。

   SNMPv1設定ウィンドウが表示されます。

4. SNMPv1設定セクションに次の値を入力します。

   - SNMPv1リクエスト
   - SNMPv1トラップ
   - 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。

5. 変更を保存するには、アップデートをクリックします。
6. 操作を取り消す場合はキャンセルボタンをクリックします。
7. をクリックしてSNMPv1設定ウィンドウを閉じます。

サブトピック

SNMPオプション

SNMPオプション

- システムのロケーション - 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（例えば、`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（例えば、`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リクエスト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）。

  SNMPポート - SNMP通信に使用されるポート。

注記

- Hewlett Packard Enterpriseでは、必要な場合にのみSNMPを有効にすることをお勧めします。また、public、SNMPなどの一般的なコミュニティ名を使用する代わりに、強力で複雑なコミュニティ文字列を使用してください。

SNMPアラートの構成の概要

前提条件

iLOの設定を構成する権限

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、アラートとログをクリックします。

   アラートとログページが表示されます。

2. SNMP設定をクリックします。

   SNMP設定ページが表示されます。

3. （概要セクション）をクリックします。

4. 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設定します。

5. 以下の値を構成します。

   - システムのロケーション
   - システム連絡先
   - システムの役割
   - システムの役割詳細
   - SNMPv3リクエスト
   - SNMPv3トラップ
   - 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

6. （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。SNMPv1トラップとSNMPv3トラップの両方が無効になっている場合、このオプションは無効になります。

   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。

7. 構成を保存するには、アップデートをクリックします。

8. 操作を取り消す場合はキャンセルボタンをクリックします。

9. をクリックしてウィンドウを閉じます。

サブトピック

SNMPアラートの設定
SNMPv3ユーザーの追加
SNMPアラートの送信先の追加

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。

SNMPv1リクエスト

iLOを有効にすると、外部SNMPv1要求を受信します。

SNMPv1トラップ

iLOを有効にすると、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。

SNMPv3リクエスト

iLOを有効にすると、外部SNMPv3要求を受信します。

SNMPv3トラップ

iLOを有効にすると、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SNMPv3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。例えば、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（例えば、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。

SNMPv3ユーザーの追加

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. 左ナビゲーションペインでiLO設定をクリックし、アラートとログをクリックします。

   アラートとログページが表示されます。

2. SNMP設定セクションをクリックします。

   SNMP設定ページが表示されます。

3. 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、追加をクリックします。

4. 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
   - プライバシープロトコル
   - プライバシーパスフレーズ
   - ユーザーエンジンID

