

Dell Management Plug-In for VMware vCenter
ユーザーズガイドバージョン 1.6_12月



メモ、注意、警告

-  **メモ:** コンピュータを使いやすくするための重要な情報を説明しています。
-  **注意:** ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。
-  **警告:** 物的損害、けが、または死亡の原因となる可能性があることを示しています。

© 2012 Dell Inc.

本書に使用されている商標 : Dell™、Dell のロゴ、Dell Boomi™、Dell Precision™、OptiPlex™、Latitude™、PowerEdge™、PowerVault™、PowerConnect™、OpenManage™、EqualLogic™、Compellent™、KACE™、FlexAddress™、Force10™ および Vostro™ は Dell Inc. の商標です。Intel®、Pentium®、Xeon®、Core® および Celeron® は米国およびその他の国における Intel Corporation の登録商標です。AMD® は Advanced Micro Devices, Inc. の登録商標、AMD Opteron™、AMD Phenom™ および AMD Sempron™ は同社の商標です。Microsoft®、Windows®、Windows Server®、Internet Explorer®、MS-DOS®、Windows Vista® および Active Directory® は米国および/またはその他の国における Microsoft Corporation の商標または登録商標です。Red Hat® および Red Hat® Enterprise Linux® は米国および/またはその他の国における Red Hat, Inc. の登録商標です。Novell® および SUSE® は米国およびその他の国における Novell, Inc. の登録商標です。Oracle® は Oracle Corporation またはその関連会社、もしくはその両者の登録商標です。Citrix®、Xen®、XenServer® および XenMotion® は米国および/またはその他の国における Citrix Systems, Inc. の登録商標または商標です。VMware®、Virtual SMP®、vMotion®、vCenter® および vSphere® は米国またはその他の国における VMware, Inc. の登録商標または商標です。IBM® は International Business Machines Corporation の登録商標です。

2012

Rev. A04

目次

メモ、注意、警告.....	2
章 1: 概要.....	9
VMware vCenter 用の Dell Management プラグイン.....	9
主な機能.....	9
Dell Management プラグインは vCenter 管理でどのように役立ちますか?	9
Dell Management プラグインの機能.....	10
章 2: Dell Management プラグイン設定.....	11
セキュリティの役割および許可.....	11
データ整合性.....	11
アクセス制御認証、許可、および役割.....	12
Dell 操作の役割.....	12
Dell インフラストラクチャ展開の役割.....	13
権限について.....	13
章 3: Dell Management Plug-in の設定または編集方法の理解	17
Dell Management Plug-in ホームページ.....	17
設定ウィザードようこそページ.....	18
新規接続プロファイルの作成ウィザード.....	18
イベントおよびアラームの設定ウィザード.....	19
プロキシサーバーの設定ウィザード.....	20
インベントリジョブのスケジュールウィザード.....	20
保証取得ジョブウィザードの実行.....	21
展開資格情報の設定ウィザード.....	21
デフォルトのファームウェアアップデートリポジトリの設定ウィザード.....	21
OMSA リンクの有効化ウィザード.....	22
Dell iDRAC 自動検出および初期始動の設定.....	22
NFS 共有の設定.....	23
設定の概要.....	23
一般設定の概要.....	24
新しい接続プロファイルの作成.....	25
イベントおよびアラームの設定	26
プロキシの設定について.....	27
インベントリジョブの実行.....	28
保証取得ジョブの実行.....	28
展開資格情報の表示または編集.....	29

ファームウェアリポジトリの設定	29
展開のためのサーバーセキュリティの設定.....	30
ホスト、ベアメタルおよび iDRAC 対応問題について.....	31
非対応 vSphere ホストの解決ウィザードの実行.....	32
非ベアメタルサーバーの解決ウィザードの実行.....	33
iDRAC ライセンスの対応.....	33
Dell Management Plug-In For VMware vCenter のアップグレード.....	34
バージョン 1.0 から現行バージョンへのアップグレード.....	34
試用バージョンから完全製品バージョンへのアップグレード.....	35
Dell Management Plug-in の旧バージョン (1.0.1 以降) から現行バージョンへのアップデート.....	35
Dell Management Plug-in License について.....	36

章 4: エンドツーエンドのハードウェア管理.....37

データセンターおよびホストシステムの監視.....	37
イベントとアラームの理解.....	37
vSphere クライアントホストの概要.....	41
インベントリスケジュールについて.....	43
インベントリジョブスケジュールの変更.....	43
vCenter におけるシングルホストシステムのインベントリ表示.....	44
インベントリおよびライセンス.....	45
ストレージインベントリの表示.....	45
ホスト電源監視の表示.....	46
全データセンターハードウェアの設定およびステータスの表示.....	46
接続プロファイルの管理.....	47
新しい接続プロファイルの作成.....	47
既存の接続プロファイルの表示または編集.....	48
接続プロファイルの削除.....	49
接続プロファイルのテスト.....	49
接続プロファイルの更新.....	49
vSphere クライアントのホストビューにおけるシステムイベントログの理解.....	49
Dell Management Center におけるログ表示.....	50
個別ホストのイベントログの表示.....	50
ファームウェアアップデートについて.....	51
ファームウェアアップデートウィザードの実行.....	52
古いファームウェアバージョンのアップデート	53
vCenter を使用した高度なホスト管理.....	53
物理サーバー前面インジケータライトの設定.....	54
サーバーベース管理ツール.....	54
保証の取得.....	54

章 5: ゼロタッチハードウェアプロビジョニングおよび展開.....57

ハードウェアの必要条件.....	57
------------------	----

プロビジョニングの概要.....	58
展開ジョブ時間の理解.....	58
展開シーケンス実行中のサーバー状態.....	58
カスタム Dell ISO イメージのダウンロード.....	59
ハードウェアプロファイルの設定方法の理解.....	59
参照サーバーにおける CSIOR の有効化.....	60
新規ハードウェアプロファイルの作成.....	61
新規ハードウェアプロファイルのクローン.....	62
ハードウェアプロファイル管理について.....	63
ハードウェアプロファイルの表示または編集.....	63
ハードウェアプロファイルの複製.....	63
ハードウェアプロファイル名の変更.....	64
ハードウェアプロファイルの削除.....	64
アップデートされたハードウェアプロファイルの更新.....	64
新しいハイパーバイザープロファイルの作成.....	64
ハイパーバイザープロファイルの管理.....	65
VLAN のサポート.....	65
ハイパーバイザープロファイルの表示または編集.....	67
ハイパーバイザープロファイルのコピー.....	67
ハイパーバイザープロファイル名の変更.....	68
ハイパーバイザープロファイルの削除.....	68
ハイパーバイザープロファイルの更新.....	68
新規の展開テンプレートの作成.....	68
展開テンプレートの管理.....	69
展開ウィザードの実行.....	69
展開ウィザード - 手順 1: サーバーの選択.....	70
展開ウィザード手順 2: 展開テンプレート.....	70
展開ウィザード手順 3: グローバル設定.....	71
導入ウィザード手順 4: サーバー識別情報.....	71
展開ウィザード手順 5: 接続プロファイル.....	72
展開ウィザード手順 6: ジョブのスケジュール.....	72
ジョブキューの理解.....	73
手動によるサーバーの追加.....	74
ベアメタルサーバーの取り外し.....	74
章 6: Dell Management Plug-in の管理.....	75
ウェブベース管理コンソール.....	75
vCenter サーバー接続の管理.....	75
vCenter サーバーの登録.....	75
管理コンソールへの Dell Management Plug-in ライセンスのアップロード.....	77
仮想アプライアンス管理.....	77
仮想アプライアンスの再スタート.....	77

リポジトリの場所と仮想アプライアンスのアップデート.....	78
仮想アプライアンスソフトウェアバージョンのアップデート.....	78
トラブルシューティングバンドルのダウンロード.....	78
HTTP プロキシの設定.....	79
NTP サーバーの設定.....	79
証明書署名要求の生成.....	79
グローバル警告の設定.....	80
バックアップおよび復元の管理.....	81
バックアップおよび復元の設定.....	81
自動バックアップのスケジュール.....	82
即時のバックアップの実行.....	82
バックアップからのデータベースの復元.....	82
vSphere クライアントコンソールタブの理解.....	83
ネットワークの設定.....	83
仮想アプライアンスパスワードの変更.....	83
ローカルタイムゾーンの設定.....	83
仮想アプライアンスの再起動.....	84
仮想アプライアンスの工場出荷時設定へのリセット.....	84
コンソールタブビューの更新.....	84
読み取り専用ユーザーロール.....	84

章 7: トラブルシューティング.....85

アップグレードの問題.....	85
よくあるお問い合わせ (FAQ).....	85
Dell Management Plug-in が SNMP トラップを設定およびサポートするのは、Dell サーバーのどの世代ですか?.....	85
Dell Management Plug-in で管理されるのは、リンクモードのどの vCenter ですか?.....	85
Dell Management Plug-in はリンクモードの vCenter をサポートしますか?.....	85
Dell Management プラグインのための必須ポート設定は何ですか?.....	86
仮想アプライアンスの正常なインストールと操作のために最低限必要な要件は何ですか?.....	87
保証を更新するための翻訳はどのようにして見つければいいですか?.....	88
新しい iDRAC バージョンの詳細が、vCenter ホストとクラスタ のページに表示されないのはなぜですか?.....	88
OMSA を使用して温度ハードウェア障害をシミュレートすることによってイベント設定をテストする方法は?.....	89
Dell ホストシステムに OMSA エージェントをインストールしていますが、OMSA がインストールされていないというエラーメッセージが今でも表示されます。どうしたらよいですか?.....	89
Dell Management プラグインはロックダウンモードが有効になっている ESX/ESXI をサポートできますか?.....	90
再起動後、ロックダウンモードのホスト ESXi 4.0 Update2 および ESXi Update 3 でインベントリが失敗します。.....	90
ロックダウンモードを使用しようとしたら、失敗しました。.....	90

ESXi 4.1 U1 で UserVars.CIMoeMProviderEnable にはどのような設定を使用すべきですか?.....	90
ハードウェアプロファイルの作成にリファレンスサーバーを使用していますが、失敗しまし た。どうしたらよいですか?.....	90
ブレードサーバーに ESX/ESXi を展開しようとしていますが、失敗しました。どうしたらよ いですか?.....	91
ハイパーバイザー展開が R210 II マシンで失敗するのはなぜですか?.....	91
展開ウィザードにモデル情報のない自動検出されたシステムが表示されるのはなぜですか?.....	91
ESX/ESXi ISO で NFS 共有がセットアップされていますが、共有の場所をマウントするときの エラーで失敗します。.....	91
仮想アプライアンスを強制削除するにはどのようにしたらよいですか?.....	91
今すぐバックアップ画面にパスワードを入力するとエラーメッセージが表示されます.....	92
vSphere で Dell Server Management (Dell サーバー管理) タブまたは Dell Management アイコ ンをクリックすると 404 エラーが返されます.....	92
ファームウェアアップデートが失敗しました。どうしたらよいですか?.....	92
vCenter アップデートが失敗しました。どうしたらよいですか?.....	92
接続プロファイルの資格情報テスト中、パフォーマンスが非常に遅くなったり、応答しなく なります。.....	92
Dell Management Plug-in は、VMware vCenter Server Appliance をサポートしますか?.....	93
Dell Management Plug-in は vSphere Web Client をサポートしますか?.....	93
ベアメタル展開の問題.....	93
新たに購入したシステムでの自動検出の有効化.....	93
Contacting Dell.....	94
本ソフトウェアのためのその他情報.....	94
VMware vCenter 用の Dell Management プラグインの関連情報.....	94
章 8: 仮想化 — 関連イベント.....	95

概要

VMware vCenter 用の Dell Management プラグイン

VMware vCenter は、IT 管理者が VMware vSphere ESX/ESXi ホストを管理および監視するために使用するプライマリコンソールです。標準の仮想化環境では、システム管理者に個別のコンソールを起動してハードウェア問題を解決するように指示するためには、VMware アラートと監視が使用されます。現在、VMware vCenter 用の Dell Management プラグインの使用により、管理者は仮想化環境内で Dell ハードウェアを管理および監視するための新しい機能を利用できます。機能には次のようなものがあります。

- アラート通知と環境の監視
- 単一サーバー監視と報告
- ファームウェアアップデート
- 拡張された展開オプション

主な機能

Dell のユーザーは Dell Management プラグインを使用して、次の操作を行うことができます。

インベントリ	主要資産のインベントリを実行、設定タスクを実行、Dell プラットフォームのクラスタビューとデータセンタビューを提供。
監視とアラートの実施	主要なハードウェア障害を検知し、仮想化を認識した動作（たとえば、作業負荷の移行、あるいはホストをメンテナンスモードに設定）を実行。
ファームウェアアップデート	Dell ハードウェアを最新バージョンの BIOS とファームウェアにアップデート。
展開とプロビジョニング	ハードウェアプロファイル、ハイパーバイザプロファイルを作成し、vCenter を使用して、リモートかつ PXE 無しでベアメタル Dell PowerEdge サーバーにこの 2 つの任意の組み合わせを展開。
サーバー情報	Dell からオンラインで保証情報を取得。

Dell Management プラグインは vCenter 管理でどのように役立ちますか?

VMware vCenter 用の Dell Management プラグインは、現在の vCenter 管理機能を補完する追加の仮想化機能を提供します。

- タスクを要約し、ファームウェアアップデートやベアメタル展開などの管理プロセスを vCenter Server 管理コンソールに追加します。
- 起動前実行環境 (PXE) を必要とすることなく、複数のベアメタルサーバーの展開を準備します。
- サーバー問題を診断するための追加の情報 (インベントリ、イベント、警告) を提供します。
- 標準の vCenter 認証、規則、権限と一体化します。

Dell Management プラグインの機能

Dell Management プラグインの高レベル機能は次のとおりです。

- 標準の vCenter イベントとアラームサブシステムを使用した Dell プラットフォームの監視
- 高度なハードウェア管理と設定の実施
- PXE を使用せずにベアメタルシステム上で VMware ESX ハイパーバイザーのゼロタッチ展開を実行
- ハードウェアと VMware ESX ハイパーバイザーのプロファイルを構築
- ファームウェアアップデートの実行
- インフラストラクチャ問題のトラブルシューティング
- データセンターとクラスタビューでの報告 — CSV ファイルへのエクスポート
- Dell Management プラグイン機能を標準 vCenter 役割と許可に統合

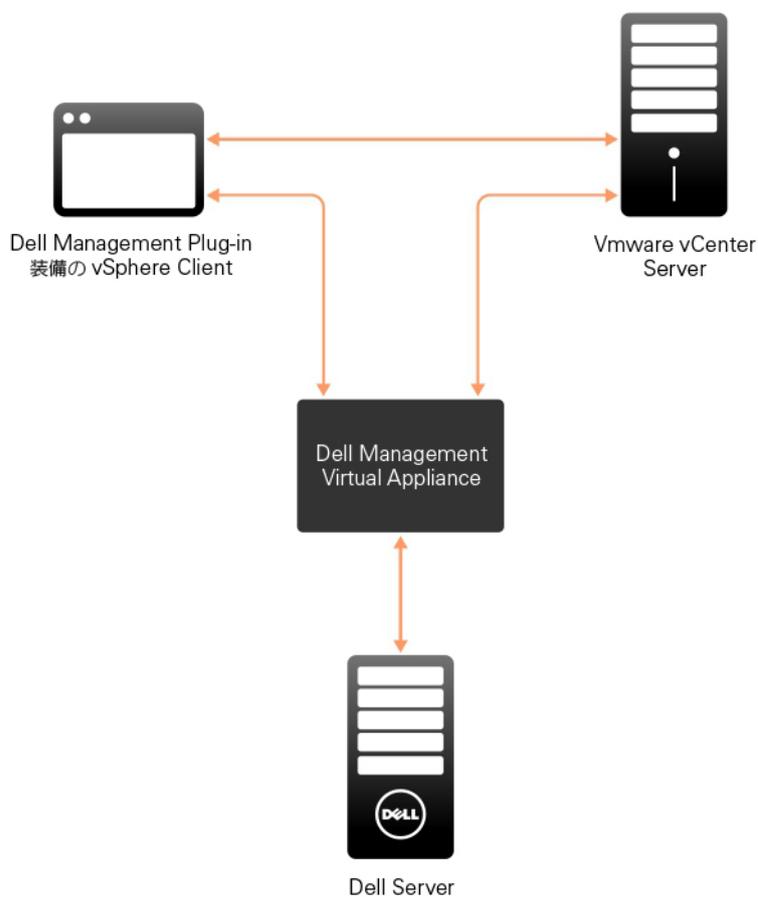


図 1. Dell Management プラグインのアーキテクチャ概要

Dell Management プラグイン設定

次の項では、Dell Management プラグインの初期設定の順を追った手順を説明します。アップグレード、アンインストール、およびセキュリティ役割についての情報も次の項に記載されています。

セキュリティの役割および許可

Dell Management プラグインは、ユーザー資格情報を暗号化フォーマットで保管します。問題につながる可能性のある不適切な要求を避けるため、クライアントアプリケーションにはパスワードを一切提供しません。データベースのバックアップは、カスタムセキュリティフレーズで完全に暗号化されるため、データが誤使用されることはありません。

デフォルトで、管理者グループに属するユーザーは全ての権限を持っており、ユーザーは Dell Management Center および Dell Server Management タブを含む Dell Management プラグインのすべての機能が使うことができます。管理ユーザーではないユーザーに Dell Management Center および Dell Server Management タブを使用させるには、両方の Dell 役割を含む新規役割を作成し、インベントリのルート/トップノードで許可を割り当て、必要に応じてユーザーにアクセスを与えたい子ノードに許可を伝搬します。たとえば、あるユーザーにクラスタ A のみを管理させる場合は、クラスタ A の許可を残して、その他のクラスタの許可を取り除きます。管理ユーザーではないユーザーに Dell Management Center のみを使用させる場合は、両方の Dell 役割を含む新規役割を作成し、ルートノードのみに許可を追加して、子ノードには伝搬しません。管理ユーザーではないユーザーに Dell Server Management タブのみを使用させる場合は、ユーザーアクセスを許可したいノードに Dell 操作役割の許可のみを追加します。

データ整合性

Dell Management プラグイン、仮想アプライアンス、管理コンソール、および vCenter の間の通信は、SSL/HTTPS を使用して行われます。Dell Management プラグインは、vCenter およびアプライアンスの間の信頼された通信のために SSL 証明書を生成します。また、通信と Dell Management プラグイン登録の前に vCenter サーバーの証明書を検証して信頼します。Dell Management プラグインコンソールタブ (VMware vCenter) は、管理コンソールおよびバックエンドサービスとの間でキーをやり取りする間、セキュリティプロシージャを使用して不適切な要求を回避します。このタイプのセキュリティではクロスサイトリクエストフォージェリは成り立ちません。

セキュア管理コンソールセッションには 5 分間のアイドルタイムアウトがあり、セッションは現行のブラウザウィンドウおよび/またはタブでのみ有効です。ユーザーが新しいウィンドウまたはタブでセッションを開こうとすると、有効なセッションを求めるセキュリティエラーが作成されます。この処置は、管理コンソールセッションを攻撃する可能性のある悪意のある URL をユーザーがクリックすることを防ぎます。

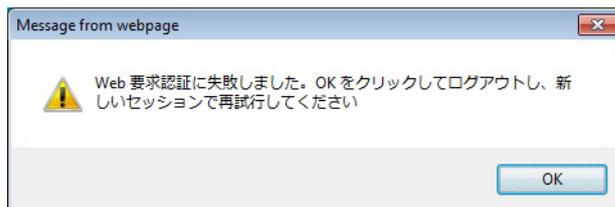


図 2. エラーメッセージ

アクセス制御認証、許可、および役割

Dell Management プラグインは、仮想アプライアンスが vCenter 操作を実行するように、vSphere クライアントの現在のユーザーセッションと保存された管理資格情報を使用します。Dell Management プラグインは、vCenter サーバーのビルトイン役割と権限モデルを使い、仮想アプライアンスおよび vCenter の管理下オブジェクト（ホストおよびクラスタ）に対するユーザー処置を許可します。

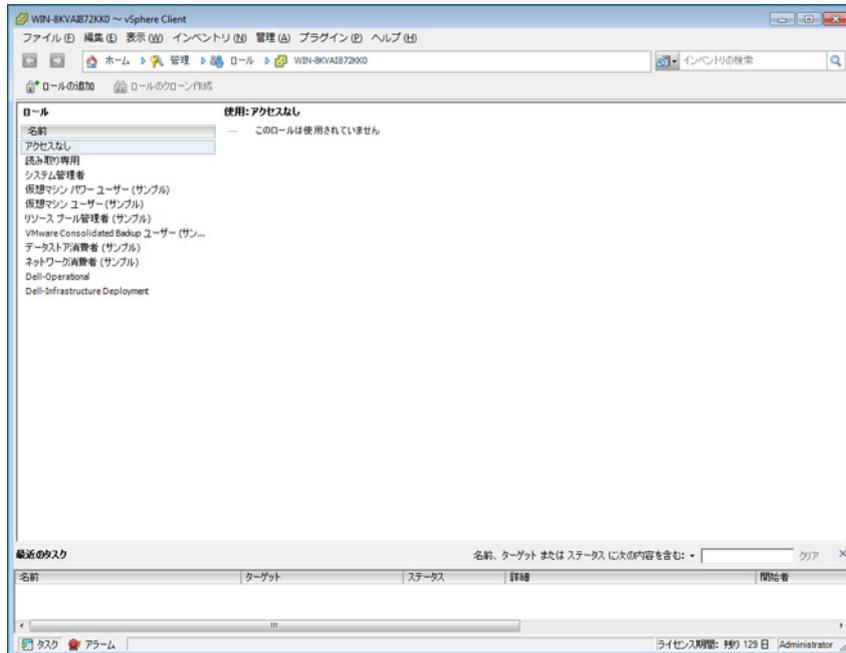


図 3. vCenter vSphere クライアントの役割と権限

Dell 操作の役割

ファームウェアアップデート、ハードウェアインベントリ、ホストの再起動、ホストをメンテナンスモードに設定、vCenter Server タスクの作成を含む、アプライアンスおよび vCenter サーバーのタスクを実行する権限 / グループが含まれます。

この役割には次の権限グループが含まれます。

- 権限グループ - Dell.Configuration** 権限 - ホスト関連タスクの実行、vCenter 関連タスクの実行、SellLog の設定、ConnectionProfile の設定、ClearLed の設定、ファームウェアアップデート
- 権限グループ - Dell.Inventory** 権限 - インベントリの設定、保証取得の設定、読み取り専用
- 権限グループ - Dell.Monitoring** 権限 - 監視の設定、監視
- 権限グループ - Dell.Reporting (使用されていません)** 権限 - レポートの作成、レポートの実行

Dell インフラストラクチャ展開の役割

この役割には、ハイパーバイザー展開機能に特化した権限が含まれます。

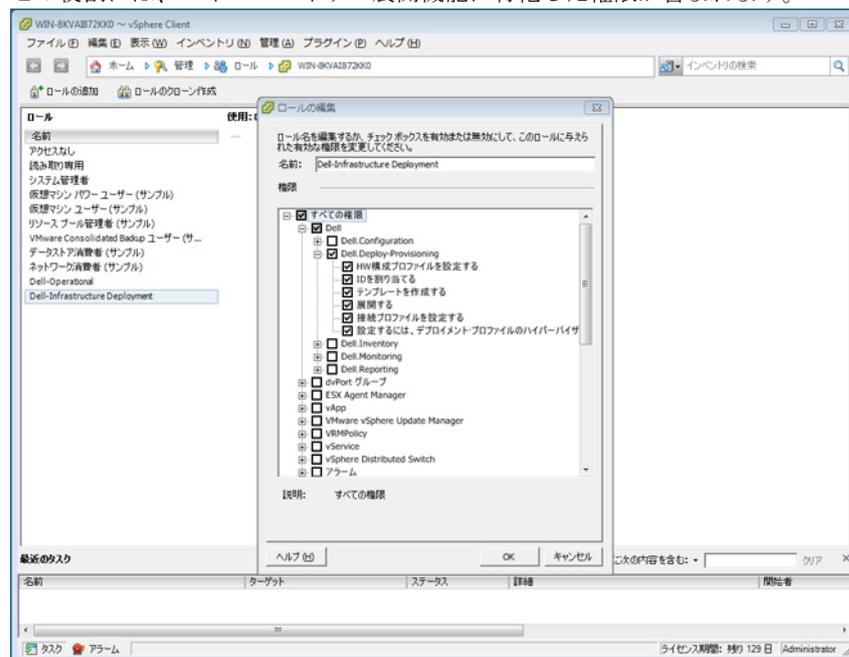


図 4. Dell インフラストラクチャ展開の役割

この役割の権限は、テンプレートの作成、HW 設定プロファイルの設定、ハイパーバイザー展開プロファイルの設定、接続プロファイルの設定、ID の割り当て、および展開です。

権限グループ テンプレートの作成、HW 設定プロファイルの設定、ハイパーバイザー展開プロファイルの設定、接続プロファイルの設定、ID の割り当て、展開
— Dell.Deploy —
プロビジョニング

権限について

Dell Management プラグインによって実行されるすべての処置は、権限に関連付けられています。次の項では、実行可能な処置と、それに関連付けられている権限をリストします。

- **Dell.Configuration.Perform vCenter-Related Tasks**
 - メンテナンスモードを終了および実行
 - 許可をクエリするために vCenter ユーザーグループを取得
 - 警告を登録および設定。たとえば、イベント設定ページでのアラートの有効化/無効化
 - vCenter にイベント/アラートを掲示
 - イベント設定ページでイベント設定を実行
 - イベント設定ページでデフォルトのアラートを復元
 - アラート/イベント設定を実行しながら、クラスタの DRS ステータスをチェック
 - アップデートまたはその他の設定処置を実行した後にホストを再起動

- vCenter タスクのステータス / 進捗状態を監視
 - vCenter タスクを作成。たとえば、ファームウェアアップデートタスク、ホスト設定タスク、およびインベントリタスク
 - vCenter タスクのステータス / 進捗状態をアップデート
 - ホストプロファイルを取得
 - データセンターにホストを追加
 - クラスタにホストを追加
 - ホストにプロファイルを適用
 - CIM 資格情報を取得
 - コンプライアンスのためにホストを設定
 - コンプライアンスタスクのステータスを取得
- **Dell.Inventory.Configure ReadOnly**
 - 接続プロファイルの設定中に、すべての vCenter ホストを取得して vCenter ツリーを構築
 - タブが選択されているときにホストが Dell サーバーかどうかをチェック
 - vCenter のアドレス / IP を取得
 - ホストの IP / アドレスを取得
 - vSphere クライアントセッション ID に基づいて現在の vCenter セッションユーザーを取得
 - vCenter インベントリツリーを取得して、vCenter インベントリをツリー構造で表示
- **Dell.Monitoring.Monitor**
 - イベントを掲示するためのホスト名を取得
 - イベントログ操作を実行。たとえば、イベント数の取得、またはイベントログ設定の変更
 - イベント / アラートを登録、登録解除、および設定 - SNMP トラップの受信とイベントの受信
- **Dell.Configuration.Firmware Update**
 - ファームウェアアップデートを実行
 - ファームウェアアップデートウィザードページにファームウェアリポジトリと DUP ファイル情報をロード
 - ファームウェアインベントリをクエリ
 - ファームウェアリポジトリ設定を実行
 - ステージングフォルダを設定、およびステージング機能を使用したアップデートを実行
 - ネットワークとリポジトリ接続をテスト
- **Dell.Deploy-Provisioning.Create Template**
 - 展開テンプレートの作成、表示、削除、および編集
- **Dell.Configuration.Perform Host-Related Tasks**
 - Dell Server Management (Dell サーバー管理) タブから LED を点滅、LED をクリア、OMSA URL を設定
 - OMSA コンソールを起動
 - iDRAC コンソールを起動
 - SEL ログを表示およびクリア
- **Dell.Inventory.Configure Inventory**
 - Dell Server Management (Dell サーバー管理) タブでシステムインベントリを表示
 - ストレージ詳細を取得

- 電源監視詳細を取得
- 接続プロファイルページで接続プロファイルを作成、表示、編集、削除、およびテスト
- インベントリスケジュールを計画、アップデート、および削除
- ホストでインベントリを実行

Dell Management Plug-in の設定または編集方法の理解

Dell Management Plug-in の基本的なインストールを終了した後、2つの方法のどちらかを使用して、アプライアンスの設定を行うことができます。設定ウィザードの使用が最も一般的な方法ですが、Dell Management Center のアプライアンスの設定ページからでも同じように設定を行うことができます。

両方共、ユーザーインターフェースは似通っていますが、ウィザードでは *保存して続行* をクリックするのに対し、設定オプションでは *適用* をクリックします。

設定ウィザード使用の設定タスク

設定ウィザードを使用して Dell Management Plug-in を設定するには、このタスクを使用します。

1. [設定ウィザードようこそページ](#)
2. [新しい接続プロファイルの作成](#)
3. [イベントおよびアラームの設定](#)
4. [プロキシサーバーの設定](#)
5. [インベントリジョブのスケジューリング](#)
6. [保証取得ジョブの実行](#)
7. [展開資格情報の設定](#)
8. [デフォルトファームウェアアップデートリポジトリの設定](#)
9. [OMSA リンクの有効化](#)

設定オプションを使用した設定タスク

これらのタスクを使用して、Dell Management Plug-in 設定タスクを設定または編集します。

- [新しい接続プロファイルの作成](#)
- [イベントおよびアラームの設定](#)
- [プロキシサーバーの設定](#)
- [インベントリジョブスケジュールの変更](#)
- [保証の取得](#)
- [展開資格情報の表示または編集](#)
- [ファームウェアリポジトリおよび資格情報の設定](#)
- [OMSA リンクの有効化](#)

Dell Management Plug-in ホームページ

Dell Management Plug-in ホームページにログインすると、ナビゲーションボタンが左ペインに、便利なリンクや情報が右ペインに提供されます。このデザインは、最も頻度が高いタスクへの主要リンクを提供します。これらのタスクはすべて左ペインのナビゲーションにあります。使いやすいようにホームページでも見ることができます。このページで提供されるタスクは、次のカテゴリに属します。

