iLO7
ユーザーズガイド

NEC Expressサーバー

Express5800シリーズ

Express5800サーバー

発行: 2026 年 6 月 29 日

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

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

他社の Web サイトへのリンクは、弊社の Web サイトの外に移動します。弊社は、弊社の Web サイト以外にある情報を管理する権限を持たず、また責任を負いません。

商標

Microsoft®、Azure®、Azure Stack®、Azure Stack Hub®、および Windows®は、米国および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。

Intel®および Intel® Xeon®は、米国およびその他の国における Intel Corporation の商標です。

VMware is a registered trademark or trademark of Broadcom in the United States and other countries. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

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。

本製品は、日本国内で使用するための仕様になっており、日本国外で使用される場合は、仕様の変更を必要とすることがあります。

本書に掲載されている製品情報には、日本国内で販売されていないものも含まれている場合があります。

公開日	版数	変更概要
2026/06/29	3	iLO7 1.21.00 に対応。 • 以下のセクションを更新。 ◦ BIOS ◦ 電源装置概要の詳細 ◦ 電源配電盤のオプション ◦ 電力読み取り値 ◦ パワーマネジメントコントローラー ◦ GPU 消費電力上限設定 ◦ リモートコンソール ◦ TLS 証明書の管理 ◦ 自動証明書登録 • 誤記訂正
2025/09/25	2	iLO7 1.17.00 に対応。 • 以下のセクションを更新。 ◦ 仮想 NIC 機能の構成 ◦ iLO7 で削除された機能 ◦ TLS 証明書の管理（SSL を TLS に置き換え） ◦ ボリューム ◦ ストレージコントローラー ◦ 温度構成オプション ◦ サポートされるファームウェアタイプ ◦ スロットの詳細ペイン ◦ セッションリスト詳細 ◦ SSH 暗号、キー交換、および MAC のサポート ◦ TLS 暗号および MAC のサポート ◦ 電源装置のリスト ◦ iLO セキュリティ状態 ◦ ファームウェア検証 ◦ 証明書署名要求 ◦ 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 ◦ iLO Web インターフェイスを使用した新しい SSH キーの認証 ◦ システムボードの交換 • "LLDP 設定の表示"を追加。 • 以下のセクションのマイナー変更。 ◦ One-button セキュア消去の完了後のシステムへの影響 ◦ One-button セキュア消去の FAQ ◦ アクセス設定オプション ◦ システム IAK 証明書 • "温度グラフの表示"を追加 • "時間設定の構成"セクションを更新 • "iLO7 で削除された機能"セクションを更新 • "アクセス設定オプション"のセクションに"ログを表示"を追加 • "iLO セッションの管理"セクションに LDAP サーバー設定の注意書きを追加 • "CA からの信頼済み証明書の取得"セクションに iLO TLS 証明書の注意書きを追加 • トラブルシューティングセクションの項目修正、新規項目追加。 • SSH 設定に関する注意事項を追加。
2025/08/04	初版	iLO7 1.14.00 に対応。

目次

1. はじめに

iLO の概要

iLO は、Express5800 サーバーのマザーボードに内蔵されているリモートサーバー管理プロセッサーです。iLO では、リモートからサーバーを監視および制御できます。iLO は、サーバーをリモートから構成、更新、監視、および修復する複数の方法を提供します。iLO(Standard ライセンス)は、追加コストおよびライセンスなしで Express5800 サーバーに事前設定されています。

サーバー管理者の生産性を更に向上させる機能にはライセンスが必要です。

ライセンスが必要な機能は「iLO ライセンスオプション」を参照してください。

iLO7

iLO7 搭載の Express5800 サーバーは、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 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。

iLO7 の新機能

- **iLO 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** - iLO7 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。
- **CNSA 2.0 署名アルゴリズムの使用** - 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が直接 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)に物理接続します。
  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。
- **iLO サービスポート** – USB Type C 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、iLO 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、iLO サービスポートと標準の 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)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 フラッシュドライブを接続して、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 ライセンスオプション」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。
- **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)** - iLO7 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。
- **iLO 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(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 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。
- **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。
- **シャーシのパワーレギュレーターモード** - シャーシのパワーレギュレーションページのユーザー構成可能モード設定を使用するにはライセンスが必要です。このモードを構成すると、ユーザーは、事前定義された範囲から有効な消費電力上限値を指定できます。
- **Commercial National Security Algorithm (CNSA) セキュリティ状態** - CNSA セキュリティ状態 (SuiteB とも呼ばれる) は、FIPS セキュリティ状態が有効になっている場合にのみ使

用できます。CNSA セキュリティ状態を有効にした場合の iLO への影響は次のとおりです。

  - iLO は、NSA によって定義された CNSA 要件への準拠を目的とするモードで動作します。
  - iLO は、米国政府機密として分類されたデータを保持するシステムの保護を目的とするモードで動作します。
  - SUM を使用して iLO にアクセスする場合は、iLO 認証情報が必要です。
  - TLS 1.2 をサポートしていないネットワークベースのツールを使用してサーバーに接続することはできません。
  - システムメンテナンススイッチの iLO セキュリティ設定 (iLO セキュリティオーバーライドスイッチと呼ばれる)は、iLO へのログインに関するパスワード要件を無効にしません。

- **ディレクトリサービス認証** - Microsoft Active Directory などのディレクトリサービスを統合して、ディレクトリユーザーに対して、iLO プロセッサーに割り当てられたユーザーロールを持つことを認可します。
- **Email ベースのアラート** - ホストオペレーティングシステムから独立して検出された iLO アラート条件を、指定したメールアドレスに送信します。
- **内蔵システムヘルス** - システム管理ドライバーをロードせずに、ファン、温度センサー、電源装置センサー、および VRM を監視します。これらのコンポーネントのステータスには、ホストオペレーティングシステムから独立して、すべての iLO インターフェイスからアクセスできます。また、管理プロセッサーは、IPMI 指定のインターフェイスを介して、センサーステータスをオペレーティングシステムにレポートします。iLO のインテリジェンス機能は、Sea of Sensors による温度制御の管理、動的消費電力上限テクノロジーの制御、およびサーバーコンポーネントの稼動状況の監視を行います。
- **iLO リモートコンソールによるグローバルチームコラボレーション** - リモートコンソール権限を持つ最大 6 人までの iLO ユーザーが、ILO リモートコンソールを使って連携してリモートサーバーのトラブルシューティング、メンテナンス、および管理を行うことができます。
- **サーバーの UID ボタンを使用した iLO のリセット** - UID ボタンを 5 秒間押すと、サーバーを停止せずに iLO を手動でリセットできます。
- **iLO リモートコンソールの録画および再生** - 起動、ASR イベント、および検出されたオペレーティングシステムの不具合のようなイベントのビデオストリームを記録し、再生します。コンソールビデオの録画を手動で開始および停止することもできます。iLO リモートコンソールから保存された iLO ビデオファイルを再生できます。
- **IPMI over LAN/DCMI** - LAN または IPMI 仕様のデータセンター管理インターフェイス機能を使用して、プロセッサー、ファームウェア、および OS から独立してリモート接続を確立します
- **IPv6** - IPv6 ネットワークのサポートを提供します。
- **Kerberos 認証** - Kerberos のサポートにより、ユーザーは、ログインページの [Zero サインイン]ボタンをクリックし、iLO にログインすることができます。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。

- **パフォーマンス監視** - Innovation Engine のサポートによってサーバーでサポートされたセンサーから収集したパフォーマンスデータを表示します。収集したデータに基づいてアラートを構成できます。
- **リモート Syslog** - Syslog サーバーにイベント通知メッセージを送信します。
- **サーバー構成ロック** - サーバー構成ロック機能は、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。
- **サーバーヘルスサマリー** - iLO を使用すると、外部モニターにサーバーヘルスサマリーを表示できます。この機能は、サーバーが起動しないときのトラブルシューティングに役立ちます。これは、サーバーの IP アドレスやその他のヘルス情報を表示するためにも使用できます。
- **Silicon Root of Trust (シリコンレベルの信頼性)** - ハードウェアに Silicon Root of Trust を組み込んだ初の業界標準サーバーを提供しています。Silicon Root of Trust は、既知の良好な状態を確保するため、下位レベルのファームウェアから BIOS やソフトウェアに至るまでの一連の信頼済みハンドシェイクを提供します。
- **SSH コマンドラインインターフェイス** - セキュアシェル CLI による監視と管理を行います。サービスアクセス設定のアップデート - このアクセス設定を使用すると、ダウングレードポリシーを構成し、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決定できます。
- **仮想電源ボタン** - ホストの電源ボタンを遠隔操作します。例えば、ホストサーバーがオフの場合、電源を入れることができます。また、サーバーの電源を一度にオフ/オンすることもできます。OS に障害が発生しているサーバーの電源を切る際に、瞬間的に押す操作では不十分な場合に、「押し続ける」オプションを使用できます。
- **仮想シリアルポート** - サーバーのシリアルポートによる双方向のデータフローを実現します。リモートコンソールを使用すると、リモートサーバーシリアルポート上に物理シリアル接続が存在するかのように操作できます。
- **仮想シリアルポートの録画および再生** - 仮想シリアルポートにより、サーバーのシリアルポートと双方向データフローが提供されます。リモートコンソールを使用すると、リモートサーバーシリアルポート上に物理シリアル接続が存在するかのように操作できます。仮想シリアルポートはテキストベースのコンソールとして表示されますが、その情報はグラフィカルビデオデータを通じて描画されます。iLO では、サーバーがプレオペレーティングシステム状態であるときに、この情報が SSH クライアント経由で表示されます。この機能を使用すると、iLO 標準システムで POST 中のサーバーを監視および操作できます。
- **ゾーンマッピング、ゾーンの優先度** - シャーシ全体でグループ化されるか、既存のユーザー定義ゾーンでグループ化されるように、各ノードを設定できます。ゾーンを構成すると、各ゾーンのパワーレギュレーションの優先順位を設定できます。消費電力上限が設定されている場合、優先順位が高いゾーンには、優先順位が低い設定があるゾーンよりも多くの電力が割り当てられます。

注記
IPMI には IPMI 仕様におけるパスワードハッシュを取得される脆弱性(CVE-2013-4786)問題が含まれています。

脆弱性概要

IPMI の仕様は、RMCP+ Authenticated Key-Exchange Protocol (RAKP) 認証をサポートしているため、パスワードハッシュを取得される、およびオフラインパスワード推測攻撃を実行される脆弱性が存在します。

解決方法

この問題に対する解決策はありません。IPMI2.0仕様の認証プロセスは、クライアント認証に先がけてサーバーが要求されたユーザーのパスワードのSHA1、MD5ハッシュをクライアントに送るのを規定しています。BMCは、要求されたユーザーアカウントのパスワードハッシュを返しますが、このパスワードハッシュは、オフラインパスワード推測攻撃で壊すことができます。この機能は、IPMI2.0仕様の重要な部分でIPMI2.0仕様から逸脱せずこの問題を解決することはできません。そのためこのリスクを軽減させるため以下を行うことを推奨します。

- IPMI を使用しない場合、IPMI over LAN を無効化してください。iLO Web インターフェイスの**[iLO 設定] > [アクセス]**ページで**[IPMI/DCMI over LAN]**を無効化することができます。デフォルトは無効化です。
- 最新の iLO ファームウェアを適用してください。
- システム、ネットワーク上のパスワード管理において最善な方策をとってください。強固なパスワードを使用してください。
- IPMI を使用する場合、iLO 管理インターフェイスへのアクセスを制限し、個別のマネジメント LAN/VLAN、アクセス制御リスト(ACL)または VPN を使用してください。

iLO7 で削除された機能

- iLO Web インターフェイスからの EXPRESSBUILDER の Always On 機能
- iLO 連携
- 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
- iLO でセキュアシェル(SSH)ポートの標準ポート 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 へのアクセス

iLOには、iLO Webインターフェイス、BMC構成ユーティリティ、iLO RESTful API、またはRESTfulインターフェイスツールからアクセスできます。

iLO Web インターフェイス

iLO Web インターフェイスを使用して、サポートされるブラウザーを介して iLO にアクセスし、管理対象サーバーを監視および構成できます。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。iLO 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てから表示するタブの名前をクリックします。

iLO ROM ベースセットアップユーティリティ(BMC 構成ユーティリティ)

UEFI システムユーティリティの BMC 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。

BMC 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 BMC 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。BMC 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。

BMC 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、BMC 構成ユーティリティの順にクリックします。

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。

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、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。

2. iLO セットアップ

iLO をセットアップするための準備

iLO マネジメント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 はどのようにネットワークに接続しますか？
2. iLO 共有ネットワークポート構成で NIC チーミングを使用できますか？
3. iLO はどのように IP アドレスを取得しますか？
4. 必要なアクセスセキュリティと、必要なユーザーアカウントと特権は何ですか？
5. iLO の設定にはどのようなツールを使用しますか？

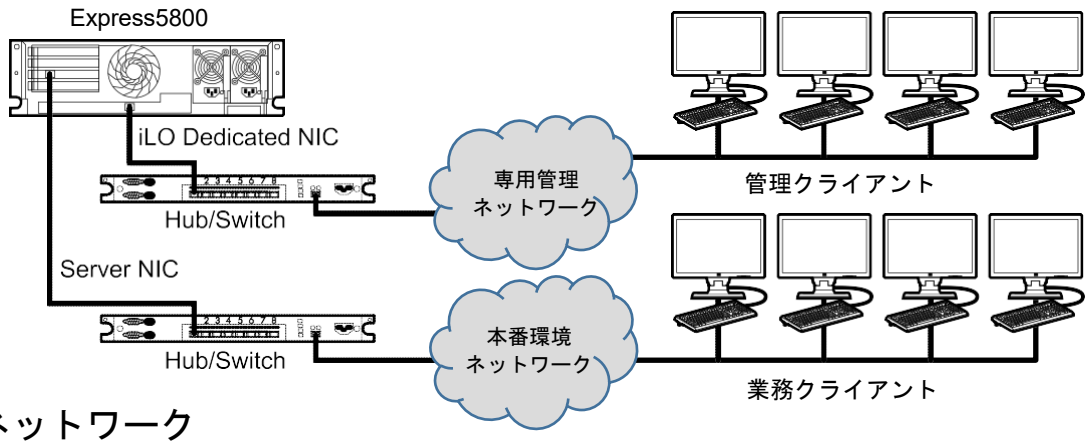
iLO のネットワーク接続の選択

iLO は専用管理ネットワークまたは企業ネットワーク上の共有接続を通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 専用ネットワーク接続例

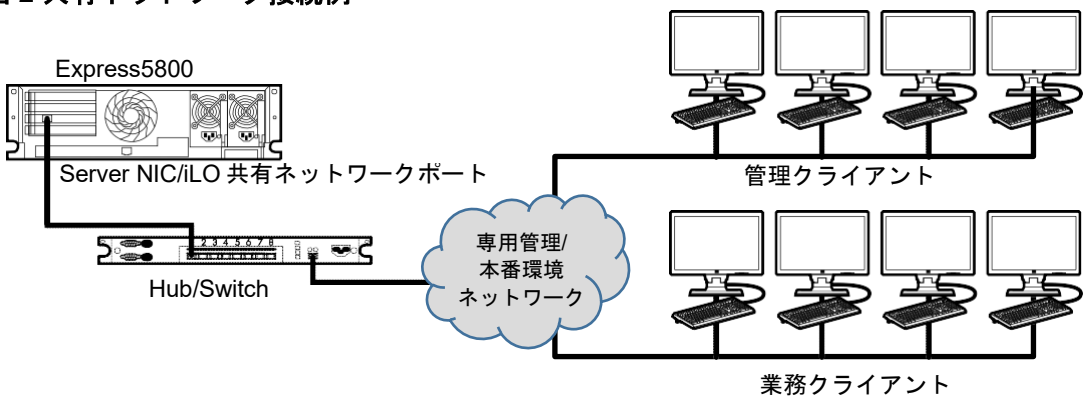


共有ネットワーク

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、100Mbps 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例



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。

iLO 共有ネットワークポート構成時の 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。

NIC チーミングの制約

iLO 共有ネットワークポートを構成する際に、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。

NIC チーミングモード

サーバーで 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。

  - 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。

iLO の IP アドレス取得方法

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ているネットワークに接続される必要があります。本体装置に電源を入れる前に、iLO がネットワークに接続されている必要があります。 iLO は、電源が投入された直後に DHCP 要求を送信します。 iLO が最初に起動したときに DHCP 要求に応答しないと、90 秒間隔で要求が再発行されます。
- DHCP サーバーは、DNS を提供するように構成する必要があります。

- **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、BMC 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 の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。

- **ローカルユーザーアカウント**

  iLO には、最大 12 のアカウントを格納できます。これは、研究所や中小企業のような小規模環境に最適です。ローカルユーザーアカウントを使用したログインセキュリティは、iLO のアクセス設定と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。このガイドでは、次のインターフェイスについて説明します。

- **iLO Web インターフェイス**

  iLO 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。

- **iLO ROM ベースセットアップユーティリティ**(BMC 構成ユーティリティ)

  システム環境において、DHCP または DNS を使用しない場合は、BMC 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、その他に以下の設定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。

初期セットアップ手順

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、BMC 構成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. ローカルユーザーアカウントを使用する場合は、BMC 構成ユーティリティを使用してユーザーアカウントの追加を行います。
5. (オプション) iLO ライセンスをインストールします。
6. iLO Standard ライセンスは、追加コストまたはライセンスなしで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。

iLO をネットワークへ接続

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。

BMC 構成ユーティリティを使用した iLO のセットアップ

初めて iLO をセットアップする場合と、DHCP、DNS を使用しないで iLO のネットワークを構成する場合は、システムユーティリティ内の BMC 構成ユーティリティを使用することをおすすめします。BMC 構成ユーティリティを使用して iLO Web インターフェイスへアクセスするために必要な最低限の設定を行った後に、iLO Web インターフェイスへアクセスしてください。

BMC 構成ユーティリティを使用した静的 IP アドレスの設定

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、iLO では DNS または DHCP を使用することをおすすめします。

手順

1. サーバーを再起動するかまたは電源を入れます。
2. サーバーの POST 画面で F9 キーを押して、システムユーティリティを起動します。
3. [システム構成]画面で上向きまたは下向きの矢印キーおよび Enter キーを使用して[システム構成] > [BMC 構成ユーティリティ] > [ネットワークオプション]に移動します。
4. DHCP を無効にします。

a. [DHCP 有効]で[オフ]を選択します。

5. IP アドレス、サブネットマスク、およびゲートウェイの IP アドレスを入力します。
   a. [IP アドレス]を入力します。
   b. [サブネットマスク] を入力します。
   c. [ゲートウェイ IP アドレス]を入力します。
6. F10 キーを押して、変更を保存します。

   BMC 構成ユーティリティによって、保留中の構成変更をすべて保存するか確認するメッセージが表示されます。
7. Y キーを押して変更を保存し、終了します。

   BMC 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。

> **重要**
> 本書では iLO の再起動という意味で iLO のリセットという用語を使用することがあります。

8. Enter キーを押します。

   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。
9. 通常の起動プロセスを再開します。
   a. ESC キーを数回押して、[システム構成]ページに移動します。
   b. ESC キーを押して、システムユーティリティを終了し、通常の起動プロセスを再開します。

BMC 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

ユーザーアカウントの追加

1. サーバーを再起動するかまたは電源を入れます。
2. サーバーの POST 画面で F9 キーを押して、システムユーティリティを起動します。
3. [システムユーティリティ]画面で、[システム構成] > [BMC 構成ユーティリティ]-[ユーザー管理] > [ユーザーの追加]の順に選択し、[Enter] キーを押します。
4. 次の権限のいずれかを選択し、[Enter] キーを押します。
   - [ユーザーアカウント管理]
   - [リモートコンソールアクセス]
   - [仮想電源およびリセット]
   - [仮想メディア]
   - [設定の構成]
   - [ホスト BIOS]
   - [ホスト NIC]

- [ホストストレージ]

5. 各オプションで、次の設定のいずれかを選択し、[Enter] キーをもう一度押します。
   - **[はい]**(デフォルト) - このユーザーの権限を有効にします。
   - **[いいえ]** - このユーザーの権限を無効にします。
6. 次のオプションから選択し、[Enter] キーを押します。
   - [新しいユーザー名]
   - [ログイン名]
   - [パスワード]と [パスワードの確認]
7. 新しいユーザーの各オプションの設定を完了し、[Enter] キーを押します。
8. 必要な数のユーザーアカウントを作成し、F10 キーを押します。
9. メインメニューが表示されるまで、Esc キーを押します。
10. メインメニューで [終了して起動を再開]を選択し、Enter キーを押します。
11. 要求の確認を求めるメッセージが表示されたら、Enter キーを押してユーティリティを終了し、起動プロセスを再開します。

ユーザーアカウントの編集または削除

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 キーを押して、システムユーティリティを起動します。
4. [システムユーティリティ]画面で、[システム構成] > [BMC 構成ユーティリティ] > [ユーザー管理] > [ユーザーの編集/削除]を選択し、[Enter]キーを押します。
5. 編集または削除するユーザー名の[Action]メニューを選択し、Enter キーを押します。
6. 次のいずれかを選択し、Enter キーを押します。
   - **[変更なし]** - メインメニューに戻ります。
   - **[削除]** - このユーザーを削除します。
   - **[編集]** - ユーザーを編集します。
7. 手順 6 での選択内容に応じて、次のいずれかの操作を行います。
   - [変更なし]を選択した場合、それ以上の処置は必要ありません。
   - [削除]を選択した場合は、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。
   - [編集]を選択した場合は、ログイン名、パスワード、またはユーザーのアクセス権を更新します。
8. 必要な数のユーザーアカウントを更新し、F10 キーを押します。
9. メインメニューが表示されるまで、Esc キーを押します。
10. メインメニューで [終了して起動を再開]を選択し、Enter キーを押します。
11. 要求の確認を求めるメッセージが表示されたら、Enter キーを押してユーティリティを終了し、起動プロセスを再開します。

iLO Web インターフェイスを使用した 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

1. **https://<iLO ホスト名または IP アドレス>**を入力します。
   iLO Web インターフェイスのアクセスには HTTPS(TLS 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。

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 名が事前に設定されています。デフォルトのユーザー情報は、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。これらの記載内容を使用し、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。

デフォルトの値は次のとおりです。

- **ユーザー名** - Administrator
- **DNS 名** – iLOXXXXXXXXXXXX(**X** は、サーバーのシリアル番号)

重要

ネットワークを介して制御できる機器において、制御用パスワードを初期値のまま使用し続けると、悪意のある第三者による不正アクセスを許すリスクが高まります。不正アクセスにより機器が乗っ取られた場合、情報漏えいのみならず、可用性や完全性を阻害してシステムに被害を生じさせたり、ボットネットによるサイバー攻撃の足場に悪用されたりする可能性があります。

当製品の初期パスワードは、あくまでも保守運用における初期設定のために設けられています。**初期設定時に必ずパスワード変更を行ってください。**初期パスワードのまま運用して不正アクセスの被害を受けたとしても、**当社は一切の責任を負いません。**

なお、パスワード変更を行っても、強度の低いもの(桁数の少ないもの)や容易に考えられるもの(“123456789”, “abcdefg”, “password”, “Administrator” など)では不正アクセスの防止が困難です。**強度の高いパスワード(8 文字以上で大文字/小文字/数字混在のものを推奨)**に変更頂きますようお願い致します。

iLO 工場出荷時デフォルト設定へのリセットを行った場合は、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ログインします。

3. iLO Web インターフェイスの使用

サポートされるブラウザー

iLO7 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 モバイル版およびデスクトップ版
- Mozilla Firefox
- Microsoft Edge

