



**Hewlett Packard  
Enterprise**

## Smart Update Manager お使いになる前に

### 摘要

このガイドでは、SUM を使用して、HPE Synergy、Edgeline、ProLiant サーバーにファームウェアアップデートを適用し、ProLiant サーバーにソフトウェアアップデートを適用する方法について説明します。このガイドは、Microsoft Windows、Windows Server、Linux、Smart コンポーネント、VMware の構成および操作、ならびにアップデートの実行に伴うデータ消失の危険性について理解している SUM の新規ユーザーを対象にしています。

部品番号: 882463-197  
発行: 2019 年 12 月  
版数: 1

## ご注意

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

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

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

## 商標

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

UNIX<sup>®</sup>は、The Open Group の登録商標です。

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

# 目次

<b>SUM の概要</b> .....	<b>5</b>
<b>はじめに</b> .....	<b>6</b>
ローカルサーバーの更新.....	6
リモートサーバーの更新.....	6
<b>アップデートのダウンロード</b> .....	<b>7</b>
SPP カスタムダウンロードのダウンロード.....	7
個々のコンポーネントのダウンロード.....	7
<b>ブラウザーのセキュリティ証明書のインポート</b> .....	<b>8</b>
ブラウザーのセキュリティ証明書について.....	8
Firefox へのセキュリティ証明書のインポート.....	8
Google Chrome へのセキュリティ証明書のインポート.....	8
Internet Explorer へのセキュリティ証明書のインポート.....	8
<b>ローカルホストサーバーの更新</b> .....	<b>9</b>
ISO から GUI モードでの SUM の起動.....	9
ローカルホストガイドアップデートの使用.....	9
ノードレポートの生成.....	9
<b>リモートサーバーの更新</b> .....	<b>11</b>
ISO から GUI モードでの SUM の起動.....	11
IP または DNS 名を使用して 1 つのノードを追加する.....	11
ノードのインベントリの実行.....	12
ノードの展開.....	13
Absaroka と OS を介したオンラインアップデート.....	16
使用される SUM のネットワークポート.....	17
ベースラインの追加.....	18
<b>一般的な問題</b> .....	<b>20</b>
SUM がポートエラーを報告する.....	20
SUM がコンポーネントを検証しない.....	20
SUM がノードに接続できない.....	20
<b>Web サイトおよびサポート</b> .....	<b>22</b>
Web サイト.....	22
サポートと他のリソース.....	22
Hewlett Packard Enterprise サポートへのアクセス.....	22
アップデートへのアクセス.....	23
リモートサポート (HPE 通報サービス) .....	23
保証情報.....	24

規定に関する情報.....	24
ドキュメントに関するご意見、ご指摘.....	24

# SUM の概要

SUM は、ProLiant サーバー、BladeSystem エンクロージャー、およびその他のノードのファームウェア、ドライバー、およびソフトウェアのメンテナンスツールです。

この「お使いになる前に」はサーバーの更新に役立ちます。

SUM の使用について詳しくは、<https://www.hpe.com/info/sum-docs> にある Smart Update Manager ユーザーガイドを参照してください。

SUM の前提条件については、<https://www.hpe.com/info/sum-docs> にある Smart Update Manager リリースノートを参照してください。

SUM の主な機能は、次のとおりです。

- ・ SUM は、ノード上にインストールされたハードウェア、ファームウェア、およびソフトウェアのバージョンを検出します。
- ・ SUM は、アップデートを正しい順序で展開します。また、アップデートの展開前にすべての依存関係が満たされていることを確認します。
- ・ 複数のリモートノード用のファームウェアとソフトウェアの同時展開。

コマンドライン経由でのサーバーの更新方法について説明が必要なユーザーは、Smart Update Manager CLI および対話側 CLI ガイド (<http://www.hpe.com/info/sum-docs>) を参照してください。

# はじめに

## ローカルサーバーの更新

ローカルサーバーを自動的に更新するには、以下の手順を実行します。

ノードを手動で更新する場合は、リモートサーバーの更新手順に従います。SUM が SUM を実行するノードを自動的に追加するため、リモートノードを追加する必要はありません。

### 手順

1. SPP をダウンロードするか、または SPP カスタムダウンロードをダウンロードします。
2. 更新するサーバーに ISO をマウントまたはコピーします。
3. GUI モードで SUM を起動します。
4. Localhost ガイド付きアップデートを使用します。
5. オプション : SUM を使用してレポートを生成します。

## リモートサーバーの更新

リモートサーバーにアップデートを展開するには、以下の手順を実行します。

### 手順

1. SPP カスタムダウンロードをダウンロードします。
2. ローカルシステムに ISO をマウントまたコピーします。
3. GUI モードで SUM を起動します。
4. リモートノードを追加します。
5. リモートノードでインベントリを実行します。
6. リモートノードにアップデートを展開します。
7. オプション : SUM を使用してレポートを生成します。

# アップデートのダウンロード

## SPP カスタムダウンロードのダウンロード

以下の設定が可能です。

- ・ カスタム SPP を作成する。
- ・ 使用可能なファイルをダウンロードする。
- ・ カスタム SPP を削除する。デフォルトの SPP は、ページから削除できません。