5. 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。

6. 操作を取り消す場合はキャンセルボタンをクリックします。
7. ✕ をクリックしてウィンドウを閉じます。

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AESを使用して暗号化されます。
- 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
  ```

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トラップが有効であること。
- SNMPv3アラートの送信先を構成する場合、SNMPv3トラップが有効で、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. 左側のナビゲーションペインでiLO設定をクリックし、アラートとログをクリックします。

   アラートとログページが表示されます。
2. SNMP設定セクションをクリックします。

   SNMP設定ページが表示されます。
3. SNMPアラートの送信先セクションで追加をクリックします。

   アラート送信先の追加ウィンドウが表示されます。
4. 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
5. 追加をクリックして設定を保存します。
6. 操作を取り消す場合はキャンセルボタンをクリックします。
7. ✕ をクリックしてアラート送信先の追加ウィンドウを閉じます。

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）。

  SNMPv1トラップオプションは、SNMPアラートセクションでSNMPv1トラップが有効になっている場合に使用できます。

  SNMPv3トラップオプションは、SNMPアラートセクションでSNMPv3トラップが有効になっており、少なくとも1人のSNMPv3ユーザーが構成されている場合に使用できます。

  SNMPv3通知オプションは、少なくとも1人のSNMPv3ユーザーが構成されている場合に使用できます。

- 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トラップまたはSNMPv3通知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は、SNMPアラートセクションでSNMPv1トラップオプション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を使用するようにアラート送信先を変更する場合は、SNMPアラートセクションでSNMPv3トラップオプションが有効になっていること、および少なくとも1人のSNMPv3ユーザーが構成されていること。
- 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は、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. 左側のナビゲーションペインでiLO設定をクリックし、アラートとログをクリックします。

   アラートとログページが表示されます。

2. SNMP設定セクションをクリックします。

   SNMP設定ページが表示されます。

3. 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。

   編集ウィンドウが開きます。

4. 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

5. 変更を保存するには、アップデートをクリックします。
6. 操作を取り消す場合はキャンセルボタンをクリックします。
7. をクリックして編集ウィンドウを閉じます。

サブトピック

SNMPアラート送信先の削除

SNMPアラート送信先の削除

前提条件

iLOの設定を構成する権限

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、アラートとログをクリックします。

   アラートとログページが表示されます。

2. SNMP設定セクションをクリックします。

   SNMP設定ページが表示されます。

3. 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。

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。

SNMPv3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

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通知が送信されると、保存されます。通知は、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. 左側のナビゲーションペインでiLO設定をクリックし、アラートとログをクリックします。

   アラートとログページが表示されます。

2. SNMP設定をクリックします。

   SNMP設定ページが表示されます。

3. （SNMPv3設定）をクリックします。

   SNMPv3設定ウィンドウが表示されます。

4. 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。

5. 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（秒）

注記

- Hewlett Packard Enterpriseでは、必要な場合にのみSNMPを有効にすることをお勧めします。また、public、SNMPなどの一般的なコミュニティ名を使用する代わりに、強力で複雑なコミュニティ文字列を使用してください。

6. 変更を保存するには、アップデートをクリックします。
7. 操作を取り消す場合はキャンセルボタンをクリックします。
8. ✕ をクリックしてSNMPv3設定ウィンドウを閉じます。

サブトピック

SNMPv3の設定オプション
SNMPv3認証

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。

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。

SNMPv3ユーザーの編集

前提条件

iLOの設定を構成する権限

手順

1. 左ナビゲーションペインでiLO設定をクリックし、アラートとログをクリックします。

   アラートとログページが表示されます。

2. SNMP設定セクションをクリックします。

   SNMP設定ページが表示されます。

3. SNMPv3ユーザーセクションで、編集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、 編集をクリックします。

4. 変更を保存するには、アップデートをクリックします。

5. 操作を取り消す場合はキャンセルボタンをクリックします。

6. をクリックしてウィンドウを閉じます。

SNMPv3ユーザーの削除

前提条件

iLOの設定を構成する権限

手順

1. 左ナビゲーションペインでiLO設定をクリックし、アラートとログをクリックします。

   アラートとログページが表示されます。

2. SNMP設定セクションをクリックします。

   SNMP設定ページが表示されます。

3. 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。

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。

SNMPアラート送信先の削除

前提条件

iLOの設定を構成する権限

手順

1. 左側のナビゲーションペインでiLO設定をクリックし、アラートとログをクリックします。

   アラートとログページが表示されます。

2. SNMP設定セクションをクリックします。

   SNMP設定ページが表示されます。

3. 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。

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。

AMSコントロールパネルを使用したSNMPおよびSNMPアラートの構成（Windows専用）

このタスクについて

注記

SNMP設定オプションは、後続のリリースからはAMSコントロールパネルで利用できません。

- Agentless Management Service for Microsoft Windows x64の場合、バージョン2.51.4.1。
- HPE Gen12 Agentless Management Service for Microsoft Windows x64の場合、バージョン3.40.0.0。

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）iLO 7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

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
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
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

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
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
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

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
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
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

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
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
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

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
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
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

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
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
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

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
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
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

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
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
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

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
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
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

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
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
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、iLO 7およびサポートされるHPE ProLiant Compute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
該当なし	LiquidCoolingWarning1	警告
	LiquidCoolingWarning2	警告
	LiquidCoolingWarning3	クリティカル
0	該当なし	該当なし
4	SNMPAuthenticationFailure	OK
1006	ProcessorStatusUnknown	警告
	ProcessorStatusOK	OK
	ProcessorStatusDegraded	警告
	ProcessorStatusDisabled	警告
	ProcessorStatusFailed	クリティカル
1010	USBStorageDeviceReadError	OK
1011	USBStorageDeviceWriteError	OK
1012	USBStorageDeviceRedundancyLost	警告
1013	USBStorageDeviceRedundancyRestored	OK

トラップID	RESTアラートID	RESTの重大度
1014	USBStorageDeviceSyncFailed	警告
1015	PCIeDiskTemperatureFailed	クリティカル
1016	PCIeDiskTemperatureOk	OK
1017	PCIeDriveConditionOk	OK
	PCIeDriveConditionDegraded	警告
	PCIeDriveConditionFailed	クリティカル
1018	PCIeDriveWearStatusOk	OK
	PCIeDriveWearStatusFiftySixDayThreshold	警告
	PCIeDriveWearStatusFivePercentThreshold	警告
	PCIeDriveWearStatusTwoPercentThreshold	警告
	PCIeDriveWearStatusWearOut	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	警告
	MetricValueBelowLowerThreshold	警告
3033	DrvArrControllerFailed	クリティカル
	DrvArrControllerOK	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	OK
	DrvArrayAccBoardTempDisabled_RedundantCacheFailure	警告
	DrvArrayAccBoardPermDisabled_ExcessiveECCErrors	クリティカル
	DrvArrayAccBoardTempDisabled_RAID_ADG_EnablerModuleMissing	クリティカル
	DrvArrayAccBoardPermDisabled_PostECCErrors	OK
	DrvArrayAccBoardPermDisabled_BackupPowerSourceHotRemoved	クリティカル
	DrvArrayAccBoardPermDisabled_CapacitorChargeLow	クリティカル
	DrvArrayAccBoardPermDisabled_NotEnoughBatteries	警告
	DrvArrayAccBoardPermDisabled_NotSupportedByFirmware	警告
	DrvArrayAccBoardPermDisabled_BatteryNotSupported	クリティカル
	DrvArrayAccBoardPermDisabled_NoCapacitorAttached	クリティカル
	DrvArrayAccBoardPermDisabled_FlashBackedBackupFailed	警告
	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	クリティカル
	DrvArrayAccBoardTempDisabled_MegaCellNotCabled	クリティカル
	DrvArrAcceleratorFlashMemoryNotAttached	警告
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	クリティカル
	PowerFailureErrorInputPowerLoss	クリティカル
	PowerFailureErrorBadFuse	クリティカル
	PowerFailureStandby	クリティカル
	PowerFailureRuntime	クリティカル
	PowerFailurePowerOn	クリティカル
	PowerFailureUnknown	クリティカル
	PowerFailureCpuThermalTrip	クリティカル
6075	InterlockFailureErrorStandby	クリティカル
	InterlockFailureErrorRuntime	クリティカル
	InterlockFailureErrorPowerOn	クリティカル
	InterlockFailureErrorUnknown	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
6125	cpqHeUserTempThreshWarning	警告
6126	cpqHeUserTempThreshCritical	クリティカル
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

トラップID	RESTアラートID	RESTの重大度
11003	TestAlert	OK
11018	PowerThresholdBreach	警告
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

トラップID	RESTアラートID	RESTの重大度
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メール

iLOメールを使用すると、ホストの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を構成したり、Two-Factor認証のSMTPを有効にしたり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、IML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。例えば、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

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://-WWWDOC-）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
- 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. 左ナビゲーションペインでiLO設定をクリックし、アラートとログをクリックします。
2. アラートとログページが表示されます。
3. メール設定の横にある省略記号アイコンをクリックし、設定の編集を選択します。

   メール設定ページが表示されます。
4. 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。
5. 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
6. 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。
7. 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。
8. 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。

9. 変更を保存するには、アップデートをクリックします。

10. 操作を取り消す場合はキャンセルボタンをクリックします。

11. ✕ をクリックしてウィンドウを閉じます。

12. （オプション）構成したメールアドレスにテストアラートメールを送信するには、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。

13. （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。複数のメールアドレスをコンマまたは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。例えば、<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。例えば、<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://-WWWDOC-）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. 左ナビゲーションペインでiLO設定をクリックし、アラートとログをクリックします。
2. アラートとログページが表示されます。
3. メール設定の横にある省略記号アイコンをクリックし、設定の編集を選択します。

   メール設定ページが表示されます。
4. 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。
5. 変更を保存するには、アップデートをクリックします。
6. 操作を取り消す場合はキャンセルボタンをクリックします。
7. ✕ をクリックしてウィンドウを閉じます。

Two-Factor認証のSMTPの有効化

前提条件

- iLOの設定を構成する権限
- SMTPサーバーを構成してあること

手順

1. 左ナビゲーションペインでiLO設定をクリックし、アラートとログをクリックします。
2. アラートとログページが表示されます。