- ホストおよびサーバーの展開
この項は、ホストおよびサーバー展開に関してさらに詳しい情報を提供します。

- **vSphere** ホストおよびベアメタルサーバーの対応性
この項では、さらに詳しい情報が提供され、非対応のホストまたはベアメタルサーバーの詳細を表示したり、あるいはウィザードを実行して解決することができます。
- **インベントリスケジュール**
この項では、インベントリスケジュールについてより多く学ぶことができます。
- **保証データ検索スケジュール**
この項では、保証スケジュールについて学び、または表示 / 変更ができます。
- **ライセンス**
この項では、ライセンスについてより多く学ぶことができます。ライセンスタスクに移動するには、リンクを使用してください。
- **イベントおよびアラームの設定**
イベントおよびアラームについてさらに学び、あるいはリンクを使って設定を行うことができます。
- **ホスト接続ライセンス**
ここでは、リアルタイムでホスト接続ライセンスを表示することができます。また、今すぐ購入リンクを使用して、複数ホストを管理できる完全版のライセンスを購入することができます。今すぐ購入リンクは、デモライセンスを使用している場合にのみ表示されます。

設定ウィザードようこそページ

Dell Management Plug-in をインストールした後は、設定が必要です。

1. **vSphere** クライアントの **管理** で、**Dell Management Center** アイコンをクリックします。
2. 初めて **Dell Management Center** アイコンを実行する場合、**設定ウィザード** が開きます。このウィザードには、**Dell Management Center** → **設定** ページでアクセスすることもできます。
3. ようこそタブで、これから実行する手順を確認し、**次へ** をクリックします。

新規接続プロファイルの作成ウィザード

接続プロファイルは、仮想アプライアンスが Dell サーバーと通信するのに使用する資格情報を保存します。各 Dell サーバーは、Dell Management Plug-in によって管理される接続プロファイルに関連付けられていなければなりません。複数のサーバーを 1 つの接続プロファイルに割り当てることができます。接続プロファイルの作成方法は、設定ウィザードと Dell Management Center、設定オプションではほぼ同様です。

 **メモ:** 本リリース、および第 12 世代のサーバーを使用するホストでのインストールでは、OMSA エージェントのインストールは必要ありません。第 11 世代のサーバーのインストールでは、OMSA エージェントは展開プロセス中に自動的にインストールされます。

ウィザードを使用する新規接続プロファイルの作成には、以下を行います。

1. **接続プロファイル** タブで、**新規作成** をクリックします。
2. **プロファイル名と説明** パネルでカスタム接続プロファイルを管理しやすくするために使われる **プロファイル名** とオプションの **説明** を入力し、**次へ** をクリックします。
3. **関連ホスト** パネルで、当該接続プロファイル用のホストを選択し、**次へ** をクリックします。
4. 資格情報と接続プロトコルの情報を表示し、**次へ** をクリックします。
5. **iDRAC** パネルで、**iDRAC 資格情報** を入力します。
 - a) **ユーザー名**、**パスワード**、および **パスワードの確認** に入力します。ユーザー名にはスペースを含めて 16 文字を使用できます。次の文字は使用できません: / (スラッシュ)、\ (バックスラッシュ)、@ (アットマーク)、" (引用符)、および文字を全く含まないスペース。両パスワードは一致する必要があり、印刷可能な ASCII 文字のみを使用できます。

-  **メモ:** パスワードには最高 20 までの印刷可能な ASCII 文字を使用できます。ドメイン名には、英数字、- (ダッシュ)、および . (ピリオド) のみを使用できます。
- b) **証明書のチェック** では、**有効** を選択し、すべての将来の接続に iDRAC 証明書をダウンロードして検証するか、または **無効** を選択して、証明書の確認と保存を行わないようにします。
Active Directory を使う場合は有効を選択する必要があります。
6. **次へ** をクリックします。
7. ホストルートの **資格情報** パネルでは、以下を行います。
- a) **ユーザー名**、**パスワード**、および **パスワードの確認** に入力します。両パスワードは一致する必要があります。
-  **メモ:** パスワードは、31 文字を超えることはできません。また、特殊文字を含めることはできません。
-  **メモ:** iDRAC Express または Enterprise カードがないサーバーでは、iDRAC テスト接続結果は、このシステムには該当しませんが表示されます。
-  **メモ:** OMSA 資格情報は、ESX および ESXi ホストに使われたものと同じです。
- b) **証明書のチェック** では、**有効** を選択し、すべての将来の接続に OMSA 証明書をダウンロードして検証するか、または **無効** を選択して、証明書の確認と保存を行わないようにします。Active Directory を使用する場合は有効を選択します。
8. **次へ** をクリックします。
9. **接続性のテスト** ウィンドウで、選択されたサーバー用に入力された iDRAC およびホストルートの資格情報がテストされます。次のいずれかを行います。
- テストを開始するには、**選択したテスト** をクリックします。他のオプションは無効になっています。
 - テストを中止するには、**すべてのテストを中止** をクリックします。
10. プロファイルを完了するには、**保存** をクリックします。
11. イベントとアラームの設定を続けるには、**保存して続行** をクリックします。

イベントおよびアラームの設定ウィザード

設定ウィザードを使用して、または Dell Management Center、イベントおよびアラームの設定オプションからイベントおよびアラームの設定を行います。

 **メモ:** 12G より前のホストでは、vCenter でホストイベントを表示するには、仮想アプライアンスは OMSA でトラップ先に設定されている必要があります。

イベントおよびアラームを設定するには、以下を行います。

1. **設定ウィザードの イベント掲載レベル** で、以下のいずれかを選択します。
- すべてのイベントを掲載をしない - ハードウェアイベントはブロックされます。
 - すべてのイベントを掲載する - すべてのハードウェアイベントが掲載されます。
 - 重要および警告イベントのみを掲載する - 重要または警告レベルのハードウェアイベントのみが掲載されます。
 - 仮想化関連の重要および警告イベントのみを掲載する - 仮想化関連の重要および警告イベントのみが掲載されます。これはデフォルトのイベント掲載レベルです。
2. すべてのハードウェアアラームとイベントを有効化するには、**Dell ホストのアラームを有効にする** チェックボックスを選択します。
-  **メモ:** アラームが有効化されている Dell ホストは、重要イベントに対応して保守モードに入ります。
3. 表示されるダイアログボックスで **続行** をクリックしてこの変更を確定するか、または **キャンセル** をクリックします。

 **メモ:** この手順は、Dell ホストのアラームを有効にするが選択されている場合にのみ表示されます。

- すべての管理されている Dell サーバーで、デフォルトの vCenter アラーム設定を復元するには、**デフォルトのアラームの復元**をクリックします。
変更が有効になるには、最大1分間かかることがあります。
- ウィザードを続けるには、**保存して続行**をクリックします。

プロキシサーバーの設定ウィザード

設定ウィザードまたは後に Dell Management Center の **設定** → **プロキシ** ページでプロキシサーバーを設定します。

プロキシサーバーを設定するには、以下を行います。

- HTTP プロキシの設定** ウィンドウで以下のいずれかを行います。
 - プロキシサーバーを使用しない場合は、**保存して続行**をクリックします。
 - プロキシサーバーを使用する場合は、**設定**で**プロキシサーバーのアドレス**を入力します。
- プロキシポート番号**を入力します。
- 必要に応じて、**資格情報が必須です** チェックボックスを選択します。
- 資格情報が必須です** を選択した場合は、以下を行います。
 - プロキシユーザー名** テキストボックスにプロキシユーザー名を記入します。
 - プロキシパスワード** テキストボックスにプロキシパスワードを入力します。
 - プロキシパスワードの確認** テキストボックスにプロキシパスワードを再入力します。
- プロキシでプロキシを使用する** チェックボックスを選択します。
- これらのオプションを保存して継続するには**保存して続行**をクリックします。

インベントリジョブのスケジュールウィザード

インベントリスケジュール設定は、設定ウィザードと Dell Management Center の設定オプション間でほぼ同じです。唯一の違いは、ウィザードではインベントリをただちに実行するオプションを選択できることです。

 **メモ:** Dell Management プラグインが常に更新された情報を表示することを確実にするため、定期的なインベントリジョブをスケジュールすることをお勧めします。インベントリジョブは最小限のリソースしか使用せず、ホストパフォーマンスを劣化させません。

インベントリジョブのスケジュールには、以下を行います。

- 設定ウィザードのインベントリのスケジュール** ウィンドウで、以下の中から1つを行います。
 - インベントリスケジュールを実行するには、**選択した曜日** をクリックします。
 - インベントリスケジュールを実行しない場合は、**Dell ホストではインベントリを実行しない** を選択します。
- 選択した曜日** を選択した場合は、以下を行います。
 - インベントリを実行したい各曜日の横にあるチェックボックスを選択します。
 - テキストボックスに、時刻を HH:MM フォーマットで入力します。
入力時刻は現地時刻です。インベントリの収集を適切な時刻に実行するよう、時間差を計算します。
 - ウィザードの完了後、インベントリタスクを自動的に実行するには、**ウィザードの最後にインベントリを実行します (推奨)** チェックボックスを選択します。
このチェックボックスは、選択した曜日のチェックボックスが選択された場合にのみ表示されます。
- 変更を適用して継続するには、**保存して続行** をクリックします。

保証取得ジョブウィザードの実行

保証取得ジョブの設定は、ウィザードと **Dell Management Center** の設定オプションの場合でほぼ同様です。唯一の違いはウィザードの場合、保証取得をただちに実行するオプションが提供されることです。また、保証取得ジョブはジョブキューからすぐに実行することもできます。

保証取得ジョブを実行するには以下を行います。

1. **設定ウィザードの保証のスケジュール**ウィンドウで、以下のいずれかを行います。
 - 保証スケジュールを実行するには、**選択した曜日**をクリックします。
 - 保証スケジュールを実行しないようにするには、**保証情報を取得しない**を選択します。
2. **選択した曜日**を選択した場合は、以下を行います。
 - a) 保証ジョブを実行したい各曜日の横にあるテキストボックスを選択します。
 - b) テキストボックスに、時刻を **HH:MM** フォーマットで入力します。
入力した時刻は入力地の現地時刻です。保証ジョブを実行する必要のある正しい時刻について時差を計算してください。
3. 変更を適用して継続するには、**保存して続行**をクリックします。

展開資格情報の設定ウィザード

展開資格情報は、最初の検出から展開プロセスの終了まで、**iDRAC** を使ってベアメタルシステムとセキュアな通信を行うために使用されます。展開が完了すると、資格情報は展開ウィザードから接続プロファイルでベアメタルシステムに一致するものに変更されます。展開資格情報を変更されると、その時点以降に新たに検出されるシステムは新しい資格情報でプロビジョニングが行われます。ただし、変更前に検出されたサーバーの資格情報には影響を及ぼしません。

展開資格情報の設定には、以下を行います。

1. **展開資格情報** ウィンドウで、資格情報を表示または変更できます。ベアメタルサーバーは、これらの資格情報から接続プロファイルで指定されたものに切り替えます。
2. これらの資格情報を変更するには、**ベアメタルサーバー展開用の資格情報** 下で以下を行います。
 - a) **ユーザー名** テキストボックスでユーザー名を編集します。
 - b) **パスワード** テキストボックスでパスワードを編集します。
 - c) **パスワードの確認** テキストボックスでパスワードを確認します。
3. 特定した資格情報を保存して設定ウィザードを続けるには、**保存して続行** をクリックします。

デフォルトのファームウェアアップデートリポジトリの設定ウィザード

ファームウェアリポジトリ設定には、展開サーバーのアップデートに使用されるファームウェアカタログロケーションが含まれます。ファームウェアは、最初にウィザードで設定するか、あるいは、後に **Dell Management Center** 設定オプションで設定できます。さらに、ファームウェアアップデートは **Dell Server Management** タブから後ほど実行することもできます。

デフォルトのファームウェアアップデートリポジトリを設定するには、以下を行います。

1. **設定ウィザードのファームウェアリポジトリ** で、ファームウェアアップデートのためにデフォルトリポジトリを選択するには、以下のいずれか1つを選択します。
 - Dell Online

ステージングフォルダを持つデフォルトのファームウェアリポジトリ (ftp.dell.com) です。Dell Management プラグインは選択されたファームウェアアップデートをダウンロードし、ステージングフォルダに保存します。その後、それらのアップデートが必要に応じて適用されます。

– ローカル/共有リポジトリ

これは Dell Repository Manager アプリケーションで作成されます。このローカルリポジトリは、Windows ベースのファイル共有で見つけることができます。

2. ローカル/共有リポジトリを選択した場合、以下を行います。

a) 次のフォーマットを使って、**カタログファイルの場所**を入力します。

- * xml ファイル用の NFS 共有: host/share/filename.xml
- * gz ファイル用の CIFS 共有: \\host\share\filename.gz
- * xml ファイル用の CIFS 共有: \\host\share\filename.xml
- * gz ファイル用の CIFS 共有: \\host\share\filename.gz

b) CIFS 共有を使用する場合、**ユーザー名**、**パスワード**、**パスワードの確認**を入力します。両パスワードは一致する必要があります。これらの欄は CIFS 共有を入力する場合にのみアクティブになります。

 **メモ:** 共有ネットワークフォルダのユーザー名/パスワードには、@ 文字は使用できません。

c) 入力情報を確認するには、**テストの開始**をクリックします。

3. この選択を保存して **設定ウィザード**を継続するには、**保存して続行**をクリックします。

OMSA リンクの有効化ウィザード

Dell Management Plug-in 仮想アプライアンスで OMSA を起動するには、OMSA Web Server (OMSA ウェブサーバー) のインストールと設定が必要です。ウェブサーバーのインストールおよび設定に関する手順については、『*Dell OpenManage Server Administrator Installation Guide*』（Dell OpenManage Server Administrator インストールガイド）を参照してください。

 **メモ:** OMSA は、バージョン 12G より前の Dell サーバーでのみ必要になります。

OMSA を使用して、以下を行うことができます。

- vCenter エレメント（詳細センサ/コンポーネントレベルの正常性情報）の管理。
- コマンドログおよびシステムイベントログ (SEL) の消去。
- NIC 統計情報の取得。
- Dell Management Plug-in が選択されたホストからのイベントをキャプチャしていることを確認します。

1. 設定ウィザードの **OpenManage Server Admin** ページで **OMSA ウェブサーバーの URL** テキストボックスを使って OMSA URL を入力します。HTTPS を含む完全な URL を入力する必要があります。

2. この URL を保存して、設定ウィザードを終了するには、**終了**をクリックします。

Dell iDRAC 自動検出および初期始動の設定

 **メモ:** 自動検出とハンドシェイクを実行するには、管理者レベルのすべてのユーザーのアクセスを無効化する必要があります。また、アプライアンスの展開資格情報が既存ユーザーの資格情報と一致する場合、既存ユーザーのパスワードはアプライアンスの資格情報と一致させるために変更されます。

Dell iDRAC 自動検出および初期始動を設定するには、以下を行います。

1. iDRAC ユーザーインターフェースにログインします。
2. 左側のツリーメニューで、**リモートアクセス**をクリックします。
3. メインペインの上部タブで **ネットワーク/セキュリティ**をクリックします。

4. ユーザーサブタブをクリックして、ユーザー ID リンクを選択することにより、編集するユーザーを選択します。
5. ユーザーの設定オプションボタンが選択されていることを確認し、次のページに進みます。
6. ユーザーを設定するには、次のいずれかを行います。
 - ユーザーを無効化するにはユーザーの有効化チェックボックスを外し、適用をクリックします。
 - ユーザーを有効化するにはユーザーの有効化チェックボックスをマークし、適用をクリックします。
7. 手動で iDRAC ユーザーインターフェースを閉じ、システムを再起動して再度ログインします。
8. システム再起動後に iDRAC IP アドレスが表示されたら、<CTRL-E> を押します。
9. LAN ユーザーの設定に移動し、自動検出フラグの有効化を設定します。
iDRAC 管理者アカウントが無効化されていることを確認してください。または、ネットワークを自動検出とハンドシェイク用に設定する場合は <http://www.delltechcenter.com/page/Lifecycle+Controller> にある、「Dell Auto-Discovery Network Setup Specification」（Dell 自動検出ネットワーク設定仕様）を参照してください。
10. サーバーのプロビジョニングフィールドで仮想アプライアンスの IP アドレスを入力し、Enter を押します。
11. 検出と初期始動を開始するには、保存をクリックします。

NFS 共有の設定

Dell Management Plug-in でバックアップと復元作業、ファームウェアアップデート、および作業フォルダとして NFS 共有を使用するには、一定の設定項目の実行が必要です。CIFS 共有には追加設定は必要ありません。NFS 共有の設定には、以下を行います。

1. NFS 共有をホストしているマシンで、`/etc/exports` を編集して `/share/path <appliance IP> (rw) *(ro)` を追加します。
これにより、仮想アプライアンスは完全に共有の読み書きができるようになりますが、他のユーザーは読み取り専用となります。
2. nfs サービスの開始 :
`service portmap start service nfs start service nfslock status`
 **メモ:** 上記の手順は、使用している Linux ディストリビューションによって異なる場合があります。
3. すでにいずれかのサービスが実行されている場合は、以下を行います。
`exportfs -ra`

設定の概要

Dell Management Plug-in 設定の項:

- Dell Management Plug-in 構成の設定を記載します。
- 最初に VMware vCenter でサーバーを管理、展開するのに必要な Dell Management Plug-in 機能を手順ごとに説明する、設定ウィザードを起動します。
- Dell Management Plug-in 管理コンソールを起動し、vCenter の登録、仮想アプライアンスの管理、アラート管理、および Dell Management Plug-in データベースのバックアップ/復元ができるようにします。

関連タスク:

- [一般](#): vCenter の Dell ホストタブに表示される OMSA URL を設定します。また、保証期限通知を有効化または無効化することもできます。

- [イベントとアラーム](#): すべてのハードウェアアラームを有効化または無効化します（現在のアラートステータスはアラームタブに表示されます）。また、受信するイベントおよびアラートのフィルタリングも設定します。
- [プロキシ](#): インターネットサイトとの通信中のプロキシの使用を有効化または無効化します。
- [インベントリのスケジュール](#): vCenter ホストインベントリスケジュールを設定します。
- [保証のスケジュール](#): Dell Online から Dell ホストへの保証情報の検索スケジュールを設定します。
- [展開資格情報](#): 初期検出時に Dell サーバーと通信する際、およびベアメタルサーバー展開で使用される資格情報を設定します。
- [ファームウェアリポジトリ](#): ファームウェアアップデートを保存するロケーションの編集を可能にします。
- [セキュリティ](#): 展開できるサーバーを制限するサーバーホワイトリストを提供します。

一般設定の概要

一般設定は、以下を行うために使われます。

- OpenManage Server Administrator (OMSA) URL の定義。
- 保証期限通知の有効化または無効化。

OMSA ソフトウェアは以下のために使用できます。



メモ: OMSA ソフトウェアはバージョン 12G より前の Dell サーバーでのみ必要となります。

- vCenter エレメントの管理（詳細センサー、コンポーネントレベルの正常性情報）。
- コマンドログおよびシステムイベントログ（SEL）の消去。
- NIC 統計情報の取得。
- Dell Management Plug-in が選択されたホストからのイベントをキャプチャしていることを確認します。

保証期限通知は、以下のために使用できます。

- 保証期限の監視。
- 最低保証残余期間基準の警告または重要アラートの発生以降の設定。アラートは、ホストの Dell Server Management タブにアイコンとして表示されます。

関連タスク:

- [OMSA リンクの有効化](#)
- [保証期限通知の有効化または無効化](#)

設定ウィザード外での OMSA リンクの有効化

Dell Management Plug-in 仮想アプライアンス内で OMSA を起動するには、OMSA Web Server がインストールされ、設定されている必要があります。ウェブサーバーをインストールして設定する方法に関する説明は、使用中の OMSA バージョンに対する『*Dell OpenManage Server Administrator Installation Guide*』（Dell OpenManage Server Administrator インストールガイド）を参照してください。



メモ: OMSA は、バージョン 12G より前の Dell サーバーでのみ必要になります。

OMSA リンクを有効化するには、以下を行います。

1. OMSA 起動ツール下の **Dell Management Plug-in** → **設定** → **一般**で、**編集**をクリックします。
2. **OMSA Web Server** の URL テキストボックスを使用して、OMSA の URL を入力します。HTTPS を含む完全な URL を入力する必要があります。
3. この URL を保存するには、**適用**をクリックします。

OMSA トラップ先を設定することに関する情報は、「[OMSA トラップ先の設定](#)」を参照してください。

サーバー保証期限通知の有効化または無効化

保証設定は、保証スケジュールを有効化または無効化し、最小日数しきい値アラートを設定することで、Dell オンラインからサーバー保証情報を検索する時期を管理することができます。このページを使用してホストとクラスタのサーバー保証期限通知を有効化または無効化します。この機能は、Dell Management Center の設定、一般ページで設定または編集できます。

サーバー保証期限通知の有効化または無効化には、以下を行います。

1. **Dell Management Center** で、**設定** → **一般** をクリックします。
2. 一般ページで、通知を有効化するには **保証状態の通知を有効にする** チェックボックスを選択します。
3. **最小日数しきい値アラート**を設定するには、以下を行います。
 - a) 警告を設定するには、**警告**ドロップダウンリストでサーバー警告ステータスに関する日数を選択します。
 - b) 重要ライセンスステータスを設定するには、**重要**ドロップダウンリストで重要サーバー保証ステータスに日数を設定します。
4. 変更を適用するには、**適用**をクリックします。

新しい接続プロファイルの作成

接続プロファイルは Dell サーバーと通信するために仮想サーバーが使用する資格情報を保存します。各 Dell サーバーは Dell Management Plug-in が管理する 1 つだけの接続プロファイルに関連付けられている必要があります。1 つの接続プロファイルに複数のサーバーを割り当てることができます。接続プロファイルの作成方法は、接続ウィザードからであっても、**Dell Management Center** → **設定**であってもほぼ同じです。設定ウィザードは初めて Dell Management Console にアクセスしたとき、またはその後、設定ウィンドウから実行することもできます。

 **メモ:** このリリースおよび、バージョン 12G 以降のホストのインストールでは、OMSA エージェントのインストールは必要ありません。11G のホストにインストールする場合、現在では展開プロセスで OMSA エージェントが自動的にインストールされるようになってます。

新しい接続プロファイルを作成するには、次の手順を実行します。

1. **Dell Management Center** の左ペインで、**接続プロファイル**をクリックします。
2. **使用可能なプロファイル**で **新規作成**をクリックします。
3. **新規接続プロファイル**ウィンドウで、**プロファイル名**と、オプションでカスタム接続プロファイルの管理を便利にするために使われる、**説明**を入力し、**次へ**をクリックします。
4. **関連ホスト**については、チェックボックスを使ってこの接続プロファイルを使用するホストを選択して、**次へ**をクリックします。
5. **資格情報**ウィンドウで、資格情報および接続プロトコルに関する情報を表示し、**次へ**をクリックします。
6. iDRAC ウィンドウで **iDRAC 資格情報**を入力します。
 - a) **ユーザー名**、**パスワード**および**パスワードの確認**を入力します。両パスワードは一致する必要があります。また、ASCII 印刷可能文字だけを使用することができます。

 **メモ:** パスワードは 20 文字を超えることはできず、特殊文字を含むこともできません。
 - b) **証明書のチェック**で、iDRAC 証明書をダウンロードおよび保存し、すべての将来の接続で検証するには、**有効にする**を選択します。または、**無効にする**を選択すると、証明書の確認および保存は行われません。

Active Directory を使用する場合は、**有効にする**を選択する必要があります。
7. **次へ**をクリックします。

8. ホストルートの資格情報ウィンドウで、以下を行います。
 - a) ユーザー名、パスワード、およびパスワードの確認を入力します。両パスワードは一致する必要があります。
 -  **メモ:** パスワードは 31 文字を超えることはできず、特殊文字を含むこともできません。
 -  **メモ:** iDRAC Express または Enterprise カードがないサーバーでは、iDRAC テスト接続結果は、このシステムには該当しませんが表示されます。
 -  **メモ:** OMSA の資格情報は、ESX および ESXi ホストに使われる資格情報と同じです。
 - b) 証明書のチェックで OMSA 証明書をダウンロードして保存し、すべての将来の接続で検証するには、有効にするを選択します。または無効にするを選択すると、証明書の確認および保存は行われません。Active Directory を使用する場合は、有効にするを選択します。
9. 次へをクリックします。
10. 接続性のテストウィンドウで、選択されたサーバー用に入力された iDRAC およびホストルートの資格情報がテストされます。次のいずれかを行います。
 - テストを開始するには、選択したテストをクリックします。その他のオプションはアクティブになっていません。
 - テストを中止するには、テストを中止をクリックします。
11. プロファイルを完了するには、保存をクリックします。
接続プロファイルを管理するには、「[接続プロファイルの管理](#)」を参照してください。

イベントおよびアラームの設定

Dell Management Center イベントおよびアラームページでは、すべてのハードウェアアラームを有効または無効にできます。現在のアラートステータスは vCenter アラームタブに表示されます。重要イベントは実際のまたは切迫したデータ喪失あるいはシステム異常を示します。警告イベントは必ずしも重大ではないが、将来の潜在的な問題を示す可能性があります。イベントおよびアラームは VMware Alarm Manager を使用して有効化することもできます。イベントは、ホストとクラスタビューの vCenter タスクとイベントタブに表示されます。

 **メモ:** 12G より前のホストでは、ホストイベントを vCenter で表示するには、仮想アプライアンスが OMSA でトラップ先として設定されている必要があります。OMSA に関する詳細は、「[OMSA トラップ先の設定](#)」を参照してください。

イベントおよびアラームは、Dell Management Center のイベントとアラームの設定オプションで設定できます。

イベントおよびアラームを設定するには、以下を行います。

1. Dell Management Center の設定 → イベントとアラーム で編集をクリックします。
2. イベント掲載レベル で以下のいずれかを選択します。
 - すべてのイベントを掲載をしない - ハードウェアイベントはブロックされます。
 - すべてのイベントを掲載する - すべてのハードウェアイベントが掲載されます。
 - 重要および警告イベントのみを掲載する - 重要または警告レベルのハードウェアイベントのみが掲載されます。
 - 仮想化関連の重要および警告イベントのみを掲載する - 仮想化関連の重要および警告イベントのみが掲載されます。これはデフォルトのイベント掲載レベルです。
3. すべてのハードウェアアラームとイベントを有効化するには、Dell ホストのアラームを有効にするチェックボックスを選択します。
 -  **メモ:** アラームが有効化されている Dell ホストは、重要イベントに対応して保守モードに入ります。
4. 表示されるダイアログボックスで 続行 をクリックしてこの変更を確定するか、または キャンセル をクリックします。

- すべての管理されている Dell サーバーで、デフォルトの vCenter アラーム設定を復元するには、**デフォルトのアラームの復元**をクリックします。
変更が有効になるには、最大 1 分間かかることがあります。
- 保存するには、**保存** をクリックします。

プロキシの設定について

プロキシ設定は、HTTP プロキシおよびウェブ（Dell オンラインからを含む）から情報を検索するために使用される、必要な資格情報を定義します。それには以下が含まれます。

- プロキシサーバーの有効化または無効化
- 必要なプロキシサーバーとポート番号の入力
- 必要な資格情報（ユーザー名およびパスワード）の定義

 **メモ:** プロキシパスワードは、31 文字を超えることはできません。

関連タスク:

- [プロキシサーバーの設定](#)
- [ウェブベースデータを検索するための HTTP プロキシの使用](#)
- [管理コンソールを使用した HTTP プロキシの設定](#)

プロキシサーバーの設定

設定ウィザードを使用してプロキシサーバーを設定するか、後に設定オプション、プロキシを使って設定します。

 **メモ:** プロキシパスワードは、31 文字を超えることはできません。

プロキシサーバーを設定するには、以下を行います。

- Dell Management Center で **設定** → **プロキシ** を選択して、**編集** をクリックします。
- HTTP プロキシの設定** ウィンドウで以下のいずれかを行います。
 - プロキシサーバーを使用しない場合は、**保存して続行** をクリックします。
 - プロキシサーバーを使用する場合は、**設定** で **プロキシサーバーのアドレス** を入力します。
- プロキシポート番号** を入力します。
- 必要に応じて、**資格情報が必須です** チェックボックスを選択します。
- 資格情報が必須です** を選択した場合は、以下を行います。
 - プロキシユーザー名** テキストボックスにプロキシユーザー名を入力します。
 - プロキシパスワード** テキストボックスに、プロキシパスワードを入力します。
 - プロキシパスワードの確認** テキストボックスに、今タイプしたばかりのプロキシパスワードを再入力します。
- プロキシでプロキシを使用する** チェックボックスを選択します。
- これらのオプションを保存するには、**保存** をクリックします。

ウェブベースデータを検索するための HTTP プロキシの使用

HTTP プロキシを使用してウェブベースのデータを検索するには、以下を行います。

- Dell Management Center で **設定 HTTP プロキシ** を選択して、**編集** をクリックします。
- プロキシを使用する** チェックボックスを選択します。
- 適用** をクリックします。

4. 設定を確認するには、**接続性のテスト**をクリックします。

インベントリジョブの実行

インベントリジョブを実行するには、以下を行います。

1. **設定ウィザード**が完了したら、**ジョブキュー**→**インベントリ**→**今すぐ実行**をクリックしてインベントリジョブをただちに実行します。
2. インベントリジョブのステータスを見るには、**更新**をクリックします。
3. **ホストおよびクラスタビュー**に進み、いずれかの **Dell ホスト**をクリックして **Dell Server Management タブ**をクリックします。次の情報が表示されます。
 - 概要ページ
 - システムイベントログ
 - ハードウェアインベントリ
 - 保管時
 - ファームウェア
 - 電源モニタ
 - 保証ステータス

以下のホストコマンドは、**Dell Server Management タブ**で、またはホスト上で右クリックすることにより動作します。

- インジケータライトの点滅
- ファームウェアアップデートウィザードを実行
- リモートアクセスの起動
- OMSA プラグイン設定の起動
- CMC の起動
- 保証の更新

保証取得ジョブの実行

保証の取得ジョブの設定方法は、ウィザードと **Dell Management Center** → **設定オプション**間ではほぼ同様です。唯一の違いは、ウィザードの場合、保証の取得ジョブをただちに行うオプションが提供されることです。ウィザードの実行後はいつでも、**Dell Management Center** → **設定** → **保証のスケジュール** ページで編集できます。保証の取得ジョブは、**ジョブキュー** → **保証履歴** ページで今すぐ実行することができます。

保証の取得ジョブのスケジュールリングには、以下を行います。

1. **Dell Management Center** で **設定** → **保証のスケジュール** を選択します。
2. **保証のスケジュール** ウィンドウで **編集** をクリックします。
3. スケジュールを設定するには、次のいずれかを行います。
 - a) 保証スケジュールを実行するには、**選択した曜日** をクリックします。
 - b) 保証スケジュールを実行しない場合は、**Dell ホストではインベントリを実行しない** を選択します。
4. **選択した曜日** を選択した場合は、以下を行います。
 - a) 保証ジョブを実行したい曜日の横にあるチェックボックスを選択します。
 - b) テキストボックスに、時刻を **HH:MM** フォーマットで入力します。