SPP カスタムのダウンロードページのヘルプについては、[SPP カスタムダウンロードの FAQ](#) ページを参照してください。

### 手順

1. Web ブラウザーを開き、<https://spp.hpe.com/custom> にアクセスしてください。
2. SPP へのアクセスは、HPE サポートセンターを介して確認する必要があります。アクティブ保証または HPE のサポート契約は、SPP をダウンロードするために必要とされます。詳しくは、[SPP 保証/サポート契約の確認に関するドキュメント](#)を参照してください。HPE パスポートへのログインが必要です。
3. 必要に応じて、**HPE パスポートサインイン**をクリックして、HPE パスポートユーザーの認証情報を入力します。
4. ページの左側から、SPP を選択します。

## 個々のコンポーネントのダウンロード

SUM 8.0 以降では、展開するコンポーネントに、有効な署名ファイルが含まれていることを検証します。コンポーネントをダウンロードする場合、必ず、関連する .compsig ファイルをダウンロードして、同じディレクトリに保存します。

# ブラウザのセキュリティ証明書のインポート

## ブラウザのセキュリティ証明書について

初めて SUM を起動すると、証明書の問題が表示される場合があります。ご使用のブラウザに証明書をインポートして、今後 SUM を起動したときに、この問題がブラウザに表示されないようにします。

## Firefox へのセキュリティ証明書のインポート

### 手順

1. オプションを開き、**詳細 > 証明書 > 証明書を表示**を選択します。
2. インポートをクリックして、SUM ディレクトリ `packages\assets\certificates` に移動します。**CA.crt** ファイルを選択します。
3. **Trust CA to identify websites** を選択します。
4. ブラウザーのキャッシュをクリアして、ブラウザを閉じます。
5. ブラウザーを起動します。

## Google Chrome へのセキュリティ証明書のインポート

### 手順

1. Chrome の設定を開いてから、**詳細設定を表示**をクリックします。
2. **HTTPS/SSL セクションで証明書の管理**をクリックします。
3. インポートをクリックして、SUM ディレクトリ `packages\assets\certificates` に移動します。**CA.crt** ファイルを選択します。証明書を**信頼されたルート証明機関**のストアに配置します。
4. ブラウザーのキャッシュをクリアして、ブラウザを閉じます。
5. ブラウザーを起動します。

## Internet Explorer へのセキュリティ証明書のインポート

### 手順

1. **インターネットオプション**をクリックして**コンテンツ**を選択し、Internet Explorer のバージョンに応じて**証明書**または**証明書の表示**を選択します。
2. インポートをクリックして、SUM ディレクトリ `packages\assets\certificates` に移動します。**CA.crt** ファイルを選択します。証明書を**信頼されたルート証明機関**のストアに配置します。
3. ブラウザーのキャッシュをクリアして、ブラウザを閉じます。
4. ブラウザーを起動します。



# ローカルホストサーバーの更新

## ISO から GUI モードでの SUM の起動

Windows または Linux オペレーティングシステム上で SUM を実行します。

**注記:** SUM を起動するときに Windows ノードに CHIF ドライバーがないと、SUM は CHIF ドライバーを自動的にインストールします。CHIF ドライバーのインストールをスキップするには、`/skip_prereqs` パラメーターを使用します。

### 手順

1. ISO からローカルホストにファイルをコピーします。
2. ISO を含むディレクトリから `launch_sum.bat` (Windows) または `launch_sum.sh` (Linux) を実行します。

**注記:** Gnome 仮想ファイルシステムを使用する場合は、手動で ISO を抽出し、ディレクトリに保存します。次に、SUM を起動します。

## ローカルホストガイドアップデートの使用

### 手順

1. ナビゲーションメニューのローカルホストガイドアップデートをクリックします。
2. 自動をクリックします。

**注記:** サーバーの iLO が高セキュリティモードのいずれかで構成されているか、またはホスト認証が必要を有効にしている場合は、iLO 管理者の認証情報の入力が必要です。更新を続行するには、認証情報を入力するか、iLO で高度なセキュリティモードを無効にします。

3. SUM は、ローカルホスト用に選択された現在のベースラインを表示します。
  - a. 現在選択されているベースラインを使用する場合は、次の手順に移ります。
  - b. 別のベースラインを使用する場合は、ベースラインの横にある **X** をクリックします。別のベースラインまたは追加のパッケージを選択するには、異なるベースラインの割り当てを選択します。
4. **OK** をクリックします。

**注記:** **OK** をクリックすると、SUM がアップデートの展開を開始します。ローカルホストガイドアップデート機能の自動モードでは、アップデートを中断することはできません。自動モードでは、SNMP および WBEM Provider コンポーネントはインストールできません。これらのコンポーネントをインストールする場合は、対話式モードを使用してください。