Chrome、Firefox、Edge が iLO7 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

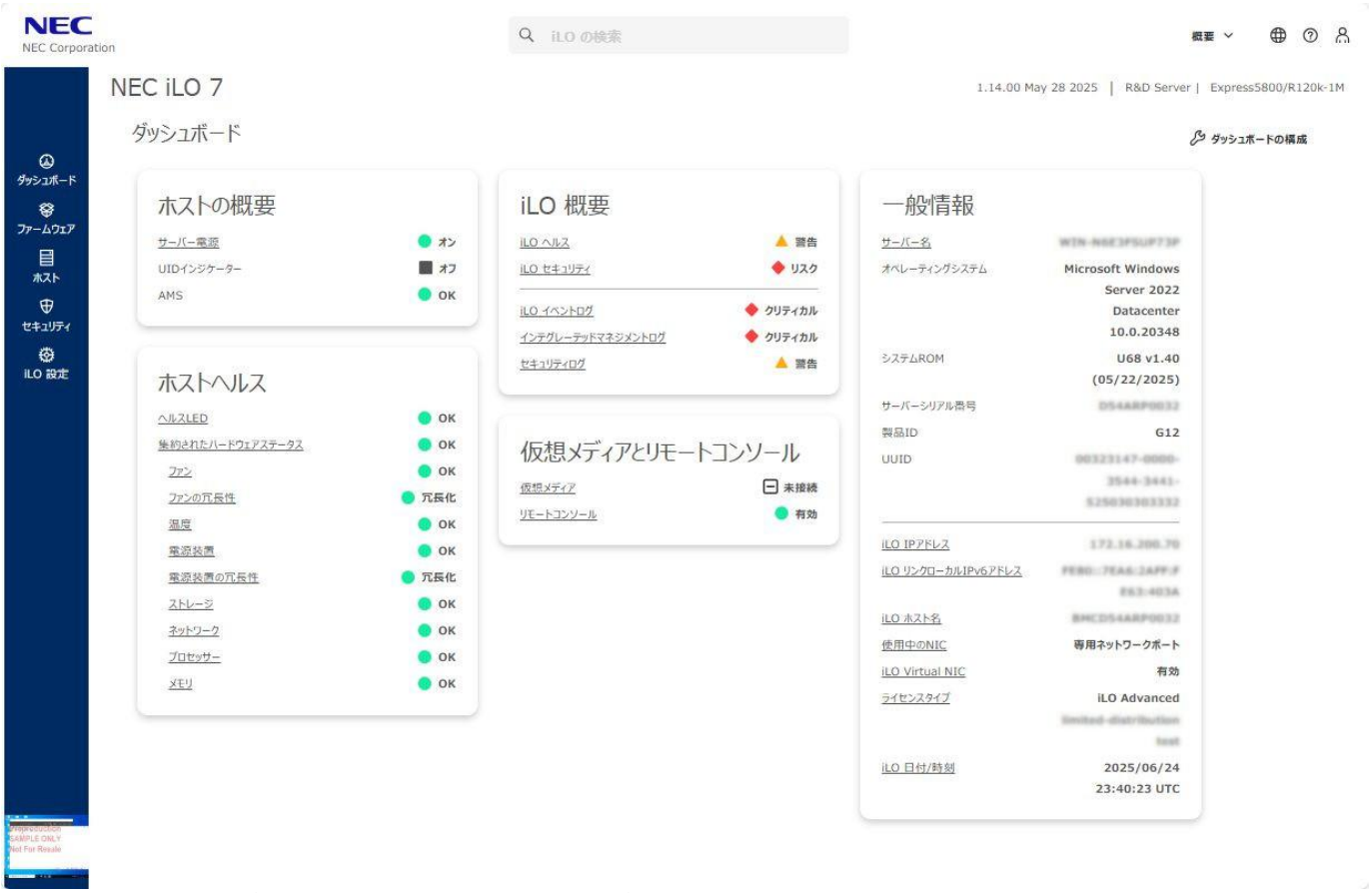
1. **https://<iLO** ホスト名または **IP** アドレス**>** を入力します。

   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 TLS 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、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ユーザーアカウントの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。
   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 インターフェイスの概要

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。iLO 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てから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 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。デフォルトのホスト名は<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”に関する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 コンソール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言語の変更

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。

前提条件

言語パックがインストールされていること。

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。

4. iLO 情報およびログの表示

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。

- **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。

- **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。

  IPv6 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 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ページに移動するには、[iLO ホスト名]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

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。

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。

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。
  - **リスクあり** - 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。
  - **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。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

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、関連する iLO Web インターフェイスのページに移動してください。

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。

  △注意
  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。
  本機能は装置構成によってはサポートされません。

  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。
  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 TLS 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。
  信頼済みの証明書を TLS 証明書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。
  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。
  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、
  「iLO ライセンスオプション」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。
  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。
この機能を有効にすることをお勧めします。

- **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。
  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**

  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[リスクあり]に変わります。
  iLO は、[グローバルコンポーネントの完全性]が有効の場合、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が、無効の場合には 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。

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

ホストの設定の表示

- **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。
  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。

- **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。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。

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]をクリックしてから[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てから 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。

> **注記**
> LDAP サーバーのタイムアウト設定を 45 秒以上に設定することを推奨します。これにより、LDAP セッションがアクティブに保たれ、ネットワークのタイムアウトを回避できます。デフォルトの LDAP サーバーのタイムアウト設定は 9000 秒です。

セッションリスト詳細

iLO は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)テーブルで以下の詳細を表示します。

- **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は、User：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は、Service User：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、iLO 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、仮想 NIC 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。

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]をクリックしてから[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、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、[フィルター]ウィンドウを閉じます。

イベントログの詳細

イベントログを表示すると、記録されたイベントの合計数がフィルターログアイコンの下に表示されます。
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]をクリックしてから[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]をクリックしてから[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。

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]をクリックしてから[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]をクリックしてから[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、[フィルター]ウィンドウを閉じます。

IML の詳細

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

- **修復済みマーク用チェックボックス** - iLO 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。iLO 工場出荷時デフォルト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

IMLにメンテナンスノートを追加する

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

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]をクリックしてから[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]をクリックしてから[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、✚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]をクリックしてから[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]をクリックしてから[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]をクリックしてから[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]をクリックしてから[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]をクリックしてから[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]をクリックしてから[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]をクリックしてから[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]をクリックしてから[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]をクリックしてから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

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。

前提条件
iLO の設定を構成する権限

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]をクリックしてから[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]をクリックしてから[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。

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]をクリックしてから[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]をクリックしてから[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、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、[フィルター]ウィンドウを閉じます。

セキュリティログの詳細

セキュリティログを表示すると、記録されたイベントの合計数がフィルターログアイコンの下に表示されます。 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。iLO 工場出荷時デフォルト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]をクリックしてから[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]をクリックしてから[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]をクリックしてから[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]をクリックしてから[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

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 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** - iLO RESTful API および RESTful インターフェイスツールを使用して、ログをダウンロードします。

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]をクリックしてから[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、プライバシーに関する声明に準拠して取り扱われます。
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。

Active Health System ログ全体のダウンロード

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、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]をクリックしてから[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、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。

Active Health System ログの消去

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。

前提条件

- iLO の設定を構成する権限
- Active Health System ログページで、AHS ロギングが無効化されていない。

手順

1. 左側のナビゲーションペインで[iLO 設定]をクリックしてから[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、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、データー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

手順

1. 左側のナビゲーションペインで[iLO 設定]をクリックしてから[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、ウィンドウを閉じます。

5. iLO とシステム診断の使用

iLO セルフテスト結果の表示

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]をクリックしてから[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。

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 のリセット(再起動)

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。

iLO のリセット方法

- **iLO Web インターフェイス**

  iLO のリセットオプションを使用します。
- **iLO ROM ベースセットアップユーティリティ(BMC 構成ユーティリティ)**

  UEFI システムユーティリティの BMC 構成ユーティリティを使用します。
- **iLO RESTful API**

  詳しくは、iLO7 スクリプティング/コマンドラインガイドを参照してください。
- **IPMI**

  詳しくは、iLO7 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。

iLO 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

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。

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]をクリックしてから[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 工場出荷時デフォルト設定へのリセットが行われたなど) 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、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。

BMC 構成ユーティリティを使用したリセット

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、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、BMC 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。
   BMC 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 BMC 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、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 iLO のリセットの実行

サポートされているサーバーの UID ボタンを使用して、iLO のリセット(ソフトリセット)ができます。
iLO リセットを開始すると、iLO ファームウェアが iLO のリブートを開始します。
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 をリセットできません。

手順
正常な iLO リセットを開始するには、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 リセッ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 iLO のハードリセットの実行

サポートされているサーバーの UID ボタンを使用して、iLO のハードリセットを開始できます。
iLO のハードリセットを開始すると、ハードウェアによって iLO のリセットが開始されます。

手順
iLO のハードリセットを開始するには、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。

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。

システムデフォルト設定のリストア

システムデフォルト設定のリストア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。

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。

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。
2. 左側のナビゲーションペインで[iLO 設定]をクリックしてから[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] > [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。
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。

システムインテリジェント診断モードで起動

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を開始すると、POST 中のブート障害が自動的に診断されます。

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。

手順
1. 左側のナビゲーションペインで[iLO 設定]をクリックしてから[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。
   [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。
2. [はい、続行します]をクリックします。
   システムインテリジェント診断モードで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。

工場デフォルト設定のリストア

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。

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。

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]をクリックしてから[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

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。

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。

手順
1. 左側のナビゲーションペインで[iLO 設定]をクリックしてから[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

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。

前提条件
仮想電源およびリセット権限

手順
1. 左側のナビゲーションペインで[iLO 設定]をクリックしてから[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。

> **△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

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。

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。

手順
1. 左側のナビゲーションペインで[iLO 設定]をクリックしてから[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。

AUX 電源再投入

AUX 電源再投入オプションを使用すると、補助電源をリモートでオフにしてからオンに戻すことができます。このアクションにより、スタンバイ電源で電源が供給されているコンポーネントも含め、すべてのハードウェアコンポーネントがリセットされます。

前提条件

- 仮想電源およびリセット権限
- サーバーの電源がオフになっている

手順

1. 左側のナビゲーションペインで[iLO 設定]をクリックしてから[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] > [AUX 電源再投入]をクリックします。
3. [はい、続行します]をクリックします。
   iLO がリセットされます。

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

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。バインドは、DC-SCM モジュールがないサーバープラットフォームには適用されません。また、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のボードを対象としています。

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。

手順

1. 左側のナビゲーションペインで[iLO 設定]をクリックしてから[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、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、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保守員にお問い合わせください。

6. 全般的なシステム情報の表示

プロセッサーと GPU の情報の表示

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]をクリックしてから[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。

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

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]をクリックしてから[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。

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。
  - **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)**

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、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。

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]をクリックしてから[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

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(エンベッデッド NIC、OCP NIC、PCIe NIC)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(エンベッデッド NIC、OCP NIC、PCIe NIC)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(エンベッデッド NIC、OCP NIC、PCIe NIC)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(エンベッデッド NIC、OCP NIC、PCIe NIC)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(エンベッデッド NIC、OCP NIC、PCIe NIC)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

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 vMainDeviceDiscovery Complete 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]をクリックしてから[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。

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(プロダクト情報エリアフォーマットの製品名値)。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(プロダクト情報エリアフォーマットの製品バージョン値)。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(プロダクト情報エリアフォーマットの製品名/モデル番号値)。

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。
- ダウンストリーム UBM は、デバイスインベントリページに SKU 番号、部品番号、シリアル番号を表示しません。

- **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(プロダクト情報エリアフォーマットのボード部品番号値)。
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(プロダクト情報エリアフォーマットの製品シリアル番号値)。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

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

> ⚠ **警告**
> - 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、ワークロードアドバイザーの各ページは使用できません。

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]をクリックしてから[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、[検出設定]を閉じます。

MCTP 工場出荷時リセットの開始

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。

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]をクリックしてから[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。
5. 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。
6. [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

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 vMainDeviceDiscovery Complete 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]をクリックしてから[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]をクリックしてから[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。

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 EDSFF 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

- iLO ポート/M.2 SSD/RS-232C コネクタ増設キット
- NVMe ドライブ
- RAID コントローラ(MR, 8GB, RAID 0/1/5/6, PCI)
- RAID コントローラ(MR, 8GB, RAID 0/1/5/6, OCP)
- RAID コントローラ(MR, 4GB, RAID 0/1/5/6, OCP)
- RAID コントローラ(MR, RAID 0/1, PCI)
- RAID コントローラ(MR, RAID 0/1, OCP)
- Intel VROC 9.0
- OS Boot 用デバイス専用スロット

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** - 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** - 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。
- **ファームウェアバージョン** - ファームウェアバージョン
- **暗号化モード** - 暗号化モード
- **エンクロージャー** - エンクロージャー
- **ボリューム** - ボリューム

- **ドライブ** - ドライブ

[コントローラー名]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。

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** - 論理ボリューム名
- **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。
- **ヘルス** - 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** - 論理ボリュームの容量
- **RAID のタイプ** - RAID の種別
- **ドライブ** - 論理ボリュームを構成するドライブ数
- **暗号化** - 暗号化有無

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。

ボリュームの作成

手順

1. 左側のナビゲーションペインで[ホスト]をクリックしてから[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. [ボリューム]をクリックします
   ボリュームページが表示されます。
4. [ボリュームの作成]をクリックします。
   ボリュームの作成ウィンドウが開きます。
5. 以下の情報を指定します。
   - **ストレージコントローラ**
   - **RAID のタイプ**
   - **ドライブ**
   - **表示名**
   - **容量**
   - **ストリップサイズタイプ**
   - **リードキャッシュポリシー**
   - **ライトキャッシュポリシー**
6. ボリュームの作成を行うには[作成]をクリックします。
7. 操作のキャンセルを行うには[キャンセル]をクリックします。
8. ウインドウを閉じるには✕をクリックします。

ボリュームの削除

手順

1. 左側のナビゲーションペインで[ホスト]をクリックしてから[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. [ボリューム]をクリックします
   ボリュームページが表示されます。
4. 削除したいボリュームを選択します。
   選択したボリュームページが表示されます。
5. [ボリュームの削除]をクリックします。
   確認ウィンドウが表示されます。
6. ボリュームの削除を行うには[削除]をクリックします。
7. 操作のキャンセルを行うには[キャンセル]をクリックします。

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** - エンクロージャーの名前。
- **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** - エンクロージャーの種別。
- **スイッチ** - 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** - ドライブの名前
- **状態** - 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** - 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(バイト)** - 容量
- **永続的な名前** - 永続的な名前
- **永続的な名前の形式** - 永続的な名前の形式
- **EUI** - ユニークな識別番号
- **モデル** - モデル
- **プロトコル** - プロトコル
- **シリアル番号** - シリアル番号
- **メディアタイプ** - メディア種別
- **予測されるメディアの残りの寿命(%)** - メディア寿命
- **ロケーションタイプ** - ロケーション種別
- **位置** - ドライブのポート、ボックス、およびベイ番号。

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** - マルチパス
- **偽** - 異常状態の有無
- **ドライブの形状** - ドライブの形状
- **ファームウェアバージョン** - ファームウェアバージョン
- **障害予告** - 障害予告
- **ステータスインジケーター** - ステータスインジケーター
- **ホットスペアタイプ** - ホットスペアタイプ
- **暗号化機能** - 暗号化機能
- **暗号化ステータス** - 暗号化ステータス
- **書き込みキャッシュ有効** - 書き込みキャッシュ有効
- **対応速度(Gbs)** - 対応速度(Gbs)
- **ネゴシエート済み速度(Gbs)** - ネゴシエート済み速度(Gbs)
- **スロット対応プロトコル** - スロット対応プロトコル

ドライブの電源の管理

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。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。

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]をクリックしてから[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。

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。

7. 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

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。

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。

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、RESTful インターフェイスツール(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 login <iLO7 IP アドレス> -u <iLO7 ユーザー名> -p <iLO7 パスワード>
   ilorest flashfwpkg <ファイル名.fwpkg>
   ilorest logout
   ```

   ※ローカルホスト OS から実行する場合、<iLO7 IP アドレス>は指定不要です。
3. 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。
  - 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。

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]をクリックしてから[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。

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

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。

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。

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]をクリックしてから[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、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。
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、[ファームウェアのアップデート]ウィンドウを閉じます。

ファームウェアアップデートを有効にするための要件

アップデートを有効にするには、ファームウェアタイプに応じて、追加のアクションが必要になる場合があります。

- **iLO のファームウェアまたは言語パック** - これらの種類のファームウェアは、自動起動される iLO リセットの後に有効になります。
- **システム ROM (BIOS)** - サーバーの再起動が必要です。
- **システムプログラマブルロジックデバイス (CPLD)** - サーバーの再起動が必要です。

> **注記**
> CPLD ファームウェアアップデート後のサーバーの再起動は、サーバーの AC 電源サイクルに変換されます。AC 電源サイクルの一環として、iLO はリセットされます。

- **Power Management Controller および NVMe バックプレーンファームウェア** - サーバーの再起動やシステムのリセットは必要ありません。
  NVMe ファームウェアバージョンは、次のサーバー再起動後に iLO Web インターフェイスに表示されます。

サ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。

> **注記**
> FIPS および CNSA のセキュリティモードでは、サードパーティの PLDM パッケージのインストールはサポートされません。

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)

> **注記**
> iLO リセット後、iLO と BIOS のヘルス情報が表示されます。他のサポートされているコンポーネントのヘルス情報は次のスキャン後に表示されます。。

ファームウェア検証スキャンの実行中は、ファームウェアアップデートをインストールしたり、iLO レポジトリにファームウェアをアップロードしたりすることはできません。
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。

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、「iLO ライセンスオプション」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[ファームウェア]をクリックしてから[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、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、[スキャン設定]ウィンドウを閉じます。

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に[ダウングレードには、'リカバリセット'の権限が必要です]が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。

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、「iLO ライセンスオプション」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[ファームウェア]をクリックしてから[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。

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、「iLO ライセンスオプション」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]をクリックしてから[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。

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。

隔離されたファームウェアのダウンロード

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。

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、「iLO ライセンスオプション」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[ファームウェア]をクリックしてから[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。
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、「iLO ライセンスオプション」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[ファームウェア]をクリックしてから[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

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と、システムリカバリセットのインストールが含まれます。

> **△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。

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、「iLO ライセンスオプション」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がサーバーを管理するように構成されている。

手順

1. 左側のナビゲーションペインで[ファームウェア]をクリックしてから[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、「iLO ライセンスオプション」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[ファームウェア]をクリックしてから[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]をクリックしてから[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。

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 Starter Pack を使用して追加されたソフトウェアおよび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。

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。

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]をクリックしてから[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。

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

手順

1. 左側のナビゲーションペインで[ファームウェア]をクリックしてから[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在時刻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、[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]をクリックしてから[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てから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、[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
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]をクリックしてから[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てから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、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 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

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]をクリックしてから[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。

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

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。

前提条件
iLO 設定の構成権限

手順

1. 左側のナビゲーションペインで[ファームウェア]をクリックしてから[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てから[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]のリンクをクリックし、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。

時間枠のスケジュール設定

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。

前提条件
iLO の設定を構成する権限

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

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。

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。

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。
   [iLO レポジトリにアップロード]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)ファイルをドラッグ&ドロップするか、[browse]をクリックし、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)ファイルをドラッグ&ドロップするか、[browse]をクリックし、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、[iLO レポジトリにアップロード]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。

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

手順

1. 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すると、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。
   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。

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てから[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 Starter Pack 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。

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]をクリックしてから[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、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。
- 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

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。

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。

手順

1. 左側のナビゲーションペインで[ファームウェア]をクリックしてから[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. インストールするインストールセットの横にある省略記号アイコンをクリックしてから[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設定]の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]のリンクをクリックし、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のインストールを行う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、[コンポーネントのインストール]ウィンドウを閉じます。

時間枠のスケジュール設定

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。

前提条件
iLO の設定を構成する権限

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]をクリックしてから[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。

インストールキューの表示

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]をクリックしてから[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。

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、値は前の時間枠のスケジュール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、iL0 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。時間枠のスケジュール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時間枠のスケジュール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]をクリックしてから[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メニューから ✚ [インストールキューに追加]をクリックします。
   [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 BMC と UEFI のタスクを作成します。
   UpdatableBy フィールドに指定されたデバイスがない場合は、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、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 の情報を保存する時間枠のスケジュール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。

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
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]をクリックしてから[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、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]をクリックしてから[インストールキュー]をクリックします。
2. 削除したいタスクの横にある[削除]をクリックします。
   すべてのタスクを削除する場合は、[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。

リモートコンソール

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。

iLO Web インターフェイスから、以下のリモートコンソールにアクセスできます。
- **HTML5 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。

サーバーで、OS の起動後に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。

リモートコンソールの使用に関する留意事項
- 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、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。

> **注記**
> iLO 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。

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]をクリックしてから[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、[概要]ウィンドウを閉じます。

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、「iLO ライセンスオプション」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]をクリックしてから[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。
   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

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。

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]をクリックしてから[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、[セキュリティ]ウィンドウを閉じます。

コンソールの録画

コンソールの録画を使用すると、起動、および検出されたオペレーティングシステムの不具合のようなイベントのビデオストリームを記録し、再生することができます。
録画タイプには、[サーバースタートアップ]と[サーバー事前障害](障害発生時の障害アクションを行う前の事前処理)があり、iLO によって自動的に取得されます。コンソールビデオの録画を手動で開始および停止することもできます。
コンソールの録画を使用する場合、以下の点に注意してください。

- コンソールの録画は HTML5 コンソールのみで使用できます。CLI や iLO RESTful API からはアクセスできません。
- サーバースタートアップとサーバー事前障害シーケンスは、ファームウェアのアップデート中またはリモートコンソールの使用中には録画されません。

- サーバースタートアップとサーバー事前障害シーケンスは、自動的に iLO メモリに保存されます。ファームウェアのアップデート、iLO のリセット、および電源の消失時には失われます。.HTML5 コンソールを使用すると、取得したビデオをローカルドライブに保存できます。
- サーバー起動ファイルは、サーバーの起動が検出されたときに取得を開始し、容量が一杯になったときに停止します。このファイルは、サーバーが起動するたびに上書きされます。
- サーバー事前障害シーケンスの録画は、サーバー起動ファイルの録画完了後に開始されます。障害検知時までのデータが、ラウンドロビンで上書き保存されます。障害検出時点で自動録画は停止します。サーバー事前障害シーケンスにより、録画が再生された時点で録画データは更新されます。それまでは更新されません。
- 次のコントロールを利用できます。
  - [**画面のキャプチャ**] - 画面のキャプチャを採取します。
  - [**画面の録画**] - 画面の録画を開始します。
  - [**再生**] - 現在選択されているファイルが再生されていない場合や一時停止されている場合は、再生を開始します。
  - [**全画面表示**] - ウィンドウを最大化します。
  - [**録画の停止**] - 録画を停止します。

サーバースタートアップとサーバー事前障害シーケンスの表示

前提条件

iLO Advanced ライセンスがインストールされている。

手順

1. HTML5 コンソールを起動します。
2. [再生]ボタンをクリックします。

   再生ソースダイアログボックスが表示されます。

3. [サーバースタートアップ]または[サーバー事前障害]を選択します。
4. [再生]をクリックします。

ビデオファイルの手動録画

前提条件
iLO Advanced ライセンスがインストールされている。

手順
コンソールの録画を使用すると、サーバー起動およびサーバー事前障害以外のシーケンスのビデオファイルを手動で取得できます。

1. HTML5 コンソールを起動します。
2. [画面の録画]ボタンをクリックします。
3. [録画の停止]ボタンを押して録画を停止します。
4. Save Recording ダイアログボックスが開きます。
5. ファイル名、保存場所を入力し、[保存]をクリックします。

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、iLO 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。

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]をクリックしてから[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」では、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、[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。

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]をクリックしてから[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、[ホットキーをリセット]ウィンドウを閉じます。

HTML5 コンソールの起動

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。

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、「iLO ライセンスオプション」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。

手順
1. 左側のナビゲーションペインで[ホスト]をクリックしてから[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。

BIOS

BIOS の詳細の表示

BIOS 機能を使用すると、ユーザーは iLO Web インターフェイスを通じてすべての BIOS 設定を表示および構成できます。

前提条件
ホスト BIOS 構成権限

手順

1. 左側のナビゲーションペインで[ホスト]をクリックしてから[BIOS]をクリックします。
   BIOS ページが表示されます。
   サーバー構成に応じて、BIOS ページに属性が表示されます。iLO Web インターフェイスは、Redfish でサポートされているすべての属性をサポートします。
2. (オプション) 属性を検索するための[属性を検索]フィールドにキーワードを入力します。
3. (オプション) ▸(属性の横にある)をクリックすると、サブコンポーネントと現在の設定を確認できます。
4. BIOS 構成設定から発生した既存のエラーを表示するには、詳細の表示をクリックします。
   エラーの詳細は、ホストの再起動後にのみ表示されます。
5. (オプション) [アクション] > [すべてを展開]をクリックすると、すべてのサブコンポーネントが展開されます。
6. (オプション) [アクション] > [すべてを閉じる]をクリックすると、すべてのサブコンポーネントが折りたたまれます。
7. (オプション) [アクション] > [サーバー再起動]をクリックすると、サーバーが再起動されます。

BIOS 設定の構成

BIOS セクションを使用して、iLO Web インターフェイスから BIOS 設定を構成します。

前提条件
ホスト BIOS 構成権限

手順

1. 左側のナビゲーションペインで[ホスト]をクリックしてから[BIOS]をクリックします。
   BIOS ページが表示されます。
2. ⌄(属性またはサブコンポーネントの横にある)をクリックし、サブコンポーネントを表示します。
3. [依存関係マップ]をクリックし、依存関係の詳細を表示します。依存関係マップについて詳しくは、「依存関係マップのオプション」を参照してください。
4. 必要な属性またはサブコンポーネントに必要な設定を選択または入力します。
5. [ドラフトを保存]をクリックします。
   変更内容がドラフトとして保存されます。
6. ドラフト設定を確認して構成をアップデートするため、[ドラフトをレビューして適用します]をクリックします。ドラフトの確認と適用について詳しくは、「ドラフトを確認して適用のオプション」を参照してください。
   [ドラフトをレビューして適用します]ウィンドウが表示されます。
7. ドラフト設定を確認し、適用オプションの選択から次のいずれかのオプションを選択します。
   - [今すぐ適用して再起動します]
   - [次回の再起動時に適用します]
8. 免責事項を選択します。
9. 設定をアップデートするには、はい、続行しますをクリックします。
10. ドラフト設定を破棄するには、ドラフトを破棄をクリックします。
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。

依存関係マップのオプション

依存関係マップには次の詳細が表示されます。

- [以下に依存]テーブルは、現在の属性の状態が他の関連する属性の値にどのように依存しているかを示します。

- [影響する]テーブルは、現在の属性の値を変更すると、他の関連する属性の値にどのような影響または変更が発生するかを示します。

[以下に依存]テーブルの場合：

- **属性** - 依存名を示します。
- **条件** - 依存属性に関連する条件を示します。可能な値は、[等しい]、[以上]、[より大きい]、[以下]、[より小さい]、[等しくない]です。
- **値** - 依存属性の現在の値を示します。
- **現在の属性状態** - 現在の属性の状態を示します。可能な値は、[読み取り専用 True](リードオンリー属性)、[構成不可]です。

[影響する]テーブルの場合：

- **条件** - 現在の属性の条件を示します
- **現在の値** - 現在の属性の値を示します。可能な値は、[等しい]、[以上]、[より大きい]、[以下]、[より小さい]、[等しくない]です。
- **影響を受ける属性** - 影響を受ける属性の名前を示します。
- **結果の値** - 現在の属性のアップデート後に影響を受ける属性のアップデートされた値を示します。

ドラフトを確認して適用のオプション

ドラフトを確認して適用セクションには、次の詳細が表示されます。

- **属性** - 属性名を示します。
- **現在の値** - 属性の既存の値を示します。
- **保留中の値** - 再起動前の属性のアップデートされた値を示します。
- **新しい値** - iLO Web インターフェイスに保存されたドラフト値を示します(再起動後にアップデートされます)。
- **リスクの適用** - 構成を適用する際のリスクを示します。

適用オプションの選択では、次のいずれかのアップデートおよびリブートオプションを選択できます。

- **今すぐ適用して再起動します** - ドラフト設定をアップデートしてすぐに再起動するには、このオプションを選択します。
- **次回の再起動時に適用します** - 次回の再起動時にドラフト設定をアップデートするには、このオプションを選択します。

8. 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、iLO Web インターフェイス、SSH、または iLO RESTful 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、iLO7 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。

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。
- Microsoft Windows Server 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 配下の 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、TLS 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、iLO7 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を使用してください。該当パッチは KB5039236 または 2024-6B で入手できます。
- Red Hat Enterprise Linux 9.x Server
- VMware ESXi 8.0 U3
- 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]をクリックしてから[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が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** - Red Hat Enterprise Linux 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。

d. 次の ping または curl コマンドを実行して、iLO がホスト OS からアクセス可能かどうか確認してください。

Ping command