3. メール設定の横にある省略記号アイコンをクリックし、設定の編集を選択します。

   メール設定ページが表示されます。
4. Two-Factor認証のSMTPを有効オプションを有効に設定します。
5. 変更を保存するには、アップデートをクリックします。
6. 操作を取り消す場合はキャンセルボタンをクリックします。
7. ✕ をクリックしてウィンドウを閉じます。

Two-Factor認証のSMTPの無効化

前提条件

- iLOの設定を構成する権限

手順

1. 左ナビゲーションペインでiLO設定をクリックし、アラートとログをクリックします。
2. アラートとログページが表示されます。
3. メール設定の横にある省略記号アイコンをクリックし、設定の編集を選択します。

   メール設定ページが表示されます。
4. Two-Factor認証のSMTPを有効オプションを無効に設定します。

   Two-Factor認証のSMTPを無効にすると、LDAPユーザーのTwo-Factor認証が無効になります。
5. 変更を保存するには、アップデートをクリックします。
6. 操作を取り消す場合はキャンセルボタンをクリックします。
7. ✕ をクリックしてウィンドウを閉じます。

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には、その機能をサポートするライセンスが必要です。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://-WWWDOC-）にあるライセンス文書を参照してください。

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。

リモートsyslog形式はRFC5424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

前提条件

- iLOの設定を構成する権限
- 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. 左ナビゲーションペインでiLO設定をクリックし、アラートとログをクリックします。
2. アラートとログページが表示されます。
3. リモートSyslogの横にある省略記号アイコンをクリックし、設定の編集を選択します。

   リモートSyslog設定ページが表示されます。
4. iLOリモートSyslogを有効オプションを有効に設定します。
5. 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
6. 変更を保存するには、アップデートをクリックします。
7. 操作を取り消す場合はキャンセルボタンをクリックします。
8. ✕ をクリックしてウィンドウを閉じます。
9. （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。

iLOリモートsyslogの無効化

前提条件

- iLOの設定を構成する権限

手順

1. 左ナビゲーションペインでiLO設定をクリックし、アラートとログをクリックします。
2. アラートとログページが表示されます。
3. リモートSyslogの横にある省略記号アイコンをクリックし、設定の編集を選択します。

   リモートSyslog設定ページが表示されます。
4. iLOリモートSyslogを有効オプションを無効に設定します。
5. 変更を保存するには、アップデートをクリックします。
6. 操作を取り消す場合はキャンセルボタンをクリックします。
7. ✕ をクリックしてウィンドウを閉じます。

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

OneView Remote Support

HPE iLO 7には、OneView Remote Support (OVRS) 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サイトで確認できます。https://www.hpe.com/info/privacy

> **重要**
> リモートサポートに登録するには、HPE OneViewを使用します。リモートサポートを無効化するには、iLO Webインターフェイスを使用する必要があります。

サブトピック

OneView Remote Supportの詳細の表示
OneView Remote Supportの無効化
メンテナンスモードの設定

リモートサポートのデータ収集
iLOでのActive Health Systemレポートステータスの表示
リモートサポートサービスイベント

OneView Remote Supportの詳細の表示

手順

1. 左側のナビゲーションペインでHPEアプリをクリックします。

   HPEアプリページが表示されます。

2. HPE OneViewをクリックします。

   HPE OneViewページが表示されます。
   概要セクションにOneView Remote Supportのステータスが表示されます。

3. （オプション）OneView UIの起動リンクをクリックしてHPE OneView Webインターフェイスに移動します。

4. （オプション）削除をクリックしてセッションを削除し、ダッシュボードページに移動します。

OneView Remote Supportの無効化

手順

1. 左側のナビゲーションペインでHPEアプリをクリックします。

   HPEアプリページが表示されます。

2. HPE OneViewをクリックします。

   HPE OneViewページが表示されます。

3. 概要セクションで無効をクリックします。

   確認ウィンドウが表示されます。

4. はい、わかりましたを選択して無効をクリックします。

5. 操作を取り消す場合はキャンセルボタンをクリックします。

6. ✕ をクリックして確認ウィンドウを閉じます。

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。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. 左側のナビゲーションペインでHewlett Packard Enterpriseアプリをクリックします。

   Hewlett Packard Enterpriseアプリページが表示されます。

2. （メンテナンスモードセクション内）をクリックします。

   システムメンテナンスモード設定ウィンドウが表示されます。

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. 有効期限メニューから時間を選択します。
5. 保存をクリックします。

   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。

6. 操作を取り消す場合はキャンセルボタンをクリックします。
7. をクリックして、システムメンテナンスモード設定ウィンドウを閉じます。

サブトピック

システムメンテナンスモードのステータスの表示
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

システム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

左側のナビゲーションペインでHewlett Packard Enterpriseアプリをクリックします。

Hewlett Packard Enterpriseアプリページが表示されます。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。

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. 左側のナビゲーションペインでHewlett Packard Enterpriseアプリをクリックします。

Hewlett Packard Enterpriseアプリページが表示されます。

2. （メンテナンスモードセクション内）をクリックします。

   システムメンテナンスモード設定ウィンドウが表示されます。

3. 有効期限メニューで新しい値を選択し、保存をクリックします。

   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。

4. 操作を取り消す場合はキャンセルボタンをクリックします。

5. をクリックして、システムメンテナンスモード設定ウィンドウを閉じます。

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. 左側のナビゲーションペインでHewlett Packard Enterpriseアプリをクリックします。

   Hewlett Packard Enterpriseアプリページが表示されます。

2. （メンテナンスモードセクション内）をクリックします。

   システムメンテナンスモード設定ウィンドウが表示されます。

3. メンテナンスモードチェックボックスをクリアして、アップデートをクリックします。

   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。

4. 操作を取り消す場合はキャンセルボタンをクリックします。

5. をクリックして、システムメンテナンスモード設定ウィンドウを閉じます。

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

データコレクション情報の送信

データコレクション情報の送信

前提条件

iLOの設定を構成する権限

このタスクについて

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. 左側のナビゲーションペインでHPEアプリをクリックします。

   HPEアプリページが表示されます。

2. HPE OneViewをクリックします。

   HPE OneViewページが表示されます。

3. データ収集の送信をクリックします。

4. 要求を確認するメッセージが表示されたら、はい、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。

iLOでのデータ収集ステータスの表示

手順

1. 左側のナビゲーションペインでHPEアプリをクリックします。

   HPEアプリページが表示されます。

2. HPE OneViewをクリックします。

   HPE OneViewページが表示されます。データ収集セクションには、データ収集のステータスが表示されます。

iLOでのActive Health Systemレポートステータスの表示

手順

1. 左側のナビゲーションペインでHPEアプリをクリックします。

   HPEアプリページが表示されます。

2. HPE OneViewをクリックします。

   HPE OneViewページが表示されます。Active Health Systemレポートセクションには、現在のステータスが表示されます。

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

サービスイベントログの表示
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クリア

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

1. 左側のナビゲーションペインでHPEアプリをクリックします。

   HPEアプリページが表示されます。

2. HPE OneViewをクリックします。

   HPE OneViewページが表示されます。サービスイベントログセクションには、イベントログの詳細が表示されます。

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（例えば、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ー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ー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ー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

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

リモートサポート構成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. 左側のナビゲーションペインでHewlett Packard Enterpriseアプリをクリックします。
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. 左側のナビゲーションペインでHPEアプリをクリックします。

   HPEアプリページが表示されます。

2. HPE OneViewをクリックします。

   HPE OneViewページが表示されます。

3. イベントログ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、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。

HPE Compute Ops Management

HPE 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。

HPE 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。

サブトピック

HPE 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。
- iLOの日付と時刻が正しく設定されていることを確認する。

手順

1. ダッシュボードページで、HPE Compute Ops Managementをクリックします。

   HPE Compute Ops Managementページが表示されます。

   > **注記**
   >
   > Hewlett Packard Enterpriseでは、HPE 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、アクセスページまたは接続の構成ページで構成または編集できます。詳しくは、アクセス設定オプションを参照してください。

2. 有効をクリックして、HPE Compute Ops Managementへの接続を開始します。

   HPE Compute Ops Managementページに以下の情報が表示されます。

   - 接続ステータス - HPEiLOとHPE Compute Ops Managementの接続状態を示します。詳しくは、HPE Compute Ops Managementの接続状態を参照してください。
   - 接続タイプ - 接続ステータスが接続済みの場合に接続タイプを示します。接続タイプは直接接続またはセキュアゲートウェイです。

     詳しくは、接続タイプの構成を参照してください。
   - 接続の前提条件 - HPEiLOとHPE Compute Ops Managementの接続に必要な前提条件を示します。
     - iLOネットワーク構成
     - Web接続
     - Compute Ops Managementの接続

   システムがHPE OneViewによって管理されている場合、HPE Compute Ops Managementを有効にすると、HPE OneViewから切断されます。

   iLOが**HPE 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、**HPE Compute Ops Management**が有効に設定されます。

   リセット中、**HPE 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**HPE Compute Ops Management**を手動で無効にした場合にのみ、**HPE Compute Ops Management**が無効に設定されます。

   HPE iLOは、画面に表示された時間に自動的に再接続を試みます。今すぐ接続をクリックして接続を再試行することも可能です。

接続タイプの構成

前提条件

- iLO設定の構成権限。

このタスクについて

Web接続でエラーが発生した場合、ネットワークにプロキシが必要かどうかを確認し、接続タイプを構成します。

手順

1. ダッシュボードページで、HPE Compute Ops Managementをクリックします。

   HPE Compute Ops Managementページが表示されます。

   > **注記**
   > Hewlett Packard Enterpriseでは、HPE 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、アクセスページまたは接続の構成ページで構成または編集できます。詳しくは、アクセス設定オプションを参照してください。

2. 接続の構成をクリックします。

   接続の構成ページが表示されます。

3. 接続タイプを選択します。

   - 直接接続 – ネットワークでWeb接続にプロキシが必要な場合は、このオプションを選択します。
   - セキュアゲートウェイ – セキュアゲートウェイを使用してHPE Compute Ops Managementに接続するには、このオプションを選択します。

     > **注記**
     > Hewlett Packard Enterpriseでは、セキュアゲートウェイをプロキシサーバーとしてポートアドレス8080で使用することを強くお勧めします。

4. （オプション）Direct Connectを選択した場合、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。詳しくは、アクセス設定オプションを参照してください。

   アクティベーションキーはオプションです。接続を構成するときにキーを入力できます。

5. （オプション）セキュアゲートウェイを選択した場合、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を取得するには、**HPE GreenLake**にログインし、Compute Ops Managementサービスを起動します。概要ページのサーバーの追加セクションで、キーを取得をクリックしてキーを生成します。

   アクティベーションキーは、**HPE Compute Ops Management**への接続を開始するために必須ではありません。**HPE 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。**HPE 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。詳しくは、HPE Compute Ops Managementの接続状態を参照してください。

6. 保存をクリックして、HPE Compute Ops Managementへの接続を開始します。

HPE Compute Ops Managementからの切断

手順

1. ダッシュボードページで、HPE Compute Ops Managementをクリックします。

   HPE Compute Ops Managementページが表示されます。

2. HPE Compute Ops Managementから切断するために無効をクリックします。

   Compute Ops Managementの無効化ページが表示されます。

3. HPE Compute Ops Managementを無効にすることを確認しましたを選択し、無効をクリックします。

   HPE Compute Ops Managementが無効になると、次のアクションが開始されます。

   - iLOが**HPE Compute Ops Management**から切断されます。
   - Webプロキシ設定を除くすべての構成設定がクリアされます。
   - iLO Advancedライセンスが削除されます。

   HPE Compute Ops Managementに接続するには、設定を再構成する必要があります。

HPE Compute Ops Managementの接続状態

次の表は、HPE Compute Ops Managementの接続状態とエラーを示しています。

表 1. HPE Compute Ops Managementの接続状態と説明

接続の状態	説明
無効	HPE Compute Ops Managementが有効ではありません。
初期化中	HPE Compute Ops Managementへの接続はiLOのリセット後に初期化されます。
進行中	HPE Compute Ops Managementへの接続が進行中です。
接続済み	iLOはHPE Compute Ops Managementに正常に接続されています。
iLO IPアドレスが設定されていません	iLOをネットワークに接続するには、画面上の推奨事項に従ってください。 詳しくは、一般的なネットワーク設定を参照してください。
DNS解決エラー	iLOをネットワークに接続するには、画面上の推奨事項に従ってください。 詳しくは、一般的なネットワーク設定を参照してください。
プロキシ設定が無効	提供されたWebプロキシを使用して接続できませんでした。プロキシの詳細が正しいことを確認してください。 詳しくは、接続タイプの構成を参照してください。
プロキシまたはファイアウォールの問題	サーバーがHPE Compute Ops Managementに接続するためのIDを取得するためにHPEに接続できませんでした。HPEをHPE Compute Ops Managementに接続するには、画面上の推奨事項に従ってください。 詳しくは、接続タイプの構成を参照してください。
正しくないiLO時間	HPEのシステム時刻が正しくないため、サーバーがHPE Compute Ops Managementに接続するためのIDを取得できませんでした。NTP構成またはRBSUの時刻をアップデートするには、画面上の推奨事項に従ってください。 詳しくは、iLO SNTP設定の構成を参照してください。
アクティベーションキーが必要です	画面上の推奨事項に従ってアクティベーションキーを生成してください。アクティベーションキーの入力画面で、アクティベーションキーをクリックし、保存をクリックします。 問題が続く場合は、HPEサポートに連絡してください。
無効なアクティベーションキー	画面上の推奨事項に従って新しいアクティベーションキーを生成してください。アクティベーションキーの入力画面で、アクティベーションキーをクリックし、保存をクリックします。 問題が続く場合は、HPEサポートに連絡してください。