## ノードレポートの生成

ノードの詳細、インストール可能なコンポーネント、失敗した依存関係を含め、SUM セッションに関する詳細情報を表示するレポートを生成できます。

ノードのレポートは、HTML、XML、および CSV 形式で作成できます。SUM は、レポート画面のレポートセンターに、以前に生成したレポートを表示します。

---

**注記:** SUM は、すべてのノードタイプに対して、同じ機能を使用レポートを生成します。

---

## 手順

1. ノード画面でノードを選択して、**アクション > レポート**の順に選択します。
2. 生成するレポートを選択します。

### ファームウェアの詳細

ノードに現在インストールされているファームウェアのバージョンが表示されます。

### 展開プレビュー

ノードにインストールできるコンポーネントが表示されます。

### 失敗した依存関係の詳細

ノードでの失敗した依存関係が表示されます。

### 展開詳細

ノードにインストールした内容の詳細が表示されます。

### インベントリ

ベースラインにどのコンポーネントが含まれているかについて、詳細が表示されます。

### 統合レポート

各レポートタイプのうちの 1 つが生成されます。

---

**注記:** レポートを選択できない場合は、SUM にとってレポートを生成する情報が十分でないことが考えられます。

---

3. SUM で生成するレポートの形式 (**HTML**、**CSV**、または **XML**) をクリックします。

---

**注記:** HTML および XML のレポートは、JavaScript 対応のブラウザで表示できます。

---

4. **高度なレポートオプション**では、次のことを行うことができます。

- a. レポートを保存するディレクトリを選択します。ディレクトリが存在しない場合は、SUM が作成します。

---

**注記:** Windows クライアントのデフォルト位置は `C:\cpqsystem\sum\log` です。

---

- b. レポートをバックグラウンドで実行するかどうかを選択します。

5. **生成**をクリックします。

# リモートサーバーの更新

## ISO から GUI モードでの SUM の起動

Windows または Linux オペレーティングシステム上で SUM を実行します。

**注記:** SUM を起動するときに Windows ノードに CHIF ドライバーがないと、SUM は CHIF ドライバーを自動的にインストールします。CHIF ドライバーのインストールをスキップするには、`/skip_prereqs` パラメーターを使用します。

### 手順

1. ISO からローカルホストにファイルをコピーします。
2. ISO を含むディレクトリから `launch_sum.bat` (Windows) または `launch_sum.sh` (Linux) を実行します。

**注記:** Gnome 仮想ファイルシステムを使用する場合は、手動で ISO を抽出し、ディレクトリに保存します。次に、SUM を起動します。

## IP または DNS 名を使用して 1 つのノードを追加する

### 手順

1. ノード画面で、**+ノードの追加**をクリックします。
2. 選択操作ドロップダウンリストから**単一ノードあるいは既存の範囲のノードを追加**を選択します。
3. IP アドレス、DNS 名、IP アドレスの範囲、またはコマンドで区切られた複数のアドレスを入力します。たとえば、「10.0.1.1 - 10.0.1.20」と入力すると、20 個のノードが追加されます。「10.0.1.1, 10.0.1.2, 10.0.1.7」と入力すると 3 つのノードが追加されます。ノードが同じ認証情報を使用する場合、SUM はノードを追加します。

### 注記:

- ・ サポートされている DNS 文字セットは、ASCII のみ (A~Z、a~z、アンダースコア、ドット、ハイフンを含む 0~9) です。

最大 50 のノードを追加できます。

- ・ VC ノードを追加する場合は、プライマリ Enet モジュールの IP アドレスを使用します。FC モジュールを含めて、インストールされているすべての VC モジュールが、プライマリ Enet モジュールを通して更新されます。

4. ノードの説明を入力します。
5. **ノードタイプ**フィールドで、ノードタイプを選択します。ノードタイプがわからない場合は、**不明**を選択します。インベントリプロセスの実行中に SUM がノードタイプを決定します。  
一部のノードでは、SUM による自動の検出および関連するノードの追加が可能です。

**注記:** 正しいノードタイプを選択すると、ノードのインベントリをより速く追加することができます。

- オプション：前提条件となるインベントリコンポーネントのインストールをスキップするには、**前提条件コンポーネントがまだインストールされていない場合はインストールします**チェックボックスをクリアします。

❗ **重要:** このアクションを実行すると、SUM が完全なインベントリを実行しないというシナリオが発生する可能性があります。このような場合に更新を完了するには、セッションが2つ必要になる場合があります。

- オプション：このノードに適用するベースライン、追加パッケージ、またはその両方を選択します。
- オプション：リストからグループを選択します。
- 次のいずれかを選択します。

- ・ **現在の認証情報を使用（ノードとの既存の信頼関係が必要）：**このオプションは、Windows ノードのみを対象としています。
- ・ **管理者の認証情報を入力：**ノードに対する管理者権限を持つユーザーのユーザー名とパスワードを入力します。Windows ユーザーに管理者権限がある場合は、ドメイン\ユーザー名を使用します。

- Linux ノードでは、ルート認証情報を使用してノードにログインせずに、sudo 認証情報を使用してアップデートを展開できます。sudo コマンドを使用するには、ノードに sudo 機能をインストールする必要があります。

**注記:** すべてのノードでスーパーユーザーおよび sudo を使用できるわけではありません。

直接 root 権限がないアカウントを使用する場合、**アクセスレベル**フィールドで以下のいずれかを選択します。

- ・ sudo の認証情報を使用する場合、**ここまでの操作で入力した認証情報で、sudo を使用する**をクリックします。
- ・ スーパーユーザーの認証情報を入力する場合は、**コンポーネントをアップデートするためにスーパーユーザーの認証情報を入力してください**をクリックします。