入力した時刻は入力地の現地時刻です。保証ジョブを実行する必要のある正しい時刻について時差を計算してください。
5. 保証ジョブを今すぐ実行するには、**ジョブキュー** → **保証履歴** へ移動し、**今すぐ実行** をクリックします。

展開資格情報の表示または編集

Dell Management Center で展開資格情報を編集することができます。展開資格情報は、最初の検出から展開プロセスの最後まで、iDRAC を使用するベアメタルシステムとセキュアな通信を行うために使われます。展開が完了すると、資格情報は展開ウィザードからベアメタルシステムの接続プロファイルと一致するものに変更されます。展開資格情報を変更されると、その時点以降新たに検出されるすべてのシステムは、新しい資格情報でプロビジョニングが行われます。資格情報の変更前に検出されたサーバーの資格情報はこの変更での影響は受けません。ユーザー名は、16 文字以下（ASCII 印刷可能文字）である必要があります。パスワードは 20 文字以下（ASCII 印刷可能文字）である必要があります。

展開資格情報を表示または編集するには、以下を行います。

1. **Dell Management Center** → **設定** → **展開用資格情報** で、**編集** をクリックします。
2. **ベアメタルサーバー展開用の資格情報の 資格情報** で以下を行います。
 - **ユーザー名** テキストボックスにユーザー名を入力します。
ユーザー名は、16 文字以下（ASCII 印刷可能文字のみ）である必要があります。
 - **パスワード** テキストボックスにパスワードを入力します。
パスワードは、20 文字以下（ASCII 印刷可能文字のみ）である必要があります。
 - **パスワードの確認** テキストボックスにパスワードを再度入力します。
両パスワードは一致する必要があります。
3. **適用** をクリックします。

ファームウェアリポジトリの設定

ファームウェアリポジトリおよび資格情報を設定するには、以下を行います。

1. **Dell Management Center** で、**設定** → **ファームウェアリポジトリ** を選択し、**編集** をクリックします。
2. **ファームウェアリポジトリ** ページでファームウェアのアップデートのためのデフォルトリポジトリを選択するには、以下のいずれかを選択します。
 - **Dell Online**
これは、**Dell Online (ftp.dell.com)** のデフォルトファームウェアアップデートリポジトリを使用するもので、中継フォルダが必要です。**Dell Management Plug-in** は選択されたファームウェアアップデートをダウンロードし、中継フォルダに保存します。そこから必要に応じて適用されます。
 - **ローカル/共有リポジトリ**
これは **Dell Repository Manager** アプリケーションで作成されます。このローカルリポジトリは、**Windows** ベースのファイル共有で見つけることができます。
3. **ローカル/共有リポジトリ** を選択した場合、以下を行います。
 - a) 次のフォーマットを使って、**カタログファイルの場所**を入力します。
 - * xml ファイル用の NFS 共有: host/share/filename.xml
 - * gz ファイル用の NFS 共有: /share/filename.gz
 - * xml ファイル用の CIFS 共有: \\host\share\filename.xml
 - * gz ファイル用の CIFS 共有: \\host\share\filename.gz
 - b) CIFS 共有を使用する場合、**ユーザー名**、**パスワード**、**パスワードの確認** を入力します。両パスワードは一致する必要があります。これらの欄は CIFS 共有を入力する場合にのみアクティブになります。
 **メモ:** 共有ネットワークフォルダのユーザー名/パスワードには、@ 文字は使用できません。
 - c) 入力情報を確認するには、**テストの開始** をクリックします。

4. **適用** をクリックします。

展開のためのサーバーセキュリティの設定

ホワイトリストを使用して展開可能サーバーセットを制限します。サーバーがホワイトリストにある場合、自動検出時およびハンドシェイクプロセス中に認証情報が提供され、展開に使用されるサーバーリストに表示されます。ホワイトリストは、サーバーサービスタグの追加、サービスタグの削除、または CSV ファイルからサービスタグリストをインポートすることにより、手動で保守されます。

 **メモ:** サーバーをインポートするには、CSV の区切り付きファイルを使用します。これには別々の行の複数のレコードが含まれ、各レコードには1つまたはカンマで区切られた複数のサービスタグが含まれません。

ホワイトリストを設定し、管理するには、以下から選択してください。

- [サーバーホワイトリストの有効化](#)
- [ホワイトリストへのサーバーの追加](#)
- [ホワイトリストからのサーバーの削除](#)

展開可能サーバーホワイトリストの有効化

展開可能サーバーのセキュリティ設定に関する情報については、「[展開のためのサーバーセキュリティ設定](#)」を参照してください。

サーバーホワイトリストを有効化するには、以下を行います。

1. **Dell Management Center** の左ペインで **設定** を選択します。
2. 右ペインで、**セキュリティ** を選択します。
3. **セキュリティ** ウィンドウで、**編集** をクリックします。
4. サーバーの展開を制限するためにホワイトリストを使用するには、**サーバーホワイトリストを強制する** チェックボックスを選択します。
5. **適用** をクリックすると、サーバーホワイト設定が有効に変わります。

ホワイトリストへの展開可能サーバーの追加

展開可能サーバーに対するセキュリティ設定に関する情報については、「[展開のためのサーバーセキュリティ設定](#)」を参照してください。実施した場合、サーバーホワイトリストに記載されている Dell サーバーのみが Dell Management Plug-in を使用して展開可能となります。ホワイトリストに展開可能サーバーを追加するには、手動で、またはリストを使ってインポートすることができます。

展開可能サーバーをホワイトリストに追加するには、以下を行います。

1. **Dell Management Center** の左ペインで **設定** → **セキュリティ** を選択します。
2. **サーバーホワイトリスト** ウィンドウで、**編集** をクリックして、以下のいずれかを行います。
 - サーバーをホワイトリストに手動で追加するには、**サーバーの追加** をクリックします。
 - * **サービスタグの追加** ダイアログで、サービスタグを入力します。
 - * タグを追加するには、**続行** をクリックします。
 - サービスタグのリストをインポートするには、**ホワイトリストのインポート** をクリックします。
 - * **アップロードファイルの選択** ダイアログボックスが表示されたら、該当の CSV ファイルを参照し、**開く** をクリックします。
 - * **ファイルでこれらのサービスタグを検出しました** ダイアログが表示されたら、**適用** をクリックします。

サービスタグが、サービスタグリストに表示されます。

ホワイトリストからの展開可能サーバーの削除

展開可能サーバーのセキュリティ設定に関する情報については、「[展開のためのサーバーセキュリティ設定](#)」を参照してください。

展開可能サーバーをホワイトリストから削除するには、以下を行います。

1. **Dell Management Center** の左ペインで、**設定**を選択します。
2. 右ペインで、**セキュリティ**を選択します。
3. **セキュリティ**ウィンドウで **編集**をクリックします。
4. 次の手順のいずれか1つを実行します。
 - 個別サーバーを削除するには、**サービスタグ**チェックボックスをクリックして、次に **選択項目の削除**をクリックします。
 - 全サーバーを削除するには、**サービスタグ**チェックボックスをクリックして、次に **選択項目の削除**をクリックします。
5. **選択したサービスタグを削除してよろしいですか** ダイアログが表示されたら、**適用**をクリックするか、または **キャンセル**をクリックして取り消します。
6. 変更が完了したら、**適用**をクリックします。

ホスト、ベアメタルおよび iDRAC 対応問題について

ホスト、ベアメタルサーバー、および iDRAC を **Dell Management Plug-in** で管理するには、それぞれが一定の最低基準を満たさなければなりません。対応していない場合、**Dell Management Plug-in** で正しく管理できません。非対応のホスト、ベアメタルサーバー、および iDRAC 対応リンクを使って、どのホスト/ベアメタルサーバー/iDRAC が非対応となっているか確認し、修正します。このウィザードは次の状態にあるホスト/ベアメタルサーバー/iDRAC を表示します。

- ホストが接続プロファイルに割り当てられていない。
接続プロファイルがホストに割り当てられない場合、接続プロファイル画面に移動するためのダイアログボックスが表示されます。この設定はこのウィザードの範囲外です。後でこのウィザードの実行に戻ってください。
- 再起動時にシステムインベントリを収集 (CSIOR) が無効化されている、または実行されたことがないので手動の再起動が必要。
- OMSA エージェント (ホストルート資格情報) がインストールされていない、古い、または正しく設定されていない。
- ベアメタルサーバーの **Integrated Dell Remote Access Controller (iDRAC)** ファームウェア、**Lifecycle Controller (LC)** ファームウェア、または BIOS バージョンが古い。

△ **注意:** ロックダウンモードのホストは、非対応であっても対応確認に表示されません。表示されないのは対応ステータスが確認できないからです。これらのシステムの対応状況は手動で確認してください。確認が必要な場合は警告が表示されます。

それぞれの場合、以下のいずれかを実行して対応問題を解決する必要があります。

- vSphere ホスト対応問題を解決するには、「[非対応の vSphere ホスト解決ウィザードの実行](#)」を参照してください。
- 対応問題のあるベアメタルサーバーを解決するには、「[非対応のベアメタルサーバー解決ウィザードの実行](#)」を参照してください。
- iDRAC 対応問題を解決するには、「[iDRAC ライセンス対応](#)」を参照してください。

関連情報

- [ベアメタルサーバー対応性の再確認](#)
- [手動ファームウェアアップデートのための ISO のダウンロード](#)

非対応 vSphere ホストの解決ウィザードの実行

非対応 vSphere ホストの解決ウィザードを実行して、非対応ホストを解決します。対応については、「[ホストおよびベアメタルの対応問題について](#)」を参照してください。非対応 ESXi ホストの一部では再起動が必要です。OMSA がインストールまたはアップデートされる ESXi ホストでは再起動が必要です。また、CSIOR を実行したことがないホストも再起動が必要です。ESXi ホストを自動的に再起動するよう選択した場合は、次の動作が行われます。

- **CSIOR ステータスの解決のために:**
ホストで CSIOR が実行されたことがない場合、CSIOR はホストで オンと設定され、ホストはメンテナンスモードに入り、再起動されます。
- **OMSA ステータスの解決のために:**
 - a. OMSA がホストにインストールされます。
 - b. ホストは、メンテナンスモードに入り、再起動されます。
 - c. 再起動が完了すると、OMSA は変更が適用されるよう設定されます。
 - d. ホストはメンテナンスモードを終了します。
 - e. インベントリが実行され、データが更新されます。

非対応 vSphere ホストの解決ウィザードを実行するには、以下を行います。

1. **Dell Management Center** の左ペインで **対応 → vSphere ホスト** をクリックします。
2. **vSphere ホストの対応** ウィンドウで、非対応ホストを表示し、次に **非対応 vSphere ホストの修正** をクリックします。
3. **非対応 vSphere ホストの修正** ウィザードで、解決したいホストのチェックボックスを選択します。
4. **次へ** をクリックします。
5. 接続プロファイルのないサーバーがある場合は、ウィザードを終了してそれらのシステムを **接続プロファイル** ページで解決するか、このウィザードを継続するかのオプションが示されます。「[新規接続プロファイルの作成](#)」を参照してください。完了したらこのウィザードに戻ります。
6. **CSIOR をオンにする** ウィンドウで、選択されたホストの **CSIOR** を起動するチェックボックスを選択します。
7. **次へ** をクリックします。
8. **OMSA の修正** ウィンドウで、選択されたホストの **OMSA** を解決するチェックボックスを選択します。
9. **次へ** をクリックします。
10. **ホストの再起動** ウィンドウで、再起動しなければならない ESXi ホストを表示します。ESXi ホストは、OMSA がインストールまたはアップデートされる場合、再起動が必要です。また、CSIOR が実行されたことがないホストも再起動が必要です。以下のいずれかを行います。
 - 自動的にホストを保守モードにして、必要ときに再起動するには、**ホストを自動的にメンテナンスモードに切り替えて、必要に応じて再起動する** チェックボックスを選択します。
 - 手動で再起動したい場合、以下を行う必要があります。
 1. ホストで **OMSA** のインストールタスクが完了したら、ホストを再起動します。
 2. ホストが立ち上がったら、OMSA が設定されていない場合は、OMSA を手動で設定するか、対応ウィザードを使用します。
 3. インベントリを再実行します。「[インベントリジョブの実行](#)」を参照してください。
11. **次へ** をクリックします。
12. **概要** ウィンドウで、非対応ホストで行われる操作を確認します。これらを適用するには、手動での再起動が必要です。
13. **終了** をクリックします。

非ベアメタルサーバーの解決ウィザードの実行

非対応ベアメタルサーバーの解決ウィザードを実行して、非対応ベアメタルサーバーを解決します。対応に関する情報は、「[ホストおよびベアメタルの対応問題について](#)」を参照してください。

非対応ベアメタルサーバーの解決ウィザードを実行するには、以下を行います。

1. **Dell Management Center** の左ペインで、**対応** → **ベアメタルサーバー** をクリックします。
2. ベアメタルサーバーウィンドウで非対応ホストを表示し、**非対応ベアメタルサーバーの修正** をクリックします。
3. **ベアメタルサーバーの修正** ウィザードで、解決したいホストのチェックボックスを選択します。
4. **次へ** をクリックします。
5. **概要** ウィンドウで、非対応ベアメタルサーバーで行われる操作を確認します。
6. **終了** をクリックします。

ベアメタルサーバー対応性の再確認

Dell Management Plug-in 外で解決したサーバーについては、この手動でのサーバー対応性再確認を実行する必要があります。これは **Dell Management Center**、**対応**、**ベアメタルサーバー** ページで見つけることができます。

ベアメタルサーバー対応性を再確認するには、以下を行います。

1. **Dell Management Center** → **対応** → **ベアメタルサーバー** ページで、**対応の再チェック** をクリックします。
2. **非対応サーバー** ウィンドウで、リストを更新するには、**更新** をクリックします。
3. 再確認を実行するには、**対応のチェック** をクリックします。
4. 再確認を中止するには、**すべてのテストを中止** をクリックします。
5. システムが正しく解決された場合、リストは更新されシステムがリストから取り外されます。そうでない場合は、非対応システムはリストに残ります。
6. 終了したら、**完了** をクリックします。

手動ファームウェアアップデートのための ISO のダウンロード

Dell Management Plug-in はほとんどの問題を自動的に解決します。ときには、手動の **ISO** インストールが必要な場合があります。必要な **ISO** は、**Dell Management Center** の対応セクションからブラウザでダウンロードすることができます。

1. **Dell Management Center** → **対応** → **ベアメタルサーバー** ページで、**ISO** をダウンロードするには、**ISO のダウンロード** をクリックします。
2. **ISO のダウンロード** ダイアログボックスで、**ISO** のロケーションを見つけるには、**ダウンロード** をクリックします。

 **メモ:** 外部ブラウザウィンドウがこのアプリケーションウィンドウの背後で開く可能性があります。

3. 対応させる必要があるベアメタルサーバーの **ISO** ファイルに移動します。

iDRAC ライセンスの対応

iDRAC ライセンス対応のページを選択すると、対応テストが実行されます。このテストには数分かかります。このページに記載されている **vSphere** ホストおよびベアメタルサーバーは互換性のある **iDRAC** ライセンスがないため非対応です。テーブルには、**iDRAC** ライセンスのステータスが表示されます。このページには、ライセンスの残余期間が示されるので、必要に応じてアップデートします。[インベントリジョブの実行リンク](#)が無効になっている場合、それは、**iDRAC** ライセンスのために非対応となっている **vSphere** ホストがないこと

を示しています。ベアメタルサーバー対応の再チェックリンクが無効になっている場合、それは iDRAC ライセンスのために非対応となっているベアメタルサーバーがないことを示しています。

1. **Dell Management Center** の左ペインで、**対応**をクリックします。
2. **対応**を展開して **iDRAC ライセンス**をクリックします。
このページに到着すると、対応テストが実行されます。これは **更新**をクリックしたときに実行されるものと同じテストです。
3. ライセンスが古い場合、**iDRAC ライセンスの購入/更新**をクリックします。
4. **Dell ライセンス管理**ページにログインし、新しい iDRAC ライセンスにアップデートまたは購入します。
このページの情報を使って、iDRAC を識別およびアップデートします。
5. iDRAC ライセンスのインストール後、vSphere ホスト用にインベントリジョブを実行し、インベントリジョブ完了後このページに戻ります。ベアメタルサーバーに関しては、ライセンスされたベアメタルサーバーの対応性を再確認します。

Dell Management Plug-In For VMware vCenter のアップグレード

Dell Management Plug-in のアップグレードには 3 つのシナリオがあります。

- [バージョン 1.0 から現行バージョンへのアップグレード](#)
- [試用バージョンの Dell Management Plug-in から完全製品バージョンへのアップグレード](#)
- [Dell Management Plug-in の旧バージョン \(1.0.1 以降\) から現行バージョンへのアップデート](#)

 **メモ:** アップグレードの開始前に、アプライアンスバックアップを実行します。「[即時のバックアップの実行](#)」を参照してください。

バージョン 1.0 から現行バージョンへのアップグレード

バージョン 1.0 から現行バージョンにアップグレードするには、次の手順を実行します。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール**タブに表示されている、設定したい仮想マシンの**管理コンソール**を起動するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL には <https://<アプライアンスの IP アドレス>> フォーマットが使用され、大文字と小文字が区別されます。
2. 管理コンソールで、vCenter インスタンスから登録されている 1.0 アプライアンスの登録を取り消すには、**VCENTER 登録** → **登録の解除**を選択します。
3. 仮想アプライアンスデータをネットワーク共有ロケーションにバックアップするには、**管理コンソール**の左ペインから **バックアップおよび復元**を選択します。
4. vSphere で 1.0 仮想アプライアンスをシャットダウンします。
5. アプライアンスコンソールのユーザーインターフェイスで、vSphere クライアントから新しい 現行バージョンのアプライアンス OVF を展開し、管理パスワードを設定してネットワークを設定します。

 **メモ:** 現行バージョンのアプライアンスが 1.0 バージョンと同じ IP アドレスを使用している場合は、Internet Explorer キャッシュを消去します。

6. 完全製品バージョンにアップグレードするには、手順 1 を繰り返します。
7. **管理コンソールログイン**ダイアログボックスの、下に**パスワードを入力**テキストボックスにパスワードを入力し、**ログイン**をクリックします。
8. 製品ダウンロードパッケージには、**Dell_Management_Center_license.bin** ファイルが含まれています。このファイルには製品ライセンスが含まれており、アプライアンスにアップロードする必要があります。ライセンスファイルをアップロードするには、**管理コンソール**の **vCenter 登録** ページで、**ライセンスのアップロード**をクリックします。
9. **ライセンスのアップロード**ダイアログボックスで **参照**をクリックし、ライセンスファイルを参照します。

10. ライセンスファイルをアップロードするには、**アップロード**をクリックします。
11. 現行バージョンの管理コンソールを使用して、ネットワーク共有からバックアップされていた 1.0 ユーザーデータを現行バージョンのアプライアンスに復元します。「[バックアップからのデータベースの復元](#)」を参照してください。
12. 新しい現行バージョンのアプライアンスを vCenter インスタンスに登録します。「[vCenter サーバーの登録](#)」を参照してください。
13. 現行バージョンの仮想アプライアンス通信に使用される新しいセキュリティ証明書をリロードするには、実行中の vSphere クライアントインスタンスを閉じ、再度開きます。
14. 現行バージョンの仮想アプライアンスが新しい環境で正常に動作していることを確認した後、1.0 仮想アプライアンスを削除することができます。

試用バージョンから完全製品バージョンへのアップグレード

試用バージョンから完全製品バージョンにアップグレードするには、次の手順を実行します。

1. **Dell ウェブサイト** へ移動し、完全製品バージョンを購入します。
または、**Dell Management Plug-in** で、管理ポータル**のライセンス供与** ウィンドウにあるリンクのような、**今すぐ購入** リンクを使って **Dell ウェブサイト** にアクセスすることもできます。
2. ダウンロードには、新しい完全バージョンの製品と新しいライセンスファイルが含まれています。
3. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、**Dell Management Console** → **設定** ページのリンクを使用します。URL には **https://<アプライアンスの IP アドレス>** フォーマットが使用され、大文字と小文字が区別されます。
4. **管理コンソールログイン** ウィンドウで、パスワードを入力し、**ログイン** をクリックします。
5. 製品ダウンロードパッケージには、**Dell_Management_Center_license.bin** ファイルが含まれています。このファイルには、製品ライセンスが含まれており、仮想アプライアンスにアップロードする必要があります。ライセンスファイルをアップロードするには、**アップロード** をクリックします。
6. **ライセンスのアップロード** ウィンドウで **参照** をクリックし、ライセンスファイルを参照します。
7. ライセンスファイルを選択して、**アップロード** をクリックします。

Dell Management Plug-in の旧バージョン (1.0.1 以降) から現行バージョンへのアップデート

1. ブラウザウィンドウを起動して、vSphere vCenter コンソールタブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、**Dell Management Console** → **設定** ページのリンクを使用します。URL には **https://<アプライアンスの IP アドレス>** フォーマットが使用され、大文字と小文字が区別されます。
2. **管理コンソール** の左ペインで、**アプライアンス管理** をクリックします。
3. アップグレードには、以下のいずれかを行います。
 - デフォルトのリポジトリパスのアップデートを使用するには、アプライアンス設定で **仮想アプライアンスのアップデート** をクリックし、手順 7 に進みます。
 - 新しくダウンロードされた RPM へのパスにアクセスするには、アプライアンス管理ページで、**編集** をクリックします。
4. **編集グループ** のリポジトリパスのアップグレードテキストボックスに、RPM へのパスを入力します。次に記載する表に従って、フォルダの場所をポイントするようにしてください。

	次からアップグレード		アップグレードフォルダ
	最新版	最新版 — 最高	最新版 — 最高 — 最高
1.0.1	x		
1.5.0	x		
1.5.1		x	
1.6.0			x

- この変更を保存するには、**適用** をクリックします。
- 仮想アプライアンスへのアップデートを適用するには、**アプライアンスの設定** で仮想アプライアンスのアップデートをクリックします。
- アプライアンスのアップデートダイアログボックスで**アップグレード**をクリックします。アップグレードをクリックすると、管理コンソールからログオフされます。

Dell Management Plug-in License について

Dell Management Plug-in には 2 つのタイプのライセンスがあります。

デモライセンス トライアルバージョンには、**Dell Management Plug-in** で管理できる 1 つの vCenter および 1 台のホスト（サーバー）用のデモライセンスが含まれています。

製品ライセンス 完全な製品バージョンには、**Dell Management Plug-in** で管理できる 3 つの vCenter および購入数分のホスト接続用の製品ライセンスが含まれています。

デモライセンスから完全製品ライセンスにアップグレードする場合、ダウンロードパッケージには、新しいライセンス XML ファイルが含まれています。管理コンソールを使ってこの新しいライセンスファイルをインストールします。ライセンスには、次の情報が表示されます。

- vCenter 接続ライセンスの最大数 - 最大 3 つの登録済みおよび使用中の vCenter 接続が許容されます。
- ホスト接続ライセンスの最大数 - 購入されたホスト接続数。
- 使用中 - 使用中の vCenter 接続またはホスト接続ライセンス。ホスト接続においては、この数は検出されインベントリされたホスト（またはサーバー）数を示します。
- 使用可能 - 将来使用可能な vCenter 接続またはホスト接続ライセンス数。
- ライセンスのないホスト - ライセンス数を越えたホスト接続数。Dell Management Plug-in は継続して正常に動作しますが、この警告を解消するには、新しいライセンスを購入してインストールする必要があります。

エンドツーエンドのハードウェア管理

エンドツーエンドのハードウェア管理の目的は、管理者が **Dell Management Center** または **vCenter** を離れずに、重大なハードウェア事象に対応するために必要な、システム正常性ステータスや最新のインフラストラクチャ情報を入手できるようにすることです。**Dell Management Plug-in** によるエンドツーエンドハードウェア管理は、4つの部分に分かれています。

- 監視
- インベントリ
- アドバンスホスト管理
- 保証検索

データセンターおよびホストシステムの監視

データセンターおよびホストシステム監視では、**vCenter** のタスクとイベントタブにハードウェア（サーバーおよびストレージ）および仮想化関連イベントを表示することにより、管理者はインフラストラクチャの正常性を監視することができます。また、重要ハードウェア警報によって **Dell Management Plug-in** はホストシステムを保守モードにし、場合によっては仮想マシンを他のホストシステムに移行します。**12G** より前のホストの場合、**Dell Management Plug-in** は **OMSA** アラームを転送して、特定のイベントについて新しいアラームを生成します。これらのアラームを使用して、再起動、保守モードまたは移行などの **vCenter** が許容する動作を起動することができます。例えば、デュアル電源が故障しアラームが生成された場合、その後の処置としてそのマシンの仮想マシンを他のマシンに移行することができます。

監視を実施するには以下を行います。

1. イベントとアラームを設定します。
2. 必要に応じて **OMSA** トラップ先を設定します（**12G** より前のホスト）。
3. **vCenter** でタスクとイベントタブを使用して、イベント情報を確認します。

イベントとアラームの理解

Dell Management Plug-in の **Management Center** における **設定** → **イベントとアラーム** でイベントとアラームを編集することができます。この項で、イベント掲載レベルの選択、**Dell** ホストへのアラームの有効化、またはデフォルトのアラームの復元を行うことができます。

4つのイベント掲載レベルがあります。

表 1. イベント掲載レベルの説明

イベント	説明
イベントは掲載しない	Dell Management Plug-in に対して、関連 vCenter にイベントまたは警告を送出させないようにします。
全イベントを掲載	管理下 Dell ホストから Dell Management Plug-in が受信する、非公式イベントを含むすべてのイベントを関連 vCenter に掲載します。

重要および警告イベントのみ掲載

重要または警告イベントのみを関連 vCenter に掲載します。

仮想化関連の重要および警告イベントのみを掲載

ホストから受信する仮想化関連イベントのみを、関連 vCenter に掲載します。仮想化関連イベントとは、仮想マシンを実行しているホストにとって最も重要であるとデルが選定したものです。

イベントとアラームを設定する際に、それらを有効にすることができます。有効化されると、重要なハードウェアアラームによって Dell Management Plug-in はホストシステムを保守モードにし、場合によって仮想マシンを別のホストシステムに移行します。Dell Management Plug-in は管理下 Dell ホストから受信したイベントを転送し、該当イベントに対するアラームを出します。このアラームを使い、vCenter に対し、再起動、保守モードまたは移行などの措置を起動できます。例えば、デュアル電源が故障しアラームが出された場合、対応措置はそのマシン上の仮想マシンを別のホストに移行します。

ホストはリクエストされた場合のみ、保守モードを起動または終了します。保守モードを起動するホストがクラスタの一部の場合、停止した仮想マシンを退避するオプションを選択できます。このオプションを選択した場合、停止した仮想マシンは、同一クラスタ内に当該仮想マシンとの互換性のあるホストがない場合を除き、それぞれ別のホストに移行されます。保守モードにある限り、ホストは仮想マシンの使用または起動を行いません。保守モードとなるホストで実行されている仮想マシンは、手動または VMware Distributed Resource Scheduling (DRS) により自動的に、別のホストに移行するかシャットダウンする必要があります。

クラスタ外のホスト、または VMware Distributed Resource Scheduling (DRS) が起動されていないクラスタにあるホストでは、重要イベントのために仮想マシンはシャットダウンされる可能性があります。DRS は全リソースプールの使用率を連続的に監視し、使用可能なリソースをビジネスニーズにしたがって各仮想マシンに知的に割り当てます。DRS と Dell Alarms が設定されたクラスタを使って、重要なハードウェアイベントの際に仮想マシンが自動的に移行されるようにしてください。画面上のメッセージの詳細に記載されているのは、この vCenter インスタンスにある、影響を受ける可能性のあるクラスタです。イベントと警報を有効化する前に、クラスタが影響を受けるかどうか確認してください。

デフォルトアラーム設定を復元する必要がある場合は、デフォルトアラームにリセットボタンで行います。このボタンは、製品のアンインストールと再インストールを行わずにデフォルトのアラーム設定を行うことができますので便利です。インストール以降に Dell アラーム設定が変更された場合、このボタンで元に戻すことができます。

 **メモ:** Dell Management Plug-in は、ホストが仮想マシンを実行するのに不可欠な仮想化関連イベントを予め選択します。Dell ホストアラームはデフォルトで無効化されています。Dell アラームを有効化する場合、クラスタは VMware Distributed Resource Scheduler を使って、重要イベントが送られる仮想マシンの移行を自動的に行うようにしなければなりません。

関連タスク:

- [イベントおよびアラームの設定](#)

イベントおよびアラームの設定

Dell Management Center イベントおよびアラームページでは、すべてのハードウェアアラームを有効または無効にできます。現在のアラートステータスは vCenter アラームタブに表示されます。重要イベントは実際のまたは切迫したデータ喪失あるいはシステム異常を示します。警告イベントは必ずしも重大ではないが、将来の潜在的な問題を示す可能性があります。イベントおよびアラームは VMware Alarm Manager を使用して有効化することもできます。イベントは、ホストとクラスタビューの vCenter タスクとイベントタブに表示されます。

 **メモ:** 12G より前のホストでは、ホストイベントを vCenter で表示するには、仮想アプライアンスが OMSA でトラップ先として設定されている必要があります。OMSA に関する詳細は、「[OMSA トラップ先の設定](#)」を参照してください。

イベントおよびアラームは、Dell Management Center のイベントとアラームの設定オプションで設定できます。

イベントおよびアラームを設定するには、以下を行います。

1. **Dell Management Center** の設定 → イベントとアラーム で **編集** をクリックします。
2. **イベント掲載レベル** で以下のいずれかを選択します。
 - すべてのイベントを掲載をしない - ハードウェアイベントはブロックされます。
 - すべてのイベントを掲載する - すべてのハードウェアイベントが掲載されます。
 - 重要および警告イベントのみを掲載する - 重要または警告レベルのハードウェアイベントのみが掲載されます。
 - 仮想化関連の重要および警告イベントのみを掲載する - 仮想化関連の重要および警告イベントのみが掲載されます。これはデフォルトのイベント掲載レベルです。
3. すべてのハードウェアアラームとイベントを有効化するには、**Dell ホストのアラームを有効にする** チェックボックスを選択します。
 **メモ:** アラームが有効化されている Dell ホストは、重要イベントに対応して保守モードに入ります。
4. 表示されるダイアログボックスで **続行** をクリックしてこの変更を確定するか、または **キャンセル** をクリックします。
5. すべての管理されている Dell サーバーで、デフォルトの vCenter アラーム設定を復元するには、**デフォルトのアラームの復元** をクリックします。
変更が有効になるには、最大 1 分かかることがあります。
6. 保存するには、**保存** をクリックします。