期限切れのアクティベーションキー	画面上の推奨事項に従って新しいアクティベーションキーを生成してください。アクティベーションキーの入力画面で、アクティベーションキーをクリックし、保存をクリックします。 問題が続く場合は、HPEサポートに連絡してください。

接続の状態	説明
サポート対象外のiLOバージョン	HPE Compute Ops Managementを使用するにはiLOの最新版にアップグレードします。詳しくは、iLOまたはサーバーファームウェアのアップデートを参照してください。
デバイスの割り当てに失敗	HPE GreenLakeで、デバイスを選択して、このデバイスが別のCompute Ops Managementインスタンスに追加されていないことを確認してください。設定の編集をクリックし、アクティベーションキーをアップデートすることもできます。詳しくは、次のWebサイトを参照してください。https://common.cloud.hpe.com/
デバイスの獲得が承認されていません	HPE GreenLake管理者に連絡して、HPE GreenLakeのデバイスインベントリにデバイスを追加するための適切な権限があることを確認してください。設定の編集をクリックし、アクティベーションキーをアップデートすることもできます。詳しくは、次のWebサイトを参照してください。https://common.cloud.hpe.com/
デバイスが見つかりません	この問題を解決するには、HPEサポートに連絡してください。設定の編集をクリックし、アクティベーションキーをアップデートすることもできます。詳しくは、次のWebサイトを参照してください。https://common.cloud.hpe.com/
不明なエラー	iLOをリセットして、接続を再試行してください。問題が続く場合は、HPEサポートに連絡してください。詳しくは、Webインターフェイスを使用したiLOプロセッサーのリセットを参照してください。
外部エラー	iLOをリセットして、接続を再試行してください。問題が続く場合は、HPEサポートに連絡してください。詳しくは、Webインターフェイスを使用したiLOプロセッサーのリセットを参照してください。
Compute Ops Managementによって無効になりました	インテグレーテッドマネジメントログとCompute Ops Managementのアクティビティダッシュボードを確認してください。HPE GreenLakeの起動をクリックしてHPE Compute Ops Managementを有効にします。詳細については、次のWebサイトを参照してください。https://common.cloud.hpe.com/

注記

- iLOのリセットが発生すると、HPE 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HPE 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HPE 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

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。

サブトピック

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。

- iLO
- iLO RESTful APIおよびiLOREST

このトピックでは、iLOからOne-buttonセキュア消去にアクセスする方法について説明します。

One-buttonセキュア消去プロセスを開始するための前提条件

前提条件

- Hewlett Packard Enterpriseでは、消去したくないリムーバブルドライブ、外部ストレージ、または共有ストレージを切断またはデタッチすることをお勧めします。
- 自分のiLOユーザーアカウントに、リカバリセットも含めすべての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。
- 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。
- 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。

    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。

    手順については、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の手順を参照してください。

- Intel VROC暗号化

  手順については、Intel 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。

- 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。
- 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。One-buttonセキュア消去がサポートされているドライブに及ぼす影響について詳しくは、One-buttonセキュア消去のFAQを参照してください。

  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。

- Hewlett Packard Enterpriseでは、SNMPアラート、メール設定、またはiLO RESTful APIアラートを構成してから、One-buttonセキュア消去プロセスを開始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。IMLログは、SNMPアラート、メール設定、またはiLO RESTful APIアラートを使用して確認できます。IMLは、後で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にステータスの概要情報が表示されます。

- 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 Smartcard、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。

- Microsoft® Secured-coreサポートを無効にします。

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。

> **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。システムに表示される内部および外部接続のストレージデバイス上のすべてのデータが失われます。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。

手順

1. 左側のナビゲーションペインでセキュリティをクリックしてセキュア消去をクリックするか、左側のナビゲーションペインでiLO設定をクリックしてクイックリンクからセキュア消去リンクをクリックします。

   セキュア消去ページが表示されます。
   サーバーでOne-buttonセキュア消去プロセスが完了した場合は、最新の消去レポートの参照ボタンが使用できます。

2. 完全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。

3. 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た後、One-buttonセキュア消去プロセスが開始します。サーバーの起動中に、BIOSは管理しているデータを削除します。BIOSがデータを削除した後、サーバーの電源がオフになります。次に、iLOは残りのデータを削除します。

   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。

4. （オプション）システムを稼働状態に戻します。

5. （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。

6. （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。

サブトピック

One-buttonセキュア消去ステータス値

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が完了した後、iLOがIPアドレスで構成された。

手順

1. 左側のナビゲーションペインでセキュリティをクリックしてセキュア消去をクリックするか、左側のナビゲーションペインでiLO設定をクリックしてクイックリンクからセキュア消去リンクをクリックします。

   セキュア消去ページが表示されます。
   サーバーでOne-buttonセキュア消去プロセスが完了した場合は、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。

サブトピック

One-buttonセキュア消去レポートの詳細

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フラッシュのステータスのみが含まれます。
- ロケーション - 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が完了した後、iLOがIPアドレスで構成された。

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. 左側のナビゲーションペインでセキュリティをクリックしてセキュア消去をクリックするか、左側のナビゲーションペインでiLO設定をクリックしてクイックリンクからセキュア消去リンクをクリックします。

   セキュア消去ページが表示されます。

2. ダウンロードをクリックします。

   セキュア消去レポートがダウンロードされます。

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が完了した後、iLOがIPアドレスで構成された。
- 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. 左側のナビゲーションペインでセキュリティをクリックしてセキュア消去をクリックするか、左側のナビゲーションペインでiLO設定をクリックしてクイックリンクからセキュア消去リンクをクリックします。

   セキュア消去ページが表示されます。
   サーバーでOne-buttonセキュア消去プロセスが完了した場合は、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。

- 影響を受けたストレージドライブおよび不揮発性メモリ上にあるすべてのデータは消去され、回復可能ではありません。すべてのRAID設定、ディスクパーティション、およびOSインストールは削除されます。

  以下のBIOSおよびiLO 7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）は消去されます。

    注記

    iLO IDevIDPCA、iLO IAK、システムIDevID、およびシステムIAK証明書は、One-buttonセキュア消去では消去されません。

  - 工場出荷時にプロビジョニングされたiLO HPE LDevID、iLO LAK、システムLDevID、およびシステムLAKは消去されます。

- プラットフォーム証明書および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 7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データは削除され、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。

サブトピック

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
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

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

One-buttonセキュア消去プロセスは次のコンポーネントに影響を及ぼしません。

- 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

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
- 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

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HPE SRコントローラー、MRコントローラー、およびNSコントローラーがサポートされています。

One-buttonセキュア消去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。

RAIDコントローラーは、パージ操作をサポートしていないドライブをワイプする（あるパターンで上書きする）ことができます。One-buttonセキュア消去では、このセキュリティ保護されていないワイプを実行するようコントローラーに要求することはありません。このようなドライブのデータをワイプするには、Intelligent Provisioningの「システムの消去およびリセット」機能を使用してください。

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
内蔵フラッシュ (NAND)	拡張CSDレジスタの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。
Intel 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Secure Encryption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 [2]	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	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	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。
	NVM Express SANITIZE（サポートされている場合）（NVM Expressバージョン1.3以降をサポートするドライブの場合） シングルパスのNVM Express FORMAT with SES = 1。このオプションは、ドライブがSANITIZEをサポートしていない場合に使用されます。	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 SRコントローラーおよびMR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 これらのドライブは、HPE SRコントローラーおよびMR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。

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は、初期化プロセスの実行時に構成情報をバックアップします。この構成情報が破損している場合、iLOはバックアップファイルから復元を試みます。自動リストア操作はIMLに記録されます

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。

注記

ホストOSのブート中、バックアップおよびリストア機能はiLO RESTful APIを介して利用できません。ホストのブート状態に関係なく、この機能はiLO Webインターフェイスを介して利用可能です。

手動でのバックアップとリストア

iLOでは、構成情報の手動復元がサポートされています。

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。

サブトピック

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。

例えば、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。

工場出荷時の設定へのリセット

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。

失われたライセンスキー

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復元できます。

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がセキュア標準のセキュリティ状態を使用するように構成されている。iLOがさらに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. クイックアクションメニューでiLO構成のバックアップをクリックします。

   バックアップ構成設定ウィンドウが表示されます。

2. （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。

3. 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。

  セキュア標準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復元を実行した場合、復元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. 左側のナビゲーションペインで、iLO設定をクリックします。

   iLOページが表示されます。

2. クイックアクションメニューでiLO構成のリストアをクリックします。

   iLO構成のリストアウィンドウが表示されます。

3. 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、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。

4. バックアップファイルをバックアップファイルボックスにドラッグするか、参照をクリックしてバックアップファイルに移動します。

5. リストアの確認をクリックします。

6. 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。

7. 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。

サブトピック

システムボード交換後のiLO構成のリストア

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。

  セキュア標準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復元を実行した場合、復元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。

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

iLO 7では、HPE OneViewなどのサポート対象ツールによるリモート管理がサポートされます。

iLO 7では、サポート対象ツールによるリモート管理がサポートされます。

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。

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の名前>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。

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。HPE OneViewからサーバーを削除した後、iLO Webインターフェイスウィンドウを更新してください。
> ネットワーク上で使用されており、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. 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。
2. 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iLO 7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勧めします。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）

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 SPP、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、電源装置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

注記
ARMベースのHPE Gen11サーバー（HPE ProLiant RL3xx Gen 11など）では、RBSUを介して設定されたサーバーの AssetTag は、RedfishまたはIPMIを使用するiLOインターフェイス、例えばpostmanやipmitoolに影響を与えません。同様に、RedfishまたはIPMIを使用しiLOインターフェイスを介して設定された AssetTag は、BIOS内の AssetTag 設定に影響を与えません。

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**https://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**https://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**https://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**https://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。**https://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（例えば、 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（例えば、 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（例えば、 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
```