**注記:** スーパーユーザーの認証情報を使用する場合は、**認証情報**フィールドに通常ユーザーの認証情報を入力してから、**アクセスレベル**フィールドにスーパーユーザーの認証情報を追加します。SUM は、まず通常ユーザーの認証情報でログインしてから、スーパーユーザーの認証情報でスーパーユーザーのアカウントにログインします。

- サーバーの iLO が高セキュリティモードのいずれかで構成されているか、またはホスト認証が必要を有効にしている場合は、指定された iLO 認証情報セクションに iLO 管理者の認証情報を入力します。
- 追加**をクリックします。  
ノードの**追加**セクションに、選択したノードが表示されます。

## ノードのインベントリの実行

ノードインベントリは、ノードに関する情報、そのノードにインストールされているファームウェア、ソフトウェア、ドライバのバージョンに関する情報を収集します。SUM は、コンポーネントの依存関係が見つからない場合はこれを検出します。

SUM は、新しい各セッションの実行中に、ノードのインベントリを実行して、ノード上のファームウェアやソフトウェアを確認する必要があります。

認証情報が無効な場合、SUM はノードのインベントリを実行できません。ノードの認証情報が無効な場合は、認証情報を編集してください。

**注記:** OA ノードでインベントリを実行する場合、SUM が関連ノードを自動的に追加してインベントリを実行します。関連ノードを追加するには、ノードの追加画面でチェックボックスを選択します。VC の認証情報は別々に追加します。ここでブレード iLO または VC のインベントリを実行しても、SUM はインベントリ処理が終了するまで関連 OA を検索しません。OA に認証情報を追加してから、OA ノードのインベントリを実行してください。

## 手順

1. ノード画面で、ノードをハイライトして**アクション > インベントリ**の順に選択します。
2. ノードに関連するベースラインが表示されます。インベントリに使用されるベースラインを再割り当てする場合は、ベースライン、追加のパッケージ、またはその両方を選択します。  
Gen10 サーバーでは、**インベントリページ**でベースラインとして保存したインストールセットを選択できます。
3. **インベントリ**をクリックします。SUM は、アップデートを展開する前に解決する必要があるエラーを表示します。

## ノードの展開

展開画面では、展開するノードの設定を変更できます。以下を変更できます。

- ・ インストールオプション。
- ・ 再起動オプション。
- ・ iLO レポジトリオプション (Gen10 iLO 5 Windows および Linux ノードのみ)。
- ・ 展開するコンポーネント。コンポーネントの構成は、ベースラインライブラリ画面から行ってください。

### ❗ 重要:

- ・ サポートされているオペレーティングシステムを実行している仮想マシン上で SUM を実行する場合は、ローカルホストシステムにアップデートを展開しないでください。リモートノードのホスト OS、またはそれらのノードの iLO にアップデートを展開します。
- ・ SUM で展開ボタンがアクティブになっている場合は、SUM が管理するコンポーネントの更新またはダウングレードを手動で実行しないでください。コンポーネントを手動で更新すると、SUM ではコンポーネントがスキップされてエラーが報告されます。
- ・ SUM 8.5.0 は、HPE VC Flex-20 Enet モジュール上のファームウェアバージョン 4.80 のフラッシュをブロックします。
- ・ SUM は、iLO 5 ファームウェアを v2.10 に更新する前に v1.40 をフラッシュします。これは、ファームウェア v2.10 をフラッシュするための前提条件であるためです。

## 手順

1. ノード画面で、アップデートするノードを選択して**アクション > レビュー/展開**の順に選択します。
2. **インストールオプション**タブを選択して以下を変更します。

---

**注記:** ベースラインに同じ製品のバージョンが複数ある場合は、同じコンポーネントの別バージョンから1つだけを選択できます。同じバージョンの他のコンポーネントを選択すると、すでに選択されているコンポーネントが自動的にクリアされます。以下の場合、より新しいバージョンのコンポーネントがデフォルトで選択されます。

- ・ ダウングレードおよび再書き込みのオプションが設定されている。
- ・ より新しいバージョンのコンポーネントがインストールされていない。

- 
- ・ インストールオプション

#### **ファームウェアおよびソフトウェアのアップグレード**

ファームウェアコンポーネントおよびソフトウェアコンポーネントをアップグレードします。

#### **ファームウェアのアップグレード**

ファームウェアコンポーネントだけをアップグレードします。

#### **ソフトウェアのアップグレード**

ソフトウェアコンポーネントだけをアップグレードします。

#### **両方のダウングレードおよび書き換え**

ファームウェアコンポーネントおよびソフトウェアコンポーネントを、アップグレード、ダウングレード、および再書き込みします。

#### **ファームウェアのダウングレードおよび書き換え**

ファームウェアコンポーネントだけを、アップグレード、ダウングレード、および再書き込みします。

#### **ソフトウェアのダウングレードおよび書き換え**

ソフトウェアコンポーネントだけを、アップグレード、ダウングレード、および再書き込みします。

#### **両方のダウングレード**

ファームウェアコンポーネントおよびソフトウェアコンポーネントをアップグレードおよびダウングレードします。

#### **ファームウェアのダウングレード**

ファームウェアコンポーネントだけを、アップグレードおよびダウングレードします。

#### **ソフトウェアのダウングレード**

ソフトウェアコンポーネントだけを、アップグレードおよびダウングレードします。

#### **両方の書き換え**

ファームウェアコンポーネントおよびソフトウェアコンポーネントを、アップグレードおよび再書き込みします。

#### **ファームウェアの書き換え**

ファームウェアコンポーネントだけを、アップグレードおよび再書き込みします。

#### **ソフトウェアの書き換え**

ソフトウェアコンポーネントだけを、アップグレードおよび再書き込みします。

- ・ 詳細ログまたは通常ログ

- ・ 依存エラーのあるコンポーネントをスキップ
- ・ 展開後に一時ファイルをクリーンアップするかどうかを選択
- ・ 展開後にデバッグログと一時ファイルをクリーンアップするかどうかを選択