```
C:\Users\Administrator> ping 16.1.15.1
Pinging 16.1.15.1 with 32 bytes of data:
Reply from 16.1.15.1: bytes=32 time<1ms TTL=64
Reply from 16.1.15.1: bytes=32 time<1ms TTL=64
Reply from 16.1.15.1: bytes=32 time<1ms TTL=64
Reply from 16.1.15.1: bytes=32 time<1ms TTL=64

Ping statistics for 16.1.15.1:
        Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Curl command

```
C:\Users\Administrator> curl -k https://16.1.15.1/redfish
{"v1": "/redfish/v1/"}
C:\Users\Administrator>
```

仮想 NIC の IP アドレスの構成 - Red Hat Enterprise Linux コマンド

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。

Windows でのドライバー状態の表示

NCM ドライバーは、Microsoft Windows Server 2025 ではデフォルトで使用できます。Microsoft Windows Server 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てから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。

仮想 NIC の IP の構成 - VMware

手順

1. 仮想 NIC の標準 switch を作成します。

   ```
   [root@localhost:~] localcli network vswitch standard add --vswitch-name <switch name>
   ```

2. 1 で作成した switch の Uplink として仮想 NIC 名を追加します。
   “localcli network nic list”の出力から仮想 NIC 名を取得します。

   ```
   [root@localhost:~] localcli network vswitch standard uplink add --uplink-name <vnic name> --vswitch-name <switch name>
   ```

3. 仮想 NIC switch のポートグループを作成します。

   ```
   [root@localhost:~] localcli network vswitch standard portgroup add --portgroup-name "<portgroup name>" --vswitch-name <switch name>
   ```

4. 仮想 NIC の vmknic を作成します。

"localcli network nic list"の出力から vNIC MAC アドレスを取得します。

```
[root@localhost:~] localcli network ip interface add -M "<vnic MAC address>" -p <portgroup name>
```

5. vmknic の IP アドレスを設定します。
   "localcli network ip interface list"の出力から、vmknic 名を取得します。

```
[root@localhost:~] localcli network ip interface ipv4 set -i <vmknic name> -t dhcp
[root@localhost:~] localcli network ip interface ipv6 set -d true -e true -r false -i <vmknic name>
```

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。

9. iLO 仮想メディアの使用

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** - 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** - 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。

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、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、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、ネットワーク上の標準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 8TB 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、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、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 コンソールの場合：iLO 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。
- 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
iLO 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、iLO 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。

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

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。

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) 直ちに接続したイメージから起動するには、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、ウィンドウを閉じます。

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]をクリックしてから[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。
4. 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]をクリックしてから[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、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

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、[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

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。

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]をクリックしてから[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、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、IIS のドキュメントを参照してください。

IIS の設定

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

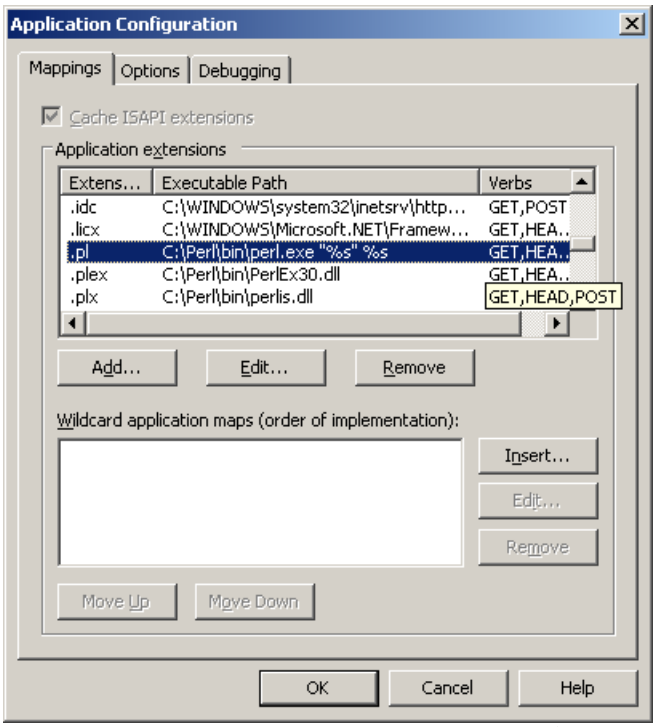
1. ディレクトリを Web サイトに追加し、イメージをディレクトリに置きます。
2. IIS が使用している MIME タイプにアクセスできることを確認します。
   たとえば、フロッピーイメージファイルが拡張子 .img を使用している場合は、その拡張子に対して MIME タイプを追加する必要があります。IIS Manager を使用して、自分の Web サイトのプロパティダイアログボックスにアクセスします。
3. HTTP ヘッダータブで、MIME の種類をクリックし、MIME タイプを追加します。
   次のタイプを追加することをおすすめします。
   - .img application/octet-stream
   - .iso application/octet-stream
4. 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、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、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。

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
#i
f ($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";
```

10. 電力および温度機能の使用

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。

サーバー

iLO7 を搭載したサーバーで 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、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。
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。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。

サーバー電力の管理

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。

前提条件
仮想電源およびリセット権限

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、[確認]ウィンドウを閉じます。

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。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

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。

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]をクリックしてから[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、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、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、ウィンドウを閉じます。

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。
- **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。
- **前回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、電源状態を戻せない可能性があります。詳しくは、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]をクリックしてから[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。
3. 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
   - Smart Storage Energy Pack
   - 電源配電盤概要

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。

サーバー電力使用量の表示

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。

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、「iLO ライセンスオプション」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。

手順

1. 左側のナビゲーションペインで[ホスト]をクリックしてから[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、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。

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。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

- **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。
- **現在のシャーシ電力測定値**(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可能)
  シャーシ全体の電力。
- **パワーレギュレーターモード**
  構成されているパワーレギュレーターモード。
- **入力電圧**
  サーバーに供給される入力電圧。
- **パワーマネジメントコントローラー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。
  - 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。
  - **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。
- **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。

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。

- **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。

- **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。
- **コンポーネントインテグリティー** - 電源ユニットの SPDM 認証ステータス。表示される値は成功、失敗、未サポートです。

注記
CNSA セキュリティモードでは、電源ユニットは SPDM 認証されません。

電源配電盤のオプション

電源配電盤のオプションは、サポートされているサーバーでのみ使用できます。電源配電盤概要セクションには以下の情報が表示されます。

- **名前** - PDB 管理の名前
- **モデル** - PDB 管理のモデル
- **部品番号** - PDB の部品番号
- **シリアル番号** - PDB のシリアル番号
- **プロデューサー** - PDB の製造元
- **ベンダー** - PDB のベンダー

電力読み取り値

- **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。

パワーマネジメントコントローラー

- **ファームウェアバージョン** - パワーマネジメント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ネジメント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。

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。

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。

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。

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、「iLO ライセンスオプション」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[ホスト]をクリックしてから[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、[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。

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

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。

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]をクリックしてから[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。

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。

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、「iLO ライセンスオプション」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。
- 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]をクリックしてから[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、[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。

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。
- 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。

GPU 消費電力上限設定の構成

サポートしている GPU の消費電力上限設定を構成します。すべての GPU に単一の消費電力上限値を適用することも、各 GPU ごとに消費電力上限値を個別に設定することもできます。最小、最大、デフォルト、現在の消費電力上限値が、ワットまたは BTU/時で表示されます。

前提条件

- iLO 設定の構成権限
- iLO Advanced ライセンスがインストールされていること。
- サーバーにパワーキャップ構成をサポートする GPU が搭載されていること。

手順

1. 左側のナビゲーションペインで[ホスト]をクリックしてから[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. [設定]をクリックします。
   [電力設定]ページが表示されます。
   [GPU 消費電力上限の設定]セクションに以下の情報が表示されます：
   - GPU Id
   - 最小制限
   - 最大制限
   - デフォルトの消費電力上限
   - 消費電力上限
3. すべての GPU の消費電力上限を構成するには：
   a. [GPU 消費電力上限設定]テーブルのタイトル行のチェックボックスを選択します。
   b. [アクション]をクリックします。
   c. [消費電力上限の設定]を選択します。
   d. パワーキャップ値を入力します。
      値は以下の範囲内である必要があります：
      - すべての GPU の中で最も大きい最小制限値から最も小さい最大制限値まで
   e. [適用]をクリックします。

（オプション）すべての GPU をリセットするには、アクションメニューから[消費電力上限のリセット]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。

f. [はい、リセットします]をクリックします。
各 GPU の消費電力上限は最大制限に設定されます。

4. 個別 GPU の消費電力上限を構成するには：
   a. 消費電力上限の設定したい GPU id の横のチェックボックスを選択します。
   b. [アクション]をクリックします。
   c. [消費電力上限の設定]を選択します。
   d. 各 GPU の最小値と最大値の範囲内で消費電力上限値を入力します。
   e. [適用]をクリックします。
   f. （オプション）個別の GPU をリセットするには、リセットしたい GPU id の横のチェックボックスを選択します。
   g. アクションメニューから[消費電力上限のリセット]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。
   h. [はい、リセットします]をクリックします。
   GPU の消費電力上限は最大制限値にリセットされます。

GPU 消費電力上限設定

- **GPU ID** - 各 GPU の固有識別子を表示します。
- **最小制限** - GPU に許可されている最小の電力制限値を表示します。
- **最大制限** - GPU に許可されている最大の電力制限値を表示します。
- **デフォルト電力制限** - GPU のデフォルトの電力制限値を表示します。
- **電力制限** - GPU の現在の電力制限値を表示します。

マウスとキーボードの持続接続の設定

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。

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]をクリックしてから[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

手順

1. 左側のナビゲーションペインで[ホスト]をクリックしてから[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、ウィンドウを閉じます。

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。

ファン情報の表示

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]をクリックしてから[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。

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 (%)。

液冷モジュール情報の表示

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]をクリックしてから[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。

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。

液冷モジュールの詳細

それぞれの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)。

液体冷却モジュールの漏れステータスをクリアする

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。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]をクリックしてから[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。

温度グラフの表示

手順

1. 左側のナビゲーションペインで[ホスト]をクリックしてから[ハードウェア] > [温度と冷却]をクリックします。
   温度と冷却ページの温度グラフセクションで、温度グラフが表示されます。
2. （任意）グラフ表示をカスタマイズします。サーバーの前面または背面のセンサーを表示するには、[Front View]または[Back View]を選択します。
3. （任意）個々のセンサーの詳細を表示するには、グラフ上の円にマウスを移動させます。センサーID、ステータス、および温度読み取り値が表示されます。

温度センサーデータの表示

手順

4. 左側のナビゲーションペインで[ホスト]をクリックしてから[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。
5. (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。

6. (オプション) 温度が摂氏単位で表示されているときは、[華氏]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、[摂氏]をクリックすると、温度が摂氏で表示されます。
7. (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。
8. (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

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。

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]をクリックしてから[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、[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]をクリックしてから[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。
- **拡張した冷却** - 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。

4. 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>
```

5. 次のコマンドを入力して、アラートを構成します。

```
rawpost filename.json
```

11. 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。

> **注記**
> CUPS 使用率の集計は、本装置では未サポートです。

パフォーマンスデータの表示

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。

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、「iLO ライセンスオプション」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。

手順

1. 左側のナビゲーションペインで[ホスト]をクリックしてから[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、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

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。

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、「iLO ライセンスオプション」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。

手順

1. 左側のナビゲーションペインで[ホスト]をクリックしてから[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、ウィンドウを閉じます。

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、「iLO ライセンスオプション」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]をクリックしてから[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。
3. 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. (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、「iLO ライセンスオプション」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]をクリックしてから[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、サーバー電源ページに移動できます。

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、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。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。

12. 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]をクリックしてから[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。

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。
- **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 iLO 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 iLO 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。

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]をクリックしてから[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 サブシステム名を使用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、[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。

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。

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。

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]をクリックしてから[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. VLAN を使用するには、[VLAN 有効]オプションを有効にします。
8. [VLAN 有効]オプションを有効にした場合は、VLAN タグを入力します。
   1～4094 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。

iLO 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、iLO 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 VLAN 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 VLAN タグを持つ必要があります。VLAN 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. iLO 共有ネットワークポート - OCP Slot A または iLO 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]をクリックしてから[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. iLO 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. VLAN を使用するには、[VLAN 有効]オプションを有効にします。
9. [VLAN 有効]オプション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、iLO 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 iLO 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。

iLO 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 VLAN 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 VLAN タグを持つ必要があります。VLAN 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。
- iLO **共有ネットワークポート** - 構成に応じて、次の iLO 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 OCP Slot A** - OCP スロット A 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 B 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。

iLO 共有ネットワークポートに関する考慮事項

iLO 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。

- iLO 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。

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 iLO 専用ネットワークポートオプションまたは iLO 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 iLO 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。
- iLO 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 iLO 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、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、iLO 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。
  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 iLO 共有ネットワークポートを通過しません。
- iLO 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。iLO 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

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。

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]をクリックしてから[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、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、[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。

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 の時刻設定を使用**
  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。iLO7 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、iLO7 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]をクリックしてから[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、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、[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。

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 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]をクリックしてから[時刻]をクリックします。
   時刻ページが表示されます。
2. [時刻のソース]で[ネットワーク]を選択します。
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 の時刻設定を使用]か[DHCPv6 の時刻設定を使用]、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。
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、[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。

SNTP オプション

- **DHCPv4 の時刻設定を使用**
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 の時刻設定を使用**
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、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。
  - **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。

LLDP 設定の表示

リンク層発見プロトコル（LLDP）設定ページは、LLDP 送信および受信情報を表示します。
LLDP 設定は、サポートされているプラットフォームでのみ利用可能です。

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]をクリックしてから[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]をクリックします。
   iLO 専用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. リンクレイヤー検出プロトコル(LLDP)をクリックします。
   リンクレイヤー検出プロトコル(LLDP)ページが表示されます。
5. LLDP 設定を見るのに概要セクションの をクリックします。
   概要ウィンドウが表示されます。
6. LLDP を有効にするには、LLDP ステータスのチェックボックスをクリックしてください。
   このオプションはデフォルトで無効になっています。

LLDP ステータスが有効になると、iLO は以下の LLDP 送信情報およびネットワーク隣接情報を表示します。

- シャーシ ID
- シャーシ ID サブタイプ
- IPv4 アドレス
- IPv6 アドレス
- MAC アドレス
- VLAN ID
- ポート ID
- ポート ID サブタイプ
- システム名
- システム説明
- システム機能

△注意

[リンクレイヤー検出プロトコル]を有効にすると、構成によっては”LLDP 情報が見つかりません”のエラーメッセージが表示されたままの状態になります。
この場合、BMC 構成ユーティリティから iLO 工場出荷時デフォルト設定へのリセットを行ってください。

Windows ネットワークフォルダー内の iLO システムの表示

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

1. iLO 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。
2. 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。

13. iLO の管理機能の使用

iLO ユーザーアカウント

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。

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。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特定アプリケーション(SUM、AMS、ILOREST 等)でのみ使用できます。

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]をクリックしてから[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の役割

- **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、iLO 工場出荷時デフォルト設定へのリセットを行ってください。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 BMC 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]をクリックしてから[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、[設定]ウィンドウを閉じます。

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]をクリックしてから[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、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

- 新しい SSH キーの認証
- ユーザーを無効
- ユーザーの削除
- 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]をクリックしてから[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、[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]をクリックしてから[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、[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]をクリックしてから[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、[ユーザーを追加]ウィンドウを閉じます。

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

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。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]をクリックしてから[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、[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]をクリックしてから[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、[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。

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。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]をクリックしてから[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、「iLO ライセンスオプション」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]をクリックしてから[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、[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、「iLO ライセンスオプション」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]をクリックしてから[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、[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、「iLO ライセンスオプション」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]をクリックしてから[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。

手順

1. 左側のナビゲーションペインで[iLO 設定]をクリックしてから[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。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。

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

1. 左側のナビゲーションペインで iLO[iLO 設定]をクリックしてから[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。

iLO ライセンス

iLO(iLO Standard ライセンス)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。

言語パック

言語パックを使用すると、iLO 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、日本語です。
- 英語版はアンインストールできません。
- 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。
- iLO 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、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 iLO 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。

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. Starter Pack の ISO イメージから言語パックの LPK ファイルを抽出します。
   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
2. 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]をクリックしてから
     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てから
     [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]をクリックしてから[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。

3. 使用するブラウザーに応じて、ファイルをドラッグ＆ドロップするか、[browse]をリックします。
4. lang_<言語>_<バージョン>.lpk を選択し、開くをクリックします。
5. (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。
6. [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

手順

1. 左側のナビゲーションペインで[iLO 設定]をクリックしてから[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、言語パックを選択します。

既定の言語を設定

この手順を使用して、デフォルトの言語を構成します。

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。

手順

1. 左側のナビゲーションペインで[iLO 設定]をクリックしてから[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、[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]をクリックしてから[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]をクリックしてから[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

> **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。

手順

1. サポートされる Starter Pack 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、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、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。

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、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。

11. ISO の作成をクリックしてから次に[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。

14. iLO のセキュリティ機能の使用

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。
  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 TLS 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。
  TLS 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役割および権限で、iLO への役割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 BMC 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 TLS 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 TLS 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 iLO 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。
- **TLS 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。
- **NEC 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。
- 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 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 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お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 TLS ポート	636	TCP
iLO 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。

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。

ポリシー設定の構成

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]をクリックしてから[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、[セキュリティ]ウィンドウを閉じます。

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": "iLO7",
    "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 、M anagerType 、 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。

- **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。

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)。

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 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、TPM2.0 の TCG(Trusted Computing Group)の提案に従っています。
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/SystemIAK/Certificates/1”
```

> **注記**
> システム IAK 証明書は、iLO のセキュリティ状態の移行や iLO 工場出荷時デフォルト設定へのリセットを経ても保持されます。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。

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”
```

システム IAK の One-button セキュア消去

iLO LAK、およびシステム LAK は、One-button セキュア消去後に削除されます。iLO IAK、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。
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 LAK、システム IAK、およびシステム LAK は無効になりますが、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。工場出荷時にプロビジョニングされた証明書 (iLO LAK、システム IAK、およびシステム LAK) は、工場外で新しいボード上に移行できません。

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。

iLO アクセス設定の構成

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]をクリックしてから[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(BMC 構成ユーティリティ)
   - iLO 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、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、
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、メッセージを無視します。
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、[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。

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 TLS 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。

- **ログを表示**
  仮想シリアルポートログを表示できるようにします。
  この設定はデフォルトで無効になっています。
- **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、「iLO ライセンスオプション」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、「iLO ライセンスオプション」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。
- **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。

△注意
iLO7 ファームウェアバージョン 1.21 未満では、iLO Web インターフェイスの[iLO 設定] > [アクセス] > [SSH]から[セキュアシェル(SSH)]を無効に変更しないでください。変更すると、HTTP/HTTPS 接続も無効となり iLO Web インターフェイスや RESTful API にアクセスできなくなってしまいます。

- **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 BMC 構成ユーティリティ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。
    iLO7 では、仮想 NIC 設定の工場出荷時のデフォルト値は有効です。
    iLO 工場出荷時デフォルト設定へのリセットを行うと、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

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。

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。

前提条件
iLO の設定を構成する権限

手順

1. ナビゲーションツリーで[セキュリティ]をクリックします。
   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 Web 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。
   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。

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。

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]をクリックしてから[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、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。
   [時刻のソース]を選択します。
3. [時刻のソース]で[ローカル]を選択した場合、以下の手順に従って時刻を設定します。
   a. (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。
   b. 日付を選択します。
   c. iLO 時刻ボックスで時刻を選択します。
   d. 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。
   e. 変更を保存するには、[アップデート]をクリックします。
4. [時刻のソース]で[ネットワーク]を選択した場合、以下の手順に従って時刻を設定します。

   注記
   ネットワークタイムを有効にするには、タイムサーバーを設定するか、DHCP オプションのいずれかを使用してください。

   a. DHCP から提供された NTP サーバーアドレスを使用するには、

- [DHCPv4 の時刻設定を使用]、[DHCPv6 の時刻設定を使用]、またはその両方を有効にしてください。

または

- NTP サーバーアドレスを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のボックスに入力してください。

b. iLO の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てください。
c. [DHCPv6 の時刻設定を使用]のみを選択した場合、またはプライマリーおよびセカンダリーのタイムサーバーを入力した場合は、[タイムゾーン]リストからサーバーのタイムゾーンを選択してください。
d. [NTP 時間をホストに転送]を構成します。
e. 変更を保存するには、[アップデート]をクリックします。

5. 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。
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、[概要]ウィンドウを閉じます。

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。
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 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。

iLO サービスポートを通じて iLO にクライアントを接続する

前提条件
- iLO サービスポートおよび USB 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 アドレスを使用して、iLO に接続します。
3. 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。
4. 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。

Windows 10 でのドライバー選択

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。

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. 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。