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

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が構成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構成する方法については、サーバーOS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

手順

1. iLOホスト名およびドメイン名を構成します。
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パラメーターを構成します。
7. iLOディレクトリグループを構成します。
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セクションをクリックします。
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. 全般セクションをクリックします。
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

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

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。例えば、`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、セキュア標準、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キータイプを使用します。

`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

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

iLOを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。

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構成します。
3. ディレクトリグループを構成します。

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. 必要なソフトウェアをインストールします。

- HPE Management Devices Schema Extender（Schema Extender）をインストールします
- HPE Management Devicesディレクトリスナップイン（x86およびx64）をインストールします

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。

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 MS01-036: 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

このタスクについて

ディレクトリサポートソフトウェアは、HPEサポートセンターからダウンロードできます。

- HPE Management Devices Schema Extender（Schema Extender）

- HPE Management Devicesディレクトリスナップインのインストール

サブトピック

HPE Management Devices Schema Extenderのインストール
HPE Management Devicesディレクトリスナップインのインストール
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

HPE Management Devices Schema Extenderのインストール

このタスクについて

手順

1. HPE Management Devices Schema ExtenderからHPE Management Devices Schema Extenderをダウンロードします。
2. ようこそウィンドウで、次へをクリックします。
3. 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。
4. 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。
5. 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。

   続いて、閉じるをクリックします。Installation Completeウィンドウが開きます。
6. 閉じるをクリックします。

HPE Management Devicesディレクトリスナップインのインストール

このタスクについて

手順

1. HPEサポートセンターから必要なソフトウェアをダウンロードします。
   a. HPE Management Devicesディレクトリスナップイン32ビット（スナップインx86）
   b. HPE Management Devicesディレクトリスナップイン64ビット（スナップインx64）
2. ようこそウィンドウで、次へをクリックします。
3. 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。
4. 情報ウィンドウで詳細を読んで、次へをクリックします。
5. 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。

   続いて、閉じるをクリックします。Installation Completeウィンドウが開きます。
6. 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HPE Management Devicesディレクトリ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。