---

**注記:** OA が FIPS モードである場合、SUM は、ファームウェアのダウングレードや再書き込みをサポートしません。SUM ではメッセージが表示され、ダウングレードと再書き込みのオプションがオフになります。

---

3. 再起動オプションタブで、次の選択を行います。

- a. システムの再起動オプション: なし、必要な場合、常時。
- b. ノードを再起動する前に SUM が遅延する分数を入力します。1~60 分の間で選択します。
- c. 表示する再起動メッセージを 255 文字以内で入力します。

---

**注記:** SLES12 OS イメージには cli コマンドとしてパラメーターを実行できないという制約があるため、`reboot_message cli` パラメーターは SLES12 OS では機能しません。

---

4. Gen10 iLO 5 Windows および Linux および iLO 5 ノードのみ : iLO レポジトリを管理するには、**iLO レポジトリオプション**タブを選択します。

- a. 選択したコンポーネントを iLO レポジトリにアップロードし、インストールセットを作成するには、**コンポーネントをインストールセットとして iLO レポジトリに保存**を選択します。SUM によって自動的に名前と説明が作成されますが、インストールセットの名前と説明を編集することができます。このインストールセットを使用して、今後、サーバーコンポーネントをロールバックできます。名前と説明は 63 文字に制限されており、使用できる特殊文字は `-` と `_` だけです。

---

**注記:** サーバーオペレーティングシステムまたは iLO を介して、SUM を使用して、ファームウェアとソフトウェアをアップデートできます。これらの方法の利点については、[Absaroka と OS を介したオンラインアップデート](#)を参照してください。

---

- b. 以前のリカバリセットを更新するには、**コンポーネント (BIOS、iLO、CPLD) を使用して既存のリカバリセットをこの実行で更新する**チェックボックスを選択します。SUM は、iLO、BIOS、および CPLD の新しいファームウェアバージョンを使用して、iLO レポジトリ内の既存のリカバリセットを現在の展開からアップデートします。
- c. 展開の開始および終了の時刻を設定するには、**スケジュールの設定**をクリックします。または、**メンテナンスウィンドウ**を選択します。
- d. 次のいずれかを選択します。
  - ・ **SUM が iLO レポジトリスペースを管理します** : 必要に応じて、SUM が iLO レポジトリ上にスペースを自動的に作成します。SUM は以下の内容を削除します。
    - 最初に、参照されていないコンポーネント。
    - 最も古いインストールセット。iLO レポジトリには最大 8 個のインストールセットを保存できます。
  - ・ **iLO レポジトリスペースを手動で管理** : 削除するインストールセットまたは参照されていないコンポーネントを選択し、iLO レポジトリの空き領域を増やします。

5. ベースラインタブおよび追加のパッケージタブで、展開するコンポーネントを選択します。

iLO 5 ノードへのアップデートを展開する場合、SUM では、ノードで実行しているオペレーティングシステムに基づいてコンポーネントが自動的に選択されます。ノードがオフの場合、SUM ではファームウェアコンポーネントがすべて選択されます。システムに Agentless Management System (AMS) が存在しない場合、iLO は OS の詳細を取得しません。このような場合、SUM ではファームウェアコンポーネントのみが選択されます。

Absaroka アップデートを実行する場合、システムに iSUT がインストールされていることを確認してください。

---

**注記:** Gen10 iLO 5 ノードでは、すべてのコンポーネントに、コンポーネント署名ファイルを含める必要があります。署名ファイルが見つからない場合、SUM では展開ボタンが無効になります。署名ファイルがないコンポーネントの選択を解除し、他のアップデートを展開します。

---

6. **展開**をクリックします。SUM は、ユーザーが加えたすべての変更が有効であることを確認し、コンポーネントの展開を開始します。

---

**注記:** 展開を開始するには、依存関係のすべての問題を解決する必要があります。またはコンポーネントをクリアして、インストールされないようにします。

---

7. ノード画面の一般セクションで、ノードの**ログの参照**をクリックした後、インストールしたコンポーネントの**ログの参照**をクリックしてインストールの詳細を確認します。

---

**注記:** SUM がアップデートを展開中に、展開のステータスを確認するには、ノードのページで **Live Log** ボタンをクリックします。

---

## Absaroka と OS を介したオンラインアップデート

Gen10 サーバプラットフォームのファームウェアとソフトウェアのオンラインアップデートでは、サーバオペレーティングシステムを介して、または iLO と iLO レポジトリを介して SUM を使用できます。iLO レポジトリベースのアップデートでは、検出とアップデートプロセスのほとんどが、iLO 5 の Redfish Absaroka サポートを使用して処理されます。

