# Dell OpenManage Server Administrator バージョン 7.3
# ユーザーズガイド

# 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。**



2013 - 06

Rev. A00

# 目次

1

# はじめに

Dell OpenManage Server Administrator（OMSA）は、包括的で 1 対 1 のシステム管理ソリューションを、統合されたブラウザベースのグラフィカルユーザーインタフェース（GUI）とオペレーティングシステム上のコマンドラインインタフェース（CLI）という 2 つの方法を提供します。Server Administrator では、システム管理者がローカルでも、ネットワーク経由でリモートでもシステムを管理できます。システム管理者に包括的で 1 対 1 のシステム管理を提供することにより、ネットワーク全体の管理に集中できます。Server Administrator のコンテキストでは、システムがスタンドアロンシステム、別のシャーシにネットワークストレージが取り付けられたシステム、またはモジュラーエンクロージャに複数のサーバーモジュールがあるモジュラーシステムを意味します。Server Administrator は次のような情報を提供します。

- 正常に動作しているシステムと問題があるシステム
- リモート回復操作が必要なシステム

Server Administrator は、包括的な一連の統合された管理サービスを通して、使いやすい管理およびローカルとリモートシステムの管理を提供します。Server Administrator は、管理下システム上で唯一のインストールであり、ローカルでもリモートでも、**Server Administrator** ホームページからアクセスできます。リモートにモニタされるシステムは、ダイアルイン、LAN、またはワイヤレス接続でアクセスできます。Server Administrator は、役割ベースのアクセスコントロール（RBAC）認証、SSL 暗号化を使って管理接続のセキュリティを保証します。

## インストール

Server Administrator は、『*Dell Systems Management ツールおよびマニュアル DVD*』を使ってインストールできます。 DVD は、Server Administrator、管理下システムおよび管理ステーションソフトウェアコンポーネントをインストール、アップグレード、およびアンインストールするセットアッププログラムを提供します。さらに、ネットワーク全体で無人インストールを行い、複数のシステムに Server Administrator をインストールできます。Dell OpenManage インストーラは、お使いの管理下システムに Dell OpenManage Server Administrator およびその他の管理下システムソフトウェアコンポーネントをインストール/アンインストールするインストールスクリプトと RPM パッケージを提供します。詳細に関しては、『*Dell OpenManage Server Administrator インストールガイド*』および『*Dell OpenManage 管理ステーションソフトウェアインストールガイド*』（**dell.com/support/manuals**）を参照してください。

**メモ:** 『*Dell Systems Management ツールおよびマニュアル*』DVD からオープンソースパッケージをインストールすると、対応するライセンスファイルがシステムに自動的にコピーされます。これらのパッケージを削除すると、対応するライセンスファイルも削除されます。

**メモ:** モジュラーシステムがある場合、シャーシに取り付けられている各サーバーモジュールに Server Administrator をインストールする必要があります。

## 個々のシステムコンポーネントのアップデート

個々のシステムコンポーネントをアップデートするには、コンポーネント特定の Dell Update Packages を使用します。『*Dell Server Update Utility*』DVD を使って、完全なバージョンレポートを表示し、システム全体をアップデートします。Server Update Utility（SUU）は、必要なアップデートを識別してお使いのシステムに適用します。SUU は、**support.dell.com** からもダウンロードできます。

メモ: Dell システムのアップデート、またはリポジトリに表示されているシステムに使用できるアップデートのリストを表示するために、Server Update Utility（SUU）を入手して使用する方法の詳細は、『*Dell Server Update Utility ユーザーズガイド*』（**dell.com/support/manuals**）を参照してください。

## Storage Management Service

Storage Management Service は、統合されたグラフィック表示でストレージ管理情報を提供します。

メモ: ストレージ管理サービスの詳細については、support.dell.com/manuals の『*Dell OpenManage Server Administrator Storage Management ユーザーズガイド*』（**dell.com/support/manuals**）を参照してください。