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、iLO 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. クライアント NIC の IPv4 設定において、IP アドレスを自動的に取得するように構成します。
   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、comma nd.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** - 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** - 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。
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

iLO 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。

   注記
   - CNSA モードにおける RSA の最小キー長は 3072 ビットです。
   - FIPS およびセキュア標準における最小キー長は 2048 ビットです。
   - すべてのセキュリティモードにおける最大キー長は 4096 ビットです。
   - すべてのセキュリティモードにおける ECDSA のキー長は 384 ビットです。
   - SSH-ed25519 はセキュア標準でのみサポートされています。

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]をクリックしてから[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、ウィンドウを閉じます。

SSH キーの削除

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。

前提条件
ユーザーアカウント管理権限

手順
1. 左ナビゲーションペインで[iLO 設定]をクリックしてから[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

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]をクリックしてから[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\SshH ostKeys) 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
w0l1agB5xY6B3pjP/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]をクリックしてから[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

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、より短いキーを生成してください。
- iLO 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
```

TLS 証明書の管理

TLS 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。TLS 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、TLS 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。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。

TLS 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]をクリックしてから[TLS 証明書]をクリックします。
TLS 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、TLS 証明書を設定することができます。

TLS 証明書の詳細

- **発行先** - 証明書の発行先の名前。
- **発行元** - 証明書を発行した CA。
- **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 TLS 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]をクリックしてから[TLS 証明書]をクリックします。
   TLS 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。
   - **TLS 証明書を自動的に管理** - 自動的に管理できる信頼済みの TLS 証明書をインポートするには、このオプションを使用します。
   - **TLS 証明書および秘密キーのインポート** - 信頼済みの TLS 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 の生成および TLS 証明書のインポート** - iLO にインポートする信頼済みの TLS 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。

TLS 証明書の削除

この機能を使用して、TLS 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。

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]をクリックしてから[TLS 証明書]をクリックします。
   TLS 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 TLS 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。
   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、ウィンドウを閉じます。

自動証明書登録

iLO は、ACME(自動証明書管理環境)プロトコルを使用した TLS 証明書の自動取得と更新をサポートするようになりました。iLO は、ACMEv2 準拠(RFC 8555)の証明機関による証明書の自動登録と更新をサポートします。
ACME サーバーは、http-01 チャレンジによってのみ iLO のドメインを検証できます。http-01 チャレンジのみがサポートされているため、ワイルドカード証明書は取得できません。
デフォルトで、この機能は無効です。この機能の有効化について詳しくは、自動証明書登録の有効化セクションを参照してください。

自動証明書登録の有効化

前提条件

- iLO の設定を構成する権限。
- iLO Advanced ライセンス。
- 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。
- DNS サーバーの構成。
- Web プロキシの構成(iLO サーバーから ACME サーバーへのアクセスにプロキシが必要な場合)。
- ACME チャレンジ検証のために、証明書登録サーバーからポート 80 経由で CSR に構成されている共通名(iLO の FQDN)を使用して iLO にアクセスできる必要があります。
- 証明書登録サーバーの URL。
- 証明書登録サーバーのルート CA 証明書。
- (オプション) ACME 外部アカウントバインディング(EAB)の認証情報。ACME プロトコルでは、iLO が認証機関(CA)の特定のアカウントにアクセスするために使用できる EAB フィールドが定義されます。ACME サーバーが EAB を適用する場合は、ACME サーバーを運用している CA から EAB のキーID とキー値を取得してください。iLO では、ACME サーバーに証明書を要求するときにこれらの認証情報が必要です。
- iLO では、すべてのセキュリティモードで署名に HS384 が使用されるため、ACME サーバー構成でも EAB 要求の署名検証アルゴリズムとして HS384 が使用されていることを確認してください。

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てから[TLS 証明書]をクリックします。
   TLS 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。
   TLS 証明書ページが表示されます。
3. [TLS 証明書を自動的に管理]を選択します。
4. ACME 証明書の登録設定に次の値を入力します。

注記
iLO は最大 10 個の ACME CA 証明書の保存をサポートします。

- **サーバーURL** - ACME 証明書登録サーバーの URL。
- **ACME サーバーアカウント連絡先情報** - (オプション) サーバー管理者のメール ID。
- **EAB ID** - (オプション) アカウントキーを識別する ASCII 文字列。
- **EAB 値** - (オプション) アカウントキーの暗号化と認証に使用される MAC キー。
- **CA 証明書** - 証明書登録サーバーの CA 証明書。CA 証明書は、iLO と証明書登録サーバー間の信頼を確立するために使用されます。

5. 証明書署名リクエストの詳細に次の値を入力します。
   - **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/地域を識別する 2 文字の国/地域番号。2 文字の省略表記を大文字で入力します。
   - **都道府県(ST)** - この iLO サブシステムを所有する会社または組織が存在する都道府県。
   - **市町村(L)** - この iLO サブシステムを所有する会社または組織が存在する市町村。
   - **組織名(O)** - この iLO サブシステムを所有する会社または組織の名前。
   - **組織ユニット(OU)** - (省略可能) この iLO サブシステムを所有する会社または組織の中の単位。
   - **共通名(CN)** - この iLO サブシステムの FQDN。
     FQDN は、共通名(CN)ボックスに自動的に入力されます。
     iLO が CSR に FQDN を入力できるように、ネットワーク共通設定ページでドメイン名を設定します。

   △注意
   iLO 工場出荷時デフォルト設定へのリセットを行うと、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。

   - **更新期間(1 - 30)日** - (オプション)iLO が自動的に更新を試みる日から TLS 証明書の有効期限までの日数を指定します。デフォルト値は 7 日です。有効範囲は有効期限の 1～30 日前です。
   - **サブジェクト代替名** - (オプション)追加のドメイン名(複数のドメイン名はカンマで区切ります)。追加のドメインが指定されていない場合、共通名はデフォルトでサブジェクト代替名フィールドに含まれます。

   注記
   - ACME では、サブジェクト代替名のエントリを含む CSR はホスト名に制限され、FQDN がサポートされます。
   - iLO は、最大 6KB のサイズの CA 証明書(PEM 形式)のインポートをサポートします。
   - iLO は、次のタイプの CA 証明書をサポートします。
     - **キュア標準および FIPS**
       - RSA 公開鍵長：2048 ビット以上
       - ECDSA 曲線：P-256、P-384、P-521
     - **CNSA**
       - RSA 公開鍵長：3072 ビット以上
       - ECDSA 曲線：P-384
   - CSR フィールドは、TLS 証明書の手動インポートと自動インポートの両方に共通です。

6. 自動証明書登録を初めて開始する場合は、構成をクリックし、登録プロセスを開始します。
   自動証明書登録が存在するが無効になっている場合は、[有効]をクリックします。
   証明書登録サービスが有効になるとすぐに、証明書の登録ステータスは[進行中]になります。

登録が成功すると、証明書の登録ステータスは[成功]になります。登録が成功した後、iLO を手動でリセットする必要があります。新しく信頼された証明書は、iLO がリセットされた後でのみ使用されるようになります。
登録が失敗すると、証明書の登録ステータスは[失敗[になります。

注記
登録サービスが有効になっている場合、CSR の手動生成、証明書の削除、および証明書のインポートは許可されません。

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、ウィンドウを閉じます。

自動証明書登録設定の編集

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から[TLS 証明書]をクリックします。
   TLS 証明書ページが表示されます。
2. [TLS 証明書サーバー]セクションの右上隅にある省略記号アイコンをクリックします。
   設定の編集に関する次のオプションを使用します。
   - TLS サーバー構成をアップデートするには、[構成のアップデート]をクリックします。
     構成オプションについて詳しくは、自動証明書登録の有効化セクションを参照してください。
   - ACME サーバーアカウント連絡先情報のみを編集するには、連絡先情報のアップデートをクリックします。
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. キャンセルまたは✕をクリックし、ウィンドウを閉じます。

注記
- 設定をアップデートしても、証明書の登録は開始されません。登録を開始するには、最初にサービスを無効にしてから再度有効にします。
  - 自動証明書登録を無効または有効にするには、[自動証明書登録の無効化]セクションを参照してください。
- ACME を有効にすると、TLS 証明書のタイプが変更された後に iLO が自動的にリセットされます。リセット後、iLO はアップデートされた証明書のタイプで新しい自己署名 TLS 証明書を生成します。iLO は新しい証明書を使用して Web サービスを開始します。
  iLO は、アップデートされた証明書のタイプの TLS 証明書を ACME サーバーに自動的に要求します。iLO が ACME によって発行された証明書をインストールするまで、Web サーバーは自己署名証明書を使用し続けます。登録が完了すると、iLO はセキュリティログに成功を記録し、Redfish アラートを送信します。ユーザーのアクションは不要です。

自動的に管理される TLS 証明書の更新

証明書登録サービスが有効になっていて、証明書の有効期限が切れそうになると、iLO はユーザーが構成した更新期間に従って自動証明書更新を開始します。

例えば、更新期間の値を 20 に構成した場合、iLO は証明書の有効期限の 20 日前に証明書の更新を自動的に開始します。
iLO が証明書の更新を開始するとすぐに、証明書の登録ステータスは進行中になります。
更新が成功すると、証明書の登録ステータスは成功になります。更新ステータスについては、「セキュリティログ」ページを参照してください。更新が成功した後、iLO を手動でリセットする必要があります。新しく信頼された証明書は、iLO がリセットされた後でのみ使用されるようになります。
更新が失敗すると、証明書の登録ステータスは失敗になります。失敗の原因と推奨されるアクションについて詳しくは、「セキュリティログ」ページを参照してください。
更新に失敗した場合、iLO は証明書の更新を成功するまで 1 日 1 回試行します。

強制的な TLS 証明書の更新の開始

次の理由から、強制的な TLS 証明書の更新を開始することもできます。
- 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更新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てから[TLS 証明書]をクリックします。
   TLS 証明書ページが表示されます。
2. Force Renew(証明書情報セクション)をクリックします。
   iLO によって要求を確認するように求められます。
3. [はい、更新します]をクリックします。
4. キャンセルまたは✕をクリックし、ウィンドウを閉じます。

自動証明書登録の無効化

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から[TLS 証明書]をクリックします。
   TLS 証明書ページが表示されます。
2. [TLS 証明書サーバー]セクションの右上隅にある省略記号アイコンをクリックします。
3. 証明書管理登録を無効にするをクリックします。
   iLO によって要求を確認するように求められます。
4. [はい、無効にします]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、ウィンドウを閉じます。

CSR の生成および TLS 証明書のインポート

iLO では、iLO にインポートする信頼済みの TLS 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 20KB 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 3KB(PEM 形式で約 4KB)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。
TLS 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 工場出荷時デフォルト設定へのリセットが行われた場合、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。

前提条件
iLO の設定を構成する権限

手順
1. CA から信頼済みの証明書を取得します。
2. 信頼済みの証明書を iLO にインポートします。

CA からの信頼済み証明書の取得

前提条件
iLO の設定を構成する権限

手順
1. 左側のナビゲーションペインで[セキュリティ]をクリックしてから[TLS 証明書]をクリックします。
   TLS 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。
   TLS 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。
   次の値を入力します。
   - 国(C)
   - 州または県(ST)
   - 都市または地域(L)
   - 組織名(O)
   - 組織ユニット(OU)
   - 共通名(CN)
4. (オプション) iLO IP アドレスを CSR に含めるには、iLO の IP アドレスを含みますチェックボックスを選択します。

   注記
   多くの認証機関(CA)では、この入力を受け入れることができません。使用中の CA でこの入力を受け入れることがわかっていない場合は、このオプションを選択しないでください。

   このオプションが有効な場合、iLO の IP アドレスが CSR サブジェクト代替名(SAN)の拡張子に含まれます。
5. [CSR の生成]をクリックします。
   [TLS 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。
6. 数分後 (最大 10 分)、CSR が TLS 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。
7. をクリックし、CSR テキストをコピーします。
8. ブラウザーウィンドウを開き、第三者認証機関に移動します。
9. 画面の指示に従って、CSR を CA に送信します。
   - 証明書の目的を選択するように求められたら、必ずサーバー証明書のオプションを選択してください。
   - CSR を CA に送信するときに、ご使用の環境でサブジェクト代替名の指定が要求される可能性があります。必要に応じて、iLO DNS 名を入力します。
10. 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。

> **注記**
> 信頼された CA 証明書により発行された iLO TLS 証明書を削除して、安全でない証明書を使用する場合、現在のブラウザのキャッシュまたはクッキーをクリアして iLO ログイン画面に移動してください。インコグニートモード（シークレットモード）を使用している場合は、モードを再度開いて iLO にアクセスしてください。

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 間の通信するための公開鍵と秘密鍵のペアが含まれています。
iLO は、SHA-256 で署名された 2048 ビット以上の RSA 鍵、または SHA-384 で署名された CNSA 準拠鍵を生成します。
生成された CSR は、新しい CSR が生成されるか、iLO 工場出荷時デフォルト設定へのリセットが行われるか、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]をクリックしてから[TLS 証明書]をクリックします。
   TLS 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。
   TLS 証明書のインポートウィンドウが表示されます。
3. TLS 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、[TLS 証明書のインポート]ウィンドウを閉じます。

TLS 証明書および秘密キーのインポート

iLO では、信頼できる TLS 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 20KB 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 TLS 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 モードでは、RSA に許可される最小キー長は 3072 ビットです。
- FIPS およびセキュア標準モードでは、許可される最小キー長は 2048 ビットです。
- すべてのセキュリティモードで許可される最大キー長は 4096 ビットです。
- すべてのセキュリティモードにおける ECDSA のキー長は 384 ビットです。

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]をクリックしてから[TLS 証明書]をクリックします。
   TLS 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[TLS 証明書および秘密キーのインポート]を選択します。
4. TLS 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。

TLS 証明書の再生成

この機能を使用して、TLS 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。

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]をクリックしてから[TLS 証明書]をクリックします。
   TLS 証明書ページが表示されます。
2. [CSR の再生成]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、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、TLS 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。

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]をクリックしてから[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、ファイルをドラッグ＆ドロップするか、[browse]をクリックし、ローカルファイルボックスでファイルを選択します。
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、[Kerberos 設定]ウィンドウを閉じます。

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 Zero 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]をクリックしてから[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. 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。
7. 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。
8. 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。
9. [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]ウィンドウに追加されます。
10. (オプション) [Add User Context]をクリックし、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。
11. 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。
12. [アップデート]をクリックし、設定を保存します。
13. (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。
14. 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
+	+
–	–
<	<
>	>
,	,
;	;
“	“
#	#
/	/
	¥
	(
	)

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。
- **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。
  ディレクトリサーバーを定義する際は、DNS ラウンドロビンを使用することを奨します。
- **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、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 TLS 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。

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 - 検索コンテキストに **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 に**@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に **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] - [認証] - [ディレクトリと LDAP]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 TLS 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]をクリックしてから[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。
- ローカルユーザー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、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]をクリックしてから[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、[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]をクリックしてから[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、[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

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]をクリックしてから[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。
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 TLS 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、[ディレクトリテスト制御]ウィンドウを閉じます。

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、役割、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 の役割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、評価された役割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。

- TLS **を使用しての接続**
  iLO は、ポート 636 経由で TLS 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 TLS 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] – [認証] – [ディレクトリと LDAP]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

サーバーに付属している iLO Standard ライセンスによって、お客様は次の 2 つのセキュリティ状態(セキュア標準、FIPS)のいずれかでサーバーを構成することができます。また、iLO Advanced ライセンスをインストールすることによって、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(CNSA)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。

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 暗号を強制的に使用します。
    - 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
  - スクリプティングツールとコマンドラインツール
  - 管理ツール
  - iLO アラートメール、syslog、LDAP、またはキーマネージャーサーバー
- HTML5 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、CNSA 準拠暗号の AES-256 ビットを強制的に使用します。

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。
- FIPS および CNSA のセキュリティモードは、サードパーティの PLDM パッケージのインストールをサポートしていません。

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

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。iLO7 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 工場出荷時デフォルト設定へのリセットを行います。
2. 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 工場出荷時デフォルト設定へのリセットを行うと、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。

3. サーバーのオペレーティングシステムを再起動します。

4. iLO 工場出荷時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 BMC 構成ユーティリティを使用します。

△注意

iLO 工場出荷時デフォルト設定へのリセットを行うと、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 工場出荷時デフォルト設定へのリセットを行った場合、サーバーのオペレーティングシステムを再起動します。
   iLO 工場出荷時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。

注記

- CNSA モードにおける RSA の最小鍵長は 3072 ビットです。
- FIPS およびセキュア標準における最小鍵長は 2048 ビットです。
- すべてのセキュリティモードにおける最大鍵長は 4096 ビットです。
- すべてのセキュリティモードにおける ECDSA の鍵長は 384 ビットです。

- **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、ecdsa-sha2-nistp384
- **FIPS**
  - aes256-ctr、aes256-gcm@openssh.com
  - diffie-hellman-group-exchange-sha256、ecdh-sha2-nistp384
  - hmac-sha2-256
  - rsa-sha2-512、rsa-sha2-256、ecdsa-sha2-nistp384
- **CNSA**
  - aes256-gcm@openssh.com
  - ecdh-sha2-nistp384
  - hmac-sha2-256

- ecdsa-sha2-nistp384、rsa-sha2-512

TLS 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。TLS 暗号化により、Web ブラウザーの データが保護されます。TLS 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、SSO 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 TLS 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 TLS 接続に適用されます。

- LDAP サーバーへの接続
- SSO 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
  - ECDSA、ECDH、および AEAD MAC(ECDHE-ECDSA-AES256-GCM-SHA384)による 256 ビット AES-GCM
  - ECDSA、ECDH、および AEAD MAC(ECDHE-ECDSA-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。
  - ECDSA、ECDH、および AEAD MAC(ECDHE-ECDSA-AES256-GCM-SHA384)による 256 ビット AES-GCM
  - ECDSA、ECDH、および AEAD MAC(ECDHE-ECDSA-AES128-GCM-SHA256)による 128 ビット AES-GCM
  - ECDSA、ECDH、および SHA384 MAC(ECDHE-ECDSA-AES256-SHA384)による 256 ビット AES-CBC
  - ECDSA、ECDH、および SHA256 MAC(ECDHE-ECDSA-AES128-SHA256)による 128 ビット AES-CBC
  - 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

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

すべてのサーバーに付属している iLO Standard ライセンスによって、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 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

FIPS および CNSA セキュリティ状態を有効にする

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。

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。

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]をクリックしてから[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 工場出荷時デフォルト設定へのリセットが行われます。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 工場出荷時デフォルト設定へのリセットを行うことです。
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]をクリックしてから[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 TLS 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]をクリックしてから[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、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。

NEC SSO

NEC SSO を使用すると、NEC 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、NEC 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。

iLO には、NEC SSO 証明書の最小要件を決定するために NEC SSO アプリケーションのサポートが含まれます。NEC 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、NEC 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。

NEC 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]をクリックしてから[認証]をクリックします。
   認証ページが表示されます。
2. [NEC SSO]をクリックします。
   NEC 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。
   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) NEC 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。
8. 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。
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、[シングルサインオン設定]ウィンドウを閉じます。

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、NEC 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、NEC 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、NEC 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 NEC 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

NEC SSO 準拠アプリケーションにログインする場合、NEC SSO 準拠アプリケーションの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

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。

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]をクリックしてから[認証]をクリックします。認証ページが表示されます。
2. [NEC 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。
4. 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。
5. 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 NEC 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。

信頼済みの証明書とレコードの表示

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]をクリックしてから[認証]をクリックします。認証ページが表示されます。
2. [NEC SSO]をクリックし、信頼済み証明書とレコードを表示します。
3. 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。

- **説明書**
  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]をクリックしてから[認証]をクリックします。
   認証ページが表示されます。
2. [NEC SSO]をクリックします。
   NEC 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、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]をクリックしてから[認証]をクリックします。
   認証ページが表示されます。
2. [NEC SSO]をクリックします。
   NEC 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

ログインセキュリティバナー機能を使用すると、iLO Web インターフェイスの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。

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]をクリックしてから[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。

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]をクリックしてから[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。

15. iLO マネジメント設定の構成

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 Service(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 • 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	該当なし

[1] Linux の場合、AMS ベースの OS ログ記録(Red Hat Enterprise Linux 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] iLO7 搭載サーバーでは 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。

- ドライブ(物理および論理)

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。
- iLO7 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。

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。
   - Windows、Red Hat Enterprise Linux の場合、Starter Pack から AMS を取得します。
   - VMware の場合、Web 公開サイトから AMS を取得します。
2. ソフトウェアをインストールします。

AMS のインストールの確認

AMS ステータスの確認：iLO Web インターフェイス

手順

1. 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：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、コマンドを入力します。

```
systemctl status amsd smad [cpqIde cpqFca cpqScsi cpqiScsi mr_cpqScsi]
```

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 ESXi/ESX 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、

```
/etc/init.d/ams.sh status
```

コマンドを入力します。

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。
- **Red Hat Enterprise Linux** - コマンドとして

```
systemctl restart amsd
systemctl restart smad
```

を入力します。

- **VMware** - 次のコマンドを入力します。
  - ESXi 8.x 以降の場合：

```
systemctl restart esxi-ams.service
```

System Management Assistant

iLO7 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。

System Management Assistant の有効化(Windows)

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。

前提条件
AMS がインストールされています。

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 に移動して、EnableSma.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。

System Management Assistant の有効化(VMware)

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
```

System Management Assistant の有効化(Linux)

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。
   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。
   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。
   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 cpqlde_rev
   - systemctl start cpqScsi_rev
   - systemctl start mr_cpqScsi_rev
   - systemctl start cpqFca_rev

System Management Assistant の無効化(Linux)

手順

次のコマンドを実行します。

- systemctl disable smad_rev
- systemctl disable amsd_rev

SNMPv1 設定の構成

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。

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]をクリックしてから[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、[SNMPv1設定]ウィンドウを閉じます。

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**
> 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]をクリックしてから[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、ウィンドウを閉じます。

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

iLO では、最大 8 人の SNMPv3 ユーザーをサポートしています。

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]をクリックしてから[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、ウィンドウを閉じます。

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

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。

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。

手順

1. 左側のナビゲーションペインで[iLO設定]をクリックしてから[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. 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、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、[アラート送信先の追加]ウィンドウを閉じます。

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

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。

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。

手順

1. 左側のナビゲーションペインで[iLO設定]をクリックしてから[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. 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、[編集]ウィンドウを閉じます。

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]をクリックしてから[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. 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

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。

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]をクリックしてから[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
   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、[SNMPv3設定]ウィンドウを閉じます。

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]をクリックしてから[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、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]をクリックしてから[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]をクリックしてから[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. 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。

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) iLO7 およびサポートされる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。

トラップ ID	イベントクラス	イベントコード	トラップ名と説明	トラップの深刻度
0	該当なし	該当なし	Cold Start Trap SNMP が初期化され、システムで POST が完了した、または AMS が起動しました。	該当なし
4	該当なし	該当なし	Authentication Failure Trap SNMP が認証失敗を検出しました。	該当なし
1006	5h	3h	cpqSeCpuStatusChange 訂正不可能なマシンチェック例外がプロセッサーで検出されました。	メジャー
1010	28h	2h	cpqSeUSBStorageDeviceReadErrorOccurred 接続されている USB ストレージデバイスで読み取りエラーが発生しました。	OK
1011	28h	3h	cpqSeUSBStorageDeviceWriteErrorOccurred 接続されている USB ストレージデバイスで書き込みエラーが発生しました。	OK
1012	28h	4h	cpqSeUSBStorageDeviceRedundancyLost USB ストレージデバイスの冗長性が失われました。	警告
1013	28h	4h	cpqSeUSBStorageDeviceRedundancyRestored USB ストレージデバイスの冗長性が回復しました。	OK
1014	28h	5h	cpqSeUSBStorageDeviceSyncFailed USB ストレージデバイスの冗長性を回復するための同期操作に失敗しました。	警告
1015	33h	5h	cpqSePCIeDiskTemperatureFailed PCIe ディスクの温度が上限クリティカルしきい値を超えました。	クリティカル
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	OK