第 11 世代ホスト向け OMSA について

第 12 世代より前のサーバーでは、Dell Management Plug-in との連動のため、OMSA のインストールが必須です。OMSA は展開中に第 11 世代ホストに自動でインストールされますが、手動でインストールしたい場合は、それも可能です。

-  **メモ:** メモ : Dell Management Center の対応性ウィンドウから利用できる *非対応 vSphere* ホストの修正リンクを使用して OMSA を展開する場合、OMSA VIB のダウンロードおよびインストールのため、Dell Management Plug-in は httpClient サービスを開始してポート 8080 を有効にし、ESXi 5.0 以降を開始します。OMSA のインストールが完了すると、サービスは自動的に停止し、ポートは閉じられます。

OMSA を第 11 世代ホストで設定するには、以下のいずれかを選択します。

- [OMSA エージェントを ESXi システムに展開](#)
- [OMSA エージェントを ESX システムに展開](#)
- [OMSA トラップ先の設定](#)
- [OMSA リンクの有効化](#)

OMSA エージェントの ESX システムへの展開

OMSA tar.gz を ESX システムにインストールし、システムからインベントリと警告情報を収集します。

-  **メモ:** Dell OpenManage エージェントは、バージョン 12G より前の Dell ホストが必要です。OMSA は Dell Management Plug-in のインストール前に Dell Management Plug-in を使って、または手動でホストにインストールできます。エージェントの手動インストールの詳細は、<http://support.dell.com/support/edocs/software/eslvmwre/sysman/sysman.htm> を参照してください。ESX/ESXi ソフトウェアの適切なバージョンのガイドを開き、「Installing the Dell OpenManage Server Administrator」(Dell OpenManage サーバー管理者のインストール) の章を参照してください。

OMSA エージェント tar.gz を ESX システムに展開し、必要なリモート有効化設定 (-c) を行うには、次の手順を実行します。

1. OMSA エージェントインストールスクリプトを実行します。

```
sh srvadmin-install.sh -x
```
2. OMSA サービスを起動します。

```
srvadmin-services.sh start
```
3. OMSA エージェントがすでにインストールされている場合、リモート有効化設定 (-c) が行われているか確認してください。設定されていない場合は、Dell Management Plug-in のインストールは正しく完了しません。-c オプションで再インストールしてサービスを再起動します。

```
srvadmin-install.sh -c srvadmin-services.sh restart
```

OMSA エージェントの ESXi システムへの展開

OMSA VIB を ESXi システムにインストールし、システムのインベントリおよび警告情報を収集します。

-  **メモ:** Dell OpenManage エージェントは、バージョン 12G より前の Dell ホストで必要です。OMSA は Dell Management Plug-in のインストール前に Dell Management Plug-in を使って、または手動でホストにインストールできます。エージェントの手動インストールの詳細は、<http://support.dell.com/support/edocs/software/eslvmwre/sysman/sysman.htm> を参照してください。ESX/ESXi ソフトウェアの適切なバージョンのガイドを開き、「Installing the Dell OpenManage Server Administrator」(Dell OpenManage サーバー管理者のインストール) の章を参照してください。

OMSA VIB を ESXi システムに展開するには、以下を行います。

-  **メモ:** 次の URL には、OMSA VIB のインストール情報とダウンロードリンクが含まれます。<http://www.delltechcenter.com/page/Install+and+Configure+OMSA+on+ESX>
1. すでにインストールされていない場合は、vSphere コマンドラインツール (vSphere CLI) を <http://www.VMWare.com> からインストールします。
 2. 次のコマンドを入力します。

```
Vihostupdate.pl -server <IP Address of ESXi host> -i -b OM-SrvAdmin-Dell-Web-6.3.0-2075.VIB-ESX41i_A00.8.zip
```

 -  **メモ:** OMSA のインストールには数分かかることがあります。このコマンドの完了後、ホストを再起動する必要があります。

OMSA トラップ先の設定

このタスクは、イベント作成に iDRAC6 の代わりに OMSA を使用するホストシステムのみにも適用されます。iDRAC6 には追加設定は必要ありません。

-  **メモ:** OMSA は、バージョン 12G より前の Dell サーバーのみで必要となります。

OMSA トラップ先を設定するには、以下を行います。

1. **設定** → **一般**にある OMSA ユーザーインターフェースへのリンクを使用するか、またはウェブブラウザ (<https://<HostIP>:1311/>) から OMSA エージェントに移動します。
2. インタフェースにログインして、**アラート管理**タブを選択します。
3. **アラート処置**を選択し、監視対象イベントに**ブロードキャストメッセージ**オプションが設定されており、イベントが送出されることを確認します。
4. タブの上部にある、**プラットフォームイベント**オプションを選択します。
5. グレーの**宛先の設定**ボタンをクリックし、次に**宛先**リンクをクリックします。
6. **トラップ先を有効にする**チェックボックスを選択します。
7. Dell Management Plug-in アプライアンス IP アドレスを**宛先 IP アドレス**欄に入力します。
8. **変更の適用**をクリックします。
9. さらなるイベントの設定には、手順 1 ~ 8 を繰り返します。

イベントの表示

イベントを表示するには、以下のいずれかを行います。

- 仮想マシンへ移動し、右クリックして **vCenter** → **vCenter のタスクとイベント** タブを表示し、**イベント** をクリックして選択したイベントレベルを表示します。
- ホストまたは **vCenter** のルートフォルダの親ノード（クラスタまたはデータセンター）をクリックします。

イベントは、**vSphere** ツリーのノードのみに表示されます。

vSphere クライアントホストの概要

この概要では、個別コンポーネントの正常性、識別、ハイパーバイザー、およびファームウェア情報などの主なホストサーバー属性に関する情報が提供されます。

ハードウェアコンポーネントの正常性

コンポーネントの正常性は、システムシャシ、電源装置、温度、ファン、電圧、プロセッサ、バッテリー、インテリジェン、ハードウェアログ、電力管理およびメモリなど、すべての主要ホストサーバーコンポーネントに関するグラフ表示です。表示可能なステータスには以下があります。

- 健全（緑色のチェックマーク） - コンポーネントは正常に動作
- 警告（黄色の三角に感嘆符） - コンポーネントには重大でない不具合があります
- 重要（赤い X 印） - コンポーネントには重大な障害があります
- 不明（疑問符） - コンポーネントステータスは不明

グローバルの正常性ステータスはヘッダーバーの右上に表示されます。

サーバー情報

サーバー情報では、以下のような識別、ハイパーバイザー、およびファームウェア情報が提供されます。

- ホスト名、電源状態、**iDRAC IP**、管理 **IP**、使用中の接続プロファイル、モデル、サービスタグおよび資産タグ番号、保証残り期間、最後のインベントリスキャン実行日。
- ハイパーバイザー、**BIOS** ファームウェア、および **iDRAC** ファームウェアバージョン。
- **10** 個の最新システムイベントログ項目。詳細をクリックして、さらなるログ詳細を表示するシステムイベントログウィンドウを起動します。

ホスト情報

ホスト概要の左ペインに、以下のようなホスト情報へのリンクが提供されます。

- システムイベントログ
ハードウェアシステムイベントログ情報を表示します。「[システムイベントログの理解](#)」を参照してください。
- ハードウェアインベントリ
以下のハードウェアデバイスについて情報を表示します。
 - DIMM、システムプラナー、電源装置、バックプレーン、コントローラカードなどのフィールド交換可能装置 (FRU)
 - メモリ - 使用可能および使用中のスロット数、最大容量および使用中のメモリ量、および個別 DIMM の詳細。
 - ネットワークインタフェースカード (NIC) - インストールされているカード数および個別 NIC の詳細。
 - PCI スロット - 全スロット数および使用スロット数ならびに個別スロットに関する詳細。
 - 電源装置 - 総数および個別 PSU の詳細。
 - プロセッサ - 総数および個別 CPU の詳細。

- リモートアクセスカード - IP アドレス情報と RAC タイプ、およびウェブインタフェース URL。

「[インベントリジョブについて](#)」を参照してください。

- 保管時

ホストシステムストレージは、ホストベースのストレージコントローラに接続されている、物理および論理ストレージの容量およびタイプのグラフおよび詳細表示を提供しています。それには以下が含まれます。

- ホストシステムの合計ストレージ容量、設定済み、未設定、グローバルおよび専用ホットスペア両方のディスク容量
- 当該コンポーネントに関する詳細情報を含む、システムコンポーネントデータテーブルに存在している各ストレージコンポーネント数のリスト

- ファームウェア

ファームウェアアップデートウィザードを実行、またはファームウェアステータスを表示します。

「[ファームウェアのアップデート](#)」を参照してください。

- 電源監視

ホストシステム電源監視は、一般的な電源情報、エネルギー統計情報、および予備電源情報を提供します。これには以下が含まれます。

- 現在の電力バジェット、プロファイル、警告および故障のしきい値
- エネルギー消費量、システムピーク電力およびアンペア数統計情報
- 予備電源およびピーク予備容量



メモ: すべての電源装置はこの機能を備えておらず、ブレードエンクロージャの電源装置には対応していません。

- 保証

保証の取得は、Dell サーバーについて以下の情報を提供します。

- アップデートされたサービス保証情報、ただしホストサービスタグのみを送信
- 定期的にアップデートされた保証情報
- プロキシサーバーおよび資格情報を使ったセキュアな送信
- 検証されたセキュアな接続による情報

「[保証の取得](#)」を参照してください。

ホストアクション

ホストアクションは、以下のような現在のホストサーバーに実行されたコマンドです。

- インジケータライトを点滅をクリックして、LCD 前面インジケータを点滅させます。「[物理サーバー前面インジケータライトの設定](#)」を参照してください。
- ファームウェアアップデートウィザードの実行をクリックして、ファームウェアアップデートウィザードを表示し、ホストサーバーファームウェアをアップデートします。「[ファームウェアアップデートウィザードの実行](#)」を参照してください。

管理コンソール

管理コンソールを使って以下のような外部システム管理コンソールを起動します。

- リモートアクセスコンソールをクリックして、Integrated Dell Remote Access Controller (iDRAC) ウェブユーザーインタフェースを起動します。
- 設定されている場合、OMSA コンソールをクリックして、OpenManage Server Administrator (OMSA) ユーザーインタフェースを起動します。[OMSA リンクの有効化](#)を参照してください。
- ブレードシャーシコンソールをクリックして、Chassis Management Controller (CMC) ウェブユーザーインタフェースを起動します。

Dell オンラインサービス

Dell オンラインサービスは、ホストシステムの保証を更新するためのアクセスを提供します。

- 保証の更新をクリックして、ホストシステムの保証を更新するために使用されるポータルを起動します。サーバー情報で残存保証期間の確認ステータスを確認し、保証の更新が必要か判断します。保証期限が近くなると警告または重大アイコンが表示されます。「[ホスト保証の更新](#)」を参照してください。

インベントリスケジュールについて

インベントリスケジュールは、以下のようにインベントリジョブを実行する時刻 / 日付を設定します。

- 毎週の特定の時刻と曜日
- 一定の期間ごと

大部分の Dell Management Plug-in 機能に必要なデータを収集するため、インベントリの実行が必要です。この情報を表示するには、すべてのホストシステムのインベントリを収集する必要があります。ホストシステムに関するインベントリを実施するには、通信と資格情報を提供する接続プロファイルを作成しなければなりません。インベントリが完了すると、全データセンターまたは個別ホストシステムのインベントリ結果を表示できます。

 **メモ:** インベントリに最新情報が含まれていることを確実にするため、インベントリジョブは最低1週間に1度行われるようスケジュールしてください。インベントリジョブは最低限のリソースしか消費せず、ホスト性能が劣化することはありません。

関連タスク:

- [インベントリジョブの実行](#)
- [インベントリジョブスケジュールの変更](#)
- [シングルホストシステムのインベントリの表示](#)
- [データセンターハードウェア設定およびステータスの表示](#)

インベントリジョブスケジュールの変更

インベントリスケジュールは、次のようにインベントリジョブを実行する日付と時刻を設定します。

- 毎週特定の曜日の特定の時刻などが設定できます。
- Dell Management Plug-in 機能の大部分で必要とされるデータを収集するため、一定間隔でインベントリを実施する必要があります。

 **メモ:** インベントリに最新情報が含まれるようにするためには、最低1週間に1度はインベントリジョブを実行するようにします。インベントリジョブは最小限のリソースしか消費しないので、ホストパフォーマンスを低下させません。

インベントリジョブスケジュールを変更するには、以下を行います。

1. Dell Management Center で **設定** → **インベントリのスケジュール** を選択します。
2. 現在のスケジュールを変更するには、**編集** をクリックします。
3. **選択した曜日** オプションボタンを選択し、次に曜日のチェックボックスを選択して、時刻を入力します。入力情報を消去するには、**クリア** をクリックします。
4. インベントリスケジュールを変更するには、**適用** をクリックします。あるいは、インベントリスケジュールを取り消すには、**キャンセル** をクリックします。
5. ジョブを今すぐ実行するには、管理センターで **ジョブキュー** と **インベントリ履歴** タブを選択します。
6. **今すぐ実行** をクリックします。
7. 前回のインベントリジョブの詳細をアップデートするには、**更新** をクリックします。

vCenter におけるシングルホストシステムのインベントリ表示

シングルホストシステムのインベントリを表示するには、以下を行います。

1. **vSphere クライアント** から、**インベントリ**の見出しの下で **ホストとクラスタ**を選択します。
2. **ホストとクラスタ**から、左ペインでホストシステムを選択し、次に **Dell Server Management** タブを選択します。
3. 選択されたホストの概要が表示されます。
概要には、個別コンポーネントの正常性、識別情報、ハイパーバイザー、およびファームウェア情報を含む、主なホストサーバー属性が提供されます。
 - ハードウェアコンポーネントの正常性は、すべての主なホストサーバーコンポーネントのステータスのグラフ表示です。それには、システムシャーシ、電源装置、温度、ファン、電圧、プロセッサ、バッテリー、インテリジェン、ハードウェアログ、電源管理、およびメモリが含まれます。以下のような利用可能なステータスがあります。
 - * 健全 (緑色のチェックマーク) - コンポーネントは正常に動作
 - * 警告 (黄色の三角に感嘆符) - コンポーネントには重大でない不具合があります
 - * 重要 (赤い X 印) - コンポーネントには重大な障害があります
 - * 不明 (疑問符) - コンポーネントステータスは不明
 - グローバルの正常性ステータスはヘッダーバーの右上に表示されます。
 - サーバー情報は、次のような識別情報、ハイパーバイザー、およびファームウェア情報を提供します。
 - * ホスト名、電源状況、iDRAC IP アドレス、管理 IP アドレス、使用中の接続プロファイル、モデル、サービスタグと資産タグ番号、保証残余期間、最後のインベントリスキャン実行日。
 - * ハイパーバイザー、BIOS ファームウェア、および iDRAC ファームウェアバージョン
 - 最新システムログには、最新 10 個のシステムイベントログ項目が提供されます。システムイベントログウィンドウを起動して、さらなるログ詳細を表示するには、**詳細**をクリックします。
4. **ホスト情報**で、**ハードウェアインベントリ**をクリックして、次のようなホストシステムにインストールされているすべてのコンポーネントのリストと、さらなる詳細を表示します。
 - フィールド交換可能装置 (FRU) - DIMMS、システムブランチ、電源装置、バックプレーン、コントローラカード等。
 - メモリ - 使用可能および使用中のスロット数、最大容量および使用中のメモリ量、および個別 DIMM の詳細。
 - ネットワークインタフェースカード (NIC) - インストールされているカード数および個別 NIC の詳細。
 - PCI スロット - 使用可能および使用中のスロット数、および個別スロットの詳細。
 - 電源装置 - 総数および個別 PSU の詳細。
 - プロセッサ - 総数および個別 CPU の詳細。
 - リモートアクセスカード - IP アドレス情報、RAC タイプ、およびウェブインタフェース URL。
5. **ホスト情報**で**ストレージ**をクリックして、次のような物理および仮想ストレージの容量とタイプのグラフおよび詳細ビューを表示します。
 - ホストシステムの合計ストレージ容量、設定済み、未設定およびグローバルホットスペアのディスク容量。
 - システムにインストールされている各ストレージコンポーネント数のリスト。
 - 当該コンポーネントに関する詳細情報を含むコンポーネントデータテーブル。
6. **ホスト情報**で、**ファームウェア**をクリックして、以下を含むすべての Dell Lifecycle Controller ファームウェア情報を表示します。

- アップデート名 - BIOS、Dell Lifecycle Controller、電源装置等。
 - アップデートタイプ - BIOS、ファームウェアまたはアプリケーション。
 - 個別アップデート詳細 - アップデートが進行中の場合、バージョン、インストール時刻、またはアップデートステータスおよびアップデートバージョン。アップデートステータスとバージョンには、アップデートがスケジュールされている場合にのみデータが含まれ、アップデートバージョンは、システムが今後アップデートされるファームウェアバージョンです。
7. **ホスト情報**で、**電源監視**をクリックし、次のような一般電源情報、エネルギー統計情報、および予備電源情報を表示します。
- 現在の電力バジェット、プロファイル、警告および障害しきい値。
 - エネルギー消費量、システムピーク電力、およびアンペア数統計情報。
 - 予備電源およびピーク予備容量。
8. **ホスト情報**で**保証**をクリックして、次のようなシステム保証情報を表示します。
- 保証プロバイダ名および保証の説明。
 - 保証の開始および終了日ならびに残余期間。
 - 保証ステータス（有効、無効）および最新保証情報アップデート日。

インベントリおよびライセンス

サーバーデータの検索と表示ができない場合、いくつかの原因が考えられます。

- サーバーが接続プロファイルによって関連付けられておらず、インベントリタスクが完了できませんでした。
- データを収集するインベントリタスクがサーバーで実行されなかったため、表示できるデータがありません。
- ホストライセンス数が超過しており、インベントリタスクを完了するにはさらなるライセンスが必要です。
- このサーバーには、12G サーバーに必要な正しい iDRAC ライセンスがないので、正しい iDRAC ライセンスを購入する必要があります。

今すぐ購入リンクは、初めて製品を購入するためのものであり、アップグレードのためではありません。今すぐ購入リンクはデモライセンスを使用している場合のみ表示されます。

関連タスク:

- [既存接続プロファイルの表示および編集](#)
- [インベントリジョブスケジュールの変更](#)

Dell Management Plug-in には 2 つのタイプのライセンスがあります。

- デモライセンス: トライアルバージョンには、Plug-in によって管理される 1 つの vCenter および 1 つのホスト（サーバー）用のデモライセンスが含まれます。
- 製品ライセンス: 完全な製品バージョンには、Dell Management Plug-in によって管理される 3 つの vCenter および購入したホスト接続数のライセンスが含まれます。

関連タスク:

- [Dell Management Plug-in License について](#)
- [管理コンソールへの Dell Management Plug-in ライセンスのアップロード](#)

ストレージインベントリの表示

ホストシステムストレージは、ホストベースのストレージコントローラに接続されている、物理および論理ストレージの容量およびタイプのグラフおよび詳細表示を提供しています。それには以下が含まれます。

- ホストシステムの合計ストレージ容量、設定済み、未設定、グローバルおよび専用ホットスペア両方のディスク容量
- システムにある各ストレージコンポーネント数のリスト
- 当該コンポーネントに関する詳細情報を含む、コンポーネントデータテーブル

ストレージデータの表示には以下を行います。

1. **vSphere** クライアントで、ホストを選択し、次に **Dell Server Management** タブを選択します。
2. ホストの**概要**ページの左ペインで、**ストレージ**をクリックします。
3. **ストレージ**ページでグラフ概要を表示するか、テーブルと **表示**および**フィルタ**ドロップダウンリストを使ってインベントリ情報を並べ替えます。

ホスト電源監視の表示

ホストシステム電源監視は、一般的な電源情報、エネルギー統計情報、および予備電源情報を提供します。これには以下が含まれます。

- 現在の電力バジェット、プロファイル、警告および故障のしきい値
- エネルギー消費量、システムピーク電力およびアンペア数統計情報
- 予備電源およびピーク予備容量

ホスト電源監視を表示するには、次を実行します。

1. **vSphere** クライアントでホストを選択し、次に **Dell Server Management** タブを選択します。
2. **ホスト情報**の左ペインで**電源監視**をクリックします。
3. **電源監視**ページで、このホスト用の電源を表示します。

全データセンターハードウェアの設定およびステータスの表示

全データセンターハードウェアの設定およびステータスを表示する前に、インベントリジョブを完了する必要があります。インベントリを実行したら、以下のいずれも表示することができます。

- ハードウェア: フィールド交換可能パーツ
- ハードウェア: プロセッサ
- ハードウェア: 電源装置
- ハードウェア: メモリ
- ハードウェア: NIC
- ハードウェア: PCI スロット
- ハードウェア: リモートアクセスカード
- ストレージ: 物理ディスク
- ストレージ: 仮想ディスク
- ファームウェア
- 電源モニタ
- 保証

全データセンターハードウェアの設定およびステータスを表示するには、以下を行います。

1. **vSphere** クライアントの**インベントリ**下で**ホストとクラスタ**を選択します。
2. **ホストとクラスタ**でツリービューからデータセンターを選択し、**Dell Server Management** タブを選択します。

3. データセンター内の全ホストの概要が表示されます。**表示** ドロップダウンリストを使用してインベントリカテゴリを表示します。
4. **フィルタ** テキストボックスを使ってインベントリデータのフィルタを入力します。
5. 表示されたインベントリを更新するには、**更新** をクリックします。
6. **ダウンロードの場所** ウィンドウでインベントリを保存するロケーションを参照し、**保存** をクリックします。

接続プロファイルの管理

接続プロファイルは、アクセスおよび導入資格情報を一連のホストシステムに関連付け、通常以下を含みます。

- 名前および固有の説明（プロファイル管理を容易にするため）
- 接続プロファイルに関連付けられたホストのリスト
- iDRAC 資格情報
- ホストルート資格情報

設定ウィザードの実行後、接続プロファイルは、**Dell Management Center** から管理できます。それには以下が含まれます。

- [新しい接続プロファイルの作成](#)
- [既存接続プロファイルの表示および編集](#)
- [接続プロファイルの削除](#)
- [接続プロファイルのテスト](#)
- [接続プロファイルの更新](#)

新しい接続プロファイルの作成

接続プロファイルは Dell サーバーと通信するために仮想サーバーが使用する資格情報を保存します。各 Dell サーバーは Dell Management Plug-in が管理する 1 つだけの接続プロファイルに関連付けられている必要があります。1 つの接続プロファイルに複数のサーバーを割り当てることができます。接続プロファイルの作成方法は、接続ウィザードからであっても、**Dell Management Center** → **設定** であってもほぼ同じです。設定ウィザードは初めて Dell Management Console にアクセスしたとき、またはその後、設定ウィンドウから実行することもできます。

 **メモ:** このリリースおよび、バージョン 12G 以降のホストのインストールでは、OMSA エージェントのインストールは必要ありません。11G のホストにインストールする場合、現在では展開プロセスで OMSA エージェントが自動的にインストールされるようになってます。

新しい接続プロファイルを作成するには、次の手順を実行します。

1. **Dell Management Center** の左ペインで、**接続プロファイル** をクリックします。
2. **使用可能なプロファイル** で **新規作成** をクリックします。
3. **新規接続プロファイル** ウィンドウで、**プロファイル名** と、オプションでカスタム接続プロファイルの管理を便利にするために使われる、**説明** を入力し、**次へ** をクリックします。
4. **関連ホスト** については、**チェックボックス** を使ってこの接続プロファイルを使用するホストを選択して、**次へ** をクリックします。
5. **資格情報** ウィンドウで、資格情報および接続プロトコルに関する情報を表示し、**次へ** をクリックします。
6. iDRAC ウィンドウで **iDRAC 資格情報** を入力します。
 - a) **ユーザー名**、**パスワード** および **パスワードの確認** を入力します。両パスワードは一致する必要があります。また、ASCII 印刷可能文字だけを使用することができます。

-  **メモ:** パスワードは 20 文字を超えることはできず、特殊文字を含むこともできません。
- b) **証明書**の**チェック**で、iDRAC 証明書をダウンロードおよび保存し、すべての将来の接続で検証するには、**有効にする**を選択します。または、**無効にする**を選択すると、証明書の確認および保存は行われません。
- Active Directory を使用する場合は、**有効にする**を選択する必要があります。
7. **次へ**をクリックします。
8. ホストルートの**資格情報**ウィンドウで、以下を行います。
- a) **ユーザー名**、**パスワード**、および**パスワードの確認**を入力します。両パスワードは一致する必要があります。
-  **メモ:** パスワードは 31 文字を超えることはできず、特殊文字を含むこともできません。
-  **メモ:** iDRAC Express または Enterprise カードがないサーバーでは、iDRAC テスト接続結果は、このシステムには該当しませんが表示されます。
-  **メモ:** OMSA の資格情報は、ESX および ESXi ホストに使われる資格情報と同じです。
- b) **証明書**の**チェック**で OMSA 証明書をダウンロードして保存し、すべての将来の接続で検証するには、**有効にする**を選択します。または **無効にする**を選択すると、証明書の確認および保存は行われません。Active Directory を使用する場合は、**有効にする**を選択します。
9. **次へ**をクリックします。
10. **接続性のテスト**ウィンドウで、選択されたサーバー用に入力された iDRAC およびホストルートの資格情報がテストされます。次のいずれかを行います。
- テストを開始するには、**選択したテスト**をクリックします。その他のオプションはアクティブになっていません。
 - テストを中止するには、**テストを中止**をクリックします。
11. プロファイルを完了するには、**保存**をクリックします。
- 接続プロファイルを管理するには、「[接続プロファイルの管理](#)」を参照してください。

既存の接続プロファイルの表示または編集

接続プロファイルの設定後、プロファイル名、説明、関連ホスト、および iDRAC と OMSA エージェントの資格情報を編集できます。

既存の接続プロファイルの表示または編集するには、以下を実行します。

1. Dell Management Center で **接続プロファイル**を選択します。
2. **使用可能なプロファイル**でプロファイルを選択し、次に **編集 / 表示**をクリックします。
3. **プロファイル名と説明**ウィンドウで、以下のいずれかを行います。
 - 情報を表示するには、このページを調査します。
 - この情報を編集するには、**編集**をクリックします。
4. 必要に応じて接続プロファイル名と説明を編集して、**保存**をクリックします。
5. 関連ホストを編集するには、左ペインで **関連ホスト**をクリックして、次に **編集**をクリックします。
6. **関連ホスト**ウィンドウで、チェックボックスを使い、ホストを選択または選択解除して**保存**をクリックします。
7. iDRAC または OMSA 資格情報を編集するには、左ペインで **資格情報**を選択し、次に iDRAC または OMSA を選択します。
8. iDRAC を選択した場合、資格情報を編集するには、**編集**をクリックして、次を編集します。
 - a) **ユーザー名**テキストボックスで、ユーザー名を編集します。
 - b) **パスワード**テキストボックスでパスワードを編集します。
 - c) **パスワードの確認**テキストボックスにパスワードを再入力します。

- d) 証明書のチェックの有効化または無効化を選択します。これは Active Directory と一緒に使用するために有効化しなければなりません。
9. 保存をクリックします。
10. OMSA を選択した場合、資格情報を編集するには、**編集**をクリックして、次を編集します。
 - a) ユーザー名テキストボックスで、ユーザー名を編集します。
 - b) パスワードテキストボックスでパスワードを編集します。
 - c) パスワードの確認テキストボックスにパスワードを再入力します。
 - d) 証明書のチェックの有効化または無効化を選択します。これは Active Directory と一緒に使用するために有効化しなければなりません。
11. 保存をクリックします。
12. ウィンドウを閉じるには、**X** (右上の隅) をクリックします。

接続プロファイルの削除

Dell Management Center から、接続プロファイルを削除することができます。
接続プロファイルを削除するには以下を実行します。

1. **Dell Management Center** で、**接続プロファイル**をクリックします。
2. **使用可能なプロファイル**でプロファイルを選択して、**削除**をクリックします。
3. プロファイルを削除するために表示されるメッセージで、**削除**をクリックするか、**キャンセル**をクリックして削除を取り消します。

接続プロファイルのテスト

接続プロファイルをテストするには、以下を行います。

1. **Dell Management Center** で、**接続プロファイル**を選択します。
2. 選択されたサーバー上で入力した iDRAC とホストルート資格情報をテストするには、**使用可能なプロファイル**で接続プロファイルを選択し、次に **接続性のテスト**をクリックします。
3. チェックボックスを使ってテストしたいホストを選択し、**選択したテスト**をクリックします。
4. 選択したテストをすべて中止し、テストを取り消すには、**すべてのテストを中止**をクリックします。
5. 終了するには、**完了**をクリックします。

接続プロファイルの更新

接続プロファイルを更新するには、以下を行います。

更新をクリックします。

 **メモ:** ホストが vCenter から削除されると、接続ファイルから削除されます。

vSphere クライアントのホストビューにおけるシステムイベントログの理解

システムイベントログは、**Dell Management Plug-in** で検出されたハードウェアのステータス情報を提供します。

システムイベントログは、以下の基準に基づいて情報を提供します。

ステータス - 情報	いくつかのステータスアイコンがあります。情報（青色の感嘆符）、警告（黄色の三角に感嘆符）、エラー（赤色の X 印）。
-------------------	--

時刻：サーバー 時刻 イベント発生時の時刻と日付を示します
時刻
このページを検索 特定のメッセージ、サーバー名、設定、その他を表示します。

重要度は次のように定義されます。

情報： Dell Management Plug-in 動作は正しく完了しました。
警告： Dell Management Plug-in 動作は部分的に正しく行われ、部分的に失敗しました。
エラー： Dell Management Plug-in 動作は失敗しました。
Security (セキュリ システムセキュリティに関する情報が含まれます。
ティ機能)

ログは、外部 CSV ファイルとして保存できます。

関連情報

- [個別ホストに対するシステムイベントログの表示](#)