## 計装サービス

計装サービス は、業界標準システム管理エージェントによって収集された故障と性能についての詳細情報への迅速なアクセスを提供して、シャットダウン、起動、およびセキュリティなど監視下システムのリモート管理を実現します。

## Remote Access Controller

Remote Access Controller は、Dell Remote Access Controller（DRAC）またはベースボード管理コントローラ（BMC）/Integrated Dell Remote Access Controller（iDRAC）ソリューションを装備したシステム向けの完全なリモートシステム管理ソリューションを提供します。Remote Access Controller は、動作不能のシステムへのリモートアクセスを行い、迅速なシステムの立ち上げを実現します。また、システムがダウンした際には、アラートで通知し、システムをリモートで再起動できるようにします。さらに、Remote Access Controller はシステムクラッシュの原因をログに記録し、一番最後のクラッシュ画面を保存します。

## ログ

Server Administrator は、システムに対してまたはシステムによって発行されたコマンド、モニタされたハードウェアイベント、およびシステムアラートのログを表示します。ログは、ホームページで表示したり、レポートとして印刷または保存したり、指定したサービス連絡先に電子メールで送信したりすることができます。

# 本リリースの新機能

- 次のオペレーティングシステムへの対応が追加されました。
  - Red Hat Enterprise Linux 5.9（32 ビットおよび 64 ビット）
  - Red Hat Enterprise Linux 6.4（64 ビット）
  - Microsoft Windows Server 2012 Essentials
  - VMware vSphere 5.1 U1
  - VMware vSphere 5.0 U2
  - Citrix XenServer 6.2
- 次のアイテムのためのセキュリティ修正および拡張が行われました。
  - CVE-2012-6272、CSRF、XSS、および汎用パス操作を修正
  - JRE バージョン 1.7 アップデート 21 にアップグレード
  - Apache Tomcat バージョン 7.0.39 にアップグレード
- Google Chrome 21 および 22 に対する追加サポート
- Apple Mac OS X での Safari 5.1.7 に対する追加サポート

- 次のネットワークインタフェースカード（NIC）に対するサポートが追加されました。
  - Broadcom 57840S クアッドポート 10G SFP+ ラック NDC
  - Broadcom 57840S-k クアッドポート 10GbE ブレード KR NDC
- 240 ボルト DC 電源装置のサポート
- iDRAC7 固有のバージョンがある第 12 世代システムでプラットフォームイベント宛先を IPv4、IPv6、または FQDN として設定する機能
- ストレージ管理における以下の諸機能のサポートが追加されました。
  - ESXi 5.1 U1 のための PCIe SSD サポート。
  - PERC 8 に接続された SAS および SATA SSD の定格書き込みの残り寿命状態。
  - Dell PowerEdge R720、R820、R620、および T620 上の PERC H810, H710 アダプタ、H710P、および H710 Mini のための、Red Hat Enterprise Linux 6.4 および Novell SUSE Linux Enterprise Server 11 SP2 におけるダイレクトアタッチトストレージ（DAS）用 Fluid Cache のサポート。

  **メモ:** 詳細については、デルサポートサイト **sdell.com/openmanagemanuals** にある『Dell OpenManage Server Administrator Storage Management ユーザーズガイド』を参照してください。
- 次のオペレーティングシステムに対するサポートが廃止されました。
  - Red Hat Enterprise Linux 6.3
  - Red Hat Enterprise Linux 5.8

**メモ:** 対応オペレーティングシステムおよび Dell サーバーのリストについては、**dell.com/openmanagemanuals** で必要なバージョンの OpenManage ソフトウェアの『Dell Systems Software サポートマトリックス』を参照してください。