2つの方法を使用する利点は次のとおりです。

- ・ **Absaroka**

- 本番環境ネットワークトラフィックに追加されません。
- 事前にステージングでき、メンテナンスウィンドウ中にインストールできます。
- 将来のロールバック用にインストールセットの作成が含まれます。

- ・ **OS を介したオンラインアップデート**

Absaroka と異なり、オペレーティングシステムを介したオンラインアップデートでは、すべてのドライバと一部のファームウェアコンポーネントを確実にインストールするために iSUT をインストールする必要はありません。

---

**注記:** USB キューティリティまたは iLO 仮想メディアを使用して、オフラインアップグレードを実行することもできます。このアップグレード方法では、サーバオペレーティングシステムを必要とせず、プロビジョニングに役立ちます。

---



## 使用される SUM のネットワークポート

SUM では、特定のネットワークポートが使用可能である必要があります。ネットワークポートをロックダウンする場合は、ネットワークポートテーブルにリストされているポートが開いていて SUM がリモートのノードサーバーやホストに接続する際に正しく機能するかどうかを確認してください。これらのネットワークポートのロックを解除できない場合は、SUM をローカルで実行し、ネットワークベースのホストをその Web インターフェイス経由でアップデートする必要があります (OA、iLO、VC モジュールなど)。

**注記:** SUM で、必要なファイアウォールポートをローカルホストおよびリモートサーバーで自動的に開くには、`open_firewall` パラメーターを使用します。

ほとんどのノードタイプのアップデートには、SUM を実行するサーバーとノード間の双方向のネットワークトラフィックが必要です。SUM を実行するサーバーはローカル HTTP サーバーを作成します。このサーバーはファームウェアバイナリをノードに提供したりノードのステータスを通知したりするために使用されます。アップデートプロセスの進行中、リモートノードは HTTP リクエストを発行し、SUM を実行するサーバーにステータスのアップデート情報を提示します。ルーティングの問題が発生する場合、またはリモートノードから SUM を実行しているシステムに戻るトラフィックをファイアウォールがブロックする場合は、ファームウェアのアップデートのブロック、ステータス更新のブロックまたは遅延、あるいはその両方が発生している可能性があります。

SUM トラフィックは、初期通信の作成によって使用できるポートのいずれかにバインドされた後、専用の大きいポート番号 (1024 より大きい番号) に移すことができます。こうすることで、最初のポートを解放して新しいリクエストで使用できます。

SUM を実行中のシステム	ターゲットのノードタイプ	インベントリフェーズ		展開フェーズ	
		ターゲットへ	ターゲットから (SUM 7.3.0 以降)	ターゲットへ	ターゲットから (SUM 7.3.0 以降)
Windows	Windows	445、135、137、138、139	なし	445、135、137、138、139	なし
Windows または Linux	Linux	22	なし	22	なし
Windows または Linux	VMware: Gen9 および以前のサーバー世代のみ	443、5989	63001	443、5989	63001
Windows または Linux	OA	22、(80)、443	なし	22、(80)、443	なし
Windows または Linux	Superdome X	22、(80)、443	なし	22、(80)、443	63001、63002

表は続く

SUM を実行中のシステム	ターゲットのノードタイプ	インベントリフェーズ	展開フェーズ
Windows または Linux	iLO、VC、FC スイッチ、SAS スイッチ	22、(80)、443 なし	22、(80)、443 63001
Windows または Linux	Superdome Flex	443 なし	443 63002

SUM は、Windows および Linux の両方のシステムで、ポート 63002 を使用して `sum_binary` アプリケーションおよび `sum_service` アプリケーションの間で通信します。ポートが両方の列に表示されている場合、双方向通信が行われます。

#### 注記:

- Windows から Windows へのトラフィックでは、WMI、つまり標準の DCOM-In ポート 135、Async-in、および WMI-in を使用します。
- iLO レポジトリを使用するには、iLO を「ターゲットのノードタイプ」として使用する必要があります。

ファイアウォールの競合がある場合は、`/port` パラメーターと `/ssl_port` パラメーターを使用して、ポートを 63001 および 63002 から変更します。`/open_firewall` を使用して、SUM が外部アクセスに使用する HTTP ポートと HTTPS ポートを開きます。リモートノード機能やリモートブラウザアクセスを実行するには、これらのポートを開きます。以下に例を示します。

```
smartupdate /port 80 /ssl_port 443
```

`/ftp_port` パラメーターを使用して、FTP サービスで使用するポートを割り当てることができます。デフォルトでは、FTP ポートは無効です。このオプションで Web サービスを有効にします。

## ベースラインの追加

### 手順

- ベースラインライブラリ画面で、**ベースラインを追加**をクリックします。

**注記:** ベースラインの追加画面をクリアする場合は、**最初からやり直す**をクリックします。

ベースラインの追加画面が開きます。

- ベースラインを追加またはカスタムを作成を選択します。
- 追加するベースラインのタイプを選択し、必要な情報を含めます。
  - SUM サーバーパスを参照

- SUM を実行しているシステムがアクセスできるディレクトリまたはファイル共有です。
  - ベースラインへのディレクトリパスを入力するか、**一覧**をクリックし、メニューを使用してディレクトリに移動します。
- ・ **UNC パス (例 : \\host\dir)**
- システムがアクセスできる UNC パスを使用します。**ベースラインの URI を入力**フィールドに、ソースベースラインの UNC アドレスを入力します。ユーザー名とパスワードを入力します。