Dell Management Center における ログ表示

Dell Management Center ログには、検出されたハードウェアのステータス情報やユーザー操作履歴が含まれます。

Dell Management Center におけるログを表示するには、以下を行います。

1. **Dell Management Center** の左ペインで、**ログ**を選択します。
2. ログを最新データでアップデートするには、**更新**をクリックします。
3. ログデータのフィルタリングのために重要度カテゴリを選択するには、**すべてのカテゴリ**ドロップダウンリストで、すべてのカテゴリ、情報、警告、エラー、またはセキュリティの中から1つを選択します。
4. ログデータのフィルタとして日付範囲を選択するには、**先週**ドロップダウンリストをクリックして、先週、先月、昨年またはカスタム範囲から1つを選択します。
カスタム範囲を選択した場合は、**開始日**および**終了日**のドロップダウンリストが表示されます。
5. カスタム日付範囲を選択した場合、以下を行います。
 - a) **開始日**を入力するため、**カレンダー**をクリックします。
 - b) **終了日**を入力するため、**カレンダー**をクリックします。
 - c) 設定を保存するには、**適用**をクリックします。
6. ログの表示方法を制御するには、表示コントロールを使って、**画面ごとの記録**を設定し、必要な **ページ**に行き、前へおよび次へのページ制御を使います。
7. ログコンテンツをカンマで区切られた (**CSV**) ファイルにエクスポートするには、**エクスポート**をクリックします。
8. ダウンロードロケーションウィンドウで、ログを保存するロケーションを表示して、**保存**をクリックします。

個別ホストのイベントログの表示

システムハードウェアイベントログは、以下の基準に基づく情報を提供します。

- ステータス - 情報
いくつかのステータスアイコンがあります。情報（青色の感嘆符）、警告（黄色の三角に感嘆符）、エラー（赤色の X 印）。
- 時刻：サーバー時刻

イベント発生時の日時を表示します。

- このページを検索
特定のメッセージ、サーバー名、設定、その他を表示します。

個別ホストのシステムイベントログを表示するには、以下を行います。

1. **vSphere クライアントの、インベントリ**の見出し下で **ホストとクラスタ**を選択します。
2. ツリービューで、ホストシステムを選択します。
3. **Dell Server Management** タブを選択します。
4. **最近のシステムログ項目**で、**システムイベントログ**ウィンドウを起動するには、**詳細**をクリックします。
5. **システムイベントログ**をアップデートするには、**ログの更新**をクリックします。
6. イベントログ項目数を制限（フィルタ）するには、以下のいずれかを選択します。
 - 検索フィルタテキストボックスに、動的にログ項目をフィルタするテキスト文字列を入力します。
 - フィルタテキストボックスを消去するには、**X**をクリックするとすべてのイベントログ項目が表示されます。
7. すべてのイベントログ項目を消去するには、**ログのクリア**をクリックします。すべてのログ項目は消去後削除されるとのメッセージが表示されます。次のいずれかを選択します。
 - ログの消去に同意する場合は、**OK**をクリックします。
 - 取り消すには、**キャンセル**をクリックします。
8. イベントログを **CSV** ファイルにエクスポートするには、**エクスポート**をクリックします。
9. システムイベントログを保存するロケーションを表示して、**保存**をクリックします。

ファームウェアアップデートについて

サーバーがファームウェアアップデートを受けるロケーションは、**Dell Management Center** で使用できるグローバル設定です。ファームウェアリポジトリは **Dell Management Center** で設定できますが、アップデートは **vSphere** クライアントにおける特定の **Dell** ホストタブで実行されます。

ファームウェアリポジトリ設定には、展開されたサーバーをアップデートするのに使用される、ファームウェアカタログロケーションが含まれています。ロケーションタイプには2種類あります。

Dell (ftp.dell.com)	Dell (ftp.dell.com) のファームウェアアップデートリポジトリを使用します。 Dell Management Plug-in が、選択されたファームウェアアップデートをデルからダウンロードします。
ローカル/共有リポジトリ	Dell Repository Manager™ によって作成されます。これらのローカルリポジトリは、 CIFS または NFS ファイル共有にあります。

-  **メモ:** リポジトリが作成されたら、登録されたホストがアクセスできるロケーションに保存します。リポジトリのパスワードは31文字を超えることはできません。パスワードには、@、&、%、'、"、, (カンマ)、<>の文字は使用できません。

ファームウェアアップデートウィザードは常に、**iDRAC**、**BIOS**、および **Lifecycle Controller** の最低ファームウェアレベルをチェックし、最低必須のバージョンにアップデートすることを試みます。**iDRAC**、**Lifecycle**、および **BIOS** ファームウェアバージョンが最低要件を満たすと、ファームウェアアップデートウィザードが、**iDRAC**、**Lifecycle Controller**、**RAID**、**NIC/LOM**、電源装置、**BIOS** などを含むすべてのファームウェアのアップデートを行います。

-  **メモ:** 第9および第10世代のサーバーにおいては、**BIOS/BMC/DRAC** ファームウェアバージョンは **vCenter** のクラスタビューレベル、または個別ホストビューの概要ページでのみ表示することができます。ファームウェアバージョン情報は、ファームウェア下の個別ホストビューでアクティブになっておらず、そのページはグレーアウト表示されます。リモートファームウェアアップデートは利用できません。

2010年10月14日以降のファームウェアバージョン

2010年10月14日以降にアップデートされたファームウェアについては、ファームウェアアップデートウィザードが実行されます。

2009年7月29日以降で10月14日より前のファームウェアバージョン

ファームウェアが2009年7月29日以降、2010年10月14日の前日までにアップデートされている場合、ファームウェアアップデートウィザードはまだ使用できませんが、ファームウェアをアップデートするためのISOバンドルが付属しています。このアップデート後、最新ファームウェアにならない可能性があります。バンドルの実行後に再度アップデートを実行することを推奨します。

2009年7月29日より古いファームウェアバージョン

ファームウェアが2009年7月29日より古い場合、ISOファイルをダウンロードして実行し、マシンのアップデートを行わなければならない可能性があります。ISOの実行後、ファームウェアアップデートウィザードを実行することを推奨します。

関連情報

- [ファームウェアリポジトリおよび資格情報の設定](#)
- [ファームウェアアップデートウィザードの実行](#)
- [古いファームウェアバージョンのアップデート](#)

ファームウェアアップデートウィザードの実行

この機能が使用できるのは、iDRAC Express または Enterprise カードが装備された第11世代のDellサーバーのみです。お使いのファームウェアが2010年10月14日以降にインストールされた場合、ファームウェアアップデートウィザードを使用してファームウェアバージョンを自動的にアップデートすることができます。ファームウェアアップデートウィザードを実行するには、次の手順を行います。

1. **vSphere クライアント → Dell Server Management タブ → ホスト情報** で、**ファームウェア → ファームウェアアップデートの実行** とクリックします。
2. **ファイルから単一のファームウェアアップデートをロード** オプションを使用するには、次の手順を行います。
 - a) 次の形式でファイルパスを入力します。
CIFS: \\<ホストがアクセスできる共有パス>\<ファイル名>.exe or NFS: host:/share/
filename.exe
 - b) NFS がある場合、手順7に進んでください。それ以外の場合は **ユーザー名** および **パスワード** を、共有ドライブにアクセスできるドメイン形式で入力します。
 - c) 手順7に進みます。このオプションのかわりに **リポジトリからアップデート** オプションを使用するには、次の手順を行います。
 - a) **リポジトリからアップデート** を選択します。
 - b) **ftp.dell.com** へのネットワーク接続があることを確認します。
 - c) **次へ** をクリックします。
3. お使いのホスト向けのバンドルを選択し、**次へ** をクリックします。
4. 使用するファームウェアアップデートを選択し、**次へ** をクリックします。ダウングレード、すでに最新、または現在アップデート用にスケジュール済みのコンポーネントは選択不可になっています。**コンポーネントのダウングレードを許可** チェックボックスを選択する場合は、ダウングレードとしてリストされているオプションを選択します。このオプションの選択は、ファームウェアのダウングレードによる影響を理解している上級ユーザーのみにお勧めします。
5. 希望する再起動オプションを選択します。
 - **メンテナンスモードにしてアップデートを適用し、再起動する。**
ホストがメンテナンスモードになります。ホストをメンテナンスモードにできない場合は、ホストは再起動されず、アップデートは次の再起動で適用されます。アップデート後にメンテナン

スモードを終了するには、ファームウェアアップデート完了後にメンテナンスモードを終了チェックボックスを選択します。

- 次回の再起動でアップデートを適用する。
サービスの中断を避けるため、再起動前にホストをメンテナンスモードにすることが推奨されます。
- メンテナンスモードにせずにアップデートを適用し、再起動を強制する。
- アップデートが適用され、ホストがメンテナンスモードでなくても再起動が行われます。この方法は推奨されません。

6. **Finish** (終了) をクリックします。

7. アップデートが正常に行われたことを確認するには、**Dell Management Center** で **ジョブキュー** → **インベントリ履歴** → **今すぐ実行** と選択し、**Dell Management Center 概要** ページで新しいバージョンを確認します。

古いファームウェアバージョンのアップデート

ファームウェアアップデートウィザードを実行するには、ファームウェアは最低必須レベルでなければなりません。最低必須レベルになっていない場合、ファームウェアアップデートウィザードを実行する前にファームウェアをアップデートするオプションが提供されます。通常、2009年7月29日より前にインストールされたファームウェアでは、ISOファイルをダウンロードして実行する必要があります。「[ファームウェアのアップデート](#)」を参照してください。2009年7月29日から2010年10月14日の間にインストールされたファームウェアでは、**Dell Management Plug-in** から自動的にインストールされるISOバンドルが提案されます。2010年10月14日以降インストールされたファームウェアの場合は、ファームウェアアップデートウィザードを実行できます。ファームウェアのアップデートはホストの **Dell Server Management** タブの **vSphere** クライアントで実行できます。リポジトリを設定するには「[ファームウェアリポジトリの設定](#)」を参照してください。

古いファームウェアバージョンをアップデートするには、以下を行います。

1. **ホスト処置**にある **Dell Server Management** タブの **vSphere** クライアントで、**ファームウェアアップデートウィザードの実行** をクリックします。
ホストのファームウェアがウィザードを実行するには低過ぎるバージョンの場合、アップデートが必要ダイアログが表示されます。ISOファイルをダウンロードして実行するか、アップデートのバンドルを実行するよう指示されます。
2. **アップデートが必要**ダイアログボックスで、次のいずれかを行います。
 - ファームウェアのアップデート後に自動的に保守モードを終了するには、**ファームウェアアップデートの完了後にメンテナンスモードを終了**チェックボックスを選択します。
 - マシンをクラスタに戻す前に検査またはテストするため、保守モードに入る場合は、このチェックボックスをマークしないでください。
3. **アップデート** をクリックします。
4. **成功**ダイアログボックスがアップデート実行中であることを示します。
ファームウェアアップデートの完了後にメンテナンスモードを終了チェックボックスを選択していた場合、ファームウェアアップデートはホストを保守モードにして、自動的に再起動されます。そうでない場合は、保守モードにとどまります。
5. アップデートの進捗を見るには、**vSphere** クライアントの **最近のタスク** エリアを参照してください。
この手順の後、ファームウェアアップデートウィザードを再度実行し、ファームウェアを完全にアップデートします。

vCenter を使用した高度なホスト管理

高度なホスト管理タスクは、管理者がデータセンター環境における物理サーバーの識別、サーバーベースの管理ツールの開始、サーバー保証情報の表示を行うことを可能にする、ホストシステムベースの作業です。

これら作業のすべては、vCenter の Dell Server Management タブから、または個別ホストシステムに対する ホストとクラスタビューでホストを右クリックすることで起動できます。

物理サーバー前面インジケータライトの設定

大規模なデータセンター環境で物理サーバーを見つけやすくするため、一定期間で前面インジケータライトを点滅させるよう設定できます。

物理サーバーの前面インジケータライトを設定するには、以下を行います。

1. インベントリの見出しの下の **vSphere クライアント** で、**ホストとクラスタ** を選択します。
2. **ホストとクラスタ** からツリービューのホストシステムを選択し、**Dell Server Management** タブを選択します。
3. **ホスト処理** で、**インジケータライトの点滅** を選択します。
4. 次のいずれかを選択します。
 - 点滅を開始し、期間を設定するには **インジケータライト** ダイアログボックスで **点滅オン** をクリックし、タイムアウトドロップダウンリストでタイムアウト間隔を選択して **OK** をクリックします。
 - 点滅を終了するには、**インジケータライト** ダイアログボックスで **点滅オフ** をクリックし、**OK** をクリックします。

サーバーベース管理ツール

vSphere クライアント → **Dell Server Management** タブから起動できるサーバーベース管理ツールには、iDRAC および OMSA の 2 つがあります。左ペインの管理コンソールリンクで、次にアクセスできます。

- リモートアクセスの起動。
このオプションを使って iDRAC ユーザーインターフェースを起動します
- OMSA の起動
このオプションを使って、OpenManage Server Administrator ユーザーインターフェース URL を起動します。これは、最初の設定ウィザード中に、または **設定** → **一般** を使用して、管理センターにこの URL を入力することで行います。Windows ベースの管理ステーション上のサーバー管理者ウェブサーバー用にこの URL をインストールする必要があります。
- ブレードシステムを使っている場合、CMC を起動してシャージ管理コントローラユーザーインターフェースを起動します。ブレードシステムでない場合、これは表示されません。

保証の取得

保証の取得は、Dell サーバーについて以下の情報を提供します。

- アップデートされたサービス保証情報、ただしホストサービスタグのみを送信
- 定期的にアップデートされた保証情報
- プロキシサーバーおよび資格情報を使ったセキュアな送信

 **メモ:** デルは、送信されたサービスタグ情報は保存しません。

関連タスク:

- [ホスト保証の更新](#)
- [保証取得ジョブの実行](#)
- [シングルホストのサービス保証情報の表示](#)
- [全データセンターの保証情報の表示](#)

ホスト保証の更新

サーバーの保証ステータスを表示し、保証ページで保証を更新することができます。

1. **vSphere クライアント** → **Dell Server Management タブ** → **ホスト情報** で、**保証**をクリックします。
2. 保証を更新して、システム保証を管理するデルのウェブページに移動するには、**保証の更新**をクリックします。
3. Dell ウェブページで **保証の更新/アップグレード**をクリックします。

全データセンターのサーバー保証情報の表示

保証ジョブが完了したら、データセンタービューページで vSphere クライアントのサーバー保証情報を表示することができます。

全データセンターのサーバー保証情報を表示するには、以下を行います。

1. インベントリの見出しの vSphere クライアントから **ホストとクラスタ**を選択します。
2. **ホストとクラスタ**でツリービューからデータセンターを選択し、**Dell Server Management** タブを選択します。
3. データセンターの全ホストの概要が表示されます。表示ドロップダウンリストで **保証**を選択します。
4. **フィルタ**テキストボックスに保証データの検索語を入力します。
5. 表示されているインベントリを更新するには、**更新**をクリックします。
6. インベントリを **CSV** ファイルでエクスポートするには、**エクスポート**をクリックします。ダウンロードの場所ウィンドウで、インベントリを保存するロケーションを参照し、**保存**をクリックします。

シングルホストのサービス保証情報の表示

保証ジョブの完了後、ホストビューページの vSphere Client でシングルホストの保証情報を表示することができます。

シングルホストのサーバー保証情報を表示するには、以下を行います。

1. インベントリの見出し下の vSphere クライアントで **ホストとクラスタ**を選択します。
2. **ホストとクラスタ**でツリービューからホストシステムを選択し、**Dell Server Management** タブを選択します。
3. システム保証情報を表示するには、**保証**を選択します。保証ステータスページの情報には以下が含まれます。
 - 保証プロバイダ名および保証の説明
 - 開始日と終了日および保証残余期間
 - 保証ステータス（有効または無効）および保証情報の最新更新日

ゼロタッチハードウェアプロビジョニング および展開

ハードウェアの必要条件

ハードウェアのプロビジョニングおよび展開を正しく行うためには、物理サーバーが展開ウィザードに表示される必要があります。すべての物理サーバーは次の必要条件を満たす必要があります。

- 具体的なハードウェアサポート情報については、『*Dell Management Plug-In for VMware vCenter Release Notes*』（VMware vCenter 用 Dell Management Plug-In リリースノート）を参照してください。
 - サーバーには、サポートされる最低必須バージョンの iDRAC ファームウェア、Lifecycle Controller および BIOS が必要です。具体的なハードウェアサポート情報については、『*Dell Management Plug-in for VMware vCenter Release Notes*』（VMware vCenter 用 Dell Management Plug-In リリースノート）を参照してください。
-  **メモ:** ファームウェアバージョンが古い場合、2段階のアップグレードプロセスが必要になる可能性があります。詳細なアップグレード手順については、ファームウェアのマニュアルを参照してください。
- Dell Management Plug-in は、組み込み/統合 LOM を使ってのみ、展開をサポートします。展開後は手動で PCI スロットの NIC を設定できます。アドオン NIC を使用する場合は、システムは、ホスト LOM を有効化していなければなりません。
 - Dell Management Plug-in は、内蔵デュアル SD モジュール（ハイパーバイザーのみ）またはローカルハードディスクドライブへの展開を行います。ハイパーバイザーを内蔵デュアル SD モジュールにインストールするには、最大 1 または 2 GB のストレージが必要です。内蔵デュアル SD モジュールは、Dell Management Plug-in でハイパーバイザーを展開する前に BIOS で有効化しておく必要があります。管理 NIC は手動で変更し、システムを vCenter に追加することができます。
 - iDRAC が専用モードになっている場合、その NIC は Dell Management Plug-in と通信ができるよう有効化されていなければなりません。
 - CSIOR は有効化されている必要があります。また、自動検出を開始する前には、検索データが最新のものであることを確認し、システムの電源を完全に切断してから再投入（ハード再起動）してください。
 - Dell サーバーは、自動検出とハンドシェイクオプションを工場出荷時に事前設定して納入するよう発注することができます。サーバーがこのオプションで事前設定されていない場合、手動で Dell Management Plug-in IP アドレスを入力し、または、この情報を提供するようローカルネットワークを設定する必要があります。
 - Dell Management Plug-in がハードウェア設定に使われない場合、ハイパーバイザーの起動前に以下の状態であることを確認してください。
 - BIOS における VT（仮想化テクノロジー）フラグが有効である。
 - オペレーティングシステムのインストールで、システム起動順を起動可能な仮想ディスク、または内蔵デュアル SD モジュールに設定する。
 - ハードウェア設定に Dell Management Plug-in を使う場合は、BIOS 設定がハードウェアプロファイルの一部でなくても、VT の BIOS 設定は自動的に有効化されます。仮想ディスクがターゲットシステムにまだ存在していない場合は、Express/Clone RAID 設定が必要になります。
 - サーバーがバージョン 12G より前のバージョンの場合、展開プロセスは OpenManage Server Administrator パッケージをターゲットシステムにインストールして、自動的に SNMP トラップ先を Dell Management Plug-in に設定します。
 - 展開には、すべての Dell ドライバを含むカスタム ESXi イメージが必要です。正しいイメージは、Dell ドライバ & ダウンロードページに移動し、展開プロセス中アクセスすることができる場所にカスタム

イメージを保存することによって、見つけることができます。本リリース向けの対応 ESXi バージョンの最新リストは、リリースノートを参照してください。

プロビジョニングの概要

データセンターの物理インベントリが完了すると、すべての自動検出ベアメタルシステムは Dell Management Plug-in のゼロタッチハードウェアプロビジョニングとハイパーバイザー展開の対象となります。プロビジョニングと展開には、次を準備する必要があります。

ハードウェアプロファイルの作成	新しいサーバーの展開に使われる参照サーバーから収集したハードウェア設定が含まれます。「 新規ハードウェアプロファイルの作成 」を参照してください。
ハイパーバイザープロファイルの作成	ESX/ESXi 展開に必要なハイパーバイザーインストール情報が含まれます。「 新規ハイパーバイザープロファイルの作成 」を参照してください。
展開テンプレートの作成	オプションで、ハードウェアプロファイル、ハイパーバイザープロファイル、またはその両方が含まれます。これらのプロファイルは保存して、必要に応じてすべてのデータセンターサーバーで使用することができます。「 展開テンプレートの構築 」を参照してください。

展開テンプレートが作成できたら、展開ウィザードを使用してサーバーハードウェアのプロビジョニングと、新しいホストを vCenter に展開するようスケジュールされたジョブを作成するために必要な情報を収集します。展開ウィザードの実行に関する情報については、「[展開ウィザードの実行](#)」を参照してください。最後に、ジョブステータスを表示し、未実行の展開ジョブを変更するには、ジョブキューを使用します。

 **メモ:** 連続実行するようスケジュールできるのは、2つの展開ジョブまでです。複数のジョブは、スケジュール機能を使って展開実行をずらすようにしてください。

展開ジョブ時間の理解

ベアメタルサーバーのプロビジョニングと展開には、特定の要素により、完了まで 30 分から数時間かかる場合があります。展開ジョブを開始する場合は、提供されたガイドラインにしたがって、展開時間を計画することを推奨します。プロビジョニングと展開にかかる時間は展開タイプ、複雑性、同時に実行される展開ジョブ数などによって異なります。以下のテーブルは、展開ジョブにかかるおおよその時間のガイドラインを提供します。展開ジョブは、総合的な展開ジョブの時間を短縮するため、最大 5 台の並列サーバーによるバッチ処理で実行されます。並列ジョブの正確な数は使用可能リソースによって異なります。

表 2. おおよその展開時間シナリオ

展開タイプ	展開ごとのおおよその時間
ハイパーバイザーのみ	30 ~ 130 分
ハードウェアのみ	設定の複雑性、RAID、BIOS および起動オプションにより、最大 2 時間
ハイパーバイザーおよびハードウェアプロファイル	1 ~ 4 時間

展開シーケンス実行中のサーバー状態

インベントリジョブの実行時に、自動検出されたベアメタルシステムは、データセンターにとって新しいサーバーか、未完了の展開ジョブがスケジュールされているかなどを特定しやすくするため、いくつかの状態に分類されます。管理者はこれらの状態を使用してサーバーを展開ジョブに含めるべきかどうかを判断できます。状態には、以下があります。

未設定	サーバーは、Dell Management Plug-in と接触しており、設定を待機している状態です。 「 展開ジョブ時間の理解 」を参照してください。
設定済み	サーバーには、正しいハイパーバイザー展開に必要なすべてのハードウェア情報が設定されています。

カスタム Dell ISO イメージのダウンロード

展開には、すべてのDell ドライバを含むカスタム ESXi イメージが必要です。Dell はカスタム ESX 4.1 イメージを作成できません。展開を行うには、すべてのドライバが VMware が生成する ISO にネイティブで存在する必要があります。本リリース向けの対応 ESXi バージョンの最新リストは、リリースノートを参照してください。

 **メモ:** Dell Management Plug-in ISO には、展開に必要な ESXi ISO イメージが含まれていません。これらのイメージは、展開中にアクセスできる場所にダウンロードしておくことが必要で、そうしない場合は展開が失敗する可能性があります。

1. support.dell.com にアクセスします。
2. 希望する言語の **ドライバおよびダウンロード** ページに行き、以下のいずれかを行います。
 - サービスタグまたはエクスプレスサービスコードを使ってドライバを選択するには、**はい** の下のテキストボックスにサービスタグまたはエクスプレスサービスコードを入力し、**送信** をクリックします。
 - 別のオプションでドライバを選択するには、**いいえ** の下で以下のいずれかを選択します。
 - * 自動的にサービスタグを検出
 - * 自分の製品およびサービスリストから選択
 - * 全 Dell 製品リストから選択

次に、**継続** をクリックして選択したオプションに対する指示に従います。

3. 選択されたサーバーに対するページで、**結果の絞り込み** にスクロールダウンし、**オペレーティングシステム** でドロップダウンリストを使って、必要な ESX または ESXi システムを選択します。
4. **エンタープライズソリューション** をクリックします。
5. **エンタープライズソリューション** リストで、必要な ISO バージョンを選択し、**ファイルのダウンロード** をクリックします。

 **メモ:** 組み込み ISO は、ハイパーバイザーのデュアル内蔵 SD モジュールへのインストールに使用されます。インストール可能 ISO はハードディスクへのインストールに使用されます。
6. ダイアログボックスで、**ブラウザ経由でのシングルファイルダウンロード用** を選択し、**今すぐダウンロード** をクリックします。
7. ダイアログボックスで、展開用に ISO イメージを保存するロケーションを参照します。

ハードウェアプロファイルの設定方法の理解

サーバーハードウェア設定を行うには、ハードウェアプロファイルを作成する必要があります。ハードウェアプロファイルは、新たに検出されたインフラストラクチャコンポーネントに適用できる設定テンプレートで、以下の情報を必要とします。

起動順序	起動順序は、起動デバイスシーケンスとハードドライブシーケンスで、起動モードが BIOS で設定されている場合のみ編集できます。
BIOS 設定	BIOS 設定には、メモリ、プロセッサ、SATA、統合デバイス、シリアル通信、内蔵サーバー管理、電源管理、システムセキュリティ、およびその他の設定が含まれます。

iDRAC Settings (iDRAC 設定)

iDRAC 設定には、ネットワーク、ユーザーリスト、およびユーザー設定 (IPMI / iDRAC 権限) が含まれます。



メモ: iDRAC Express を備えるシステムにおいては、iDRAC 構成は抽出できません。したがってサーバーは参照サーバーとして使用すべきではありません。ターゲットシステムとして使用される場合、参照サーバーからの iDRAC 設定は適用されません。

RAID 構成

RAID 構成は、ハードウェアプロファイルが抽出された時点における、RAID トポロジを、参照サーバーに表示します。



メモ: ハードウェアプロファイルで設定された RAID 構成オプションには次の 2 種類があります: 1. **RAID1 を適用 + 専用ホットスペアの作成適用可能**。ターゲットサーバーにデフォルトの RAID 構成を適用したい場合は、このオプションを使用します。RAID 構成タスクは、デフォルトで RAID1 対応の内部コントローラ上の最初の 2 つのドライブを使用して RAID1 を構成します。さらに、専用ホットスペアの基準を満たす候補ドライブがある場合は、RAID1 アレイ用の専用ホットスペアが作成されます。2. 次に示すように、**RAID 構成を参照サーバーからクローン**。参照サーバーの設定をクローンしたい場合は、このオプションを使用します。「[新規ハードウェアプロファイルの作成](#)」を参照してください。



メモ: Dell Management Plug-in は、参照サーバーの設定にかかわらず、すべての展開サーバーにおける BIOS のプロセッサグループの特定の BIOS 設定を可能とします。新規ハードウェアプロファイルの作成に参照サーバーを使用する前に、再起動時にシステムインベントリを収集 (CSIOR) 設定を有効にして再起動し、正確なインベントリおよび構成情報を収集しておく必要があります。

ハードウェアプロファイルを作成するためのタスクには、以下が含まれます。

- [参照サーバーにおける CSIOR の有効化](#)
- [新規ハードウェアプロファイルの作成](#)
- [新規ハードウェアプロファイルのクローン](#)
- [ハードウェアプロファイル管理について](#)

参照サーバーにおける CSIOR の有効化

参照サーバーを使ってハードウェアプロファイルを作成する前に、再起動時にシステムインベントリを収集 (CSIOR) の設定を有効化し、サーバーを再起動して正確なインベントリおよび設定情報を収集します。CSIOR を有効化するには 2 つの方法があります。

ローカル

これは、Dell Lifecycle Controller United Server Configurator (USC) ユーザーインターフェースを使って、個別ホストを利用します。

リモート

これは、WS-Man スクリプトを使用します。この機能をスクリプトすることに関する詳細は、「[Dell Tech Center](#)」および「[DCIM Lifecycle Controller 管理プロファイル](#)」を参照してください。

参照サーバーでの CSIOR をローカルで有効化するには、以下を行います。

1. システムに電源を入れ、POST 中に <F10> を押して USC を起動します。
2. ハードウェア設定 → 部品交換設定を選択します。
3. 再起動時にシステムインベントリを収集の設定を有効化し、USC を終了します。

新規ハードウェアプロファイルの作成

新規ハードウェアプロファイルを作成するには、以下を実行します。

1. **Dell Management Center** で **展開** → **展開テンプレート** → **ハードウェアプロファイル** を選択します。
2. **新規作成** をクリックします。
3. **新規ハードウェアプロファイル** ページで、以下を行います。
 - **プロファイル名** テキストボックスに、プロファイル名を入力します。
 - **説明** テキストボックスに、オプションの説明を記入します。
4. **保存** をクリックします。
5. 続けるには、左ペインで **参照サーバー** をクリックします。
6. 参照サーバーウィンドウで、**編集** をクリックします。
7. vCenter で管理されている、**Dell Management Plug-in** で正しくインベントリが行われている対応参照サーバーを見つけるには、**参照** をクリックします。
8. **サーバー** ダイアログボックスでリストを下にスクロールして、正しい参照サーバーを見つけ、**選択** をクリックします。
9. 参照サーバーの設定をデフォルトとしてカスタマイズするには、**参照サーバーからの設定をカスタマイズ** をクリックして、次に **保存** をクリックします。
10. 設定を抽出するのに数分かかります、というダイアログボックスが表示されます。設定を表示するには、**続行** をクリックします。選択されたサーバーの名前、iDRAC IP アドレス、およびサービスタグが **参照サーバー** ウィンドウに表示されます。
11. 左ペインで **起動順序** を選択します。プロファイルに再起動順の情報を含めるには、**このハードウェアプロファイルに起動順序を含める** チェックボックスを選択します。
12. 再起動順オプションを表示するには、**起動順序** を展開して、**編集** をクリックしてアップデートを行います。
 - a. **ブートモード** ドロップダウンリストで **BIOS** または **UEFI** を選択します。
 - b. **起動デバイスのシーケンス** 下の **表示/設定** ドロップダウンリストで、表示される再起動デバイス順を変更するには、デバイスを選択して **上へ移動** または **下へ移動** をクリックします。
 - c. **起動順序の再試行** ドロップダウンリストで、**有効** を選択し、サーバーが自動的に再起動シーケンスのリトライを行うようにするか、**無効** を選択して、リトライをしないようにします。
 - d. **保存** をクリックして変更を保存するか、**キャンセル** をクリックして変更を取り消します。
13. **BIOS 再起動モード** が選択された場合、**ハードウェアドライブのシーケンス** を展開して、ハードディスクドライブ順オプションを表示し、**編集** をクリックしてアップデートを行うことができます。
 - 表示されているハードディスクドライブ順を変更するには、デバイスを選択して **上に移動** または **下に移動** をクリックします。
 - **保存** をクリックして変更を保存するか、**キャンセル** をクリックして変更を取り消します。
14. 左ペインで **BIOS 設定** を選択します。プロファイルに BIOS 設定情報を含めるには、**このハードウェアプロファイルに BIOS 設定を含める** チェックボックスを選択します。カテゴリを展開して設定オプションを表示し、**編集** をクリックして以下のいずれかのアップデートを行います。
 - メモリ設定
 - プロセッサ設定
 - SATA 設定
 - 内蔵デバイス
 - シリアル通信
 - 組み込みサーバー管理
 - 電源管理