			PCI デバイスが追加されたか、電源がオンになりました。	
1020	33h	5h	cpqSePciDeviceRemovedOrPoweredOff PCI デバイスが削除されたか、電源がオフになりました。	OK
1021	Ah	3152h	cpqSeNVMeSecureEraseFailed NVMe ドライブのセキュア消去に失敗しました。	クリティカル
1022	32h	3020h 3021h	cpqSePcieTrainingFailed PCI Express スロットは、連結に失敗しました。	クリティカル
1023	Ah	3158h	cpqSePciResetFail システムはスロットの PCI コントローラーでリセットを実行できません。	クリティカル
2014	2h	2Dh	cpqSiIntrusionInstalled システム侵入ハードウェアが取り付けられました。	OK
2015	2h	2Eh	cpqSiIntrusionRemoved システム侵入ハードウェアが取り外されました。	OK
2016	2h	30h	cpqSiHoodReplaced システムフードが交換されました。	OK
2017	Ah	401h	cpqSiHoodRemovedOnPowerOff サーバーの電源オフ時にシステムフードが取り外されました。	メジャー
2018	35h	1h	cpqSiSysTelemetryThresholdAlert システムテレメトリのメトリック値が上限しきい値を超過したか、または下限しきい値より低くなっています。	情報
3033	13h	12h	cpqDa6CntlrStatusChange Smart アレイコントローラーのステータスの変化が検出されました。	クリティカル
3034	13h	21h	cpqDa6LogDrvStatusChange Smart アレイ論理ドライブのステータスの変化が検出されました。	クリティカル
3038	13h	17h	cpqDa6AccelStatusChange Smart アレイキャッシュモジュールのステータスの変化が検出されました。	クリティカル
3039	13h	23h	cpqDa6AccelBadDataTrap Smart アレイキャッシュモジュールのバックアップ電源が失われました。	クリティカル
3040	13h	24h	cpqDa6AccelBatteryFailed Smart アレイキャッシュモジュールのバックアップ電源が故障しました。	クリティカル
3046	13h	14h	cpqDa7PhyDrvStatusChange Smart アレイ物理ドライブのステータスの変化が検出されました。	クリティカル

3047	13h	2Ch	cpqDa7SpareStatusChange Smart アレイスペアドライブのステータスの変化が検出されました。	クリティカル
3049	13h	15h	cpqDaPhyDrvSSDWearStatusChange Smart アレイ物理ドライブの SSD Wear ステータスの変化が検出されました。	クリティカル
3903	Ah	3151h	cpqDaSmartArraySecureEraseFailed Smart アレイのセキュア消去に失敗しました。	クリティカル
5022	13h	1Eh	cpqSasPhyDrvStatusChange AMS が、SAS または SATA 物理ドライブのステータスが変化したことを検出しました。	クリティカル
5026	13h	1Fh	cpqSasPhyDrvSSDWearStatusChange AMS が、SAS または SATA 物理ドライブの SSD Wear ステータスが変化したことを検出しました。	クリティカル
6026	2h	38h	cpqHe3ThermalConfirmation 温度上昇のためにサーバーがシャットダウンされましたが、現在は稼働しています。	OK
6027	Ah	101h	cpqHe3PostError 1 つまたは複数の POST エラーが発生しました。	警告
6032	Bh	36h	cpqHe3FltTolPowerRedundancyLost 指定されたシャーシのフォールトトレラント電源装置の冗長性が失われました。	メジャー
6033	Bh	31h	cpqHe3FltTolPowerSupplyInserted フォールトトレラント電源装置が取り付けられました。	OK
6034	Bh	2Ch	cpqHe3FltTolPowerSupplyRemoved フォールトトレラント電源装置が取り外されました。	メジャー
6035	2h	1Ah	cpqHe3FltTolFanDegraded フォールトトレラントファン状態が、劣化に設定されました。	クリティカル
6036	2h	17h	cpqHe3FltTolFanFailed フォールトトレラントファン状態が、障害に設定されました。	クリティカル
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	クリティカル

			サーバーの温度を超えました。	
6041	2h	14h	cpqHe3TemperatureDegraded 温度ステータスが劣化に設定され、温度が正常な動作範囲にありません。システム構成によっては、このシステムがシャットダウンされる可能性があります。	クリティカル
6042	2h	13h	cpqHe3TemperatureOk 温度ステータスが、OK に設定されました。	OK
6048	Bh	28h	cpqHe4FltTolPowerSupplyOk フォールトトレラント電源装置の状態が OK に設定されました。	OK
6049	Bh	15h	cpqHe4FltTolPowerSupplyDegraded フォールトトレラント電源装置の状態が、劣化に設定されました。	クリティカル
6050	Bh	28h	cpqHe4FltTolPowerSupplyFailed フォールトトレラント電源装置の状態が、障害に設定されました。	クリティカル
6051	該当なし	該当なし	cpqHeResilientMemMirroredMemoryEngaged アドバンストメモリプロテクションサブシステムが、メモリ障害を検出しました。ミラーメモリがアクティブになりました。	メジャー
6054	Bh	36h	cpqHe3FltTolPowerRedundancyRestore フォールトトレラント電源装置が冗長化の状態に回復しました。	OK
6055	2h	23h	cpqHe3FltTolFanRedundancyRestored フォールトトレラントファンが冗長化の状態に回復しました。	OK
6061	該当なし	該当なし	cpqHeManagementProcInReset 管理プロセッサーはリセット中です。	マイナー
6062	該当なし	該当なし	cpqHeManagementProcReady 管理プロセッサーは使用可能です。	情報
6064	該当なし	該当なし	cpqHe5CorrMemReplaceMemModule メモリエラーが訂正されました。メモリモジュールを取り付けます。	メジャー
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 Smart ストレージバッテリが故障しました。	警告
6071	Bh	1Eh	cpqHeSysBatteryRemoved 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	警告

			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。	
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

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
6103	Bh	1Ch	cpqHeNoPowerSupplyDetected	メジャー

			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。	
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
61.16.00	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
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
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 Web インターフェイスを使用すると、このアラートを生成して、SNMP コンソールでアラートが受信されることを確認できます。	情報
11018	23h	CEh	cpqHo2PowerThresholdTrap 電力しきい値を超えました。	メジャー
11020	該当なし	該当なし	cpqHoMibHealthStatusArrayChangeTrap サーバーのヘルスステータスが変化しました。	該当なし
14004	13h	20h	cpqIdeAtaDiskStatusChange AMS が、ATA ディスクドライブのステータスが変化したことを検出しました。	クリティカル
14007	Ah	3150h	cpqIdeAtaSecureEraseFailed	クリティカル

			SATA ドライブのセキュア消去に失敗しました。	
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、MIB ファイルを参照してください。

REST アラート

次の表に、iLO7 およびサポートされる 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 ProcessorStatusFailed	クリティカル
1010	USBStorageDeviceReadError	OK
1011	USBStorageDeviceWriteError	OK
1012	USBStorageDeviceRedundancyLost	警告
1013	USBStorageDeviceRedundancyRestored	OK
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
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
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
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
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
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
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
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
140096	SsdWearOut	クリティカル

IPMI アラート

#	名前	IPMI SEL イベント (Y/N)	IPMI SEL イベントの詳細	SNMP のサポート (Y/N)	OID
1	CPU 障害	Y	IERR | 訂正不能なマシンチェックの例外がアサートされた | 構成エラーがアサートされた| アサート済み	Y	cpqSeCpuUncorrectableError cpqSeCpuStatusChange
3	メモリ ECC エラー	Y	訂正不能な ECC | アサート済み	Y	cpqHe5CorrMemReplaceMemModule
4	訂正可能なメモリエラー	Y	訂正可能な ECC | アサート済み	N	該当なし
5	メモリ障害	Y	メモリデバイスが無効になっている | 構成エラーがアサートされた| アサート済み	Y	cpqHe5CorrMemReplaceMemModule
9	電源装置で障害が発生している	Y	障害が検出された | 電源 AC の損失がアサートされた | アサート済み	Y	cpqHe4FltTolPowerSupplyFailed cpqHePwrSupplyError cpqHe4FltTolPowerSupplyACpowerloss cpqHeNoPowerSupplyDetected
10	電源装置が取り外された	Y	存在が検出された |ディアサート済み	Y	cpqHe3FltTolPowerSupplyRemoved
14	ハードディスクの障害	Y	ドライブの障害 | 事前障害がアサートされた| In Failed Array がアサートされた | アサート済み	Y	cpqDa7PhyDrvStatusChange
16	ファン障害	Y	OK に移行 | OK から重大でないへの移行がアサートされた | 軽度から回復不能への移行がアサートされた | より深刻から重大でないへの移行がアサートされた | アサート済み	Y	cpqHe3FltTolFanDegraded cpqHe3FltTolFanFailed cpqHe3FltTolFanRedundancyLost cpqHe3FltTolFanInserted
17	ファンの取り外し	N	-	Y	cpqHe3FltTolFanRemoved

iLO アラートメール

iLO アラートメールを使用すると、ホスト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、セキュアな SMTP 接続(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。

iLO 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、「iLO ライセンスオプション」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(TLS)を有効が有効になっている構成の場合は、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]をクリックしてから[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(TLS)を有効オプションを使用する場合、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iLO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(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(TLS)を有効およびSMTP認証を有効が有効になっている場合：
   - 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。
   - SMTPパスワードの変更チェックボックスを選択します。
   - 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、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iLOアラートメールを送信するには、[テストiLOアラートメールを送信]をクリックします。

    このボタンは、iLO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iLO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。

iLO 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アラートメールを受信する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、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(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iLO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(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。

iLO 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、「iLO ライセンスオプション」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]をクリックしてから[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、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]をクリックしてから[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、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]をクリックしてから[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、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、「iLO ライセンスオプション」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.
```

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]をクリックしてから[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、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。

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]をクリックしてから[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、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

16. ライフサイクル管理機能の使用

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。ガイドラインの付録では、メディアの最小サニタイズレベルを定義しています。仕様について詳しくは、「メディアサニタイズのガイドライン」のセクション 2.5 を参照してください。
One-button セキュア消去は、ユーザーデータのパージに対する NIST SP 800-88 Revision 1 のサニタイズに関する勧告を実装しており、サーバーおよびサポートされたコンポーネントをデフォルトの状態に戻します。この機能は、サーバーの揮発性に関する報告のドキュメントでユーザーが行う多くのタスクを自動化します。

One-button セキュア消去アクセス方式

次の製品から One-button セキュア消去を開始できます。

- 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 セキュア消去を開始するための前提条件

前提条件

- 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、「iLO ライセンスオプション」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
  - Smart アレイ暗号化
  - Intel VROC 暗号化
- 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。
- 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。

- Microsoft® Secured-core サポートを無効にします。

One-button セキュア消去の開始

前提条件
ご使用の環境が One-button セキュア消去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]をクリックしてから[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]をクリックしてから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。
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。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。

   この手順を完了することをお勧めします。

One-button セキュア消去ステータス値

One-button セキュア消去を開始すると、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

One-button セキュア消去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. EXPRESSBUILDERリカバリイメージを使用してEXPRESSBUILDERをインストールします。
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 セキュア消去が完了している。
- One-button セキュア消去が完了した後、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]をクリックしてから[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]をクリックしてから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。

   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。

   サーバーを廃棄するか、または別の目的で使用する前に、消去レポートを削除することをお勧めします。

One-button セキュア消去レポートの詳細

- **サーバーシリアル番号** - サーバーのシリアル番号。
  次によって開始 - One-button セキュア消去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

One-button セキュア消去機能を使用する場合、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。

前提条件

- サーバーで One-button セキュア消去が完了している。
- One-button セキュア消去が完了した後、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]をクリックしてから[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]をクリックしてから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

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。
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。

前提条件

- iLO の設定を構成する権限
- サーバーで One-button セキュア消去が完了している。
- One-button セキュア消去が完了した後、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。

手順

1. 左側のナビゲーションペインで[セキュリティ]をクリックしてから[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]をクリックしてから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. サーバーでOne-buttonセキュア消去が完了した場合は、最新の消去レポートの参照ボタンが使用できます。
3. [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。
4. 🗑 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、iLO工場出荷時デフォルト設定へのリセットが行われます。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 iLO7 設定は消去されるか、iLO 工場出荷時デフォルト設定へのリセットが行われます。
  - 工場出荷時にプロビジョニングされた iLO LAK、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 ライセンスに戻ります。
  - 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 セキュア消去が終了するとライセンスは再インストールされます。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。
- EXPRESSBUILDER は起動せず、再インストールする必要があります。

注記
iLO IAK、およびシステム IAK 証明書は One-button セキュア消去で消去されません。
ただし、システム IAK キーは TPM から消去されます。

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
- 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 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、EXPRESSBUILDER 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。
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 + iLO 工場出荷時デフォルト設定へのリセット + 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。
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 + iLO 工場出荷時デフォルト設定へのリセット + 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[4]	ATA SANITIZE with CRYPTO SCRAMBLEEXT (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 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[5]	ATA SANITIZE with CRYPTO SCRAMBLEEXT (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 OVERWRITE EXT	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

[4] これらのドライブは、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。
[5] これらのドライブは、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。

	オプション	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	SE 設定（SES）= 2 を使用した NVM エクスプレスフォーマット、サポートされている場合。	これは暗号鍵を削除することによって達成される暗号消去です。
	SANITIZE がサポートされている場合は NVM Express（NVM Express バージョン 1.3 以降をサポートしているドライブ用） SANITIZE がサポートされていない場合、このオプションは SES=1 での NVM Express FORMAT の単一パスを使用します。	すべての名前空間に関連するすべてのデータとメタデータが破壊されます。NVM サブシステムに存在するすべてのユーザーコンテンツは消去されます。

消去プロセスが失敗するサポート済みデバイス、およびサポートされていないデバイスの消去は安全ではありません。これらのデバイスに機密データが含まれている可能性があります。消去されないデバイスを分離し、他の方法を使用してデータを削除するか、所属する組織のセキュリティポリシーに従ってデバイスを安全に破棄します。

iLO のバックアップとリストア

- **自動でのバックアップとリストア**
  iLO 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。
  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。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。

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 工場出荷時デフォルト設定へのリセットを行い、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 工場出荷時デフォルト設定へのリセットを行うと、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、iLO 工場出荷時デフォルト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 工場出荷時デフォルト設定へのリセットを行ったり、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 工場出荷時デフォルト設定へのリセットを行った場合に、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 工場出荷時デフォルト設定へのリセットを行った場合は、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 工場出荷時デフォルト設定へのリセットが行われます。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、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。

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。

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 工場出荷時デフォルト設定へのリセットを行った場合は、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 工場出荷時デフォルト設定にリセットが行われます。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. 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。

17. iLO と他のソフトウェア製品およびツールとの使用

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

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。

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、 ip mitool 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
```

18. Kerberos 認証とディレクトリサービスの設定

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、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。

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

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。

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

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。

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)
```

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

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 Zero サインイン(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。

Mozilla Firefox での Zero サインインの有効化

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 Zero サインインの有効化

Google Chrome では設定は必要ありません。

Microsoft Edge での Zero サインインの有効化

Microsoft Edge では設定は必要ありません。

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。
- **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。
- **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。

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。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、TLS 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=Ad ministrators,CN=Builtin,DC=EXAMPLE,DC=COM 、OpenLDAP の場合は UID=username,ou=People,dc=nec, 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=CO M 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。

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、TLSを有効にします。

   iLOは、安全なTLS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。

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、ローカルユーザー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=NEC,DC=COM 、または @NEC.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)
    ユーザー名@ドメイン形式(Active Directory)例： jsmith@nec.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、[セキュリティ] - [認証] - [ディレクトリと LDAP]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、[セキュリティ] - [認証] - [ディレクトリと LDAP]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。

19. iLO 工場出荷時デフォルト設定へのリセット

場合によっては、iLO 工場出荷時デフォルト設定へのリセットを行う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 工場出荷時デフォルト設定へのリセットを行う必要があります。

- **iLO 工場出荷時デフォルト設定へのリセット方法**
  - BMC 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、iLO7 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。
  - コマンドライン - 詳しくは、iLO7 スクリプティング/コマンドラインガイドを参照してください。

iLO 工場出荷時デフォルト設定へのリセット

△注意
iLO 工場出荷時デフォルト設定へのリセットを行うと、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、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、BMC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。

   BMC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工場出荷時デフォルト設定へのリセットが行われます。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BMC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、リモートコンソールを起動します。

      以前のセッションのBMC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。

    iLO工場出荷時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。

20. トラブルシューティング

ログインと iLO アクセスの問題

iLO ファームウェアのログイン名とパスワードが受け付けられない

症状
iLO ファームウェアのログインに失敗します。

原因
入力されたユーザーアカウント情報が誤っています。

アクション
正しいユーザーアカウント情報を入力します。
- パスワードでは大文字と小文字が区別されます。
- ユーザー名は、大文字と小文字が区別されません。大文字と小文字は同一として扱われます (例：Administrator は administrator と同一として扱われます)。

名前を使用して iLO マネジメントポートにアクセスできない

症状
名前を使用して iLO マネジメントポートにアクセスできない。

原因
iLO マネジメントポートを DDNS サーバーに登録すると、名前を使用して iLO マネジメントポートにアクセスするために必要な名前-IP アドレス解決を提供できます。名前を使用して iLO マネジメントポートにアクセスできるように環境が構成されていません。

アクション
環境が以下の要件を満たすことを確認します。
- iLO マネジメントポートの電源を入れる前に、DDNS サーバーが稼働している必要があります。
- iLO マネジメントポートは、WINS サーバーまたは DDNS サーバーの IP アドレスを使用して構成されます。DHCP を使用して、必要な IP アドレスを構成できます。
- iLO マネジメントポートにアクセスするために使用するクライアントは、マネジメントポートの IP アドレスが登録された DDNS サーバーを使用するように構成されます。

iLO マネジメントポートが DHCP サーバーで予約されている IP アドレスを受信しない

症状
iLO マネジメントポートが、DHCP サーバーで予約されている IP アドレスを受信しなかった。

原因
iLO7 マネジメントポート用に DHCP の予約を作成する際に、DHCP クライアント識別子 (一意の識別子) として MAC アドレスが使用されました。iLO7 システムの DHCP クライアント識別子はハードウェア MAC アドレスです。

アクション
DHCP の予約が正しく作成されたことを確認します。
iLO7 マネジメントポート用に DHCP の予約を作成する場合は、後ろに 3 バイト (6 文字) の 0 が続くハードウェア MAC アドレスで構成される、DHCP クライアント識別子を使用します。

例えば、iLO7 MAC アドレスが 00-53-00-AA-BB-CC であれば、関連する DHCP クライアント識別子は 005300AABBCC0000 00 になります。

iLO ログインページにアクセスできない

症状
iLO Web インターフェイスのログインページがロードされません。

解決方法 1
原因
ブラウザーの TLS 暗号化レベルが 128 ビット以上に設定されていません。
iLO の TLS 暗号化レベルは 128 ビット以上に設定されており、変更することはできません。
ブラウザーと iLO の暗号化レベルは一致していなければなりません。

アクション
ブラウザーの TLS 暗号化レベルを 128 ビット以上に設定します。

解決方法 2
原因
iLO は共有ネットワークポートを使用するように構成され、その iLO 共有ネットワークポートが使用する NIC に対する NIC チーミングが有効になっています。この構成では、次の場合にネットワーク通信がブロックされる可能性があります。

- 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。

アクション
iLO 共有ネットワークポート構成が「NIC チーミングモード」に記載のガイドラインに従っていることを確認します。

iLO ネットワーク設定の変更後に接続できなくなった

症状
ネットワーク設定を変更した後、iLO にアクセスできません。

原因
NIC とスイッチの設定が同じではありません。

アクション
接続の両端(NIC およびスイッチ)で、トランシーバー速度の自動選択、速度、および
デュプレックスについて同じ設定が行われていることを確認してください。
たとえば、一方の側で接続が自動選択されるように設定されている場合、もう一方の側でも同じ設定を使用してください。

iLO のリセット後に iLO ログインページに戻れない

症状
iLO のリセット後に iLO ログインページが開きません。

アクション
ブラウザーのキャッシュをクリアし、ブラウザーを再起動します。

iLO ファームウェアのアップデート後に iLO 接続エラーが発生する

症状
ファームウェアのアップデート後に、iLO Web インターフェイスを使用して iLO に接続できません。

アクション
ブラウザーのキャッシュをクリアして、再試行します。

NIC を用いて iLO プロセッサーに接続できない

症状
NIC 経由で iLO プロセッサーにアクセスできません。

アクション
ROM ベースのシステムユーティリティを使用して NIC が有効になっていることを確認し、割り当てられた IP アドレスとサブネットマスクを確認します。

- ネットワーク上の別のワークステーションから、その NIC の IP アドレスを ping します。
- ブラウザーで、NIC の IP アドレスを URL として入力して、NIC との接続を試みます。このアドレスで、iLO のログインページを表示できます。
- iLO をリセットします。ネットワーク接続が確立した場合、DHCP サーバー要求を最大 90 秒待つ必要がある場合があります。

iLO の証明書のインストール後 iLO にログインできない

症状
iLO の自己署名証明書をブラウザーの証明書ストアにインストールした後、iLO にアクセスできません。

原因
iLO 工場出荷時デフォルト設定へのリセットを行うか、iLO ホスト名を変更すると、新しい自己署名証明書が生成されます。一部のブラウザーでは、自己署名証明書を永久的にインストールすると、新しい自己署名証明書を生成した後で iLO にログインできないことがあります。

アクション
自己署名証明書をブラウザーの証明書ストアから削除します。
自己署名証明書の証明書名は iLO で、発行元値にはデフォルトの発行元というテキストが含まれています。
iLO の自己署名証明書をブラウザーの証明書ストアにインストールしないでください。証明書をインストールする場合は、CA に永久的な証明書を要求し、iLO にインポートします。
証明書の使用について詳しくは、ブラウザーのドキュメントを参照してください。

iLO の IP アドレスに接続できない

症状
iLO の IP アドレスを使用して iLO に接続できません。

原因
プロキシサーバーを使用するように Web ブラウザーが構成されています。

アクション
プロキシサーバーを使用せずに iLO に接続するには、プロキシサーバーの例外リストに iLO を追加します。手順については、ブラウザーのドキュメントを参照してください。

iLO TCP/IP 通信が失敗する

症状

iLO 通信が失敗します。

原因
1 つまたは複数の TCP/IP ポートを介した iLO 通信をファイアウォールが妨げています。

アクション
iLO が使用するポートでの通信を許可するようにファイアウォールを構成します。

Firefox を使用して iLO に接続するときのセキュアな接続の失敗エラー

症状
Firefox を使用して iLO に接続しようとするときに、次のエラーが発生します。
sec_error_reused_issuer_and_serial

解決方法 1
原因
インストールされている証明書には、認証機関によって発行された別の証明書と同じシリアル番号が含まれています。

アクション
1. メニューボタンをクリックし、オプションを選択します。
2. 詳細設定をクリックします。
3. 証明書をクリックします。
4. 証明書を表示をクリックします。
5. サーバータブをクリックして iLO に関係する証明書をすべて削除します。
6. その他タブをクリックして iLO に関係する証明書をすべて削除します。
7. OK をクリックします。
8. Firefox を起動し、iLO に接続します。

解決方法 2
原因
インストールされている証明書には、認証機関によって発行された別の証明書と同じシリアル番号が含まれています。

アクション
1. Firefox を閉じます。
2. Firefox の AppData フォルダーに移動して、すべての Firefox ディレクトリにある *.db ファイルをすべて削除します。
3. AppData フォルダーは通常次の場所にあります。
   C:\\Users\<ユーザー名>\AppData\Local\\Mozilla\Firefox\

Microsoft Edge で iLO Web インターフェイスに移動するときのセキュリティ警告

症状
Microsoft Edge で iLO Web インターフェイスに移動すると、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る。

解決方法 1
アクション
Microsoft Edge(レガシー)の場合：
1. 詳細をクリックします。
2. Web ページへ移動をクリックします。

3. iLO にログインします。

アクション
Microsoft Edge(新規)の場合：
1. 詳細設定をクリックします。
2. iLO host name に進む(安全ではありません)をクリックします。
3. iLO にログインします。
   このソリューションを使用すると、iLO Web インターフェイスとオンラインヘルプを表示するときに、ブラウザーのアドレスバーに安全ではありませんというテキストが表示されます。

解決方法 2
アクション
1. iLO にログインします。
2. ナビゲーションツリーで[セキュリティ]をクリックしてから[TLS 証明書]をクリックします。
3. TLS 証明書を取得してインポートします。
4. iLO をリセットします。

chrome で iLO Web インターフェイスに移動するときのセキュリティ警告

症状
Google Chrome で iLO Web インターフェイスに移動すると、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る。

解決方法 1
アクション
1. 詳細設定をクリックします。
2. iLO host name に進む(安全ではありません)をクリックします。
3. iLO にログインします。
   このソリューションを使用すると、iLO Web インターフェイスとオンラインヘルプを表示するときに、ブラウザーのアドレスバーに保護されていない通信というテキストが表示されます。

解決方法 2
アクション
1. iLO にログインします。
2. [管理] > [セキュリティ] > [TLS 証明書]ページに移動します。
3. TLS 証明書を取得してインポートします。
4. iLO をリセットします。

Firefox で iLO Web インターフェイスに移動するときのセキュリティ警告

症状
Mozilla Firefox で iLO Web インターフェイスに移動すると、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る。

解決方法 1
アクション
1. 詳細設定をクリックします。
2. 危険性を承知で続行をクリックします。
3. iLO にログインします。
   このソリューションを使用すると、iLO Web インターフェイスとオンラインヘルプを表示するときに、ブラウザーのアドレスバーに警告アイコンが表示されます。

解決方法 2
アクション
1. iLO にログインします。
2. [管理] > [セキュリティ] > [TLS 証明書]ページに移動します。
3. TLS 証明書を取得してインポートします。
4. iLO をリセットします。

iLO ログインページに「Web サイトは不明な機関で認証されています」メッセージが表示される

原因
iLO ログインページに移動すると、「Web サイトは不明な機関で認証されています」というメッセージが表示されます。

アクション
1. 証明書を表示して、(にせのサーバーでなく)正しいマネジメントサーバーにアクセスしていることを確認します。
   - 発行先の名前がマネジメントサーバーであることを確認します。必要と思われる手順を実行して、マネジメントサーバーの識別情報を確認します。
   - これが正しいマネジメントサーバーかどうか確信が持てない場合は、先に進まないでください。にせのサーバーにアクセスしている可能性があり、ログインするときにログイン認証情報をにせのサーバーに渡すおそれがありま す。管理者に連絡してください。接続を取り消すには、証明書ウィンドウを終了し、いいえまたはキャンセルをクリックします。
2. 前のステップの項目を確認した後、次のオプションを選択します。
   - このセッションのために一時的に証明書を受け入れる。
   - 永久的に証明書を受け入れる。
   - いったん中止し、管理者から提供されたファイルからブラウザーに証明書をインポートする。

iLO が ping に断続的に応答するか、または応答しない

症状
iLO は、ping に断続的に応答するか、または応答しません。

原因
iLO 共有ネットワークポートが構成され、その NIC において NIC チーミングが構成されている時、次の場合にネットワーク通信がブロックされる可能性があります。
- 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。
- 選択した 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る以外の NIC/ポートに送信されます。

アクション
iLO 共有ネットワークポート構成が「NIC チーミングモード」に記載のガイドラインに従っていることを確認します。

Microsoft Edge(レガシー)で iLO オンラインヘルプを開こうとすると証明書の警告が表示される

症状

Microsoft Edge(レガシー)で iLO オンラインヘルプにアクセスしようとすると、証明書のエラーが表示される。

原因
Microsoft Edge(レガシー)バージョン 42 以降では、信用できないサイトの証明書を信用することにしても、そのサイト内のすべてのウィンドウで拒否されます。ヘルプトピックのウィンドウなど、そのサイトのリンクから開いたポップアップウィンドウによって、信用できない証明書の使用を再承認するように求められます。

アクション
以下の解決策を試してください。
- 信頼済みの証明書をインストールします。
- 詳細リンクをクリックしてから Go on to the webpage をクリックして続行します。この操作は、オンラインヘルプにアクセスするたびに必要になります。
- 別のブラウザーを使用します。

iLO に Zero サインイン接続が拒否される

症状
iLO は Zero サインインをサポートするように構成されているが、SSO 接続が拒否される。

原因
現在の信頼モードまたは証明書ステータスに問題があります。

アクション
1. SSO 接続でアクセスするシステム上の iLO にログインします。
2. ナビゲーションツリーで[セキュリティ]をクリックしてから[NEC SSO]をクリックします。
3. iLO が選択した SSO 信頼モードをサポートするように構成されていることを確認します。
    - 証明書による信頼を選択し、証明書が存在しない場合は、信頼できる証明書を追加します。
    - 証明書による信頼を選択し、証明書が存在する場合は、次のようにします。
        - 証明書の有効期限が切れていないことを確認します。
        - 証明書が、iLO の要件を満たすことを確認します。
        - 高セキュリティまたは FIPS セキュリティ状態が有効な場合、2048 ビット証明書が必要です。
        - CNSA セキュリティ状態が有効な場合は、3072 ビット RSA キーまたは NIST P-384 曲線の 384 ビット ECDSA キーを含む証明書が必要です。
    - 名前による信頼を選択した場合は、DNS 名をインポートします。

信頼済みの TLS 証明書がデフォルトの自己署名証明書にリセットされることがある

症状
信頼済みの TLS 証明書がデフォルトの自己署名証明書にリセットされることがある

アクション
新しい信頼済みの TLS 証明書をインポートします。

ファームウェアの問題

iLO ファームウェアのアップデートが失敗する

症状
iLO ファームウェアをアップデートしようとすると次の問題が発生します。
- iLO ファームウェアが応答していません。
- iLO がファームウェアアップデート要求を受け入れませんでした。
- iLO ファームウェアのアップデートは、アップデートが完了する前に停止しました。

解決方法 1
原因
通信またはネットワークの問題が発生しました。

アクション
1. iLO に Web ブラウザー経由で接続を試みます。接続できない場合は、通信に問題があります。
2. iLO に対して ping を実行します。成功する場合、ネットワークは動作しています。
3. ファームウェアアップデートを再度実行してください。

解決方法 2 アクション
別のファームウェアアップデート方法を試してください。

iLO ファームウェアアップデートエラー

症状
iLO は、ファームウェアをアップデートする最後の試行が失敗したことを通知します。

原因
iLO ファームウェアのアップデートで間違ったファイルを使用しました。

アクション
フラッシュプロセスをリセットするには、🗑 をクリックし、正しいファームウェアファイルでファームウェアのアップデートを再び実行します。
エラーをクリアしないと、正しいファームウェアファイルを使用しても、同じエラーが発生する場合があります。

iLO ファームウェアアップデートが終了しない

症状
iLO ファームウェアアップデートが 1%完了のままで終了しません。

原因
iLO Web インターフェイスが応答を停止しました。

アクション
1. ブラウザーウィンドウを更新します。
2. iLO ファームウェアアップデートを再度実行してください。

iLO ネットワークのフラッシュエラーリカバリ

ほとんどのファームウェアアップグレードは、正常に終了します。万一、iLO ファームウェアのアップグレード時にサーバーの電源が切れた場合でも、iLO は、電源が再投入されたときに復旧することができます。

iLO が起動すると、起動コードは、メインイメージのイメージ検証を実行します。イメージが破損しているか不完全で、セキュアリカバリ機能で自動的に復元できない場合、iLO はフラッシュエラーリカバリモードになります。フラッシュエラーリカバリにより、iLO 内の FTP サーバーがアクティブになります。この FTP サーバーを使用すると、プログラミングのためにイメージを iLO に送信できます。FTP サーバーは、他のサービスを提供しません。
この機能は、iLO が製品セキュリティ状態または FIPS セキュリティ状態を使用するように設定されている場合にのみ使用できます。
ネットワーククライアントは、FTP サーバーに接続できます。接続のためのユーザー名は