**注記:**

- UNC パスは、Windows システムのみでサポートされています。
- SUM では、マッピングされた UNC ドライブをサポートしていません。

・ **http 共有からダウンロード**

- **ディレクトリパスを入力** : ベースラインを保存するディレクトリを入力するか、そのディレクトリに移動します。必要な場合、ディレクトリを作成します。
- **HTTP URL を入力** : バンドルファイルが保存されている HTTP URL を入力します。サーバーは、ローカルでもリモートでも構いません。また、Apache、Tomcat、または IIS サーバーを使用できます。バンドル XML を含む、完全な URL を入力してください。コンポーネントは、バンドル XML と同じディレクトリに存在する必要があります。ベースラインのために十分なローカルの空き容量があることを確認します。

特定のオペレーティングシステム用のコンポーネントをダウンロードする場合は、**OS フィルターオプション**で、オペレーティングシステムを選択します。

**注記:** SUM は、ディレクトリ内で見つかったすべてのベースラインを追加します。

**4. 追加をクリックします。**

ベースラインのステータスを確認するには、アクティビティログを確かめます。ベースラインリストにベースラインが表示されない場合は、ディレクトリにアップデートが存在するかどうかを確認してください。

**注記:** ベースラインの追加を完了するとすぐに、SUM がベースラインのインベントリを開始します。別のベースラインを追加する場合は、ベースラインのインベントリが完了するまで待ってから作業を開始します。

# 一般的な問題

## SUM がポートエラーを報告する

### 症状

SUM がブロックされたポートに関するエラーを報告するか、またはポートから切断しない。

### アクション

1. SUM を終了し、システムを再起動します。
2. `sum.ini` で使用されているポートをクリアします。
3. SUM を起動します。

意図的にポートをブロックした場合は、システムを再起動してもポートのブロックが解除されません。手動でポートのブロックを解除してから、SUM を起動します。

## SUM がコンポーネントを検証しない

### 症状

ベースラインライブラリ画面で、コンポーネントが検証されません。

### 原因

`compsig` ファイルが見つかりません。Gen10 サーバーと VMware ノードには、アップデートを展開する前に `compsig` ファイルが必要です。

### アクション

1. ベースラインのディレクトリからコンポーネントを削除します。
2. コンポーネントの新しいコピーをベースラインのディレクトリにダウンロードします。
3. コンポーネントの `compsig` ファイルをダウンロードします。
4. ベースラインを検証します。

## SUM がノードに接続できない

### 症状

SUM にノードにログインできないか、またはノードをサポート対象のデバイスとして識別できませんというメッセージが表示される。

### 解決方法 1

### 原因

SUM でリモートノードとの接続の問題が発生しています。

## アクション

1. 以下の点をご確認ください。

- ・ ネットワークでノードがアクティブになっている。
- ・ ネットワークポートが開いている。
- ・ Windows のノードで\$Admin 共有が有効になっている。
- ・ Linux のノードに対して HTTP および SSH アクセスが有効になっている。

## 解決方法 2

### 原因

ユーザー認証情報が正しくありません。

### アクション

有効なユーザー認証情報が提供されていることを確認します。

# Web サイトおよびサポート

## Web サイト

Hewlett Packard Enterprise Information Library	<a href="http://www.hpe.com/info/EIL">http://www.hpe.com/info/EIL</a>
Smart Update Manager	<a href="http://www.hpe.com/servers/sum">http://www.hpe.com/servers/sum</a>
Smart Update Manager Information Library	<a href="http://www.hpe.com/info/sum-docs">http://www.hpe.com/info/sum-docs</a>
Smart Update ツール	<a href="http://www.hpe.com/servers/sut">http://www.hpe.com/servers/sut</a>
Smart Update ツールの Information Library	<a href="http://www.hpe.com/info/isut-docs">http://www.hpe.com/info/isut-docs</a>
Service Pack for ProLiant	<a href="http://www.hpe.com/jp/spp">http://www.hpe.com/jp/spp</a>
Service Pack for ProLiant のドキュメント	<a href="http://www.hpe.com/info/spp/documentation">http://www.hpe.com/info/spp/documentation</a>
Service Pack for ProLiant のダウンロード	<a href="http://www.hpe.com/jp/servers/spp_dl">http://www.hpe.com/jp/servers/spp_dl</a>
Service Pack for ProLiant カスタムダウンロード	<a href="http://www.hpe.com/servers/spp/custom">http://www.hpe.com/servers/spp/custom</a>
HPE SDR サイト	<a href="http://downloads.linux.hpe.com">http://downloads.linux.hpe.com</a>

上記以外の Web サイトについては、[サポートと他のリソース](#)を参照してください。

## サポートと他のリソース

### Hewlett Packard Enterprise サポートへのアクセス

- ・ ライブアシスタンスについては、Contact Hewlett Packard Enterprise Worldwide の Web サイトにアクセスします。

<https://www.hpe.com/info/assistance>

- ・ ドキュメントとサポートサービスにアクセスするには、Hewlett Packard Enterprise サポートセンターの Web サイトにアクセスします。