- システムセキュリティ
- その他の設定

カテゴリ内のすべてのアップデートが完了したら、**適用**をクリックして変更を保存するか、**キャンセル**をクリックして変更を取り消します。

 **メモ:** 設定オプションおよび説明を含む詳細 BIOS 情報については、選択したサーバーの『*Hardware Owner's Manual*』（ハードウェアオーナーズマニュアル）を参照してください。

15. 左ペインで **iDRAC 設定** を選択し、**ネットワーク** を選択します。
16. ネットワーク設定情報をプロファイルに含めるには、このハードウェアプロファイルに**ネットワーク設定を含める**チェックボックスを選択します。カテゴリを展開して設定オプションを表示し、**編集**をクリックして、以下のいずれかのアップデートを行います。
 - ネットワーク
 - ネットワーク設定
 - 仮想メディア

カテゴリ内のすべてのアップデートが完了したら、**適用**をクリックして変更を保存するか、**キャンセル**をクリックして変更を取り消します。

 **メモ:** 設定オプションおよび説明を含む詳細 iDRAC 情報については、選択したサーバーの『*iDRAC User's Guide*』（iDRAC ユーザーガイド）を参照してください。

17. 左ペインで、**iDRAC 設定** → **ユーザーリスト** を選択します。プロファイルにユーザーリスト情報を含めるには、このハードウェアプロファイルに**ユーザーリストを含める**チェックボックスを選択します。iDRAC ローカルユーザーリストで以下のいずれかを行います。
 - a) **ユーザーの追加:** 手動で iDRAC ユーザーと必要情報を入力します。完了したら **保存** をクリックして変更を保存するか、**キャンセル** をクリックして取り消します。
 - b) **ユーザーの削除:** 選択したユーザーを削除します。当該ユーザーのチェックボックスを選択して **削除** をクリックするか、**キャンセル** をクリックして取り消します。
 - c) **ユーザーの編集:** 手動で iDRAC ユーザー情報を編集します。完了したら **保存** をクリックして変更を保存するか、**キャンセル** で取り消します。

 **メモ:** 設定オプションおよび説明を含む詳細 iDRAC 情報については、選択したサーバーの『*iDRAC User's Guide*』（iDRAC ユーザーガイド）を参照してください。

18. 左ペインで、**RAID 設定** を選択します。プロファイルに RAID 設定情報を含めるには、このハードウェアプロファイルに**RAID 設定を含める**チェックボックスを選択します。次に、以下のいずれかを選択します。
 - **RAID1 を適用 + 専用ホットスペアの作成適用可能。**
ターゲットサーバーにデフォルトの RAID 構成を適用したい場合は、このオプションを使用します。RAID 構成タスクは、デフォルトで RAID1 対応の内部コントローラ上の最初の 2 つのドライブを使用して RAID1 を構成します。さらに、専用ホットスペアの基準を満たす候補ドライブがある場合は、RAID1 アレイ用の専用ホットスペアが作成されます。
 - **RAID 構成を参照サーバーからクローン。**
参照サーバーの設定をクローンしたい場合は、このオプションを使用します。

このプロファイルは自動的に保存され、**使用可能なプロファイル**下のハードウェアプロファイルに表示されます。

新規ハードウェアプロファイルのクローン

新規ハードウェアプロファイルのクローンには、以下を行います。

1. **Dell Management Center** で、**展開** → **展開テンプレート** → **ハードウェアプロファイル** を選択します。
2. **新規作成** をクリックします。

3. **新規ハードウェアプロファイル**ページで、以下を行います。
 - **プロファイル名**テキストボックスにプロファイル名を入力します。
 - **説明**テキストボックスに、オプションで説明を入力します。
4. **保存**をクリックします。
5. 左ペインで、**参照サーバー**をクリックします。
6. **参照サーバー**ウィンドウで **編集**をクリックします。
7. 参照サーバーからすべてのハードウェア設定を抽出するには、**参照サーバー設定のクローン**オプションボタンをクリックします。
8. **保存**をクリックします。
9. 設定の抽出には数分かかります、というダイアログボックスが表示されたら、**続行**をクリックします。設定が表示され、選択されたサーバー名、iDRAC IP アドレス、およびサービスタグが参照サーバーウィンドウに表示されます。
プロファイルは保存され、**使用可能プロファイル**下の **ハードウェアプロファイル**ウィンドウに表示されます。

ハードウェアプロファイル管理について

ハードウェアプロファイルは、参照サーバーを使ってサーバーのハードウェア設定を定義します。Dell Management Center では、以下を始め、既存のハードウェアプロファイルに対し多くの管理処理を実行することができます。

- [ハードウェアプロファイルの表示または編集](#)
- [ハードウェアプロファイルの複製](#)
- [ハードウェアプロファイル名の変更](#)
- [ハードウェアプロファイルの削除](#)
- [ハードウェアプロファイルの更新](#)

ハードウェアプロファイルの表示または編集

ハードウェアプロファイルを表示または編集するには、以下を行います。

1. **Dell Management Center** で、**展開** → **展開テンプレート** → **ハードウェアプロファイル**を選択します。
2. プロファイルを選択して、**表示 / 編集**をクリックします。
3. **ハードウェアプロファイル**ウィンドウで、変更するには、**編集**をクリックします。
4. 変更を適用するには、**保存**をクリックします。または **キャンセル**をクリックして変更を取り消します。

ハードウェアプロファイルの複製

ハードウェアプロファイルを複製するには、以下を行います。

1. **Dell Management Center** で **展開** → **展開テンプレート** → **ハードウェアプロファイル**を選択します。
2. **ハードウェアプロファイル**ページでプロファイルを選択して、**複製**をクリックします。
3. **複製**ダイアログボックスで、一意のハードウェアプロファイル名を入力します。
4. **適用**をクリックして新しい名前で作成するか、または **キャンセル**をクリックして取り消します。

ハードウェアプロファイル名の変更

ハードウェアプロファイル名を変更するには、以下を行います。

1. **Dell Management Center** で **展開** → **展開テンプレート** → **ハードウェアプロファイル** を選択します。
2. ハードウェアプロファイルページでプロファイルを選択して **名前の変更** をクリックします。
3. **名前の変更** ダイアログボックスで一意的ハードウェアプロファイル名を入力します。
4. 新しい名前を使用するには、**適用** をクリックします。あるいは **キャンセル** をクリックして取り消します。

ハードウェアプロファイルの削除

ハードウェアプロファイルを削除するには、以下を行います。

 **メモ:** 実行中の展開タスクの一部であるハードウェアプロファイルを削除すると、タスクが失敗する原因になります。

1. **Dell Management Center** で **展開** → **展開テンプレート** → **ハードウェアプロファイル** を選択します。
2. プロファイルを選択して、**削除** をクリックします。
3. プロファイルの削除メッセージダイアログボックスで、**削除** をクリックするか、または **キャンセル** をクリックして取り消します。

アップデートされたハードウェアプロファイルの更新

アップデートされたハードウェアプロファイルを更新するには、以下を行います。

1. **Dell Management Center** で **展開** → **展開テンプレート** → **ハードウェアプロファイル** を選択します。
2. **更新** をクリックします。
アップデートされたハードウェアプロファイル情報が表示されます。

新しいハイパーバイザープロファイルの作成

ESX/ESXi をサーバーに導入して設定するには、ハイパーバイザープロファイルを作成する必要があります。ハイパーバイザープロファイルには、以下の情報が必要です。

- NFS または CIFS 共有上のスクリプト可能な参照 ISO ソフトウェアメディアローション
- 導入ホストおよびオプションのホストプロファイルを管理する vCenter インスタンス
- プラグインがサーバーを導入する先の vCenter のクラスタまたはデータセンター

 **メモ:** 参照 ISO ファイル名には、次の命名法を使用します。
NFS フォーマット: `host:/share/hypervisor_image.iso`
CIFS フォーマット: `¥¥ host ¥ share ¥ hypervisor.iso`

 **メモ:** 正しい導入には、ESX ISO に正しいドライバが備わっていることが必要です。より新しい Dell システムでは、すべての必要な Dell ドライバが含まれる Dell カスタム ISO イメージが必要になる可能性があります。ESX 4.1 はより新しい Dell システムでは動作しない可能性があり、Dell から入手可能なカスタム ISO を備えていない可能性があります。

新しいハイパーバイザープロファイルを作成するには、次の手順を実行します。

1. **Dell Management Center** で、**導入** → **導入テンプレート** → **ハイパーバイザープロファイル**を選択します。
2. **ハイパーバイザープロファイル**ページで、**新規作成**をクリックします。
3. **新規ハイパーバイザープロファイル**ページで以下を行います。
 - **プロファイル名**テキストボックスに、プロファイル名を入力します。
 - **説明**テキストボックスに、オプションで説明を入力します。
4. 左ペインで、**参照 ISO** をクリックし、次に **編集** をクリックし、**ハイパーバイザーのインストール元**ダイアログボックスで以下の情報を入力します。
 - **インストール元 (ISO)** テキストボックスに、ハイパーバイザー共有ロケーションへのパスをタイプします。このハイパーバイザーイメージのコピーが変更され、スクリプトによるインストールが許容されます。参照 ISO ロケーションは、次のいずれかのフォーマットを使用する必要があります。
 - NFS フォーマット: host/share/hypervisor_image.iso
 - CIFS フォーマット: ¥¥ host ¥ share ¥ hypervisor.iso
 - **バージョンの選択**ドロップダウンリストで、ESX または ESXi バージョンを選択します。

このハイパーバイザープロファイルを使用して導入されたすべてのサーバーにはこのイメージが備わります。サーバーが 12G より前のバージョンの場合、**OpenManage Server Administrator** の最新の推奨バージョンがインストールされます。
5. CIFS 共有を使用する場合は、**ユーザー名**、**パスワード**、および**パスワードの確認**を入力します。両パスワードは一致している必要があります。
6. 設定をプロファイルに追加するには、**保存**をクリックします。
7. 左側のペインで、**vCenter 設定** をクリックして、必要な箇所を編集します。
 - **vCenter インスタンス** : 導入後にホストを管理するサーバーインスタンスを表示します。
 - **vCenter バージョン** : 現在のバージョンを表示します。
 - **vCenter 宛先コンテナ**: 新しい物理サーバーをホストするデータセンターまたはクラスターです。 **参照** をクリックして、vCenter の導入先を検索します。
 - **vCenter ホストプロファイル**: ホスト設定をカプセル化し、ホスト設定をしやすくするプロファイルを選択します。
8. 情報をプロファイルに追加するには、**保存**をクリックします。

ハイパーバイザープロファイルの管理に関する情報は、「[ハイパーバイザープロファイルの管理](#)」を参照してください。

ハイパーバイザープロファイルの管理

既存のハイパーバイザープロファイルについて実行できる管理処置には、以下が含まれます。

- [VLAN サポートの理解](#)
- [ハイパーバイザープロファイルの表示または編集](#)
- [ハイパーバイザープロファイルの複製](#)
- [ハイパーバイザープロファイル名の変更](#)
- [ハイパーバイザープロファイルの削除](#)
- [ハイパーバイザープロファイルの更新](#)

VLAN のサポート

Dell Management Plug-in は、ルータブル VLAN へのハイパーバイザー導入をサポートします。Configure VLAN サポートは「[導入ウィザード手順 4](#)」で設定します。導入ウィザードのこの部分では、VLAN の使用および

VLAN ID を指定するオプションがあります。VLAN ID が提供されると、導入の際にハイパーバイザーの管理インターフェースに適用され、すべてのトラフィックがその VLAN ID でタグ付けされます。

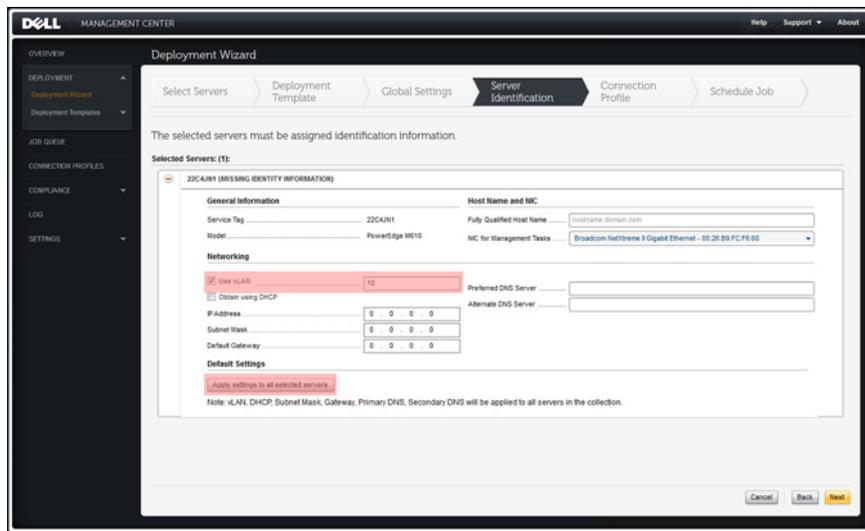


図 5. 導入ウィザードのサーバー識別ページで VLAN 設定を有効にします。

導入の際に提供された VLAN が、仮想アプライアンスと vCenter サーバーの両方と通信できることを確認してください。ハイパーバイザーを宛先のいずれかまたは両方と通信できない VLAN に導入すると、導入が失敗する原因となります。

1つの導入ジョブで複数のベアメタルサーバーを選択し、同じ VLAN ID をすべてのサーバーに適用する場合、導入ウィザードのサーバー識別の箇所にあるデフォルト設定で、**選択したすべてのサーバーに設定を適用します**ボタンを使用します。これにより、同じ VLAN ID とともにその他のネットワーク設定を、その導入ジョブのすべてのサーバーに適用することができます。

 **メモ:** Dell Management Plug-in は、マルチホーム構成をサポートしません。2つ目のネットワークとの通信のための、アプライアンスへの2つ目のネットワークインターフェースの追加は、ハイパーバイザー導入、サーバーコンプライアンス、およびファームウェアアップデート操作が関わるワークフローに問題を生じます。

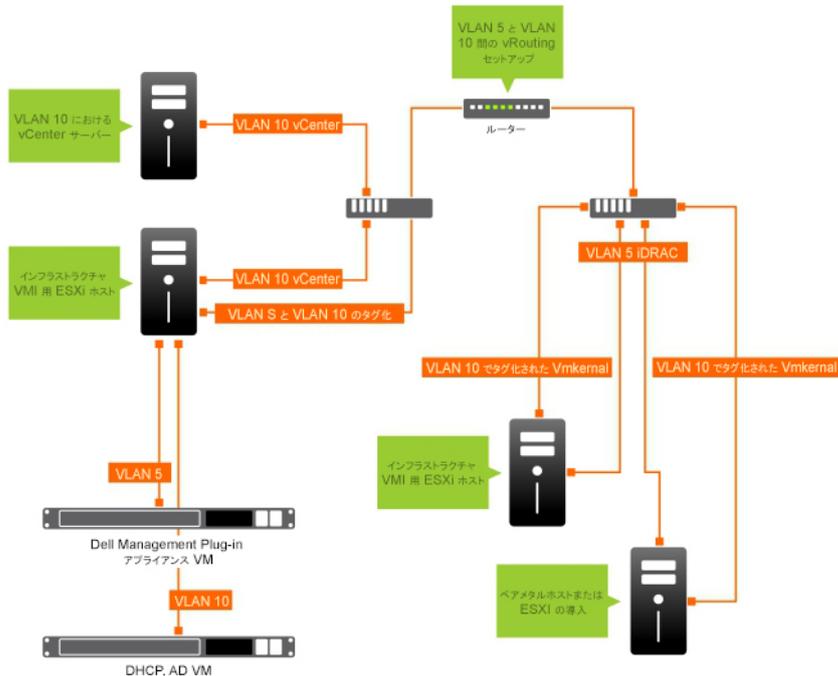


図 6. VLAN ネットワークの例。

このネットワークの例では、導入された vCenter と ESXi ホストの VMkernel が VLAN 10 にあり、Dell Management Plug-in が VLAN 5 にあります。Dell Management Plug-in が VLAN のマルチホームをサポートしないため、すべてのシステムが互いに正しく通信するためには、VLAN 5 が VLAN 10 に送られる必要があります。これらの VLAN でルーティングが有効でない場合、導入は失敗します。

ハイパーバイザープロファイルの表示または編集

ハイパーバイザープロファイルの表示または編集には以下を行います。

1. **Dell Management Center** で、**展開** → **展開テンプレート** → **ハイパーバイザープロファイル** ウィンドウを選択します。
2. プロファイルを選択して、**表示 / 編集** をクリックします。
3. **ハイパーバイザープロファイル** : **プロファイル名** ウィンドウで表示または変更のためにプロファイル項を選択して、必要な変更を行います。
4. 変更を適用するには、**保存** をクリックします。または **キャンセル** をクリックして変更を取り消します。

ハイパーバイザープロファイルのコピー

ハイパーバイザープロファイルのコピーには、以下を行います。

1. **Dell Management Center** で、**展開** → **展開テンプレート** → **ハイパーバイザープロファイル** を選択します。
2. **ハイパーバイザープロファイル** ページでプロファイルを選択して、**重複** をクリックします。
3. **重複** ダイアログボックスで、一意のハイパーバイザープロファイル名を入力します。
4. **適用** をクリックして新しい名前で作成するか、または **キャンセル** をクリックして取り消します。

ハイパーバイザープロファイル名の変更

ハイパーバイザー名を変更するには、以下を行います。

1. **Dell Management Center** で、**展開** → **展開テンプレート** → **ハイパーバイザープロファイル**を選択します。
2. **ハイパーバイザープロファイル**ページで、プロファイルを選択して**名前の変更**をクリックします。
3. **名前の変更**ダイアログボックスで、一意のハイパーバイザープロファイル名を入力します。
4. 新しい名前を使用するには、**適用**をクリックします。あるいは**キャンセル**をクリックして取り消します。

ハイパーバイザープロファイルの削除

ハイパーバイザープロファイルを削除するには、以下を行います。

 **メモ:** 実行中の導入タスクの一部となっているハイパーバイザープロファイルを削除すると、展開タスクが失敗する可能性があります。

1. **Dell Management Center** で、**展開** → **展開テンプレート** → **ハイパーバイザープロファイル**を選択します。
2. プロファイルを選択して、**削除**をクリックします。
3. メッセージダイアログボックスで、**削除**をクリックしてプロファイルを削除するか、**キャンセル**をクリックして取り消します。

ハイパーバイザープロファイルの更新

ハイパーバイザープロファイルを更新するには、以下を行います。

1. **Dell Management Center** で **展開** → **展開テンプレート** → **ハイパーバイザープロファイル**を選択します。
2. **更新**をクリックします。
アップデートされたハイパーバイザープロファイル情報が表示されます。

新規の展開テンプレートの作成

展開テンプレートには、ハードウェアプロファイル、ハイパーバイザープロファイル、またはその両方が含まれます。展開ウィザードはこのテンプレートを使用してサーバーハードウェアのプロビジョニングを行い、ホストを **vCenter** 内に展開します。

新規展開テンプレートの作成には、以下を行います。

1. **Dell Management Center** で **展開** → **展開テンプレート**を選択します。
2. **使用可能なプロファイル**で **新規作成**をクリックします。
3. **新規作成**ウィンドウで、テンプレート名を入力し、**保存**をクリックします。
4. テンプレートを完成するには、**編集**をクリックします。
5. 右ペインの **プロファイル**ドロップダウンリストで、プロファイルを選択して、以下のいずれかを行います。
 - 選択したプロファイルのハードウェア/ハイパーバイザープロファイル設定を表示するには、**表示**をクリックします。
 - 新規ハードウェア/ハイパーバイザープロファイルを作成するには、**新規作成**をクリックします。
6. 展開テンプレートについて、オプションでテンプレートの管理に役立つ **説明**を入力します。
7. プロファイルの選択を適用し、変更を保存するには、**保存**をクリックします。取り消すには、**キャンセル**をクリックします。

展開テンプレートの管理

Dell Management Center からは、既存の展開テンプレートに対して以下を始めとする管理作業を実施することができます。

- [展開テンプレートの作成](#)
- [展開テンプレートのコピー](#)
- [展開テンプレート名の変更](#)
- [展開テンプレートの削除](#)

展開テンプレートのコピー

展開テンプレートをコピーするには、以下を行います。

1. **Dell Management Center** で **展開** → **展開テンプレート** を選択します。
2. 展開テンプレートページでテンプレートを選択し、**重複** をクリックします。
3. テンプレートの新しい名前を入力し、**適用** をクリックします。テンプレートの名前は一意である必要があります。

展開テンプレートの削除

展開テンプレートを削除するには、以下を行います。

1. **Dell Management Center** で、**展開** → **展開テンプレート** を選択します。
2. **展開テンプレート** ページでテンプレートを選択し、**削除** をクリックします。
3. メッセージボックスで **削除** をクリックして、テンプレートを削除するか、**キャンセル** をクリックして取り消します。

展開テンプレート名の変更

展開テンプレート名を変更するには、以下を行います。

1. **Dell Management Center** で、**展開** → **展開テンプレート** を選択します。
2. **展開テンプレート** ページでテンプレートを選択し、**名前の変更** をクリックします。
3. テンプレートの新しい名前を入力し、**適用** をクリックします。テンプレートの名前は一意である必要があります。
4. すべてのアップデートされた展開テンプレートを表示するには、**Dell Management Center** で **展開** → **展開テンプレート** を選択して、**更新** をクリックします。

展開ウィザードの実行

展開ウィザードは、以下のベアメタルサーバー展開プロセスを順次ガイドします。

- 未展開サーバーの選択。
ハイパーバイザーを展開する場合、最低 1 GB を保存できる内蔵デュアル SD モジュールに展開することができます。内蔵デュアル SD モジュールは、ハイパーバイザーを **Dell Management Plug-in** で展開する前に、BIOS で有効化されている必要があります。
- 展開テンプレート（ハードウェアおよびハイパーバイザープロファイルの組み合わせ）の使用。
- グローバル設定のセットアップ。このページでは、ハイパーバイザーをハードディスクまたは内蔵デュアル SD モジュールのどちらに展開するか選択できます。
- 展開サーバーに対する識別情報の割り当て。
- 各サーバーへの希望する接続プロファイルの照合。

- サーバー展開ジョブ実行のスケジュール。
- 展開ジョブを管理できるジョブキューの表示。

 **メモ:** ハードウェアプロファイルのみを展開する場合は、新規グローバル設定、サーバー識別情報、および接続プロファイルページを省略して、直接ジョブのスケジュールページへ進みます。

関連タスク:

- [展開ウィザード手順1: サーバーの選択](#)
- [展開ウィザード手順2: 展開テンプレート](#)
- [展開ウィザード手順3: グローバル設定](#)
- [展開ウィザード手順4: サーバー識別情報](#)
- [展開ウィザード手順5: 接続プロファイル](#)
- [展開ウィザード手順6: ジョブのスケジュール](#)

展開ウィザード - 手順1: サーバーの選択

このページでは、サーバーの展開を説明しています。ハイパーバイザーを内蔵デュアル SD モジュールに展開したい場合、このページにそのオプションが使用可能かどうか表示されます。内蔵デュアル SD モジュールの詳細については、「[展開ウィザードの実行](#)」を参照してください。展開したいサーバーのリストに手順2が表示されない場合、サーバーを手動で追加し、この手順がリストに表示されるようにできます。「[手動によるサーバーの追加](#)」を参照してください。

サーバーを選択するには、以下を行います。

1. **Dell Management Center** で **展開** → **展開ウィザード** を選択します。
2. **サーバーの選択** ウィンドウで非展開サーバーをこの展開ジョブに割り当てるには、チェックボックスを使用して **サーバー** を選択します。
3. **次へ** をクリックします。

手順2のタスクへ進むには、[展開ウィザード手順2](#) をクリックします。

展開ウィザード手順2: 展開テンプレート

ハードウェアプロファイルへの展開は、ハイパーバイザー展開とは異なります。ハードウェアプロファイルへの展開については、「[展開ウィザード手順6](#)」を参照してください。

 **メモ:** 正しい展開には、ESX ISO に正しいドライバが備わっていることが必要です。より新しい Dell システムでは、すべての必要な Dell ドライバが含まれる **Dell カスタム ISO** イメージが必要になる可能性があります。ESX 4.1 はより新しい Dell システムでは動作しない可能性があり、Dell から入手可能なカスタム ISO を備えていない可能性があります。

展開テンプレートを選択するには、以下を行います。

1. 展開テンプレートは、以下のように1つまたは多くの方法で展開テンプレートを選択 / 作成します。
 - **使用可能なテンプレート** で既存の展開テンプレートを選択します。選択したテンプレートに対する情報が右ペインに表示されます。
 - 既存の展開テンプレートを選択し、**編集** をクリックして1つまたは両方の関連プロファイルを変更します。
 - **新規作成** をクリックして、新しいテンプレートを定義します。
2. 次のいずれか1つを選択します。
 - ハードウェアプロファイルへの展開には、**次へ** をクリックし、[展開ウィザード手順6](#) に進みます。

- ハイパーバイザープロファイルへの展開には、**次へ**をクリックし、[展開ウィザード手順3](#)に進みます。

展開ウィザード手順3: グローバル設定

ハイパーバイザーをハードディスクドライブまたは内蔵デュアル SD モジュールのいずれかに展開できます。少なくとも選択されたサーバーの1台で内蔵デュアル SD モジュールが使用できる場合は、内蔵デュアル SD モジュールオプションボタンが有効となります。ドロップダウンリストは内蔵デュアル SD モジュールオプションボタンが選択されるまで無効となっています。オプションボタンは、ドロップダウンリストでの有効/無効を切り替えます。

1. グローバル設定ページで、ハイパーバイザーをインストールするには、以下の展開ターゲットの1つを選択します。
 - ハードディスク
ハードディスクに展開する場合は、このオプションをクリックします。
 - 内蔵デュアル SD モジュール
内蔵デュアル SD モジュールに展開する場合は、このオプションをクリックして **使用可能な内蔵デュアル SD モジュールのないサーバーの最初のハードディスクにハイパーバイザーを展開します**。チェックボックスを選択します。これによって、ハイパーバイザーが当該システムの最初のディスクに展開されます。

注意: ディスクドライブのすべてのデータは消去されます!