```
test
```

、パスワードは

```
flash
```

です。ファームウェアイメージを iLO に送信するには、FTP クライアントの PUT コマンドを使用します。イメージを受信すると、iLO は、イメージを検証します。イメージが、署名された完全で有効なファームウェアイメージであれば、カーネルは、フラッシュパーティションのプログラミングを開始します。
フラッシュパーティションにイメージがプログラミングされたら、iLO は自動的にリセットされます。例：

```
F:\ilo>ftp 192.168.1.2
Connected to 192.168.1.2.
220 FTP Recovery server ready.
User (192.168.1.2:(none)): ftp
331 Password required.
Password:
231 Logged in.
ftp> put iLO.bin
200 Ok.
150 ready for file
226-Checking file
226-File acceptable
226-Flashing 3% complete
226-Flashing 4% complete
226-Flashing 6% complete
...
226-Flashing 97% complete
226-Flashing 99% complete
226-Flashing 100% complete
226-Flashing completed
226 Closing file
ftp: 8388608 bytes sent in 1.38Seconds 6100.81 Kbytes/sec.
ftp> quit
```

iLO によるシステム ROM (BIOS) 失敗のレポート

症状
システム ROM (BIOS) のステータスが失敗です。
このステータスがレポートされると、次のようになります。

- ダッシュボードページのシステムヘルスステータスはクリティカルです。
- ダッシュボードページの BIOS/ハードウェアヘルスステータスは失敗です。
- ファームウェア検証ページで、システム ROM のヘルスはクリティカルで、ステータスが”障害/オフライン”です。
- イベントが IML に記録されます。

解決方法 1

アクション
1. ファームウェア検証機能が自動修復向けに構成されている場合は、システムの修復が完了するまで待機します。
   構成によっては、修復アクションによって、システムリカバリセット (利用可能な場合) からシステム ROM ファームウェアが再インストールされる場合があります。
2. 修復が正常に完了したことを確認するには、ファームウェア検証ページを確認します。

解決方法 2
アクション
1. ファームウェア検証機能が自動修復向けに構成されていない場合は、手動でシステム ROM ファームウェアを再インストールします。
2. 修復が正常に完了したことを確認するには、ファームウェア検証ページを確認します。

iLO による無効なファームウェアコンポーネントの検出

症状
インストールされたファームウェアコンポーネントで、失敗ステータスが報告されている。

> **注記**
> このトピックは、システム ROM 以外のファームウェアタイプ用です。障害が発生したシステム ROM コンポーネントについては、iLO によるシステム ROM (BIOS) 失敗のレポートを参照してください。

このステータスが発生すると、以下のようになります。
- ダッシュボードページのシステムヘルスステータスはクリティカルです。
- ダッシュボードページの BIOS/ハードウェアヘルスステータスは失敗です。
- ファームウェア検証ページで、システム ROM のヘルスはクリティカルで、ステータスが”障害/オフライン”です。
- イベントが IML に記録されます。

•

解決方法 1
アクション
1. ファームウェア検証機能が自動修復向けに構成されている場合は、システムの修復が完了するまで待機します。
2. 修復が正常に完了したことを確認するには、ファームウェア検証ページを確認します。

解決方法 2
アクション
1. ファームウェア検証機能が自動修復向けに構成されていない場合は、手動で影響を受けるファームウェアを再インストールします。
2. 修復が正常に完了したことを確認するには、ファームウェア検証ページを確認します。

PLDM ファームウェアのアップデート中にサーバーがスタンバイモードになる

症状
PLDM ファームウェアのアップデート中にサーバーの起動または再起動が開始されると、サーバーは起動せずにスタンバイモードになり、約 20 分後に起動します。

原因
PLDM ファームウェアのアップデート中にサーバーが起動または再起動されました。

アクション
サーバーが起動するまで 20 分間待ちます。

PLDM ファームウェアのアップデート中はサーバーの起動または再起動を避けることをお勧めします。

ファームウェアのアップグレード後、ローカルユーザーアカウントが無効になる

症状

ファームウェアを iLO7 以降にアップグレードすると、ローカルユーザーアカウントが無効になります。

原因

ローカルユーザー設定は、ファームウェアを iLO7 から下位バージョンにダウングレードする際に保持され、その後 iLO7 以降のバージョンに再度アップデートされます。

アクション

必要に応じて、無効になっているユーザーを有効にします。

iLO7 ファームウェア破損時のイメージ復旧のために事前に iLO7 ファームウェア更新を行いバックアップイメージを生成しておく必要がある

症状

iLO7 ファームウェアが破損した場合に回復可能状態にするために、事前に iLO7 ファームウェアを更新して、iLO7 バックアップ ファームウェア イメージを生成しておく必要があります。

同じバージョン以降の iLO7 ファームウェアイメージで更新することで、iLO NAND に iLO7 のバックアップファームウェアイメージが作成され、iLO ファームウェアが破損した場合の回復メカニズムが確保されます。

解決方法

iLO Web インターフェイスもしくは iLO RESTful API を使用して iLO7 ファームウェアを更新します。

ライセンスの問題

ライセンスキーインストールエラー

症状
ライセンスキーエラーまたは ライセンスのインストールに失敗しましたメッセージが表示されます。

解決方法 1
原因
キーが iLO ライセンスキーではありません。

アクション
iLO ライセンスキーを入手し、もう一度やり直してください。

解決方法 2
原因
正規のライセンスがすでにインストールされた状態で、評価キーが送信されました。

アクション
なし。iLO は、正規のキーがすでにインストールされている場合、評価キーのインストールをサポートしません。

解決方法 3
原因
iLO の日時設定が不適切です。

アクション
iLO の日時設定を確認し、もう一度やり直してください。

解決方法 4
原因
入力したライセンスキーが間違っています。

アクション
ライセンスキーのエラーをチェックし、もう一度やり直してください。

仮想メディアまたはグラフィックリモートコンソールにアクセスできない

症状
仮想メディアおよびグラフィックリモートコンソール機能が使用できません。

原因
iLO の仮想メディアおよびグラフィックリモートコンソール機能は、オプションの iLO ライセンスをインストールすることによって有効にします。ライセンスがインストールされていない場合は、ライセンスがないとこれらの機能を使用できないことを示すメッセージが表示されます。

アクション
これら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。

iLO ライセンスキーのリカバリ

症状

以前にライセンスが適用されていた iLO システムにライセンスが付与されておらず、ライセンスキーのリカバリと再インストールが必要です。

解決方法 1
原因
iLO 工場出荷時デフォルト設定へのリセットが行われたが、システムボードが交換されたか、ライセンスキーが誤って置き換わりました。

アクション
バックアップファイルからライセンスキーと他の構成情報を復元します。
1. ナビゲーションツリーで[iLO 設定]をクリックします。
2. [iLO 構成のリストア]をクリックします。
3. 使用しているブラウザーに応じてファイルをドラッグ＆ドロップするか、[browse]をクリックし、バックアップファイルに移動します。
4. バックアップファイルがパスワードで保護されている場合、パスワードを入力します。
5. [アップロードおよびリストア]をクリックします。
   iLO が再起動され、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。

解決方法 2
アクション
交換キーを取得します。

リモートコンソールの問題

以下の各項では、リモートコンソールの問題のトラブルシューティングについて説明します。

> **重要**
> 新しいウィンドウの自動起動を防止するポップアップブロックアプリケーションを使用すると、リモートコンソールを実行できなくなります。この場合、ポップアップブロックプログラムを無効にしてから、リモートコンソールを起動してください。

リモートコンソールとクライアントキーボードとの間で Caps Lock が同期しない

症状
HTML5 コンソールにログインすると、Caps Lock の設定がクライアントキーボードと同期しない。

アクション
HTML5 コンソールの場合：Short Cuts をクリックし、仮想 CAPS キーをクリックします。

リモートコンソールとクライアントキーボードとの間で Num Lock が同期しない

症状
通常のセッションまたは共有リモートコンソールセッションで、Num Lock の設定がクライアントキーボードと同期しない。

アクション
HTML5 コンソールの場合：Short Cuts をクリックし、仮想 NUM キーをクリックします。

リモートコンソールセッション中に意図しないキーストロークが繰り返される

症状
リモートコンソールセッション中に意図しないキーストロークが繰り返されます。

解決方法 1
原因
ネットワークの問題がネットワーク遅延を引き起こしている可能性があります。

アクション
ネットワーク遅延を引き起こす場合がある問題を特定し、解決します。

解決方法 2
原因
リモートシステムの設定により遅延が生じています。

アクション
リモートマシンで以下の設定を調整します。

- **Increase the typematic delay** - この設定は、キーボードのキーを押したままにしたときに文字を繰り返す前の遅延を制御します。
- **Decrease the typematic rate** - この設定は、キーボードのキーを押したままにしたときに文字を繰り返す速度を制御します。

これらの設定の正式名称は、使用している OS によって異なります。キーリピート遅延と速度の変更について詳しくは、OS のドキュメントを参照してください。

カーソルがリモートコンソールウィンドウの隅にアクセスできない

症状
カーソルをリモートコンソールウィンドウの隅に移動できません。

アクション
カーソルを右クリックし、リモートコンソールウィンドウの外側にドラッグしてから、内側にドラッグして戻してください。

リモートコンソールのテキストウィンドウが正しくアップデートされない

症状
リモートコンソールを使用して、高速でスクロールするテキストウィンドウを表示する場合、テキストウィンドウが正しくアップデートされないことがあります。

原因
この問題は、iLO のファームウェアの検出/表示速度よりもビデオのアップデート速度のほうが速いときに発生することがあります。通常、テキストウィンドウの左上隅だけがアップデートされ、残りの部分の表示はアップデートされません。

アクション
テキストウィンドウのスクロールが停止した後、更新をクリックし、リモートコンソールウィンドウをアップデートします。

リモートコンソールのキーボード LED が正しく動作しない

症状
クライアントのキーボード LED は、リモートコンソールキーボードの状態を反映しません。

原因
クライアントのキーボード LED は、リモートコンソールキーボードの実際の状態を反映しません。リモートコンソールでキーボードオプションを使用すると、Caps Lock、Num Lock、および Scroll Lock キーは完全に機能します。

アクション
操作は必要ありません。

サーバーから仮想メディア USB キーにファイルをコピーした後にファイルが表示されない

症状
ファイルをターゲットサーバーから iLO 仮想メディア USB キーにコピーした場合、ファイルがクライアントコンピューター上の Windows エクスプローラーに表示されない。

原因
クライアントコンピューター上のユーザーは、Windows エクスプローラーを使用して iLO 仮想メディア USB キー上のファイルの変更を表示することはできません。
Windows エクスプローラーでは、ファイルのキャッシュされたコピーを USB キー上に保持します。USB キーがファイルの変更によってアップデートされたとき、リモートコンソールは Windows シェルに通知しません。エクスプローラーウィンドウを更新すると、キャッシュされた情報が USB キーに送り返されるため、変更された情報を表示することはできません。

アクション
1. Windows クライアントコンピューターに USB キーを接続します。
2. HTML5 コンソールを起動します。

3. USB キーを仮想ドライブメニューで選択することによって USB キーを接続します。
4. 接続したデバイス上のファイルを変更(コピー、削除など)します。
5. デバイス上のすべてのデータがアップデートされたことを確認するには、ターゲットサーバーからデバイスをアンマウントします。
6. リモートコンソールの仮想デバイスメニューを使用して USB キーを切断します。
   USB キーの内容の更新に、Windows エクスプローラーを使用しないでください。
7. ハードウェアの安全な取り外し機能を使用して、クライアントコンピューターから USB キーを取り出します。
8. クライアントコンピューターから USB キーを取り外します。
   USB キーをコンピューターに接続すると、Windows エクスプローラーでファイルの変更を確認できます。

リモートコンソールのホットキーが HTML5 コンソールで使用できない

症状
HTML5 コンソールでリモートコンソールのホットキーを入力すると、機能しないか、予期しない結果になる。

原因
ブラウザーまたはクライアント OS が、何か他のキーを使用する目的でマッピングされています。例えば、Chrome を使用している場合、Ctrl+W で現在のタブが閉じます。

アクション
- 構成したホットキーと同じキーボードの組み合わせを使用しないブラウザーを利用します。
- ブラウザーがカスタムのショートカットをサポートしている場合は、異なるキーボードの組み合わせを使用するようにブラウザーを構成します。
- ブラウザーで競合しない別のホットキーを構成します。
- 仮想 CTRL キーを使用してホットキーのコマンドを入力します。
  1. 仮想 CTRL キーをクリックしたままにします。
  2. クライアントキーボードで残りのキーボードの組み合わせを入力します。

iLO ナビゲーションペインのリモートコンソールのサムネイルが Microsoft Edge(レガシー)で見つからない

症状
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は、ナビゲーションペインに表示されません。

原因
リモートコンソールのサムネイルイメージで使用されている形式は、Microsoft Edge(レガシー)v42 以降で正しく表示されません。

アクション
別のブラウザーを使用します。

リモートコンソールで CTRL+ALT+DEL を押すと、クライアント OS にしか影響が及ばない

症状
クライアントキーボードで CTRL+ALT+DEL を押すとクライアント OS のみに影響が及び、サーバーOS およびリモートコンソールには影響が及ばない。

アクション

- HTML5 コンソールの場合：Ctrl、Alt ボタンをクリックし、DEL キーを押下します。

HTML5 コンソール使用時のキーボード入力に予期しない影響が出る

症状
HTML5 リモートコンソールを使用すると、キーボード入力を正しく行えなかったり、予期しない結果が出たりする。

原因
入力したキーまたはキーボードの組み合わせが、クライアント OS とリモートコンソールに、あるいはクライアント OS にのみ影響を及ぼした。

アクション
- 入力するキーボードの組み合わせに適したリモートコンソールのホットキーを定義します。
- HTML5 コンソール仮想キーを使用してキーボードの操作を入力します。
  - 仮想キーを押すには、仮想キーをクリックします。
  - 仮想キーでキーボードコマンドを入力するには、仮想キーをクリックしたままにします。クライアントのキーボードで、残りのキーボードコマンドを入力します。
    たとえば、CTRL + W を入力するには、仮想 CTRL キーの上でマウスをクリックしたまま、クライアントキーボードの W を押します。

  次の仮想キーを利用できます。
  - Ctrl - コントロール
  - Shift - シフト
  - Esc - エスケープ
  - Windows - Windows キー

Mozilla Firefox ブラウザでショートカットやホットキーをクリックすると HTML5 コンソールが応答しなくなる

症状

Mozilla Firefox ブラウザから HTML5 コンソール使用時、[ショートカット]または[ホットキー]をクリックすると、HTML5 コンソールが応答しなくなります。

解決方法

Google Chrome または Microsoft Edge ブラウザを使用してください。

高フレームリフレッシュレートのアプリケーション動作中に HTML5 コンソールのキーボードとマウスを使用すると遅延が発生する場合がある

症状
HTML5 コンソールでキーボードとマウスを使用する際に、特定の種類のアプリケーションがレンダリングされる際に遅延が発生する場合があります。
この遅延は、一般的にフレームレートの高いグラフィックを使用するアプリケーションで発生します。
遅延時間は、フレームのリフレッシュレートの高さによって異なります。数秒の場合もあれば、数分の場合もあります。マウスを動かしたり、キーを押したりしても、マウスの動きやキー入力が画面に表示されるまでには一定の時間がかかります。

解決方法
以下を行ってください。
- 物理コンソール、マウス、およびキーボードを使用してください。

パフォーマンスに関する問題

iLO Web インターフェイスにパフォーマンス機能がない

症状
パフォーマンスメニューが利用できないか、iLO Web インターフェイスに 1 つ以上の
パフォーマンスページが表示されない。

解決方法 1
原因
サーバー構成が、パフォーマンス機能を使用するための iLO ライセンスまたはサーバーファームウェアの前提条件を満たしていません。

アクション
前提条件を確認してください。必要に応じて、ライセンスまたはサーバーファームウェアアップデートをインストールしてください。

解決方法 2
原因
iLO Web インターフェイスからサーバーのリセットが開始されました。

アクション
1. サーバーのリセットが終了するまで待ちます。
2. iLO Web インターフェイスのブラウザーウィンドウを更新します。

解決方法 3
原因
iLO 工場出荷時デフォルト設定へのリセットが行われた。

アクション
1. サーバーを再起動します。
2. iLO をリセットします。
3. iLO にもう一度ログインします。

解決方法 4
原因
サーバー上の MCTP 検出が無効です。

アクション
サーバーで MCTP 検出を有効にします。

ディレクトリの問題

Kerberos 認証による iLO へのログインが失敗する

症状
Kerberos へのログインを試みて失敗しました。

解決方法 1
原因
クライアントにチケットがないか、チケットが無効である。

アクション
クライアント PC をロックして新しいチケットを取得するには、Ctrl+Alt+Del を押します。

解決方法 2
原因
Kerberos ログインの設定が誤っています。考えられる原因は、以下のとおりです。

- クライアント PC がログインしている Kerberos レルムが、iLO が設定されている Kerberos レルムと一致しない。
- iLO に保存されている Kerberos キータブファイル内のキーが、Active Directory のキーと一致しない。
- iLO が不正な KDC サーバーアドレス用に構成されている。
- クライアント PC、KDC サーバー、および iLO の間で、日時が一致しない。これらのシステム上の日時を同じ値に設定します。これらのシステム上の日時は 5 分以上異なっていてはいけません。

アクション
ご使用の環境が、Kerberos サポートの要件を満たしていることを確認します。

解決方法 3
原因
ディレクトリユーザーアカウントに関わる問題があります。次のような問題が考えられます。

- iLO コンピューターアカウントが Active Directory 内に存在しないか、アカウントが無効になっている。
- クライアント PC にログインしているユーザーが、iLO アクセスを認可された(汎用またはグローバルな)ディレクトリグループのメンバーでない。

アクション
ユーザーアカウントが存在することと、そのユーザーアカウントが iLO へのアクセス権のあるグループのメンバーであることを確認します。

解決方法 4
原因
DNS サーバーが正常に稼働していない。iLO では、Kerberos をサポートするために、稼働している DNS サーバーが必要です。

アクション
DNS サーバーを修復します。

解決方法 5
原因
ブラウザーが正しく設定されていない。

アクション
ブラウザーが Kerberos ログイン用に正しく設定されていることを確認します。

Kerberos ログインの試行中に iLO 認証情報プロンプトが表示される

症状
ユーザーが[Zero サインイン]ボタンをクリックしたとき、認証情報プロンプトが表示されます。

原因
ブラウザーが Kerberos ログイン用に正しく構成されていません。

アクション
Kerberos ログインをサポートするようにブラウザーを構成します。

名前による Kerberos ログインの試行中に iLO 認証情報プロンプトが表示される

症状
ユーザーが Kerberos SPN 形式のユーザー名および関連付けられているドメインパスワードを使用して iLO にログインしようとするときに、認証情報プロンプトが表示されます。

原因
iLO 用のコンピューターアカウントは子ドメインの一部であり、Kerberos 構成パラメーターは親ドメインを参照します。

アクション
以下の Kerberos パラメーターが正しく構成されていることを確認します。
Kerberos Realm、Kerberos KDC Server Address、Kerberos KDC Server Port。

iLO へのディレクトリ接続が途中で終了する

症状
アクティブディレクトリセッションが途中で終了します。

原因
ネットワークエラーによって、iLO は、ディレクトリ接続が無効になったと判断することがあります。iLO がディレクトリを検出できない場合、iLO は、ディレクトリ接続を終了します。終了された接続を使用して作業の継続を試みても、ブラウザーは、ログインページに転送されます。
この問題は、以下の状況で発生する可能性があります。

- ネットワーク接続が切断された。
- ディレクトリサーバーがシャットダウンした。
-

アクション
ログインしなおして iLO の使用を継続します。
ディレクトリサーバーを使用できない場合は、ローカルユーザーアカウントを使用してログインします。

構成されているディレクトリユーザーコンテキストが iLO ログインで動作しない

症状
ディレクトリユーザーコンテキストが構成されていますが、ディレクトリユーザーコンテキストが提供するログインオプションが機能しません。

原因
ディレクトリまたはユーザーコンテキスト内のユーザーオブジェクトが正しく構成されていません。

アクション
- ユーザーオブジェクトの完全な DN がディレクトリに存在することを確認します。
  この情報は DN の最初の CN= の後にあります。
- DN の残りの部分はユーザーコンテキストとして追加されていることを確認します。
  ユーザーコンテキストは、大文字と小文字を区別しません。また、それ以外の文字は、空白も含めて、ユーザーコンテキストの一部です。

ディレクトリタイムアウトになった後もディレクトリユーザーアカウントがログアウトしない

症状
ディレクトリユーザーは、ディレクトリログインタイムアウトのために構成された時間が経過した後、ログアウトされません。

原因
iLO セッションがタイムアウトしないように、iLO のアイドル接続タイムアウト値は無限に設定されています。iLO セッションがアクティブになると、iLO ファームウェアはディレクトリに定期的にユーザーパーミッションをクエリします。このクエリによりディレクトリ接続がアクティブであり続け、ディレクトリタイムアウト設定に基づくユーザーのログアウトが行われなくなります。

アクション
- iLO の使用が終わったらログアウトします。
- アイドル接続タイムアウト設定を変更します。

ディレクトリユーザーのログインが失敗する

症状
ディレクトリユーザーのログインが失敗します。ただし、ローカルユーザーのログインは成功します。

原因
ディレクトリユーザーセッションが多すぎます。

アクション
- iLO に管理者としてログインします。複数のディレクトリユーザーセッションがセッションリストに表示されている場合は、不要なセッションを切断します。
- 問題が続く場合は、iLO をリセットしてください。

Zero サインイン構成用の Kerberos キータブファイルの生成の失敗

症状
ktpass を使用してキータブファイルを生成しようとしたときにプロセスが失敗します。

原因
ktpass コマンドの書式が正しくありませんでした。

アクション
もう一度実行し、 ktpass コマンド内のプリンシパル名の書式が正しいことを確認してください。

iLO Kerberos 構成での Setspn の実行中のエラー

症状
Setspn コマンドの実行中にエラーが発生しました。

アクション
1. ADSIEdit スナップインを備えた MMC を使用し、iLO のコンピューターオブジェクトを検索します。
2. DNSHostName プロパティを iLO の DNS 名に設定します。

例： cn=iloname,ou=us,ou=clients,dc=example,dc=net

入れ子型グループで構成されている場合に OpenLDAP 認証が失敗する

症状
ディレクトリが入れ子型グループで構成されている場合に OpenLDAP 認証が失敗します。

原因
iLO では、OpenLDAP での入れ子型グループをサポートしません。

アクション
iLO に LDAP ユーザーがダイレクトメンバーシップを持つグループを構成します。OpenLDAP ディレクトリグループがタイプ groupOfNames の objectClass を持つことを確認します。

OpenLDAP ディレクトリ認証を使用して iLO にログインすると失敗する

症状
OpenLDAP(汎用)ディレクトリユーザーのログイン試行が失敗します。

原因
OpenLDAP ディレクトリユーザーは、一意のユーザーDN ではなくユーザーログイン名のみを使用してディレクトリグループにリストされています。

アクション
iLO にディレクトリユーザーコンテキストを 1 つだけ構成して、ユーザーをログイン名のみで一意に識別するようにします。

ドメインコントローラーOS の再インストール後に Zero サインインが失敗する

症状
ドメインコントローラーOS を再インストールした後に iLO Web インターフェイスの Zero サインインオプションが動作しません。

原因
ドメインコントローラーOS が再インストールされると、キーバージョン番号がリセットされます。

アクション
新しい Kerberos キータブファイルを生成してインストールします。

Active Directory の認証情報での iLO ログインに失敗する

症状
Active Directory を使用するように iLO が構成されている場合にユーザー認証に失敗します。

原因

証明書の問題があります。

- Active Directory サーバーに TLS 証明書がインストールされていません。
- Active Directory サーバー上の古い TLS 証明書は、現在の証明書の CA と同じ名前の以前の信頼済み CA を指しています。これは、証明書サービスが追加された後削除され、再度、追加された場合に発生することがあります。

ディレクトリテストページの TLS 接続テスト結果を確認することによって、この原因を確認できます。

アクション

1. MMC を起動します。
2. 証明書スナップインを追加します。
3. プロンプトが表示されたら、表示する証明書のタイプとしてコンピューターアカウントを選択します。
4. 証明書スナップインに戻るために、OK をクリックします。
5. 個人 > 証明書フォルダーを選択します。
6. フォルダーを右クリックし、新しい証明書の要求を選択します。
7. 証明書の種類がドメインコントローラーになっていることを確認したら、証明書が発行されるようになるまで次へをクリックします。

Directory Server DNS Name テストで失敗が報告される

症状

Directory Server DNS Name テストで、ステータス失敗が報告されます。

原因

iLO は、ディレクトリサーバーの IP アドレスを取得できません。

アクション

- iLO に設定されている DNS サーバーが正しいことを確認します。
- ディレクトリサーバーの FQDN が正しいことを確認します。
- トラブルシューティングツールとして、FQDN の代わりに IP アドレスを使用します。
- 問題がなくならない場合は、DNS サーバーの記録とネットワークルーティングをチェックします。

ディレクトリサーバーへの Ping テストが失敗を報告する

症状

ディレクトリサーバーへの Ping テストが失敗ステータスを報告します。

原因

iLO は、ディレクトリサーバーを Ping し、応答を受信しませんでした。

アクション

- ディレクトリサーバーでファイアウォールが有効かどうかをチェックします。
- ネットワークルーティング問題をチェックします。

Connect to Directory Server テストで失敗が報告される

症状

Connect to Directory Server テストで、ステータス失敗が報告されます。

原因

指定したディレクトリサーバーとの LDAP 接続を iLO が開始できませんでした。

アクション

- 構成されたディレクトリサーバーが正しいホストであることを確認します。
- (iLO とディレクトリサーバー間のすべてのルーターやファイアウォールを考慮して)iLO がポート 636 経由でディレクトリサーバーとのクリアな通信パスを持っていることを確認します。
- ディレクトリサーバー上のローカルファイアウォールが有効になっており、ポート 636 経由で通信できることを確認します。

Connect using TLS テストで失敗が報告される

症状

Connect using TLS テストで、ステータス失敗が報告されます。

原因

iLO とディレクトリサーバー間の TLS ハンドシェークと交渉が失敗しました。

アクション

- ディレクトリサーバーで TLS 交渉を有効にします。
- Microsoft Active Directory を使用する場合は、Active Directory 証明書サービスがインストールされていることを確認します。

Bind to Directory Server テストで失敗が報告される

症状

Bind to Directory Server テストで、ステータス失敗が報告されます。

原因

iLO は、指定されたユーザー名との接続のバインドまたは匿名バインドに失敗しました。

アクション

- ディレクトリサーバーが匿名バインドを許可することを確認します。
- テストボックスにユーザー名を入力した場合は、認証情報が正しいことを確認します。
- ユーザー名が正しいことを確認した場合は、 user@domain.com 、 DOMAIN\username 、 username (Active Directory の表示名)、または userlogin のような他のユーザー名フォーマットを使用してみてください。
- 指定したユーザーがログインを許可され、有効であることを確認します。

Directory Administrator Login テストで失敗が報告される

症状

Directory Administrator Login テストで、ステータス失敗が報告されます。

原因

オプションのディレクトリ管理者識別名およびディレクトリ管理者パスワードボックスに値を入力しましたが、ディレクトリサーバーへのログインが失敗しました。

アクション

ディレクトリ管理者の認証情報が正しく入力されていることを確認します。

ユーザー認証テストで失敗が報告される

症状

ユーザー認証テストで失敗ステータスが報告されます。

原因
入力されたユーザー名とパスワードを使用した認証に失敗しました。

アクション
- ユーザー認証情報が正しく入力されていることを確認してください。
- user@domain.com 、 DOMAIN\username、username (Active Directory の表示名)、または userlogin のような他のユーザー名形式を使用してみてください。
- 指定したユーザーがログインを許可され、有効であることを確認します。
- 指定したユーザーアカウントにアクセス制限が構成されているかどうかを確認します。

ユーザー承認テストで失敗が報告される

症状
ユーザー承認テストで失敗ステータスが報告されます。

原因
入力されたユーザー名とパスワードを使用した承認に失敗しました。

アクション
- 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することを確認します。
- 指定したユーザーアカウントにアクセス制限が構成されているかどうかを確認します。

ディレクトリユーザーコンテキストテストで失敗が報告される

症状
ディレクトリユーザーコンテキストテストで、ステータス失敗が報告されます。

原因
iLO が、指定されたディレクトリ管理者識別名を使用して、指定されたユーザーコンテキストを検索するときに、ディレクトリでコンテナーが見つかりませんでした。

アクション
検索コンテキストが正しく入力されていることを確認します。

ディレクトリユーザーのログインが失敗する

症状
ディレクトリユーザーのログインが失敗します。

原因
ディレクトリユーザーが属するディレクトリグループの数が 300 を超えています。

アクション
ディレクトリユーザーが属するディレクトリグループの数が 300 を超えないようにします。

iLO7 で Zero サインインが機能しない

症状
Kerberos 認証のアドオンである Zero サインインは、iLO7 では機能しません。
iLO7 の場合、"Zero Sign-in authentication failed" のメッセージが表示されます。

解決方法

「Kerberos 経由でログイン」を使用してください。

iLO Web インターフェイスまたは iLO RESTful API を使用した IPv6 LDAP サーバアドレス設定変更時にポートが変更され、アドレスが切り詰められる場合がある

症状
iLO Web インターフェイス、および iLO RESTful API を使用して IPv6 LDAP サーバアドレスを設定・変更を行うと、以下の事象が発生する場合があります。

- LDAP ポート番号が、IPv6 アドレスの一部（例：セグメント値）で上書きされる。
- iLO Web インターフェイスにおいて、LDAP サーバアドレスが途中で切り詰めて表示される。
- LDAP 認証やディレクトリ接続が失敗、または誤った設定になる可能性がある。

解決方法

- iLO RESTful API を使用して LDAP ポートを手動で再設定してください。
- この問題は、iLO7 ファームウェアバージョン 1.21 以降で修正されています。該当バージョンにアップデートしてください。

Agentless Management、AMS、および SNMP の問題

AMS がインストールされているのに、iLO で使用できない

症状
AMS がサーバーにインストールされているのに、iLO Web インターフェイスで利用不可と表示されます。

アクション
1. AMS がインストールされていることを確認します。
2. OS のサービスツールを使用して"Agentless Management Service"を停止させます。
3. AMS 用のアプリケーションアカウントを再登録します。
   amscli delete appaccount
   amscli appaccount create -u <iLO Account> -p <iLO password>
   iLO Web インターフェイスの[設定] > [ユーザー管理] > [ユーザー]の[アプリケーションアカウント]セクションに”AMS”アカウントが登録されていることを確認してください。
4. OS のサービスツールを使用して"Agentless Management Service"を開始させます。
5. iLO をリセットします。

SSH の問題

iLO との PuTTY の初期接続時の入力が緩慢である

症状
PuTTY クライアントを使用して初めて iLO に接続を行う際、入力の受け付けが緩慢(約 5 秒間)になります。

アクション
- クライアントの構成オプションが正しいことを確認します。
- Low-level TCP connection options の Disable Nagle's algorithm チェックボックスの選択を解除してください。

iLO 共有ネットワークポートを使用する場合、PuTTY クライアントが応答しない

症状
iLO 共有ネットワークポートで PuTTY クライアントを使用する場合、PuTTY セッションが応答しなくなります。

原因
大量のデータが転送されているか、仮想シリアルポートとリモートコンソールを使用しています。

アクション
PuTTY クライアントを終了して、セッションを再開してください。

iLO への SSH 接続を使用する場合にテキストが正しく表示されない

症状
80 文字×25 行を超える拡張テキスト構成は、SSH を使用する場合は、正しく表示されません。

原因

テキストベースのリモートコンソールからの SSH アクセスでは、標準の 80 文字×25 行構成のテキスト画面がサポートされます。このモードは、ほとんどのテキストモードインターフェイスで、テキストベースのリモートコンソール に対する互換性を備えています。

アクション
テキストアプリケーションを 80 文字×25 行モードで設定するか、グラフィックリモートコンソールを使用することをお勧めします。

SSH セッションが起動に失敗する、または予期せず終了する

症状
SSH セッションが起動に失敗する、または予期せず終了する。

原因
iLO 共有ネットワークポートが構成され、その NIC において NIC チーミングが構成されている時、次の場合にネットワーク通信がブロックされる可能性があります。

- 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。

アクション
iLO 共有ネットワークポート構成が、iLO ユーザーガイドの「NIC チーミングモード」に記載のガイドラインに従っていることを確認します。

ホストから仮想 USB コントローラーと仮想 NIC の詳細を表示する

前提条件
仮想 NIC の有効化

手順

1. OS から取得した仮想 USB コントローラーの情報を表示するには、lspci コマンドを実行します。
   例：