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

- HPE Management Devices Schema Extender - HPEにバンドルされている`.xml`ファイルManagement Devices Schema Extenderには、ディレクトリに追加されるスキーマが含まれています。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。
- HPE Management Devicesディレクトリスナップイン（64ビット）またはHPE Management Devicesディレクトリスナップイン（32ビット）- HPE Management Devicesディレクトリスナップインのインストーラーは、Microsoft Active Directoryユーザーとコンピューターのディレクトリまたは Novell ConsoleOneディレクトリ内のiLOオブジェクトを管理するために必要な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構成できます。

  `HPLOMIG.exe`ファイル、必要なDLL、ライセンス契約などのファイルが次のディレクトリにインストールされます：`C:\Program Files (x86)\Hewlett Packard Enterprise\Directories Support for ProLiant Management Processors`。別のディレクトリを選択することもできます。インストーラーにより、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がスタートメニューに作成されます。
  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。

HPE Management Devices Schema Extenderの実行

手順

1. WindowsのスタートメニューからHPE 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。

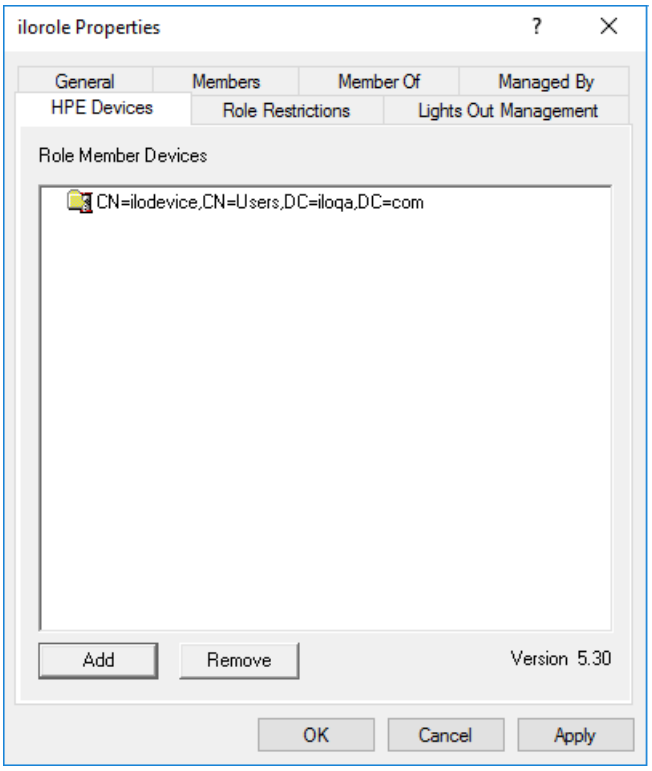
HPE Management Devicesディレクトリスナップインのインストール後、iLOオブジェクトとiLOロールを、ディレクトリ内で作成できます。次のタスクは、Active Directory Users and Computersツールを使用して行います。

- 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

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

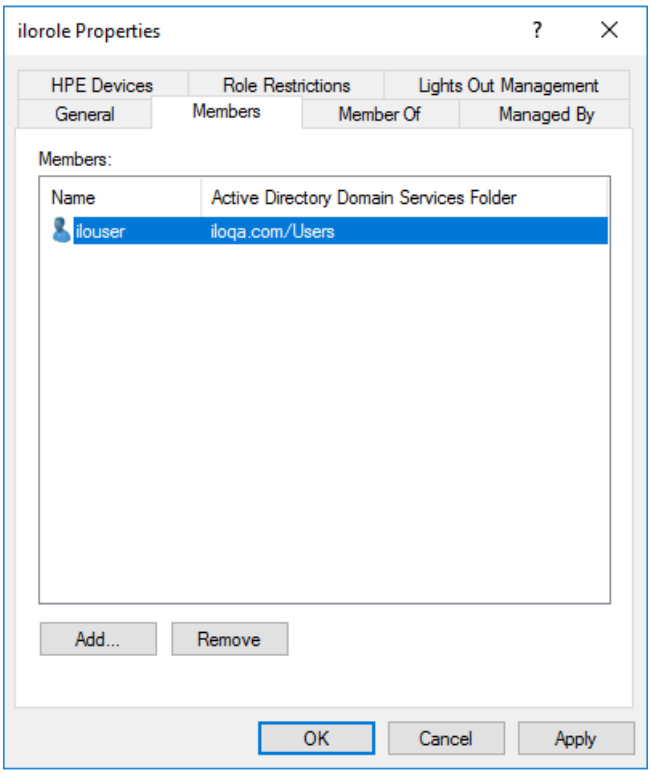
Hewlett Packard Enterpriseスナップインをインストールした後、Active Directoryユーザーとコンピューターで次の管理オプションが使用できるようになります。

Devicesタブ



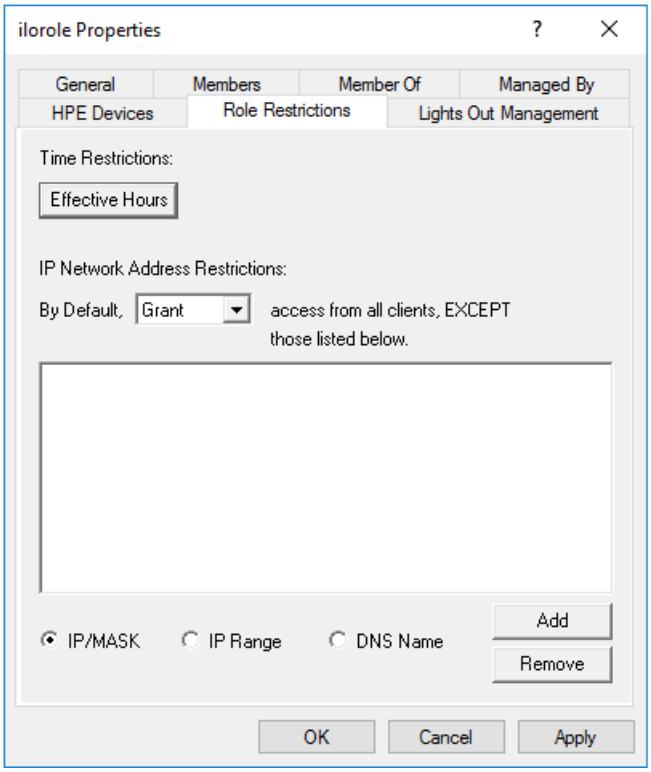
このタブでは、ロール内で管理するHewlett Packard Enterpriseデバイスを追加できます。Addをクリックすると、デバイスにアクセスして、そのデバイスをメンバーデバイスのリストに追加することができます。既存のデバイスを選択して、Removeをクリックすると、そのデバイスは有効なメンバーのデバイスリストから削除されます。