<https://www.hpe.com/support/hpesc>

#### ご用意いただく情報

- ・ テクニカルサポートの登録番号（該当する場合）
- ・ 製品名、モデルまたはバージョン、シリアル番号
- ・ オペレーティングシステム名およびバージョン
- ・ ファームウェアバージョン

- ・ エラーメッセージ
- ・ 製品固有のレポートおよびログ
- ・ アドオン製品またはコンポーネント
- ・ 他社製品またはコンポーネント

## アップデートへのアクセス

- ・ 一部のソフトウェア製品では、その製品のインターフェイスを介してソフトウェアアップデートにアクセスするためのメカニズムが提供されます。ご使用の製品のドキュメントで、ソフトウェアの推奨されるソフトウェアアップデート方法を確認してください。
- ・ 製品のアップデートをダウンロードするには、以下のいずれかにアクセスします。

**Hewlett Packard Enterprise サポートセンター**

<https://www.hpe.com/support/hpesc>

**Hewlett Packard Enterprise サポートセンター：ソフトウェアのダウンロード**

<https://www.hpe.com/support/downloads>

**Software Depot**

<https://www.hpe.com/support/softwaredepot>

- ・ eNewsletters およびアラートをサブスクライブするには、以下にアクセスします。

<https://www.hpe.com/support/e-updates-ja>

- ・ お客様の資格を表示、アップデート、または契約や保証をお客様のプロファイルにリンクするには、Hewlett Packard Enterprise サポートセンターの **More Information on Access to Support Materials** ページに移動します。

<https://www.hpe.com/support/AccessToSupportMaterials>

- 
- ❗ **重要:** 一部のアップデートにアクセスするには、Hewlett Packard Enterprise サポートセンターからアクセスするときに製品資格が必要になる場合があります。関連する資格を使って HPE パスポートをセットアップしておく必要があります。
- 

## リモートサポート（HPE 通報サービス）

リモートサポートは、保証またはサポート契約の一部としてサポートデバイスでご利用いただけます。リモートサポートは、インテリジェントなイベント診断を提供し、ハードウェアイベントを Hewlett Packard Enterprise に安全な方法で自動通知します。これにより、ご使用の製品のサービスレベルに基づいて、迅速かつ正確な解決が行われます。ご使用のデバイスをリモートサポートに登録することを強くおすすめします。

ご使用の製品にリモートサポートの追加詳細情報が含まれる場合は、検索を使用してその情報を見つけてください。

**リモートサポートおよびプロアクティブケア情報**

**HPE 通報サービス**

<http://www.hpe.com/jp/hpalert>

**HPE プロアクティブケアサービス**

<http://www.hpe.com/services/proactivecare>

**HPE データセンターケアサービス**

<http://www.hpe.com/services/datacentercare>

HPE プロアクティブケアサービス：サポートされている製品のリスト

<http://www.hpe.com/services/proactivecaresupportedproducts>

HPE プロアクティブケアアドバンスドサービス：サポートされている製品のリスト

<http://www.hpe.com/services/proactivecareadvancedsupportedproducts>

## 保証情報

ご使用の製品の保証情報を確認するには、以下のリンクを参照してください。

HPE ProLiant と IA-32 サーバーおよびオプション

<https://www.hpe.com/support/ProLiantServers-Warranties>

HPE Enterprise および Cloudline サーバー

<https://www.hpe.com/support/EnterpriseServers-Warranties>

HPE ストレージ製品

<https://www.hpe.com/support/Storage-Warranties>

HPE ネットワーク製品

<https://www.hpe.com/support/Networking-Warranties>

## 規定に関する情報

安全、環境、および規定に関する情報については、Hewlett Packard Enterprise サポートセンターからサーバー、ストレージ、電源、ネットワーク、およびラック製品の安全と準拠に関する情報を参照してください。

<https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts>

### 規定に関する追加情報

Hewlett Packard Enterprise は、REACH（欧州議会と欧州理事会の規則 EC No 1907/2006）のような法的な要求事項に準拠する必要に応じて、弊社製品の含有化学物質に関する情報をお客様に提供することに全力で取り組んでいます。この製品の含有化学物質情報レポートは、次を参照してください。

<https://www.hpe.com/info/reach>

RoHS、REACH を含む Hewlett Packard Enterprise 製品の環境と安全に関する情報と準拠のデータについては、次を参照してください。

<https://www.hpe.com/info/ecodata>

社内プログラム、製品のリサイクル、エネルギー効率などの Hewlett Packard Enterprise の環境に関する情報については、次を参照してください。

<https://www.hpe.com/info/environment>

## ドキュメントに関するご意見、ご指摘

Hewlett Packard Enterprise では、お客様により良いドキュメントを提供するように努めています。ドキュメントを改善するために役立てさせていただきますので、何らかの誤り、提案、コメントなどがございましたら、ドキュメントフィードバック担当 ([docsfeedback@hpe.com](mailto:docsfeedback@hpe.com)) へお寄せください。このメールには、ドキュメントのタイトル、部品番号、版数、およびドキュメントの表紙に記載されている刊行日をご記載ください。オンラインヘルプの内容に関するフィードバックの場合は、製品名、製品のバージョン、ヘルプの版数、およびご利用規約ページに記載されている刊行日もお知らせください。