選択されたサーバーのどれもが内蔵デュアル SD モジュールに対応していない場合、または内蔵デュアル SD モジュールが展開時にない場合、それらのサーバーへの展開は省略され、展開ジョブは次のサーバーに進みます。

2. **次へ**をクリックします。
手順4のタスクに進むには、「[展開ウィザード手順4: サーバー識別情報](#)」をクリックします。

導入ウィザード手順4: サーバー識別情報

サーバー識別情報は、2つの方法で提供することができます。

- ネットワーク情報を入力します (IP アドレス、サブネットマスクおよびゲートウェイ)。ホスト名の完全修飾ドメイン名は必須です。FQDN での *localhost* の使用はサポートされていません。FQDN はホストを vCenter に追加する場合に使用します。
- 動的ホスト構成プロトコル (DHCP) を使用して IP アドレス、サブネットマスク、ゲートウェイ IP、ホスト名および優先/代替え DNS サーバーを設定します。ホストを vCenter に追加する場合、DHCP が割り当てる IP アドレスが使用されます。DHCP を使用する場合、選択された NIC MAC アドレスには IP 予約を使うことを強くお勧めします。

 **メモ:** ホスト名には、*localhost* ではなく完全修飾ドメイン名 (FQDN) を使用します。ESXi 5.1 以降では、*localhost* という値は Dell Management Plug-in がホストから送信されるイベントを処理する際の障害となります。IP アドレスを FQDN に解決する DNS の記録を作成します。ESXi 5.1 からの SNMP アラートが正しく識別されるよう、DNS サーバーが逆引き要求に対応するように設定します。導入ジョブのスケジュールが実行される前に、DHCP 予約および DNS ホスト名が設定されて検証されている必要があります。

この画面は VLAN ID を指定するオプションを提供します。VLAN ID が提供されると、導入の際にハイパーバイザーの管理インターフェースに適用され、すべてのトラフィックがその VLAN ID でタグ付けされます。

サーバーを識別するには、以下を行います。

1. サーバー ID は導入されたサーバーに新しい名前とネットワーク識別情報を割り当てます。ファームウェア、BIOS に関する最低要件を満たさない、またはその他の問題があるサーバーのリストを表示するには、**非対応サーバー** をクリックします。
2. 詳細情報については、**詳細** をクリックします。
3. システムがアップデートされたら、**対応のチェック** をクリックし、再テストを行い問題解決を検証します。このリストを更新するには、**更新** をクリックし、**すべてのテストを中止** をクリックしてテストを取り消します。
4. 個別サーバー情報を表示するには、**^** をクリックして導入します。
5. **ホスト名と NIC** でサーバーの **完全修飾ホスト名** を入力します。
6. **NIC 管理タスク用** ドロップダウンリストで、サーバー管理に使用する **NIC** を選択します。
7. **IP アドレス、サブネットマスク** およびその他のネットワーク情報を入力するか、あるいは、**DHCP を使用して取得** チェックボックスを選択します。
8. **VLAN ID** を必要とするネットワークに導入する場合、**VLAN** のチェックボックスを選択してから **VLAN ID** を入力します。
VLAN ID には、1~4094 の数字を使用します。VLAN ID 0 はフレームの優先順位タグ用に予約されています。
9. 導入するすべてのサーバーについてこれを繰り返すか、**選択したすべてのサーバーに設定を適用** します チェックボックスを選択します。
10. **次へ** をクリックします。
手順 5 のタスクへ進むには、「[導入ウィザード手順 5](#)」 をクリックします。

展開ウィザード手順 5: 接続プロファイル

接続プロファイルは、ホストの接続資格情報を iDRAC またはホストルートの資格情報と関連付けることにより、その接続資格情報を確立するために使われます。接続プロファイルウィンドウでは以下ができます。

- 現在の接続プロファイルの表示または編集
- 接続プロファイルの削除
- vCenter ホストの変更を反映するための接続プロファイルリストの更新

接続プロファイルを作成するには、以下を行います。

1. 接続プロファイルは展開ジョブが完了すると、自動的にサーバーを接続プロファイルに割り当てます。接続プロファイルを選択したら、**次へ** をクリックします。
2. **すべてのサーバーを同じ接続プロファイルに割り当てる** オプションボタンを選択し、接続プロファイルをドロップダウンリストから選択し、すべてのサーバーを同じ既存プロファイルに割り当てます。
3. 新しいプロファイルを作成するには、**新規** をクリックします。選択したプロファイルの表示または編集を行うには、**表示 / 編集** をクリックします。
4. 選択された接続プロファイルを表示するには、**表示** をクリックします。
5. **各サーバーの接続プロファイルの選択** オプションボタンを選択し、ドロップダウンリストから各サーバーの接続プロファイルを選択します。
6. 接続プロファイルを選択したら、**次へ** をクリックします。
手順 6 のタスクへ進むには、「[展開ウィザード手順 6](#)」 をクリックします。

展開ウィザード手順 6: ジョブのスケジュール

スケジュールは、展開ジョブのスケジュールを設定します。展開ジョブの実行時期を設定するには、次のようなオプションがあります：ただちに実行、選択した日付と時刻に展開ジョブを実行するようスケジュール、展開ジョブを保留し手動で開始する

スケジュールを設定するには、以下を行います。

1. 日付と時刻を入力していつ展開ジョブを実行するか決定します。
 - a) サーバーの展開スケジュールの設定をクリックします。
 - b) カレンダーコントロールを使用して日付を選択します。
 - c) 時刻を入力します。
 - * ただちに: **今すぐサーバーを展開**をクリックします。
 - * ジョブの延期: **展開ジョブの作成**をクリックします。
 - * 保留: このオプションではスケジュールだけが変更でき、その他すべての展開ジョブオプションは変更できません。
2. ジョブ名とジョブの説明を入力します。
3. **Finish (終了)** をクリックします。
4. これで展開ウィザードが終了したので、**ジョブキュー**を使って展開ジョブを管理することができます。
5. ウィザードを完了させるためにファームウェアアップデートが必要な、非対応サーバーのリストを表示するには、**非対応サーバー**をクリックします。

関連タスク:

- [展開ジョブキューを使用した展開ジョブの管理](#)

ジョブキューの理解

ジョブキューは、サーバー展開およびインベントリ検索ジョブを管理します。それには以下が含まれます。

- 提出されたサーバー展開ジョブの表示。
- 展開ジョブまたはインベントリ/保証履歴キューの更新
- 現在の vCenter にある Dell サーバー属性をアップデートするためのインベントリジョブのスケジュール。
- 展開ジョブキュー項目のページ。

 **メモ:** インベントリ/保証に最新情報が含まれていることを確認するため、最低1週間に1度は、インベントリ/保証ジョブの実行をスケジュールします。インベントリ/保証ジョブは最低限のリソースしか消費しないので、ホストパフォーマンスの低下はもたらしません。

このページのタスクには、以下が含まれます。

- [展開ジョブキューの使用による展開ジョブの管理](#)
- [インベントリジョブの実行](#)
- [インベントリジョブスケジュールの変更](#)

展開ジョブキューの使用による展開ジョブの管理

展開ジョブキューを使用して展開ジョブを管理するには、以下を行います。

1. **Dell Management Center** で **ジョブキュー** → **展開ジョブ** を選択します。
2. **展開ジョブの詳細** をアップデートするには、**更新** をクリックします。
3. 展開ジョブに含まれるサーバーの詳細情報を含む展開ジョブの詳細ダイアログを表示するには、**詳細** をクリックします。これにより、以下の詳細が表示されます。
 - サービスタグ
 - iDRAC の IP アドレス
 - サーバーステータス
 - 警告の発生状況
 - 展開ジョブの詳細
 - 開始および終了時刻

ダイアログテーブルの各項目の完全な情報を表示するには、カーソルを項目に合わせるとさらにテキストポップアップが表示されます。

4. 選択されたジョブを保留し、またはアップデートされたスケジュールを入力するには、**変更**をクリックします。
5. 展開ジョブを中止するには、**中止**をクリックします。
6. メッセージが表示されたら、**ジョブを中止する**をクリックして中止するか、**ジョブを中止しない**をクリックして取り消します。

 **メモ:** 進行中の展開ジョブは中止できません。

7. 展開ジョブキューのページウィンドウを表示するには、**ページジョブのキュー**をクリックします。**日付とジョブステータスより古い**を選択して、**適用**をクリックします。選択されたジョブはキューから消去されます。

手動によるサーバーの追加

検出プロセスで追加されなかったサーバーは、手動で追加することができます。サーバーは追加されると、展開ウィザードのサーバーリストに表示されます。

1. **Dell Management Center** → **展開**で、**展開ウィザード**をクリックします。
2. **サーバーの選択**タブで、**サーバーの追加**をクリックします。
3. **サーバーの追加**ダイアログボックスで、以下を行います。
 - a) **iDRAC IP アドレス**テキストボックスに **iDRAC IP アドレス**を入力します。
 - b) **ユーザー名**テキストボックスに **ユーザー名**を入力します。
 - c) **パスワード**テキストボックスに **パスワード**を入力します。
4. **サーバーの追加**をクリックします。これには数分かかることがあります。

ベアメタルサーバーの取り外し

自動検出または手動で追加されたサーバーは、手動で取り外すことができます。

1. **Dell Management Center** → **展開**で、**展開ウィザード**をクリックします。
2. **サーバーの選択**タブで、**サーバーの削除**をクリックします。
3. **サーバーの削除**ダイアログボックスで、**取り外すサーバーのチェックボックス**を選択します。
4. **選択したサーバーの削除**をクリックします。
5. **サーバーの選択**タブで、テーブルに記載されているサーバーを表示し、取り外されたことを確認します。

Dell Management Plug-in の管理

Dell Management Plug-in とその仮想環境の管理は、2つのさらなる管理ポータルを使って行います。

- ウェブベース管理コンソール
- 個別サーバーのコンソールビュー（アプライアンス仮想マシンコンソール）。

これら2つのポータルを使用して、vCenter 管理のためのグローバル設定、Dell Management Plug-in データベースのバックアップおよび復元、並びにリセット/再起動動作をすべての vCenter インスタンスにわたって入力、使用することができます。

ウェブベース管理コンソール

ウェブベース管理コンソールはいくつかの主要機能を提供します。それは、vCenter サーバーの登録および管理、仮想アプライアンスの管理、グローバル vCenter 警告の設定、および設定のバックアップと復元です。

vCenter サーバー接続の管理

管理コンソールの alertvCenter 登録ウィンドウで、vCenter サーバーを登録してライセンスをアップロードまたは購入することができます。デモライセンスを使用している場合、今すぐ購入リンクが表示され、複数ホストを管理するための完全バージョンのライセンスを購入することができます。この項では、サーバーの変更、アップデートおよび登録の取り消しを行うこともできます。

関連タスク:

- [vCenter サーバーの登録](#)
 - [管理者 vCenter ログインの変更](#)
 - [登録 vCenter の SSL 証明のアップデート](#)
 - [vCenter からの Dell Management Plug-in のアンインストール](#)
- [管理コンソールを使用した Dell Management Plug-in ライセンスのアップロード](#)

vCenter サーバーの登録

新しい Dell Management Plug-in をインストールすると、vCenter サーバーは Dell Management Plug-in で登録することができます。Dell Management Plug-in による vCenter の操作には、管理者ユーザーアカウントを使います。vCenter サーバーを登録するには、次の手順を実行します。

1. ブラウザウィンドウを起動して、vSphere vCenter コンソール タブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。 **https://<ApplianceIPAddress>**
2. 新規サーバーを登録するには、左ペインで **VCENTER 登録** をクリックし、**新規 vCenter サーバーの登録** をクリックします。
3. **新規 vCenter の登録** ダイアログボックスの **vCenter 名** で次を行います。

- a) **vCenter サーバー IP またはホスト名** テキストボックスに vCenter IP アドレスまたはホスト名を入力します。
- b) **説明** テキストボックスに、オプションで説明を入力します。
- 4. **管理者ユーザーアカウント**で、次を行います。
 - a) **管理者ユーザー名** テキストボックスに管理者のユーザー名を入力します。
 - b) **パスワード** テキストボックスにパスワードを入力します。
 - c) **パスワードの確認** テキストボックスにパスワードを再度入力します。
- 5. **登録**をクリックします。

vCenter 管理者ログインの変更

vCenter 管理者ログインを変更するには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。 **https://<ApplianceIPAddress>**
2. 左ペインで **VCENTER** の **登録** をクリックします。登録された vCenter がテーブルに表示されます。 **管理者アカウントの変更** ウィンドウを表示するには、**資格情報** で、**変更** をクリックします。
3. vCenter 管理者の **ユーザー名**、**パスワード** および **パスワードの確認** を入力します。両パスワードは一致する必要があります。
4. パスワードを変更するには、**適用** をクリックします。または変更を取り消すには、**キャンセル** をクリックします。

登録された vCenter サーバーの SSL 証明書のアップデート

vCenter サーバーの SSL 証明書が変更された場合、Dell Management Plug-in に新しい証明書をインポートするため、次の手順を実行します。Dell Management Plug-in はこの証明書を使用して、通信相手の vCenter サーバーが正しい vCenter サーバーであって、偽装でないことを確認します。

Dell Management Plug-in は、2048 ビットキー長の RSA 暗号化標準を使用した openssl API によって、証明書署名要求 (CSR) を作成します。信頼される認証局からのデジタル署名付き証明書を取得するために、Dell Management Plug-in によって生成された CSR が使用されます。Dell Management Plug-in は通信をセキュアにするために、デジタル証明書を使用してウェブサーバーの SSL を有効にします。

登録された vCenter サーバーの SSL 証明書をアップデートするには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。 **https://<ApplianceIPAddress>**
2. 左ペインで **VCENTER** の **登録** をクリックします。登録された vCenter がテーブルに表示されます。証明書をアップデートするには、**アップデート** をクリックします。

VMware vCenter からの Dell Management Plug-in のアンインストール

Dell Management Plug-in を削除するには、管理コンソールを使って vCenter サーバーから登録を取り消す必要があります。

VMware vCenter から Dell Management Plug-in をアンインストールするには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。
https://<ApplianceIPAddress>
2. **vCenter** の **登録** ページの vCenter サーバーテーブルで、**登録解除** をクリックして Dell Management Plug-in の登録を取り消します。

1つ以上の vCenter がある可能性があるため、正しいものを選択するよう気をつけてください。

3. vCenter の登録解除ダイアログボックスで登録を取り消してもよいですかと確認されるので、登録解除をクリックします。

管理コンソールへの Dell Management Plug-in ライセンスのアップロード

Dell Management Plug-in ライセンスを管理ポータルへアップロードするには、以下を行います。

1. ブラウザウィンドウを起動して、vSphere vCenter コンソール タブに表示されている、設定したい仮想マシンの管理コンソール URL を入力するか、または Dell Management Console → 設定 ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。 **https://<ApplianceIPAddress>**
2. 左ペインで、VCENTER の登録をクリックします。登録された vCenters がテーブルに表示されます。アップロードライセンスダイアログボックスを表示するには、ライセンスのアップロードをクリックします。
3. ライセンスファイルにナビゲートするには、参照 ボタンをクリックして、次にアップロードをクリックします。

 **メモ:** ライセンスファイルが変更されたり、何らかの形で編集された場合、アプライアンスはそれが破損されているとみなし、ファイルは機能しなくなります。

仮想アプライアンス管理

仮想アプライアンス管理には、Dell Management Plug-in ネットワーク、バージョン、NTP、および HTTPS 情報が含まれており、管理者は以下を行うことができます。

- 仮想アプライアンスの再スタート
- 仮想アプライアンスのアップデート、およびアップデートリポジトリロケーションの設定
- アプライアンスログイン情報が含まれるトラブルシューティングバンドルの生成
- ネットワークタイムプロトコル (NTP) 設定の入力
- HTTPS 証明のアップロードおよび管理

関連タスク:

- [仮想アプライアンスの再スタート](#)
- [リポジトリロケーションのアップデートおよびアプライアンスのアップデート](#)
- [トラブルシューティングバンドルのダウンロード](#)
- [NTP サーバーの設定](#)
- [HTTPS 証明のアップロード](#)

仮想アプライアンスの再スタート

仮想アプライアンスを再スタートするには、以下を行います。

 **メモ:** 仮想アプライアンスを再スタートさせると、管理コンソールからログアウトされ、Dell Management Plug-in は、仮想アプライアンスとそのサービスがアクティブになるまで使用不可能となります。

1. ブラウザウィンドウを起動して、vSphere vCenter コンソール タブに表示されている、設定したい仮想マシンの管理コンソール URL を入力するか、または Dell Management Console → 設定 ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。 **https://<ApplianceIPAddress>**
2. 左ペインでアプライアンス管理をクリックします。
3. Dell Management Plug-in を再スタートするには、仮想アプライアンスの再スタートをクリックします。

4. 仮想アプライアンスの再起ダイアログボックスで、仮想アプライアンスを再起するには **適用** をクリックするか、または **キャンセル** をクリックして取り消します。

リポジトリの場所と仮想アプライアンスのアップデート

リポジトリの場所と仮想アプライアンスをアップデートするには、以下を行います。

 **注意:** 仮想アプライアンスのアップデート前にバックアップを実行し、すべてのデータを保護します。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。 **https://<ApplianceIPAddress>**
2. 左ペインで **アプライアンス管理** をクリックします。
3. アプライアンスのアップデートの横の **編集** をクリックします。
4. **アプライアンスのアップデート** ウィンドウでリポジトリホスト名の **アップデート** または **IP アドレス** を入力し、**適用** をクリックします。

 **メモ:** アップデートロケーションが、Dell FTP サイトなどの外部ネットワークにある場合、HTTP プロキシエリアの下にプロキシを入力する必要があります。

仮想アプライアンスソフトウェアバージョンのアップデート

 **注意:** データの喪失を予防するため、ソフトウェアアップデートの開始前にアプライアンスのバックアップを実行します。

仮想アプライアンスソフトウェアをアップデートするには、すべてのその他の Dell Management Center および管理コンソールセッションは閉じる必要があります。

仮想アプライアンスソフトウェアバージョンをアップデートするには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。
https://<ApplianceIPAddress>
2. 左ペインで、**アプライアンスのメンテナンス** をクリックします。
3. 仮想アプライアンスを **アプライアンスのアップデート** に記載されているソフトウェアバージョンにアップデートするには、**仮想アプライアンスのアップデート** をクリックします。
4. **アプライアンスのアップデート** ダイアログボックスには、現在および使用可能なバージョンが記載されています。アップデートを開始するには、**アップグレード** をクリックします。
5. システムはロックダウンし、保守モードになります。アップデートが完了すると、アプライアンスページに新たにインストールされたバージョンが表示されます。

トラブルシューティングバンドルのダウンロード

この情報を使用してトラブルシューティング問題の参考にしたたり、技術サポートへ送付します。

トラブルシューティングバンドルをダウンロードするには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。
https://<ApplianceIPAddress>
2. 左ペインで **アプライアンス管理** をクリックします。

3. トラブルシューティングバンドルのダイアログボックスを表示するには、**トラブルシューティングバンドルの作成**をクリックします。
4. 仮想アプライアンスログ情報を含む Zip ファイルを開くか保存するには、**トラブルシューティングバンドルのダウンロードリンク**をクリックします。
5. 終了するには、**閉じる**をクリックします。

HTTP プロキシの設定

HTTP プロキシ設定は、管理コンソールまたは Dell Management Console を使用して設定できます。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。
https://<ApplianceIPAddress>
2. 左ペインで **アプライアンス管理** をクリックします。
3. **アプライアンス管理** ページで **HTTP プロキシ設定** にスクロールし、**編集** をクリックします。
4. **編集** ページで以下を行います。
 - a) HTTP プロキシ設定の使用を有効化するには、**HTTP プロキシ設定を使用**の横の **有効** を選択します。
 - b) **プロキシサーバーのアドレス** テキストボックスにプロキシサーバーアドレスを入力します。
 - c) **プロキシサーバーポート** テキストボックスにプロキシサーバーポートを入力します。
 - d) プロキシ資格情報を使用するには、**プロキシ資格情報を使用**の横で **はい** を選択します。
 - e) 資格情報を使用している場合、**ユーザー名** テキストボックスにユーザー名を入力します。
 - f) **パスワード** テキストボックスにパスワードをタイプします。
5. **適用** をクリックします。

NTP サーバーの設定

仮想アプライアンスクロックを NTP サーバーのそれと同期させるには、ネットワークタイムプロトコル (NTP) を使用することができます。

NTP サーバーを設定するには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示されている、設定したい仮想マシンの **管理ポータル URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。
https://<ApplianceIPAddress>
2. 左ペインで **アプライアンス管理** をクリックします。
3. **NTP 用の編集** をクリックします。
4. **有効** チェックボックスをクリックします。 **ホスト名** または **IP アドレス** を **プリファランス** または **セカンダリ NTP サーバー** に入力し、**適用** をクリックします。
5. 終了するには、**キャンセル** をクリックします。

証明書署名要求の生成

新規証明書署名要求を生成することは、以前作成された CSR で作成された証明書がアプライアンスにアップロードされることを防ぎます。

証明書署名要求を生成するには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示されている、設定したい仮想マシンの **管理ポータル URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。

https://<ApplianceIPAddress>

2. 左ペインで **アプライアンス管理** をクリックします。
3. **HTTPS 証明のための証明書署名要求の生成** をクリックします。新規の要求が生成されると、以前の CSR によって作成された証明書はアプライアンスにアップロードできなくなりますというメッセージが表示されます。要求を続けるには、**続行** をクリックします。または、**キャンセル** をクリックして取り消します。
4. 要求の **コモンネーム、組織名、部署名、市区町村名、都道府県名、国名** および **E-メール** を入力します。**続行** をクリックします。
5. **ダウンロード** をクリックして、生成された HTTPS 証明書をアクセスできる場所に保存します。

HTTPS 証明書のアップロード

HTTPS 証明書は、仮想アプライアンスとホストシステム間のセキュアな通信に使用することができます。このタイプのセキュアな通信を設定するには、証明書署名要求を認証局に送り、その結果の証明書を管理コンソールを使用してアップロードする必要があります。また、自己署名によるデフォルト証明書もあり、セキュア通信に使用できます。この証明書は各インストール固有のものであります。

 **メモ:** 証明書のアップロードには、Microsoft Internet Explorer または Firefox を使用できます。

証明書をアップロードするには、次の手順を実行します。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。

https://<ApplianceIPAddress>

2. 左ペインで **アプライアンス管理** をクリックします。
3. **HTTPS 証明用の証明書のアップロード** をクリックします。
4. **証明書のアップロード** ダイアログボックスで、**OK** をクリックします。
5. アップロードする証明書を選択するには、**参照** をクリックして、**アップロード** をクリックします。
6. アップロードを中止するには、**キャンセル** をクリックします。

 **メモ:** 証明書は、PEM フォーマットを使用する必要があります。

デフォルト HTTPS 証明書の復元

デフォルト HTTPS 証明書を復元するには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。

https://<appliance IP address>

2. 左ペインで **アプライアンス管理** をクリックします。
3. **HTTPS 証明用のデフォルト証明書の復元** をクリックします。
4. デフォルト証明書の復元ダイアログボックスで **適用** をクリックします。

グローバル警告の設定

警告管理によって、管理者はすべての vCenter インスタンスに対する警告の保存方法のグローバル設定を入力できます。

グローバル警告を設定するには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter** コンソールタブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。
https://<ApplianceIPAddress>
2. 左ペインで **警告管理** をクリックします。新規の vCenter 警告設定を入力するには、**編集** をクリックします。
3. 次の項目に対する数字の値を入力します。
 - 最大警告数
 - 警告の保持日数
 - 繰り返し警告のタイムアウト時間 (秒)
4. 設定を保存するには、**適用** をクリックするか、**キャンセル** をクリックして取り消します。

バックアップおよび復元の管理

バックアップおよび復元の管理は、管理コンソールで行われます。このページのタスクには以下が含まれます。

- [バックアップおよび復元の設定](#)
- [自動バックアップのスケジュール](#)
- [即時のバックアップの実行](#)
- [バックアップからのデータベースの復元](#)

バックアップおよび復元の設定

バックアップおよび復元機能は、**Dell Management Plug-in** データベースをリモートロケーションにバックアップして、後日それに基づく復元を可能にします。このバックアップには、プロファイル、テンプレートおよびホスト情報が含まれます。データの喪失に備えるため、自動バックアップをスケジュールすることを推奨します。この手順のあと、バックアップスケジュールを設定する必要があります。

バックアップおよび復元を設定するには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter** コンソールタブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。
https://<ApplianceIPAddress>
2. 左ペインで、**バックアップと復元** をクリックします。
3. 現在のバックアップと復元設定を編集するには、**編集** をクリックします。
4. **設定と詳細** ページで、以下を行います。
 - a) **バックアップの場所** テキストボックスにバックアップファイルへのパスをタイプします。
 - b) **ユーザー名** テキストボックスにユーザー名をタイプします。
 - c) **パスワード** テキストボックスにパスワードをタイプします。
 - d) **バックアップを暗号化するために使用するパスワード** の下のテキストボックスに、暗号化パスワードをタイプします。
暗号化パスワードには、英数字および次の特殊文字を使用できます：**!@#%***。長さの制限はありません。
 - e) **パスワードの確認** テキストボックスに暗号化パスワードを再度入力します。
5. これらの設定を保存するには、**適用** をクリックします。
6. バックアップスケジュールを設定します。詳細は、「[自動バックアップのスケジュール](#)」を参照してください。

自動バックアップのスケジュール

これはバックアップおよび復元の第2部です。バックアップロケーションと資格情報に関する詳細は、「[バックアップおよび復元の設定](#)」を参照してください。

自動バックアップのスケジュールには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。
https://<appliance IP address>
2. 左ペインで、**バックアップ**と**復元**をクリックします。
3. バックアップおよび復元の設定を編集するには、**編集自動バックアップスケジュール** をクリックします（これによってフィールドがアクティブになります）。
4. バックアップを有効化するには、**有効**をクリックします。
5. バックアップを実行したい曜日のチェックボックスを選択します。
6. **バックアップ時刻 (24 時間フォーマット、HH:mm)** テキストボックスに時刻を HH:mm フォーマットで入力します。
次のバックアップに次にスケジュールされたバックアップの日付と時刻が表示されます。
7. **適用** をクリックします。

即時のバックアップの実行

即時のバックアップを実行するには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。
https://<ApplianceIPAddress>
2. 左ペインで、**バックアップ**と**復元**をクリックします。
3. **今すぐバックアップ** をクリックします。
4. バックアップ設定からロケーションと暗号化パスワードを使用するには、**今すぐバックアップ** ダイアログボックスでそのチェックボックスを選択します。
5. **バックアップの場所**、**ユーザー名**、**パスワード**、および**暗号化パスワード**を入力します。
暗号化パスワードには、英数字および次の特殊文字を使用できます：![@](#)<#>[\\$](#)[%*](#)。長さの制限はありません。
6. **バックアップ** をクリックします。

バックアップからのデータベースの復元

 **メモ:** 復元の操作では、作業完了後、仮想アプライアンスを再起動させます。

バックアップからデータベースを復元するには、以下を行います。

1. ブラウザウィンドウを起動して、**vSphere vCenter コンソール** タブに表示されている、設定したい仮想マシンの **管理コンソール URL** を入力するか、または **Dell Management Console** → **設定** ページのリンクを使用します。URL は、次のフォーマットを使用し、大文字小文字の区別があります。

https://<ApplianceIPAddress>

2. 左ペインで、**バックアップおよび復元**をクリックすると、現在のバックアップおよび復元設定が表示されます。
3. **今すぐ復元**をクリックします。
4. 今すぐ復元ダイアログボックスで、**ファイルロケーション (CIFS/NFS フォーマット)**を入力します。
5. バックアップファイルの**ユーザー名**、**パスワード**および**暗号化パスワード**を入力します。
暗号化パスワードには、英数字および次の特殊文字を使用できます：!**@#%***。長さの制限はありません。
6. 変更を保存するには、**適用**をクリックします。
適用をクリックすると、アプライアンスは再起動または再スタートします。

vSphere クライアントコンソールタブの理解

コンソールタブは vSphere クライアント内にあり、管理コンソールと関連して作動します。コンソールタブはネットワークの設定、管理パスワードの変更、ローカルタイムゾーンの設定、仮想アプライアンスの再起動、仮想アプライアンスの工場出荷時設定へのリセット、仮想アプライアンスコンソールビューの更新などの機能を提供します。コンソール画面にアクセスすると、VMware vSphere のクライアントがカーソルを制御するようになります。その制御を解除するには、**<CTRL> + <ALT>**を押します。

矢印キーを使って、上または下に移動します。望むオプションを選択できたら、**<ENTER>**を押します。

ネットワークの設定

ネットワークの設定変更は、vSphere クライアントのコンソールタブで行います。

ネットワークの設定には、以下を行います。

1. vSphere クライアントで、Dell Management Plug-in を選択して、**コンソールタブ**をクリックします。
2. コンソールウィンドウで、**ネットワークの設定**を選択し、**<ENTER>**を押します。
3. **デバイスの編集**または**DNS の編集**構成下で望ましいネットワーク設定を入力し、**保存して終了**をクリックします。変更を中止するには、**終了**をクリックします。

仮想アプライアンスパスワードの変更

仮想アプライアンスパスワードは、vSphere クライアントでコンソールタブを使用して変更します。

仮想アプライアンスパスワードを変更するには、以下を行います。

1. vSphere クライアントで、Dell Management Plug-in 仮想マシンを選択して、**コンソールタブ**をクリックします。
2. コンソールタブで、矢印キーを使って**管理パスワードの変更**を選択して、**<ENTER>**を押します。
3. **現在の管理パスワード**を入力し、**<ENTER>**を押します。
管理パスワードには、1つの特殊文字、1つの数字、1つの大文字、1つの小文字を含み、少なくとも8文字である必要があります。
4. **新規管理パスワードの入力**で新パスワードを入力し、**<ENTER>**を押します。
5. 新規パスワードを**管理パスワードを確認**してくださいテキストボックスに再度タイプし、**<ENTER>**を押します。これで管理パスワードは変更されました。

ローカルタイムゾーンの設定

ローカルタイムゾーンを設定するには、以下を行います。

1. **vSphere** クライアントで、**Dell Management Plug-in** 仮想マシンを選択して、**コンソールタブ**をクリックします。
2. **タイムゾーンの設定**を選択して **<ENTER>** を押します。
3. **タイムゾーンの選択**ウィンドウで、望ましいタイムゾーンを選択して、**OK** をクリックします。変更を取り消すには、**キャンセル**をクリックします。これでタイムゾーンがアップデートされました。

仮想アプライアンスの再起動

仮想アプライアンスを再起動するには、以下を行います。

1. **vSphere** クライアントで、**Dell Management Plug-in** 仮想マシンを選択して、**コンソールタブ**をクリックします。
2. この**仮想マシンを再起動**を選択し、**<ENTER>** を押します。
3. 次のメッセージが表示されます。
If there are any processes running on this appliance they will be terminated by this action. Are you sure you wish to do this? (このアプライアンスで実行中のプロセスがある場合、この処理で終了されます。この処理を実行しますか?)
4. 再起動するには、**y**を、取り消すには、**n**を入力します。これでアプライアンスは再起動されました。

仮想アプライアンスの工場出荷時設定へのリセット

仮想アプライアンスを工場出荷時設定へリセットするには、以下を行います。

1. **vSphere** クライアントで、**Dell Management Plug-in** 仮想マシンを選択して、**コンソールタブ**をクリックします。
2. この**仮想アプライアンスを工場出荷時設定にリセット**を選択して、**<ENTER>** を押します。
3. 次の通知が表示されます。
This operation is completely Irreversible if you continue you will completely reset *this* appliance to its original settings. All changes you have made to this appliance will be Lost. Are you sure you wish to Reset this Appliance to Factory Settings? (この操作は元に戻せません。継続すると*この*アプライアンスは当初の設定に完全にリセットされます。このアプライアンスに施したすべての変更は失われます。このアプライアンスを工場出荷時設定にリセットしてよろしいですか?)
4. リセットするには、**y**を入力します。または **n** で取り消します。アプライアンスは当初の工場出荷時設定にリセットされます。

 **メモ:** 仮想アプライアンスが工場出荷時設定にリセットされる場合、ネットワーク設定に加えられたアップデートは維持されます。この設定はリセットされません。

コンソールタブビューの更新

コンソールビューを更新するには、**更新**を選択して、**<ENTER>** を押します。

読み取り専用ユーザーロール

読み取り専用という弱い権限のユーザーロールがあります。診断目的のシェルアクセスができます。読み取り専用ユーザーにはマウント実行の限定的な権限のみが与えられます。読み取り専用ユーザーのパスワードは管理者と同様に設定されます。

トラブルシューティング

本項では、トラブルシューティングの質問に対する回答を記載します。

アップグレードの問題

使っている 1.0 アプライアンスをバックアップして電源を切り、最新バージョンの Dell Management Plug-in を導入してデータベースを復元しようとしたら、Dell Management Plug-in は無効になっています。どうしたらよいですか？

1.0 アプライアンスは、電源をオフにする前に登録解除する必要があります。詳細については、本書に記載されている対応アップグレード手順に従ってください。

1.0 仮想アプライアンスをバックアップして登録解除し、最新バージョンの Dell Management Plug-in を導入して登録した後でデータベースを復元しました。vSphere から Dell Management Plug-in Management Console を起動しようとしたら不明のエラーが表示されました。どうしたらよいですか？

最新バージョンの Dell Management Plug-in の電源を切り、1.0 仮想アプライアンスに電源を入れます。詳細は、本書で説明されているアップグレードの手順に従ってください。

1.0 アプライアンスを登録解除してデータベースをバックアップし、最新バージョンの Dell Management Plug-in を導入して登録してから、データベースを復元しました。Dell Management Plug-in 管理コンソールを起動すると、vCenter が登録されていないというメッセージが表示されます。管理コンソールには登録済み vCenter は表示されておらず、登録しようとすると、すでに登録されているというエラーメッセージが表示されます。どうしたらよいですか？

vCenter 管理下オブジェクトブラウザにアクセスすることによって拡張子を手動で登録解除する必要があります。その後、管理コンソールを使用して vCenter を Dell Management プラグインに再登録してください。

よくあるお問い合わせ (FAQ)

本項には一般的な質問と解決策を記載しています。

Dell Management Plug-in が SNMP トラップを設定およびサポートするのは、Dell サーバーのどの世代ですか？

Dell Management Plug-in は 12 世代サーバーより前の世代のサーバーで OMSA SNMP トラップを設定し、12 世代サーバーで iDRAC トラップを設定します。

Dell Management Plug-in で管理されるのは、リンクモードのどの vCenter ですか？

Dell Management Plug-in が管理するのはリンクモードの登録済み vCenter のみです。

Dell Management Plug-in はリンクモードの vCenter をサポートしますか？

はい、Dell Management Plug-in はリンクモードの vCenter を最大 3 つサポートします。Dell Management Plug-in がリンクモードでどのように機能するかについての詳細は、www.Dell.com でホワイトペーパー『Dell

『Management Plug-in for VMware vCenter: Working in Linked Mode』 (VMware vCenter 向け Dell Management Plug-in : リンクモードでの作業) を参照してください。

Dell Management プラグインのための必須ポート設定は何ですか?