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。

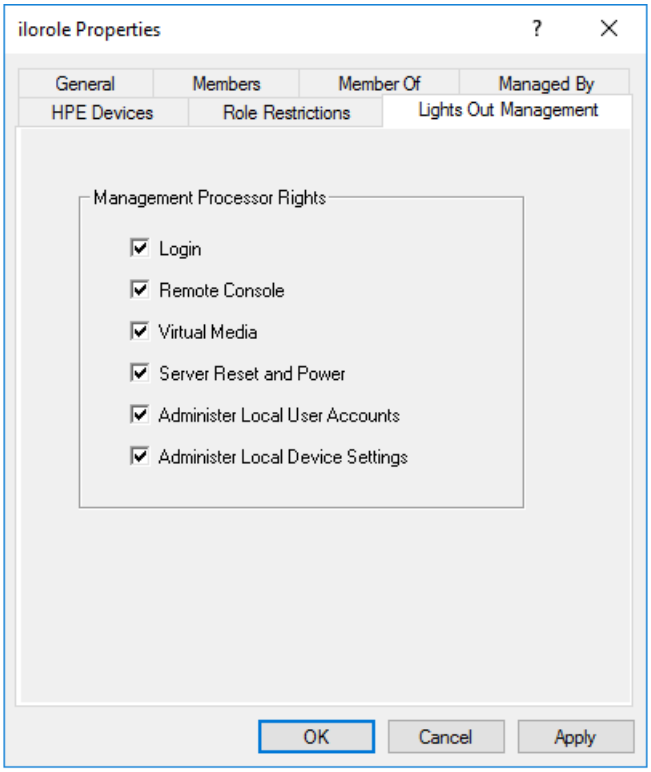
Role Restrictionsタブ



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。

サブトピック

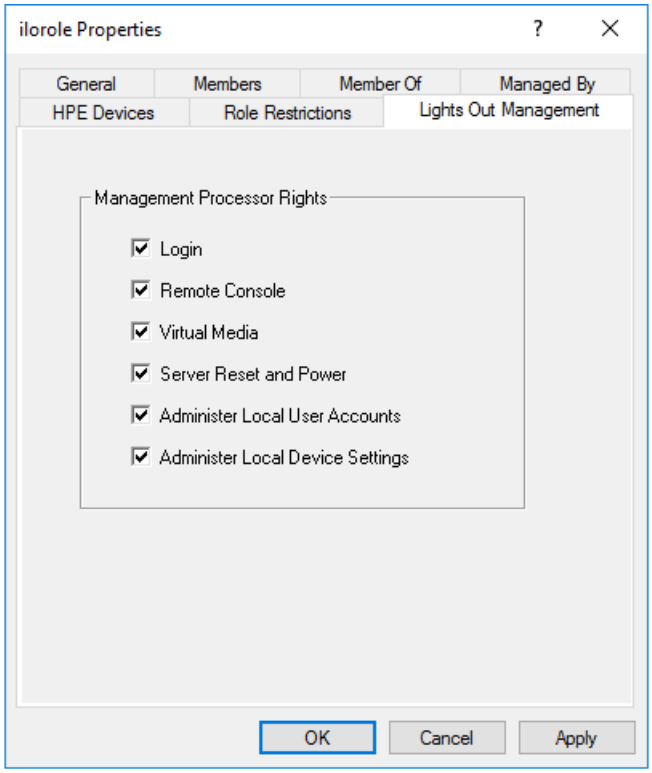
クライアントIPアドレスまたはDNS名の制限の設定

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。HPE Management Devicesディレクトリスナップインを使用してLOMオブジェクトを作成できます。

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。例えば、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
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

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

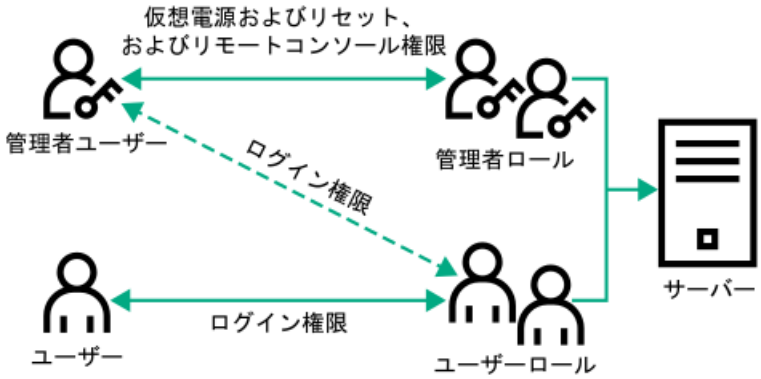
ほとんどのデプロイメントでは、同じユーザーが、同じデバイスを管理する複数のロールに入っている必要はありません。ただし、これらの構成は、複雑な権限関係を構築する際には便利です。ユーザーが複数のロールの関係を構築すると、そのユーザーには、該当する各ロールによって割り当てられるすべての権限が付与されます。ロールは、権限を付与することしかできず、権限を取り消すことはできません。あるロールがユーザーに権限を付与する場合、そのユーザーは、その権限を付与しない別のロールに入っていても、その権限を持ちます。

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。

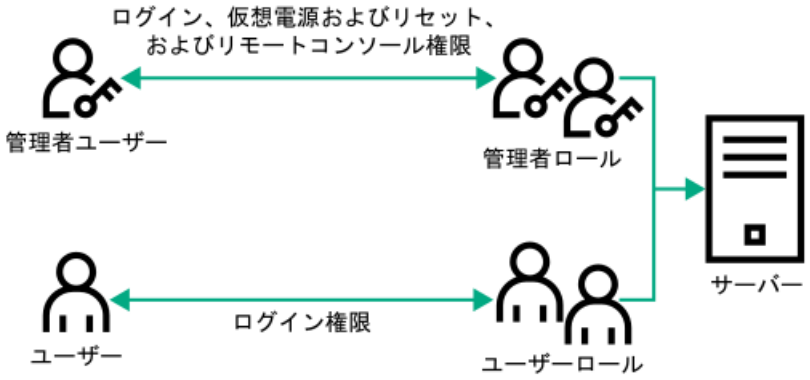
複数の（重複する）ロールには、管理者ユーザーがユーザーロールからログイン権限を取得し、管理者ロールから高度な権限が割り当てられる例を示します。