```
[root@localhost ~]# lspci -vnnk -d 103c:22f6
3f:00.4 USB controller [0c03]: Hewlett-Packard Company iLO5 Virtual USB Controller
[103c:22f6] (rev 02) (prog-if 20 [EHCI])
Subsystem: Hewlett Packard Enterprise Device [1590:03ba]
Flags: bus master, fast devsel, latency 0, IRQ 60, NUMA node 0
Memory at a9b9c000 (32-bit, non-prefetchable) [size=256]
Capabilities: [70] MSI: Enable+ Count=1/1 Maskable- 64bit+
Capabilities: [80] Express Legacy Endpoint, MSI 00
Capabilities: [f0] Power Management version 3
Capabilities: [100] Advanced Error Reporting
Capabilities: [130] Alternative Routing-ID Interpretation (ARI)
Kernel driver in use: ehci-pci
```

2. 仮想 NIC デバイスが表示されるかどうかを確認するには、lsusb コマンドを実行します。
   例：

```
[root@localhost ~]# lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 008: ID 2cc8:2927 Hewlett Packard Enterprise HPE Virtual NIC (NCM)
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 002: ID 045b:0209 Hitachi, Ltd
Bus 003 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 003 Device 002: ID 045b:0210 Hitachi, Ltd
Bus 003 Device 004: ID 0781:5581 SanDisk Corp. Ultra
Bus 003 Device 006: ID 346d:5678 USB Disk 20
```

3. (オプション) 仮想 NIC USB デバイスを表示するには、usb-devices コマンドを実行します。
   例：

```
[root@localhost ~]# usb-devices
T: Bus=01 Lev=00 Prnt=00 Port=00 Cnt=00 Dev#= 1 Spd=480 MxCh= 8
D: Ver= 2.00 Cls=09(hub ) Sub=00 Prot=00 MxPS=64 #Cfgs= 1
P: Vendor=1d6b ProdID=0002 Rev=05.14
S: Manufacturer=Linux 5.14.0-522.el9.x86_64 ehci_hcd
S: Product=EHCI Host Controller
S: SerialNumber=0000:3f:00.4
C: #Ifs= 1 Cfg#= 1 Atr=e0 MxPwr=0mA
I: If#= 0 Alt= 0 #EPs= 1 Cls=09(hub ) Sub=00 Prot=00 Driver=hub
E: Ad=81(I) Atr=03(Int.) MxPS= 4 Ivl=256ms
T: Bus=01 Lev=01 Prnt=01 Port=04 Cnt=01 Dev#= 8 Spd=480 MxCh= 0
D: Ver= 2.00 Cls=02(commc) Sub=0d Prot=00 MxPS=64 #Cfgs= 1
P: Vendor=2cc8 ProdID=2927 Rev=00.01
S: Manufacturer=Hewlett Packard Enterprise
S: Product=HPE Virtual NIC (NCM)
C: #Ifs= 2 Cfg#= 1 Atr=e0 MxPwr=250mA
I: If#= 0 Alt= 0 #EPs= 1 Cls=02(commc) Sub=0d Prot=00 Driver=cdc_ncm
```

```
E: Ad=83(I) Atr=03(Int.) MxPS= 16 Ivl=32ms
I: If#= 1 Alt= 1 #EPs= 2 Cls=0a(data ) Sub=00 Prot=01 Driver=cdc_ncm
E: Ad=02(O) Atr=02(Bulk) MxPS= 512 Ivl=0ms
E: Ad=81(I) Atr=02(Bulk) MxPS= 512 Ivl=0ms
T: Bus=02 Lev=00 Prnt=00 Port=00 Cnt=00 Dev#= 1 Spd=480 MxCh= 4
D: Ver= 2.00 Cls=09(hub ) Sub=00 Prot=01 MxPS=64 #Cfgs= 1
...
```

4. ホストの仮想 NIC デバイスが IP を取得したかどうかを確認するには、 ip -c a コマンドを実行します。
   例：

```
[root@localhost ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: ens14f0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state
DOWN group default qlen 1000
link/ether 04:32:01:9b:cd:0a brd ff:ff:ff:ff:ff:ff
altname enp139s0f0
10: enp63s0f4u5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
fq_codel state UP group default qlen 1000
link/ether fa:4b:7f:fc:bc:02 brd ff:ff:ff:ff:ff:ff
inet 16.1.15.2/30 brd 16.1.15.3 scope global dynamic noprefixroute enp63s0f4u5
valid_lft 2263sec preferred_lft 2263sec
inet6 fe80::f84b:7fff:fefc:bc02/64 scope link noprefixroute
   valid_lft forever preferred_lft forever
```

注記
上記のコマンドは Linux OS 専用です。その他の OS については、OS のマニュアルまたは管理者ガイドを参照してください。

仮想 NIC から iLO にアクセスできない

症状
仮想 NIC を介して iLO に接続しようとすると、接続は失敗します。
ホストから仮想 NIC の IP アドレス (16.1.15.1) への ping は失敗します。

解決方法 1
原因
仮想 NIC 機能が無効になっています。
仮想 NIC 機能のステータスを確認して、この原因を確認してください。

- iLO Web インターフェイスのアクセスページで仮想 NIC 機能のステータスを確認します。
- REST クライアントを使用して仮想 NIC 機能のステータスを確認します ("redfish/v1/Managers/1/HostInterfaces/1" に対して Get)。

アクション

- iLO Web インターフェイスのアクセスページで仮想 NIC 機能を有効にします。
- REST クライアントを使用して仮想 NIC 機能を有効にします。
- ("redfish/v1/Managers/1/Oem/Hpe/VirtualNICEnabled" を true に設定します)。

解決方法 2
原因
仮想 NIC インターフェイスが Linux ホストの DHCP 用に構成されていません。
ip addr または ipconfig コマンドを使用して、IP アドレス 16.1.15.2 の USB イーサネットインターフェイスを確認して、この原因を確認してください。

アクション
DHCP を使用するようにホスト上の仮想 NIC インターフェイスを構成します。

解決方法 3
原因
ホスト上の仮想 NIC インターフェイスが他のインターフェイスとチーミングされています。この構成はサポートされていません。

アクション
ホスト上の仮想 NIC インターフェイスが他のインターフェイスとチーミングされていないことを確認してください。

解決方法 4
原因
仮想 NIC の IP アドレスがホストで手動で変更されました。仮想 NIC が構成されると、アダプターにはホスト上の IP アドレス 16.1.15.2 が割り当てられます。このアドレスを変更すると、この機能にアクセスできなくなります。

アクション
1. 問題の原因を確認します。
   - Windows システムの場合： ipconfig を実行し、 Ethernet adapter Ethernet という名前のアダプターを探します。
     正しい構成では、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。
   - Linux システムの場合：ネットワークインターフェイス名を特定し、 ifconfig を実行します。
     正しい構成では、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。
2. 別の IP アドレスが使用されている場合は、アダプターの IP アドレスを 16.1.15.2 に戻します。

iLO Web インターフェイスまたは iLO RESTful API に仮想 NIC からアクセスできない

症状
iLO Web インターフェイスまたは iLO RESTful API への仮想 NIC 接続を介して iLO に接続しようとすると、接続が失敗します。
ホストから仮想 NIC の IP アドレス (16.1.15.1) への ping は成功します。

解決方法 1
原因
必要なインターフェイスまたは機能が iLO で無効になっています。

アクション

iLO Web インターフェイスを使用するには、アクセスページで iLO Web インターフェイス オプションが有効になっていることを確認してください。

解決方法 2
原因
ホストオペレーティングシステムのファイアウォール設定が iLO Web サーバーの TLS ポート (HTTPS) をブロックしています。iLO Web インターフェイスと iLO RESTful API はこのポートを使用します。Web サーバーTLS ポート (HTTPS) のデフォルト値は 443 です。

アクション
ポートのブロックを解除します。

解決方法 3
原因
ブラウザーがサポートされていません。

アクション
サポートされているブラウザーを使用してください。

解決方法 4
原因
iLO Web インターフェイスに接続するために使用したブラウザーは、プロキシーサーバーを使用するように構成されています。

アクション
IP アドレス 16.1.15.1 をプロキシサーバーの例外のリストに追加します。手順については、ブラウザーのドキュメントを参照してください。

Windows Server 2022 において特定 10G NIC によるチーミング構成時に LAN ポートの挿抜を行うと”Connectivity status changed to XXX”の IML が採取されない場合がある

症状
Windows Server 2022 において、以下の 10G NIC を使用してチーミング構成している場合、LAN ポートの挿抜を行うと、IML に以下のイベントが登録および通報されないことがあります。

- リンクステータス変化イベント

[デバイス名] Connectivity status changed to <X> for adapter in slot <Y>, port <Z>

- 対象カード
  N8104-208/212(E810 10G/25G)
  N8104-217/219(BCM5714x 10G)
  N8104-222/225(BCM5719 1000M)
  N8104-223/225(BCM57414 10G/25G)

解決方法
原因
一時的に AMS の状態が利用不可になっています。

アクション

iLO はリンクアップ、リンクダウン検出時に以下のようなイベントを IML へ登録するので、リンクステータス変化を示す”Connectivity status changed to Y”イベントが発生したと読み替えてください。

- リンクアップ時

  ConnectionEstablished (<Device ID>, <B>, <C>) Redfish event from /redfish/v1/Chassis/1/NetworkAdapters/<A>/Ports/<B>

- リンクダウン時

  ConnectionDropped (<Device ID>, <B>, <C>) Redfish event from /redfish/v1/Chassis/1/NetworkAdapters/<A>/Ports/<B>

  A:Device 識別値、B:ポート番号、C:カード依存値(ポート番号または all)

iLO 共有ネットワークポート構成のサーバーで OS のインストールが失敗する

症状
iLO 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サーバーで、iLO 仮想メディアを使用した OS のインストールに失敗する

原因
- 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、一定時間(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 の通信が復元され、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。
- サーバーの起動中に一時的に接続が失われると、Windows は、次のレジストリキーで指定された回数の再試行を試みた後、TCP リセットを実行する可能性があります。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\ tcpmaxdataretransmissions
```