 **メモ:** メモ : Dell Management Center の準拠ウィンドウから利用できる *非準拠 vSphere* ホストの修正リンクを使用して OMSA エージェントを導入する場合、OMSA VIB のダウンロードおよびインストールのため、Dell Management Plug-in は httpClient サービスを開始してポート 8080 を有効にし、ESXi 5.0 以降を開始します。OMSA のインストールが完了すると、サービスは自動的に停止し、ポートは閉じられます。

Dell Management プラグインには、以下のポート設定を使用します。

表 3. 仮想アプライアンスポート

ポート番号	プロトコル	ポートタイプ	最高暗号化レベル	方向	使用状況	設定可能
21	FTP	TCP	なし	出力	FTP コマンドクライアント	不可
53	DNS	TCP	なし	出力	DNS クライアント	不可
80	HTTP	TCP	なし	出力	Dell オンラインデータアクセス	不可
80	HTTP	TCP	なし	入力	管理コンソール	不可
162	SNMP エージェント	UDP	なし	入力	SNMP エージェント (サーバー)	不可
11620	SNMP エージェント	UDP	なし	入力	SNMP エージェント (サーバー)	不可
443	HTTPS	TCP	128 ビット	入力	HTTPS サーバー	不可
443	WSMAN	TCP	128 ビット	入力/出力	iDRAC/OMSA 通信	不可
4433	HTTPS	TCP	128 ビット	入力	自動検出	不可
2049	NFS	UDP	なし	すべて	パブリック共有	不可
4001~4004	NFS	UDP	なし	すべて	パブリック共有	不可
11620	SNMP エージェント	UDP	なし	0m	SNMP エージェント (サーバー)	不可

表 4. 管理下ノード

ポート番号	プロトコル	ポートタイプ	最高暗号化レベル	方向	使用状況	設定可能
162、11620	snmp	UDP	なし	出力	ハードウェア イベント	不可
443	WSMAN	TCP	128 ビット	入力	iDRAC/OMSA 通信	不可
4433	HTTPS	TCP	128 ビット	出力	自動検出	不可
2049	NFS	UDP	なし	すべて	パブリック共 有	不可
4001~4004	NFS	UDP	なし	すべて	パブリック共 有	不可
443	HTTPS	TCP	128 ビット	入力	HTTPS サーバ ー	不可
8080	HTTP	TCP		入力	HTTP サーバ ー; OMSA VIB をダウンロードし、非 標準 vSphere ホス トを修正	不可
50	RMCP	UDP/TCP	128 ビット	出力	リモートメー ルチェックプ ロトコル	不可
51	IMP	UDP/TCP	該当なし	該当なし	IMP 論理アド レスメンテナ ンス	不可
5353	mDNS	UDP/TCP		すべて	マルチキャス ト DNS	不可
631	IPP	UDP/TCP	なし	出力	インターネッ トプリンティ ングプロトコ ル (IPP)	不可
69	TFTP	UDP	128 ビット	すべて	トリビアルフ ァイル転送	不可
111	NFS	UDP/TCP	128 ビット	入力	SUN リモート プロシージャ コール (ポー トマップ)	不可
68	BOOTP	UDP	なし	出力	ブートストラ ッププロトコ ルクライアント	不可

仮想アプライアンスの正常なインストールと操作のために最低限必要な要件は何ですか?

以下の設定は、最低限のアプライアンス要件の概要です。

- 物理 RAM : 3 GB
- 予約メモリ : 1 GB

 **メモ:** 最適なパフォーマンスを得るため、デルは 3 GB をお勧めします。

- ディスク : 32.5 GB
- CPU : 2つの仮想 CPU

保証を更新するための翻訳はどのようにして見つければいいですか？

保証の更新ボタンをクリックすると、ウェブページには英語、またはサーバーが実際に設置されている地域のローカル言語が表示される場合があります。以下の表は予期される翻訳を示しています。

表 5. 見込まれる翻訳

	クライアントの場所	サービスタグの場所	Dell Management プラグインはクライアントのローカルをサポートしますか？	Dell Management プラグインはクライアントのローカル言語でページを表示できますか？	Dell Management プラグインはデフォルトの英語でページを表示します。
1	場所 A	場所 A	はい	はい	いいえ
2	場所 A	場所 B	いいえ	いいえ	はい
3	場所 A	場所 B	はい	いいえ	はい
4	場所 A	場所 B	はい	いいえ	はい
5	場所 A	場所 A	いいえ	いいえ	はい

以下の例を参照してください。

表 6. 例

	クライアントの場所	サービスタグの場所	Dell Management プラグインはクライアントのローカルをサポートしますか？	Dell Management プラグインはクライアントのローカル言語でページを表示できますか？	Dell Management プラグインはデフォルトの英語でページを表示します。
1	フランス	フランス	はい	はい	いいえ
2	ブラジル	中国	いいえ	いいえ	はい
3	ドイツ	中国	はい	いいえ	はい
4	中国	ブラジル	はい	いいえ	はい
5	インド	インド	いいえ	いいえ	はい

新しい iDRAC バージョンの詳細が、vCenter ホストとクラスタのページに表示されないのはなぜですか？

VMware vSphere クライアントの最近のタスクペインでファームウェアアップデートのタスクが正常に終了した後、ファームウェアアップデートのページを更新して、ファームウェアのバージョンを確認します。そのページに古いバージョンが表示される場合は、Dell Management Center のホスト対応性ページへ移動し、そのホストの CISOR ステータスをチェックします。CISOR が有効化されていない場合は、CISOR を有効化してホストを再起動してください。CISOR がすでに有効化されている場合は、iDRAC コンソールにログインし、iDRAC をリセットして数分待ち、その後 VMware vSphere クライアントのファームウェアアップデートのページを更新します。

OMSA を使用して温度ハードウェア障害をシミュレートすることによってイベント設定をテストする方法は?

イベントが正しく機能していることを確認するには、次の手順を行います。

1. OMSA インタフェースで **Alert Management (アラートと管理)** → **Platform Events (プラットフォームイベント)** と移動します。
2. **Enable Platform Event Filter Alerts (プラットフォームイベントフィルタアラートの有効化)** チェックボックスを選択します。
3. 一番下までスクロールして、**Apply Changes (変更の適用)** をクリックします。
4. 温度警告などの特定のイベントが有効になっていることを確認するには、左にあるツリービューから **Main System Chassis (メインシステムシャーシ)** を選択します。
5. **Main System Chassis (メインシステムシャーシ)** で **Temperatures (温度)** を選択します。
6. **Alert Management (アラート管理)** タブを選択して、**Temperature Probe Warning (温度プローブ警告)** を選択します。
7. **Broadcast a Message (メッセージのブロードキャスト)** チェックボックスを選択して、**Apply Changes (変更の適用)** を選択します。
8. 温度警告イベントを発生させるには、左にあるツリービューから **Main System Chassis (メインシステムシャーシ)** を選択します。
9. **Main System Chassis (メインシステムシャーシ)** で **Temperatures (温度)** を選択します。
10. **System Board Ambient Temp (システム基板環境温度)** リンクを選択して、**Set to Values (値に設定)** オプションボタンを選択します。
11. **Maximum Warning Threshold (最大警告しきい値)** を現在リストされている読み取り値未満に設定します。たとえば、現在の読み取り値が 27 の場合は、しきい値を 25 に設定します。
12. **Apply Changes (変更の適用)** を選択すると、温度警告イベントが生成されます。別のイベントを発生させるには、同じ **Set to Values (値に設定)** オプションを使用して元の設定を復元します。イベントは警告として生成されてから、正常な状態になります。すべてが適切に動作している場合は、**vCenter Tasks & Events (vCenter タスクおよびイベント)** ビューに移動します。温度プローブ警告イベントが表示されています。

 **メモ:** 重複イベントにはフィルタがあり、連続して何度も同じイベントをトリガしても、受け取るイベントは 1 つだけです。すべてのイベントを表示するにはイベント間の間隔を少なくとも 30 秒にします。

Dell ホストシステムに OMSA エージェントをインストールしていますが、OMSA がインストールされていないというエラーメッセージが今でも表示されます。どうしたらよいですか?

この問題を解決するには、次の手順を実行してください。

1. ホストシステムに **OMSA** を **Remote Enablement (リモート有効化)** コンポーネントと共にインストールします。
2. コマンドラインを使用して **OMSA** をインストールする場合は、**-c オプション** を指定してください。**OMSA** がすでにインストールされている場合は、**-c オプション** 付きで再インストールして、サービスを再起動してください。

```
srvadmin-install.sh -c srvadmin-services.sh restart
```

ESXi ホストの場合は、**VMware リモート CLI ツール** を使用して **OMSA VIB** をインストールし、システムを再起動する必要があります。

Dell Management プラグインはロックダウンモードが有効になっている ESX/ESXi をサポートできますか?

はい。ロックダウンモードは ESXi 4.1 以降のホストにおける本リリースでサポートされています。

再起動後、ロックダウンモードのホスト ESXi 4.0 Update2 および ESXi Update 3 でインベントリが失敗します。

ロックダウンモードでは ESXi 4.1 以降が必要です。これより前の ESXi バージョンを使用している場合に、ロックダウンモード中に何らかの理由でホストが再起動すると、再起動後にホストで次の手順を実行しない限り、インベントリが失敗し続けます。

ESXi 4.0 Update2 および Update3 向けの回避手順は、次のとおりです。

1. **vSphere Client (vSphere クライアント)** で **Hosts and Clusters (ホストとクラスター)** を選択し、左のペインで **Host (ホスト)** を選択して **Configuration (設定)** タブをクリックします。
2. 左のペインの **Software (ソフトウェア)** で **Security Profile (セキュリティプロファイル)** をクリックします。
3. **Lockdown Mode (ロックダウンモード)** までスクロールダウンして、**Edit (編集)** をクリックします。
4. **Lockdown Mode (ロックダウンモード)** ダイアログボックスで、ロックダウンモードを無効にするために **Enable (有効化)** チェックボックスをクリアして、**OK** をクリックします。
5. ホストコンソールにログインして、**Restart Management Agents (管理エージェントの再起動)** を選択し、**<ENTER>** を押します。確認のために **<F11>** を押します。
6. ロックダウンモードを有効にするには、1 から 4 までの手順を繰り返しますが、今回は、**Enable (有効化)** チェックボックスを選択して **OK** をクリックします。

ロックダウンモードを使用しようとしたら、失敗しました。

ロックダウンモードで接続プロファイルにホストを追加したとき、インベントリが実行されましたが、「**No Remote Access Controller was found or Inventory is not supported on this host**」(Remote Access Controller が見つからなかったか、インベントリがこのホスト上でサポートされていません) と表示されて失敗しました。インベントリはロックダウンモードのホストに対して動作するのではないのですか?

ホストをロックダウンモードにした場合、またはホストをロックダウンモードから解除した場合、Dell Management プラグインで次の操作を実行する前に 30 分待つ必要があります。

ESXi 4.1 U1 で UserVars.CIMoemProviderEnable にはどのような設定を使用すべきですか?

UserVars.CIMoemProviderEnabled を 1 に設定してください。

ハードウェアプロファイルの作成にリファレンスサーバーを使用していますが、失敗しました。どうしたらよいですか?

最低限の推奨バージョンの iDRAC ファームウェア、Lifecycle Controller ファームウェア、および BIOS がインストールされていることを確認してください。

リファレンスサーバーから取得したデータが現行のものであることを確認するには、**Collect System Inventory On Restart (CSIOR) (再起動時のシステムインベントリの収集 (CSIOR))** を有効にして、データを抽出する前にリファレンスサーバーを再起動してください。「[リファレンスサーバーでの CSIOR の設定](#)」を参照してください。

ブレードサーバーに ESX/ESXi を展開しようとしていますが、失敗しました。どうしたらよいですか?

このエラーを解決するには、次の作業を実行します。

1. **ISO の場所 (NFS パス)** と **ステージングフォルダパス** が正しいことを確認します。
2. サーバー ID の割り当て時に選択された **NIC** が仮想アプライアンスと同じネットワーク上にあることを確認します。
3. **静的 IP アドレス** を使用している場合は、指定したネットワーク情報 (サブネットマスクとデフォルトゲートウェイを含む) が正しいことを確認します。また、その IP アドレスがまだネットワーク上に割り当てられていないことを確認します。
4. 少なくとも 1 つの **仮想ディスク** がシステムによって認識されていることを確認します。ESXi は内部 RIPS SD カードにもインストールされます。

ハイパーバイザー展開が R210 II マシンで失敗するのはなぜですか?

連結された ISO からの BIOS 起動の失敗が原因で、R210 II システムのタイムアウト問題がハイパーバイザー展開失敗エラーを引き起こします。この問題を解決するには、ハイパーバイザーを手動でマシンにインストールしてください。

展開ウィザードにモデル情報のない自動検出されたシステムが表示されるのはなぜですか?

これは通常、システムに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、推奨される最低バージョン要件を満たしていないことを示しています。場合によっては、ファームウェアアップデートがシステム上に登録されていないこともあります。この問題は、システムのコールドブートまたはブレードの再装着によって解決されます。iDRAC 上で新たに有効化されたアカウントは無効にする必要があります、そうすると自動検出が再開され、Dell Management プラグインにモデル情報と NIC 情報を提供します。

ESX/ESXi ISO で NFS 共有がセットアップされていますが、共有の場所をマウントするときのエラーで失敗します。

解決法を見つけるには、次の手順を行います。

1. iDRAC がアプライアンスに対して ping を実行できることを確認します。
2. ネットワークの稼働速度が遅すぎないことを確認します。

仮想アプライアンスを強制削除するにはどのようにしたらよいですか?

1. `https://<vcenter_serverIPAddress>/mob` にアクセスします。
2. **コンテンツ** をクリックします。
3. **ExtensionManager** をクリックします。
4. **UnregisterExtension** をクリックします。
5. 拡張キーを入力して `com.dell.plugin.Dell Management Plug-in` の登録を解除し、**起動メソッド** をクリックします。
6. vSphere クライアントで、Dell Management プラグインの電源をオフにして、削除します。

今すぐバックアップ画面にパスワードを入力するとエラーメッセージが表示されます

解像度の低いモニターを使用すると、**Encryption Password**（暗号化パスワード）フィールドが **BACKUP NOW**（今すぐバックアップ）ウィンドウから見えなくなります。ページを下にスクロールして暗号化パスワードを入力する必要があります。

vSphere で Dell Server Management (Dell サーバー管理) タブまたは Dell Management アイコンをクリックすると 404 エラーが返されます

アプライアンスが稼働しているかどうかをチェックして、稼働していない場合は、vSphere クライアントから起動します。仮想アプライアンス Web サービスが起動するまで数分待ってから、ページを更新します。引き続きエラーが発生する場合は、コマンドラインから IP アドレスまたは完全修飾ドメイン名を使用してアプライアンスに対して ping を実行してください。ping が通らない場合は、ネットワーク設定を見直して、正しく設定されていることを確認してください。

ファームウェアアップデートが失敗しました。どうしたらよいですか？

仮想アプライアンスログをチェックして、タスクがタイムアウトしていないか確認してください。タイムアウトしている場合は、コールドリブートを実行して iDRAC をリセットする必要があります。システムが起動して稼働し始めたら、インベントリを実行するか、Firmware（ファームウェア）タブを使用して、アップデートが正常に完了したかどうかを確認してください。

vCenter アップデートが失敗しました。どうしたらよいですか？

vCenter 登録は通信の問題により失敗することがあるため、このような問題が発生した場合の解決法のひとつとして、静的 IP アドレスを使用することができます。静的 IP アドレスを使用するには、Dell Management プラダインの Console（コンソール）タブで、**Configure Network**（ネットワークの設定）→ **Edit Devices**（デバイスの編集）を選択して、正しい **ゲートウェイ** と **FQDN**（完全修飾ドメイン名）を入力します。Edit DNS Config（DNS Config の編集）で DNS サーバー名を入力します。

 **メモ:** 仮想アプライアンスが入力された DNS サーバーを解決できることを確認してください。

接続プロファイルの資格情報テスト中、パフォーマンスが非常に遅くなったり、応答しなくなります。

サーバー上の iDRAC のユーザーが 1 人だけ（たとえば、*root* のみ）であり、そのユーザーが無効状態であるか、すべてのユーザーが無効状態になっています。無効状態のサーバーへの通信を行うと、遅延が発生します。この問題を解決するには、サーバーの無効状態を解決、またはサーバー上の iDRAC をリセットして root ユーザーをデフォルト設定に再有効化することができます。

無効状態のサーバーを修正するには、次の手順を行います。

1. **Chassis Management Controller** コンソールを開いて、無効になっているサーバーを選択します。
2. iDRAC コンソールを自動的に開くには、**Launch iDRAC GUI**（iDRAC GUI の起動）をクリックします。
3. iDRAC コンソールでユーザーリストまで移動して、次のいずれかを選択します。
 - iDRAC 6 : **iDRAC settings**（iDRAC 設定）→ **Network/Security tab**（ネットワーク / セキュリティタブ）→ **Users tab**（ユーザータブ）を選択します。
 - iDRAC 7 : **User authentication**（ユーザー認証）を選択します。

4. 設定を編集するには、User ID (ユーザー ID) 列で、管理者 (root) ユーザーのリンクをクリックします。
5. **Configure User (ユーザーの設定)** をクリックして、**Next (次へ)** をクリックします。
6. 選択されたユーザーの User Configuration (ユーザー設定) ページで、**Enable user (ユーザーの有効化)** の横にあるチェックボックスを選択して、**Apply (適用)** をクリックします。

Dell Management Plug-in は、VMware vCenter Server Appliance をサポートしますか?

はい、Dell Management Plug-in は VMware vCenter Server Appliance をサポートします。

Dell Management Plug-in は vSphere Web Client をサポートしますか?

いいえ、今のところ Dell Management Plug-in には従来の VMware vSphere クライアントが必要です。

ベアメタル展開の問題

本項では、展開プロセスで見つかった問題の処理について説明します。

自動検出とハンドシェイクの前提条件

- 自動検出とハンドシェイクを実行する前に、iDRAC と Lifecycle Controller ファームウェア、および BIOS が推奨される最低バージョンの要件を満たしていることを確認してください。
- CSIOR は、システムまたは iDRAC で少なくとも 1 度は実行されている必要があります。

ハードウェア設定の失敗

- 展開タスクを開始する前に、システムが CSIOR を完了していて、再起動中ではないことを確認してください。
- リファレンスサーバーが全く同じシステムになるように、BIOS 設定をクローンモードで実行することを強く推奨します。
- 一部のコントローラでは、1 台のドライブでの RAID 0 アレイの作成を許可しません。この機能は高性能のコントローラでのみサポートされており、このようなハードウェアプロファイルの適用は失敗の原因になり得ます。

新たに購入したシステムでの自動検出の有効化

ホストシステムの自動検出機能はデフォルトでは有効になっておらず、購入時に有効化を請求する必要があります。購入時に自動検出の有効化が請求されると、iDRAC 上で DHCP が有効化され、管理者アカウントが無効になります。iDRAC に静的 IP アドレスを設定する必要はなく、これはネットワーク上の DHCP サーバーから取得されます。自動検出機能を利用するには、検出プロセスをサポートするように DHCP サーバーまたは DNS サーバー (または両方) を設定する必要があります。CSIOR は出荷プロセスですでに実行されています。自動検出をサポートするようにネットワークをセットアップするための方法の詳細については、<http://attachments.wetpaintserv.us/xBUlrs4t%2B2TzbrwqYkblvQ%3D%3D2 62254> にある『Lifecycle Controller 自動検出ネットワークセットアップ仕様』を参照してください。

購入時に自動検出を請求しなかった場合は、次の手順で有効にすることができます。

1. 起動プロセス中に **<Ctrl-E>** を押します。
2. iDRAC セットアップウィンドウで、NIC を有効にします (ブレードサーバーのみ)。
3. Auto-Discovery (自動検出) を有効にします。
4. DHCP を有効にします。
5. 管理者アカウントを無効にします。
6. **Get DNS server address from DHCP (DHCP から DNS サーバーアドレスを取得)** を有効にします。

7. **Get DNS domain name from DHCP** (DHCP から DNS ドメイン名を取得) を有効にします。
8. **Provisioning Server** (プロビジョニングサーバー) フィールドに次を入力します。
<Dell Management プラグイン仮想アライアンス IP アドレス>:4433

Contacting Dell

 **メモ:** If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell for sales, technical support, or customer service issues:

1. Visit www.dell.com/support.
2. Select your support category.
3. Verify your country or region in the Choose a Country/Region drop-down menu at the top of page.
4. Select the appropriate service or support link based on your need.

本ソフトウェアのためのその他情報

Dell 仮想化マニュアルの表示とダウンロード: <http://support.dell.com/support/edocs/software/eslvmwre/> で表示およびダウンロードします。 Dell vCenter Plug-In よくあるお問い合わせ: <http://i.dell.com/sites/content/business/solutions/virtualization/en/Documents/dell-management-plugin-vmware-vcenter-faq.pdf>

VMware vCenter 用の Dell Management プラグインの関連情報

- Dell PowerEdge サーバー用 VMware vSphere 4d の表示またはダウンロード
<http://en.community.dell.com/techcenter/virtualization/w/wiki/vmware.aspx>
- PowerEdge™ サーバー用 Dell サーバーマニュアルの表示またはダウンロード
<http://support.dell.com/support/systemsinfo/documentation.aspx?c=us&l=en&s=gen&~subcat=88&~cat=12>
- Dell OpenManage システム管理者マニュアル
<http://support.dell.com/support/systemsinfo/documentation.aspx?c=us&l=en&s=gen&~subcat=108&~cat=6>
- Dell 共通用語集
<http://support.dell.com/support/edocs/SOFTWARE/common/glossary.pdf>
- Dell Lifecycle Controller マニュアル
<http://support.dell.com/support/edocs/software/smusc/smlc/>

仮想化 — 関連イベント

次の表は、イベント名、説明、重要度を含む仮想化関連の重要イベントおよび警告イベントを示しています。

イベント名	説明	重要度	推奨される処置
Dell-Current sensor detected a warning value	指定したシステムの電流センサーが警告しきい値を超えました。	警告	処置は不要
Dell-Current sensor detected a failure value	指定したシステムの電流センサーが障害しきい値を超えました。	エラー	システムをメンテナンスモードにしてください
Dell-Current sensor detected a non-recoverable value	指定したシステムの電流センサーが回復不可能なエラーを検出しました	エラー	処置は不要
Dell-Redundancy regained	センサーが正常値に戻りました	情報	処置は不要
Dell-Redundancy degraded	指定したシステムの冗長性センサーが、冗長性ユニットのいずれかのコンポーネントで障害が発生したが、ユニットは引き続き冗長であることを検出しました。	警告	処置は不要
Dell - Redundancy lost	指定したシステムの冗長性センサーが、冗長性ユニットのコンポーネントのひとつが切断された、故障した、または存在しないことを検出しました。	エラー	システムをメンテナンスモードにしてください
Dell - Power supply returned to normal	センサーが正常値に戻りました	情報	処置は不要
Dell - Power supply detected a warning	指定したシステムの電源装置センサー読み取り値がユーザー定義可能な警告しきい値を超えました。	警告	処置は不要
Dell - Power supply detected a failure	電源装置の接続が切断されているか、故障しました。	エラー	システムをメンテナンスモードにしてください

Dell - Power supply sensor detected a non-recoverable value	指定したシステムの電源装置センサーが回復不可能なエラーを検出しました	エラー	処置は不要
Dell - Memory Device Status warning	メモリデバイスの修正レートが許容値を超えました。	警告	処置は不要
Dell - Memory Device error	メモリデバイスの修正レートが許容値を超えた、メモリスベアバンクがアクティブになった、またはマルチビットの ECC エラーが発生しました。	エラー	システムをメンテナンスモードにしてください
Dell - Fan enclosure inserted into system	センサーが正常値に戻りました	情報	処置は不要
Dell - Fan enclosure removed from system	指定したシステムからファンエンクロージャが取り外されました。	警告	処置は不要
Dell - Fan enclosure removed from system for an extended amount of time	ユーザー定義可能な時間にわたって、指定したシステムからファンエンクロージャが取り外されたままになっています。	エラー	処置は不要
Dell - Fan enclosure sensor detected a non-recoverable value	指定したシステムのファンエンクロージャセンサーが回復不可能なエラーを検出しました	エラー	処置は不要
Dell - AC power has been restored	センサーが正常値に戻りました	情報	処置は不要
Dell - AC power has been lost warning	AC 電源コードが電源を失いましたが、これを警告として分類するだけの十分な冗長性があります。	警告	処置は不要
Dell - An AC power cord has lost its power	AC 電源コードが電源を失っており、冗長性不足のため、これをエラーとして分類する必要があります。	エラー	処置は不要
Dell - Processor sensor returned to a normal value	センサーが正常値に戻りました	情報	処置は不要
Dell - Processor sensor detected a warning value	指定したシステムのプロセッサセンサーがスロットル状態です。	警告	処置は不要
Dell - Processor sensor detected a failure value	指定したシステムのプロセッサセンサーが無効になっている、設定エラー	エラー	処置は不要

	がある、またはサーマルトリップが発生しました。		
Dell - Processor sensor detected a non-recoverable value	指定したシステムのプロセッサセンサーが故障しました。	エラー	処置は不要
Dell - Device configuration error	指定したシステムのプラグ可能デバイスで設定エラーが検出されました。	エラー	処置は不要
Dell - Battery sensor returned to a normal value	センサーが正常値に戻りました	情報	処置は不要
Dell - Battery sensor detected a warning value	指定したシステムのバッテリーセンサーが、バッテリーが予測不具合状態にあることを検出しました。	警告	処置は不要
Dell - Battery sensor detected a failure value	指定したシステムのバッテリーセンサーが、バッテリーの故障を検出しました。	エラー	処置は不要
Dell - Battery sensor detected a nonrecoverable value	指定したシステムのバッテリーセンサーが、バッテリーの故障を検出しました。	エラー	処置は不要
Dell - Thermal shutdown protection has been initiated	このメッセージは、システムがエラーイベントによるサーマルシャットダウンに設定されたときに生成されます。温度センサー読み取り値がシステムで設定されたエラーしきい値を超えると、オペレーティングシステムがシャットダウンし、システムの電源がオフになります。このイベントは、システムからファンエンクロージャが長い時間取り外されている場合にも、特定のシステムで発生することがあります。	エラー	処置は不要
Dell - Temperature sensor returned to a normal value	センサーが正常値に戻りました	情報	処置は不要
Dell - Temperature sensor detected a warning value	指定したシステムのバックプレーン基板、システム基板、CPU、またはドレイブキャリア上の温度センサーが警告しきい値を超えました。	警告	処置は不要

Dell - Temperature sensor detected a failure value	指定したシステムのバックプレーン基板、システム基板、またはドライブキャリア上の温度センサーが障害しきい値を超えました。	エラー	システムをメンテナンスモードにしてください
Dell - Temperature sensor detected a non-recoverable value	指定したシステムのバックプレーンボード、システム基板、またはドライブキャリアの温度センサーが回復不可能なエラーを検出しました。	エラー	処置は不要
Dell - Fan sensor returned to a normal value	センサーが正常値に戻りました	情報	処置は不要
Dell - Fan sensor detected a warning value	ホスト <x> のファンセンサー読み取り値が警告しきい値を超えました。	警告	処置は不要
Dell - Fan sensor detected a failure value	指定したシステムのファンセンサーが1つまたは複数のファンの障害を検出しました。	エラー	システムをメンテナンスモードにしてください
Dell - Fan sensor detected a nonrecoverable value	ファンセンサーが回復不可能なエラーを検出しました。	エラー	処置は不要
Dell - Voltage sensor returned to a normal value	センサーが正常値に戻りました	情報	処置は不要
Dell - Voltage sensor detected a warning value	指定したシステムの電圧センサーが警告しきい値を超えました。	警告	処置は不要
Dell - Voltage sensor detected a failure value	指定したシステムの電圧センサーが障害しきい値を超えました。	エラー	システムをメンテナンスモードにしてください
Dell - Voltage sensor detected a nonrecoverable value	指定したシステムの電圧センサーが回復不可能なエラーを検出しました	エラー	処置は不要
Dell - Current sensor returned to a normal value	センサーが正常値に戻りました	情報	処置は不要
Dell - Storage: storage management error	ストレージ管理がデバイス依存のエラー状態を検出しました。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: Controller warning	物理ディスクの一部が破損しています。	警告	処置は不要
Dell - Storage: Controller failure	物理ディスクの一部が破損しています。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: Channel Failure	チャンネル障害です。	エラー	システムをメンテナンスモードにしてください

Dell - Storage: Enclosure hardware information	エンクロージャハードウェア情報です。	情報	処置は不要
Dell - Storage: Enclosure hardware warning	エンクロージャハードウェア警告です。	警告	処置は不要
Dell - Storage: Enclosure hardware failure	エンクロージャハードウェアエラーです。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: Array disk failure	アレイディスク障害です。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: EMM failure	EMM 障害です。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: power supply failure	電源装置障害です。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: temperature probe warning	物理ディスク温度プローブ警告で、低温すぎるか高温すぎます。	警告	処置は不要
Dell - Storage: temperature probe failure	物理ディスク温度プローブエラーで、低温すぎるか高温すぎます。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: Fan failure	ファン障害です。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: Battery warning	バッテリー警告です。	警告	処置は不要
Dell - Storage: Virtual disk degraded warning	仮想ディスクの劣化警告です。	警告	処置は不要
Dell - Storage: Virtual disk degraded failure	仮想ディスク劣化障害です。	エラー	システムをメンテナンスモードにしてください
Dell - Storage: Temperature probe information	温度プローブ情報です。	情報	処置は不要
Dell - Storage: Array disk warning	アレイディスク警告です。	警告	処置は不要
Dell - Storage: Array disk information	アレイディスク情報です。	情報	処置は不要
Dell - Storage: Power supply warning	電源装置警告です。	警告	処置は不要