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

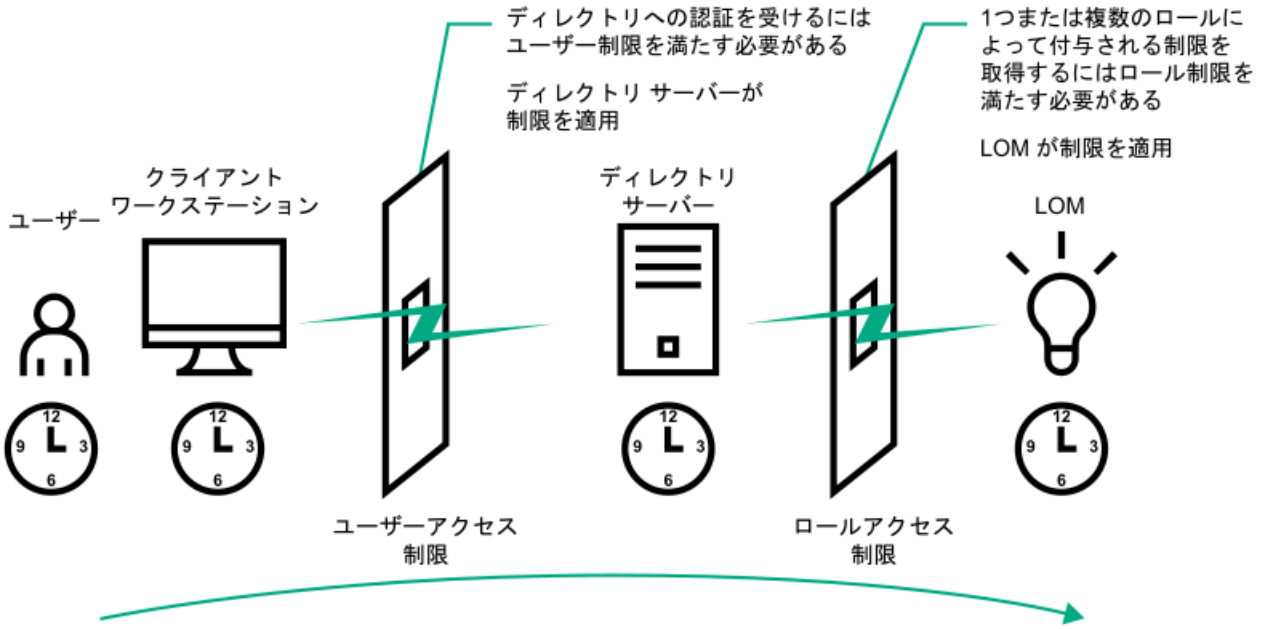


ロールアクセス制限の適用方法

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。

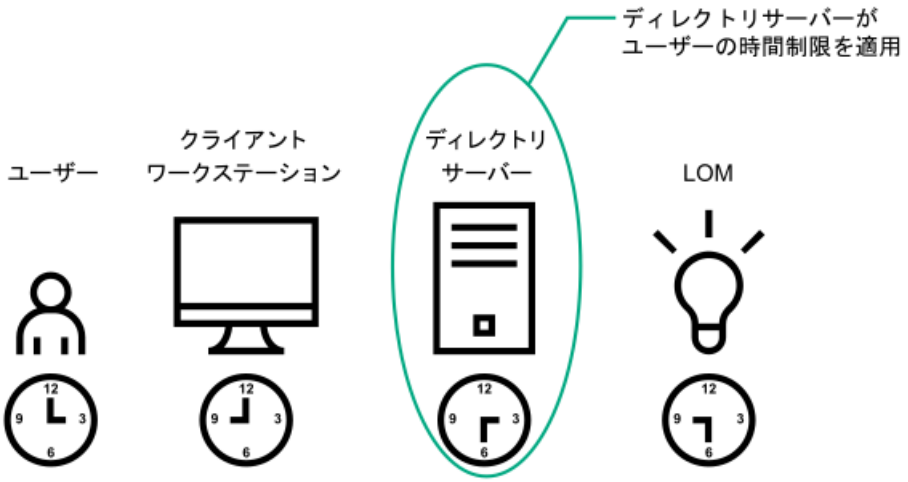
DNSベース制限を使用すると、セキュリティが複雑になる場合があります。ネームサービスプロトコルは、安全ではありません。ネットワークにアクセスできる悪意を持ったユーザーは、誰でも、不正なDNSサーバーをネットワークに配置して偽のアドレス制限基準を作成することができます。DNSベースのアドレス制限を実装している場合は、組織的なセキュリティポリシーを考慮に入れてください。

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

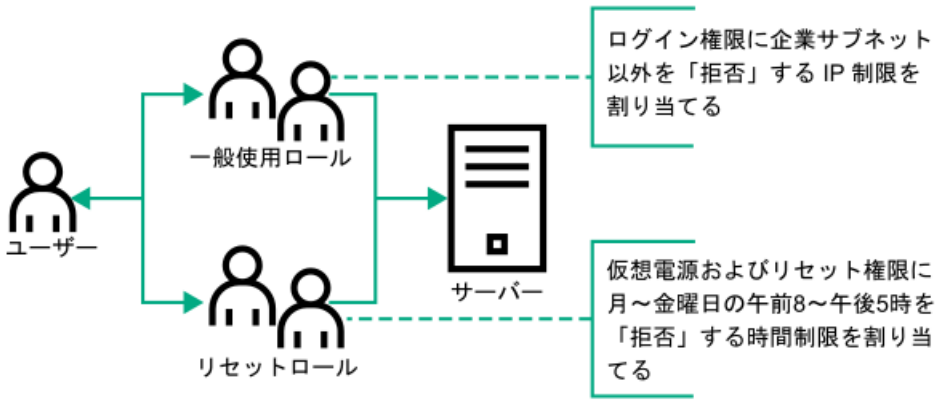
権限の適用される状況が限定されるように1つまたは複数のロールを制限したい場合には、多数のロールを作成すると非常に便利です。他のロールが、異なる権限を異なる制限で付与します。複数の制限とロールを使用すると、管理者は、任意の複雑な権限関係を最小限のロールで作成できます。

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。

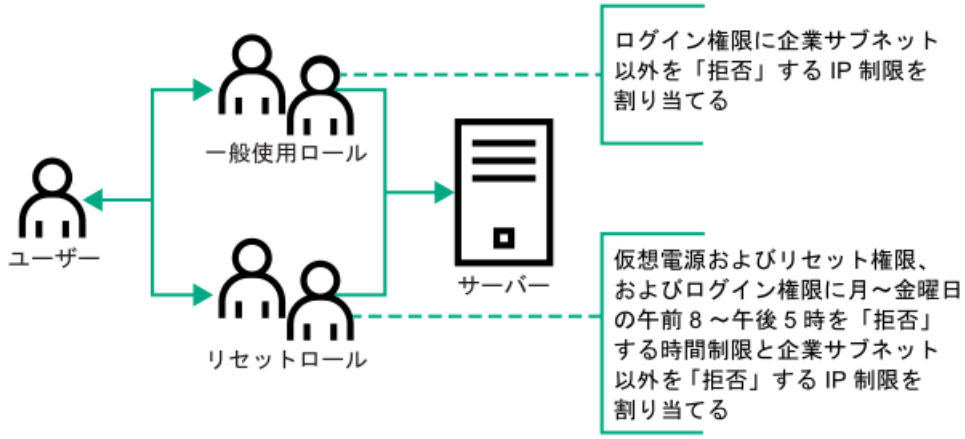
図 1. 制限およびロールの作成



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。

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. HPE Management Devices Schema Extenderの実行
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

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権限で、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

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
```

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。

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

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

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

- iLO 7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 7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（iLO 7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（iLO 7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 7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。

   iLO 7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iLO 7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iLO 7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

HPE iLO

https://www.hpe.com/jp/servers/ilo

HPE iLO 7のドキュメント

https://www.hpe.com/support/ilo7

HPE iLOクイックリンク

https://www.hpe.com/support/hpeilodocs-quicklinks

UEFIシステムユーティリティ

https://www.hpe.com/info/ProLiantUEFI/docs

Intelligent Provisioning

https://www.hpe.com/info/intelligentprovisioning/docs

HPE OneView

https://www.hpe.com/info/oneview/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
HPE製品登録
アップデートへのアクセス
リモートサポート
保証情報
規定に関する情報
ドキュメントに関するご意見、ご指摘

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Webサイトにアクセスします。

  https://www.hpe.com/support/hpesc

収集される情報

- 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

HPE製品登録

Hewlett Packard Enterpriseサポートセンターおよび購入したサポートサービスのメリットを最大限に活用するため、契約と製品をHPESCのアカウントに追加してください。

- 契約と製品を追加すると、パーソナライゼーションの強化、ワークスペースのアラート機能、ダッシュボードを通じた有益な情報が提供され、環境の管理が容易になります。
- また、問題を自己解決するための推奨事項やカスタマイズされた製品知識も提供されるほか、ケースを作成する必要がある場合は、合理化されたケース作成によって解決までの時間が短縮されます。

契約と製品を追加する方法については、https://support.hpe.com/hpesc/public/docDisplay?docId=cep-help_ja_jp&page=GUID-8C7F13D9-5EC3-4E5C-9DE2-A5E7823066D6.htmlを参照してください。

アップデートへのアクセス

- 一部のソフトウェア製品では、その製品のインターフェイスを介してソフトウェアアップデートにアクセスするためのメカニズムが提供されます。ご使用の製品のドキュメントで、ソフトウェアの推奨されるアップデート方法を確認してください。
- 製品のアップデートをダウンロードするには、以下のいずれかにアクセスします。

  Hewlett Packard Enterpriseサポートセンター

  https://www.hpe.com/support/hpesc

  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-ja
- 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アカウント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

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

https://support.hpe.com/hpesc/public/docDisplay?docId=a00041232ja_jp

HPE Tech Care Service

https://www.hpe.com/jp/techcare

HPE Complete Care Service

https://www.hpe.com/jp/completecare

保証情報

保証情報

ご使用の製品の保証に関する情報を確認するには、**標準保証確認ツール**を参照してください。

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

企業プログラム、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。ドキュメントを改善するために役立てさせていただきますので、何らかの誤り、提案、コメントなどがございましたら、 Hewlett Packard Enterpriseサポートセンターポータル（https://www.hpe.com/support/hpesc）の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る）からお寄せください。このプロセスにより、すべてのドキュメント情報が取得されます。