アクション
- iLO を使用して OS をインストールするときは、iLO 専用ネットワークポートを使用するようにサーバーを構成します。
- サーバーの CD ドライブに挿入された物理メディアを使用して OS をインストールします。
- Windows マシンを使用してサーバー上のリモートコンソールにアクセスする場合は、より多くの再試行を許可するために、Windows マシンに次のレジストリキーを構成します。

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\ tcpmaxdataretransmissions
```

デフォルト値の範囲は 3～5 です。この設定を 10(10 進数)に増やすと、この問題の原因となる TCP リセットが防止される可能性があります。このレジストリ値を編集した後、再起動が必要です。

⚠ 警告
レジストリエディターは自己責任において使用し、変更する前にレジストリをバックアップしてください。レジストリエディターの使用を誤ると、深刻な問題を引き起こす恐れがあり、その場合は OS の再インストールが必要になることがあります。詳しくは、Microsoft Knowledge Base の Article ID 番号 256986 を参照してください。上級ユーザー向けの Windows レジストリ情報。

iLO 共有ネットワークポート構成のサーバーでネットワークパフォーマンスが低い

症状
iLO 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サーバーでネットワークパフォーマンスが低い。iLO 仮想メディアを使用する OS のインストールが失敗する可能性がある。

原因
ネットワークの負荷が大きく、iLO 共有ネットワークポートが構成されている場合は、iLO ネットワーク接続が遅くなったり切断されたりする可能性があります。

アクション

- ネットワークアダプターを 100 MB/S のネットワーク速度の環境に接続します。
- OS のインストールに失敗した場合：
  - BIOS 方式による iSCSI ブートを使用して OS をインストールします。
  - iLO を使用して OS をインストールするときは、iLO 専用ネットワークポートを使用するようにサーバーを構成します。
  - サーバーの CD ドライブに挿入された物理メディアを使用して OS をインストールします。
- Linux ユーザーの場合は、Intel の NC-SI Overview and Performance - Understanding the DMTF Standard Manageability Interface のドキュメントの第 7 章の回避策を検討してください。このドキュメントは、Intel の Web サイトから入手できます。

IPMI の問題

SysHealth_Stat センサーの値のデコード

症状

IPMI にさまざまな SysHealth_Stat センサーの値が表示される。

原因

この問題は、ハードウェアコンポーネントの障害、電源の問題、または環境要因によって発生する可能性があります。

アクション

1. SysHealth_Stat センサーの#> ipmitool sensor list full コマンド出力の 4 列目を確認します。
   以下に例を示します。

   ```
   SysHealth_Stat|0x0| discrete| 0x0180| na| na| na| na| na| na
   ```

2. SysHealth_Stat の状態が 0x0180 の場合、サーバーは正常な状態です。
   以下に例を示します。

   ```
   0x0180: Transition to OK
   ```

3. SysHealth_Stat の状態が 0x0280 、0x0480 、または 0x0880 の場合は、サーバーヘルスが劣化しています。重大度は次のとおりです。

   ```
   0x0280: Transition to Non-critical from OK
   0x0480: Transition to Critical from less severe
   0x0880: Transition to Non-recoverable from less severe
   ```

4. 4. SysHealth_Stat の状態が劣化している場合は、#> ipmitool power status コマンドでシステムの電源ステータスを確認します。
   以下に例を示します。

   ```
   Chassis Power is on
   ```

   電源ステータスがオンでない場合は、電源装置の問題を示している可能性があります。
5. #>ipmitool sel elist コマンドで IPMI SEL イベントの詳細を表示して、電源装置障害、温度警告、ハードウェア障害、ハードウェアエラーなどのハードウェアのクリティカルイベントと警告イベントを確認します。
   以下に例を示します。

   ```
   b2 | 07/17/2024 | 21:56:41 | Temperature 22-Chipset | Upper Critical going high | Asserted |
   Reading 107] > [Threshold 100 degrees C
   ```

6. States Asserted の値を確認します (#>ipmitool sdr list -v コマンドを使用)。SDR データでハードウェアのクリティカルイベントや警告イベントが発生しているセンサーについて、[Transition to OK] 以外の値を確認します。SysHealth_Stat の状態が 0x0880 の場合、States Asserted は[Transition to Non-recoverable from less severe] になります。
以下に例を示します。

```
Sensor ID : SysHealth_Stat (0xac)
Entity ID : 23.1 (System Chassis)
Sensor Type (Discrete): Chassis (0x18)
Sensor Reading : 0h
Event Message Control : Global Disable Only
States Asserted : Chassis
[Transition to Non-recoverable from less severe]
Assertions Enabled : Chassis
[Transition to Non-critical from OK]
[Transition to Non-recoverable from less severe]
[Transition to Non-critical from more severe]
OEM : 1
```

7. ハードウェアのクリティカルイベントや警告イベントが発生しているセンサーについて、センサーの読み取り値の許容範囲を確認します (#>ipmitool sensor list -v コマンドを使用)。
以下に例を示します。

```
Sensor ID : 02-CPU 1 PkgTmp (0xfe)
Entity ID : 7.1
Sensor Type (Threshold) : Temperature
Sensor Reading : 48 (+/- 0) degrees C
Status : ok
Lower Non-Recoverable : na
Lower Critical : na
Lower Non-Critical : na
Upper Non-Critical : na
Upper Critical : 95.000
Upper Non-Recoverable : na
Positive Hysteresis : Unspecified
Negative Hysteresis : Unspecified
Assertions Enabled : ucr+
```

8. 8. #>ipmitool fru コマンドで FRU データを表示して、メモリ、CPU、電源装置などのハードウェアコンポーネントの警告とエラーを確認します。
以下に例を示します。

```
FRU Device Description : PSU 1 (ID 144)
Product Manufacturer : LTEON
Product Name : HpeServerPowerSupply
Product Part Number : P38995-B21
Product Version : 2.00
Product Serial : 5XLNV0KLLI342J
Product Extra : 800
FRU Device Description : PSU 2 (ID 145)
Product Manufacturer : Empty
```

ログとセンサーデータを分析して、問題の根本原因を見つけます。SysHealth_Stat センサーが正常な状態(0x0180) になるには、電源装置、ファン、温度センサーなどのすべてのセンサーが正常な状態である必要があります。何らかの障害が発生すると、SysHealth_State センサーの状態は良好 (0x180 :Transition to OK) から次のいずれかの劣化状態に変化します。

```
0x0280: Transition to Non-critical from OK
0x0480: Transition to Critical from less severe
0x0880: Transition to Non-recoverable from less severe
```

その他の問題

iLO イベントログエントリーのタイムスタンプが正しくない

症状
iLO イベントログエントリーの日付または時刻が正しくありません。

原因
SNTP 設定が正しく構成されていません。

アクション
NTP サーバーアドレスとタイムゾーンが正しいことを確認してください。

iLO サービスポートに接続された USB キーのマウントが失敗する

症状
iLO サービスポートに接続された USB キーのマウントが失敗する。

原因
USB キーは、FAT32/exFAT フォーマットでフォーマットされていないか、無効なパーティションテーブルがあります。

アクション
- USB キーが FAT32/exFAT にフォーマットされていることを確認します。フォーマットされていない場合、USB キーを再フォーマットします。
- USB キーが FAT32/exFAT にフォーマットされており、かつマウントされない場合は、Microsoft DiskPart などのユーティリティを使用してそのパーティションを削除して再作成します。

信頼できる証明書をインポートできない

症状
CA から取得した証明書をインポートしようとすると、次のメッセージが表示される。

エラー：提供された X.509 証明書データから証明書をインポートすることができません。

原因
証明書が誤った証明書目的値で作成されています。

アクション
証明書を再度要求します。
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。

iLO のリセット後にサーバーの予期しない動作が発生する

症状
iLO がリセットされた後、サーバーが予期しない動作をします。例えば、BIOS クラッシュが発生したり、Smart アレイの復号化に必要なキーを iLO が取得しなかったりします。
この問題は、サーバーの POST 中に iLO のリセットが開始された場合に発生する可能性があります。iLO のリセットを開始する前に、POST が完了していることを確認することをお勧めします。

アクション
サーバーを再起動します。

システム TPM 測定が失敗する

症状
/redfish/v1/ComponentIntegrity/TPM-0 によるシステム TPM 測定が 400 - Bad Request で失敗する。

原因
現在の BIOS バージョンではシステム TPM がサポートされていません。

アクション
TPM をサポートする BIOS バージョンをインストールします。

SSH を無効に変更すると iLO Web インターフェイスや RESTful API アクセスができなくなってしまう。

症状
iLO7 ファームウェアバージョン 1.21 未満では、iLO Web インターフェイスの[iLO 設定]->[アクセス] > [SSH]から[セキュアシェル(SSH)]を無効に変更すると、HTTP/HTTPS 接続も無効となり iLO Web インターフェイスや RESTful API にアクセスできなくなってしまう場合があります。

アクション
BMC 構成ユーティリティから iLO 工場出荷時デフォルト設定へのリセットを実施してください。

セキュリティログに警告レベルの”PCR Measurement Changed”が登録される。

症状
iLO7 ファームウェアバージョン 1.17.00 と System ROM バージョン 1.44 が適用されている場合、OS 再起動を行うと、iLO セキュリティログに下記のログが採取されるようになります。
■ログメッセージ
PCR Measurements Changed, Component Type <X> PCR Index PCR<Y>
X: コンポーネント名
Y: PCR 番号

アクション
なし。
セキュリティに関する構成変更が発生したことを示すログで、システム運用には影響ありません。

iLO7 ファームウェアバージョン 1.17.00 以降で仮想シリアルポートの出力が表示されない。

症状
VSP コマンドによる仮想シリアルポート表示が行われない。

原因
セキュリティ観点から iLO7 ファームウェアバージョン 1.17.00 以降で、仮想シリアルポートの表示機能(iLO Web インターフェイスの[iLO 設定] > [アクセス] > [仮想シリアルポート] > [ログを表示])のデフォルト値が無効に変更された。

アクション

iLO Web インターフェイスの[iLO 設定] > [アクセス] > [仮想シリアルポート] > [ログを表示]を有効に設定してください。

A. iLO ライセンスオプション

次の表に、各 iLO ライセンスで使用可能な機能に関する情報を示します。

機能の概要に関しては「iLO 機能」を参照してください。

項目	オンボード機能 (Standard)	リモートマネジメント拡張ライセンス (Advanced) N8115-33
Active Health System	X	X
アドバンスト電力管理 (電力履歴グラフ、動的消費電力上限)		X
Agentless Management	X	X
自動 Secure リカバリ		X
バックアップとリストア	X	X
シャーシのパワーレギュレーターモード		X
Commercial National Security Algorithm (CNSA) セキュリティ状態		X
ディレクトリサービス認証		X
ディレクトリサービス		X
Email ベースのアラート		X
内蔵システムヘルス	X	X
ファームウェア検証		X
サーバーの UID ボタンを使用した iLO のリセット	X	X
iLO RESTful API	X	X
iLO Web インターフェイス	X	X
iLO リモートコンソール(IRC/仮想 KVM - テキストと GUI をサポート)	Pre-OS only	X
iLO リモートコンソールの録画および再生		X
IPMI over LAN/DCMI	X	X
IPv6	X	X
Kerberos 認証		X
One-button セキュア消去		X
パフォーマンス監視		X
リモート Syslog		X
スクリプト方式または URL ベースの仮想メディア		X
セキュリティダッシュボード	X	X
サーバー構成ロック		X

サーバーヘルスサマリー	X	X
サーバーシステムの復元		X
Silicon Root of Trust	X	X
Smart アレイのセキュア暗号化		X
SSH コマンドラインインターフェイス	X	X
Two-Factor 認証(Kerberos)		X
サービスアクセス設定のアップデート		X
リモートコンソール経由の仮想メディア		X
仮想電源ボタン	X	X
仮想シリアルポート	X	X
仮想シリアルポートの録画および再生		X
Workload Matching プロファイル	X	X
ワークロードアドバイザー		X
ゾーンマッピング、ゾーンの優先度		X

△**注記:** Pre-OS only では、全てのブータブルメディア・ブータル ISO イメージファイルの起動はできません。

用語集

3DES	トリプル DES。Data Encryption Standard 暗号化アルゴリズム
ACPI	Advanced Configuration and Power Interface
AES	Advanced Encryption Standard
AHCI	Advanced Host Controller Interface
AHS	Active Health System (AHS)は、サーバーの状態や構成を監視し、変化があったときにログとして記録します。Active Health System ログは、保守の場面ですばやく障害の原因を判断するために利用されます。
AMP	Advanced Memory Protection (AMP)は、搭載メモリに対してミラーリング等の制御をすることにより、強固な耐障害性を実現する技術です。
AMS	Agentless Management Service (AMS)は、OS 上で動作し、iLO が直接収集できない OS イベントなどの情報を iLO へ送信するサービスです。 iLO は、このサービスを通じて取得した情報を Active Health System ログとして記録し、Agentless Management へ展開します。
API	Application Programming Interface。アプリケーションプログラミングインターフェイス
ARP	Address Resolution Protocol
ASR	Automatic Server Recovery。自動サーバー復旧
BIOS	Basic Input/Output System。基本入出力システム
BMC	Baseboard management controller
CA	Certificate authority。認証機関
CLP	Command Line Protocol。コマンドラインプロトコル
CN	Common Name。共通名
CNSA	Commercial National Security Algorithm。米 NSA(National Security Agency：国家安全保障局)が定めた暗号スイート。
COM ポート	Communication port。通信ポート
Cookie	Web サイトが特定の設定を保持するために、ハードディスクドライブに保存するスクリプトできない小さいテキストファイルです。サイトに戻ると、システムが前に保存された設定で Cookie を開くので、サイトに設定を渡すことができます。また、Cookie は、一時的にセッションデータを保存するために使用されます。
CR	Certificate request。証明書要求
CSR	Certificate Signing Request。証明書署名要求
CSV	Comma-separated value。カンマ区切りの値
DCMI	Data Center Manageability Interface。データセンター管理インターフェイス
DD	ファイル変換およびコピーに使われる Unix プログラム
DDNS	Dynamic Domain Name System。動的 DNS
DDR	Double data rate。ダブルデータレート
DER	Distinguished Encoding Rules
DHCP	Dynamic Host Configuration Protocol
DHE	Diffie-Hellman key exchange
DIMM	Dual In-line Memory Module。デュアルインラインメモリモジュール。メモリチップを保持する小型回路基板。
DLL	Dynamic-link library。ダイナミックリンクライブラリ
DMTF	Distributed Management Task Force
DN	Distinguished Name。識別名
DNS	Domain Name System。ドメインネームシステム
DSA	Digital Signature Algorithm。デジタル署名アルゴリズム
DVO	Digital Video Out

ECC	Error-correcting code
EMS	Emergency Management Services
ESMPRO/ServerAgentService	ESMPRO/ServerManager と連携し、本機の監視、および各種情報を取得するためのソフトウェアです。インストール時に、OS のサービスとして常駐させる(サービスモード)か、OS のサービスなし(非サービスモード)で動作させるか決めることができます(プリインストール時はサービスモードでインストールします)。非サービスモードで動作させると、CPU、メモリなどのリソースを削減できます。
ESMPRO/ServerManager	ネットワーク上の複数のサーバーの管理、監視を行うソフトウェアです。
EXPRESSBUILDER	本機をセットアップする機能を持つソフトウェアです。本機内に格納され、POST 時に F10 キーを押して起動します。
FAT	File Allocation Table。ファイルアロケーションテーブル
FIPS	Federal Information Processing Standard。連邦情報処理標準。
FQDN	Fully Qualified Domain Name。完全修飾ドメイン名
GMT	Greenwich Mean Time。グリニッジ標準時
GRUB	Grand Unified Bootloader
HPM	Host Processor Module。ホストプロセッサー モジュール
HTML5	HyperText Markup Language 5
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IIS	Internet Information Services。インターネットインフォメーションサービス
iLO	Integrated Lights-Out。標準インターフェイス仕様の IPMI2.0 に準拠してハードウェアを監視するコントローラーです。本機には標準でマザーボード上に組み込まれています。本機で採用しているコントローラーは第 7 世代のため、iLO7 と呼びます。
IML	Integrated Management Log。インテグレーテッドマネジメントログ
IPMI	Intelligent Platform Management Interface
IRC	Integrated Remote Console。iLO リモートコンソール
ISO	International Organization for Standardization。国際標準化機構
JSON	JavaScript Object Notation。JavaScript オブジェクトの表記法
KCS	Keyboard Controller Style
KDC	Key Distribution Center
KDE	K Desktop Environment（Linux 用）
KVM	Keyboard, video, and mouse。キーボード、ビデオ、およびマウス
LDAP	Lightweight Directory Access Protocol
LOM	Lights-Out Management。Lights-Out マネジメント
MAC	Media Access Control
MD5	Message-Digest algorithm 5
MIB	Management information base。管理情報ベース。ネットワーク管理プロトコルでアクセスされる管理対象オブジェクトのデータベース。SNMP MIB は、ネットワークデバイスの SNMP エージェント（ルーターなど）で SNMP 管理ステーションが照会または設定できる 1 組のパラメーターです。
MIME	Multipurpose Internet Mail Extensions
MLD	Multicast Listener Discovery。マルチキャストリスナー検出
MMC	Microsoft Management Console。Microsoft 管理コンソール
MSA	Mail Submission Agent
MTA	Mail Transfer Agent
NAND	Express サーバのマザーボードに組み込まれている、非揮発性のフラッシュメモリのパーティション。NAND 型フラッシュは Active Health System データや EXPRESSBUILDER ソフトウェアなどのファイルに使用されます。
NIC	Network interface card。ネットワークインターフェイスカード。ネットワーク経由のデバイス間の通信を処理するデバイス。
NMI	Non-maskable interrupt。マスク不可能割り込み

NTLM	NT LAN Manager
NTP	Network Time Protocol
NVMe	Non-Volatile Memory Express
NVMe-MI	NVMe Management Interface。規格名称。
OU	Active Directory Organizational Units。Active Directory 組織単位
PAL	Programmable Array Logic。プログラマブルアレイロジック
PIM	Protocol-Independent Multicast。プロトコル独立型マルチキャスト
PKCS	Public-Key Cryptography Standards。公開鍵暗号化標準
POST	Power on self test。電源投入時セルフテスト
PuTTY	SSH、Telnet、rlogin、およびロー TCP プロトコルのクライアントならびにシリアルコンソールクライアントとして機能できる端末エミュレーター。
RAID Report Service	RAID の状態を監視し、障害等が起きたとき、ESMPRO/ServerAgentService へ情報を送信するサービスです。
RBSU	ROM-Based Setup Utility。BMC 構成ユーティリティ。
RDE	Redfish Device Enablement
REST	Representational State Transfer
RESTful インターフェイスツール	Representational State Transfer (REST) アーキテクチャーに基づき設計された API を実装したツールです。本ツールをインストールすると、JSON 形式で記述した保守用コマンドを HTTP プロトコルで iLO へ送信できます。
RPM	RPM Package Manager
RSA	パブリックキー暗号化用のアルゴリズム
SAID	Service Agreement Identifier
SAS	Serial Attached SCSI。シリアル接続 SCSI
SATA	シリアル ATA。ATA(IDE)インターフェイスから発展したもので、物理アーキテクチャーをパラレルからシリアルに変更し、プライマリー/セカンダリー(マスター/スレーブ)からポイントツーポイントに変更します。プライマリー(マスター)とセカンダリー(スレーブ)として 2 台のドライブを接続するパラレル ATA インターフェイスと異なり、SATA ドライブは個別のインターフェイスに接続されます。
SD	Secure Digital
SHA	Secure Hash Algorithm。セキュアハッシュアルゴリズム
SID	Security Identifier。セキュリティ識別子
SLAAC	Stateless Address Autoconfiguration
SMASH	Systems Management Architecture for Server Hardware
SMS	System Management Software。システム管理ソフトウェア
SNMP	Simple Network Management Protocol。簡易ネットワーク管理プロトコル
SNTP	Simple Network Time Protocol。簡易ネットワークタイムプロトコル
SPN	Service Principal Name。サービスプリンシパル名
SPP	Standard Program Package (SPP)は、BIOS/FW、および OS ドライバなどを含む基本的な FW/SW をまとめたパッケージです。SPP は、Starter Pack に含まれます。
SSA	Smart Storage Administrator (SSA)は、ディスクアレイコントローラーを設定して RAID を構築するユーティリティです。Windows または Linux 上にインストールして使用するほか、本機に組み込まれた EXPRESSBUILDER から起動できます。
SSD	Solid-State Drive。ソリッドステートドライブ
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On。Zero サインイン
Starter Pack	SPP、管理用アプリケーション、および電子マニュアルを含むソフトウェアパッケージです。Starter Pack はオプション製品として購入、または Web からダウンロードし、Windows/Linux OS 上で使用します。
SUM	Software Update Manager

TLS	Transport Layer Security。トランスポート層セキュリティ
TM	Trusted Module
TPM	Trusted Platform Module
TPM キット	セキュリティーコントローラーを本機に増設するためのオプション製品です。
UBM	Universal Backplane Manager。UBM(n)は UBM モデルで、バックプレーンで使用される UBM ファームウェア(バージョン)を示します。
UDP	User Datagram Protocol。ユーザーデータグラムプロトコル
UEFI	Unified Extensible Firmware Interface
UHCI	Universal Host Controller Interface。ユニバーサルホストコントローラーインターフェイス
UID	Unit identification。ユニット識別子
UPN	User Principal Name。ユーザープリンシパル名
UPnP	Universal Plug and Play。ユニバーサルプラグアンドプレイ
UPS	Uninterruptible Power Supply。無停電電源装置
USB	Universal serial bus。ユニバーサルシリアルバス。デバイスを接続するために使用されるシリアルバス規格。
USM	User-based Security Model
UTC	Coordinated Universal Time。協定世界時
UTP	Unshielded Twisted Pair。シールドなしツイストペア
UUID	Universally Unique Identifier。ユニバーサルー意識別子
VSP	Virtual Serial Port。仮想シリアルポート
WBEM	Web-Based Enterprise Management
WINS	Windows インターネットネームサービス
エクスプレス通報サービス	電子メールなどを使い、本機が故障したときの情報(または予防保守情報)を保守センターに通報するソフトウェアです。ESMPRO/ServerAgentService または ESMPRO/ServerAgent とともに本機にインストールします。
エクスプレス通報サービス (HTTPS)	HTTPS 経由で、本機が故障したときの情報(または予防保守情報)を保守センターに通報するソフトウェアです。ESMPRO/ServerAgentService とともに本機にインストールします。
管理 PC	ネットワーク上から本機にアクセスし、本機を管理するためのコンピューターです。Windows または Linux がインストールされた一般的なコンピューターを管理 PC にすることができます。
システムメンテナンススイッチ	本機マザーボード上の DIP スイッチで、保守の場面において、初期化、パスワード、iLO セキュリティなどの機能をオンオフするときに使用します。
システムユーティリティ	システムユーティリティは、本機内に格納され、システム情報の確認、RBSU の呼び出し、およびログの採取機能などを提供します。システムユーティリティは POST 時に F9 キーを押すと起動します。
装置情報収集ユーティリティ	本機の各種情報を収集するためのソフトウェアです。保守に必要な情報をまとめて採取できます。
ターシャリー	プライマリー、セカンダリーに続く、「3 番め」を意味する単語です。
ヘクサロビュラ	ヘクスローブ、またはトルクス(「トルクス」は他社商標です)とも呼ばれるネジ規格です。サイズは小さい順から、T1 から T100 まで決められ、サイズに合わない工具を使うとネジを傷める可能性があります。6lobe と略すこともあります。

NEC Express5800 シリーズ

iLO7 ユーザーズガイド

2026 年 6 月
日 本 電 気 株 式 会 社
東京都港区芝五丁目 7 番 1 号
TEL(03)3454-1111 (大代表)