**メモ:** このリリースで新たに加わった機能に関する情報については、Server Administrator で状況に応じたオンラインヘルプを参照してください。

# 利用可能なシステム管理標準

Dell OpenManage Server Administrator では、次の主要なシステム管理プロトコルがサポートされています。

- HTTPS
- 共通情報モデル（CIM）
- 簡易ネットワーク管理プロトコル（SNMP）

ご利用のシステムが SNMP をサポートしている場合、サービスをインストールし、オペレーティングシステムで有効にする必要があります。ご利用のオペレーティングシステムで SNMP サービスが利用できる場合は、Server Administrator のインストールプログラムは、SNMP のサポートエージェントをインストールします。

HTTPS は、すべてのオペレーティングシステムでサポートされています。CIM および SNMP のサポートは、オペレーティングシステムに依存します。また、オペレーティングシステムのバージョンに依存する場合もあります。

**メモ:** SNMP のセキュリティ上の懸念については、Dell OpenManage Server Administrator の readme ファイル（Server Administrator アプリケーションに同梱）または、**dell.com/support/manuals** を参照してください。Dell の SNMP サブエージェントの安全性を確保するには、オペレーティングシステムのマスター SNMP エージェントからアップデートを適用する必要があります。

## 利用可能な対応オペレーティングシステム

対応 Microsoft Windows オペレーティングシステムでは、Server Administrator は、CIM/Windows Management Instrumentation（WMI）と SNMP の 2 つのシステム管理標準をサポートしています。対応 Red Hat Enterprise

Linux および SUSE Linux Enterprise Server オペレーティングシステムでは、Server Administrator は SNMP システム管理標準をサポートしています。

Server Administrator は、これらのシステム管理標準にかなりのセキュリティ機能を追加しました。すべての属性設定操作（資産タグの値を変更するなど）は、必要な権限を使ってログインしている間に Dell OpenManage IT Assistant で実行する必要があります。

次の表は、各対応オペレーティングシステムに対して使用可能なシステム管理標準について示しています。

**表 1. 利用可能なシステム管理標準**

| オペレーティングシステム | snmp | CIM |
|---|---|---|
| Windows Server 2008 シリーズおよび Windows Server 2003 シリーズ | オペレーティングシステムのインストールメディアから使用可能 | 常にインストール |
| Red Hat Enterprise Linux | オペレーティングシステムのインストールメディアの net-snmp パッケージから使用可能 | 使用不可 |
| SUSE Linux Enterprise Server | オペレーティングシステムのインストールメディアの net-snmp パッケージから使用可能 | 使用不可 |
| VMware ESX | オペレーティングシステムによってインストールされる net-snmp パッケージから使用可能 | 使用可能 |
| VMware ESXi | SNMP トラップのサポート<br>**メモ:** ESXi は SNMP トラップをサポートしていますが、SNMP を介したハードウェアのインベントリをサポートしていません。 | 使用可能 |
| Citrix XenServer 6.0 | オペレーティングシステムのインストールメディアの net-snmp パッケージから使用可能 | 使用不可 |

# Server Administrator（サーバー管理者）ホームページ

**Server Administrator** ホームページは、設定および使用しやすいウェブブラウザベースのシステム管理タスクを、管理下システムまたは LAN、ダイヤルアップサービス、またはワイヤレスネットワーク経由のリモートホストから提供します。Dell Systems Management Server Administrator 接続サービス（DSM SA 接続サービス）は、管理下システムにインストールおよび設定されるため、サポートされたウェブブラウザおよび接続を持つどのシステムからもリモート管理機能を実行できます。さらに、Server Administrator ホームページには包括的かつ状況に応じたオンラインヘルプが組み込まれています。

# その他の必要マニュアル

このガイド以外にも、デルサポートサイト **dell.com/support/manuals** から次のガイドを入手できます。

- 『*Dell システムソフトウェアサポートマトリックス*』は、各種 Dell システム、これらのシステムでサポートされているオペレーティングシステム、これらのシステムにインストールできる Dell OpenManage コンポーネントについての情報を提供します。
- 『*Dell OpenManage Server Administrator インストールガイド*』では、Dell OpenManage Server Administrator のインストール手順が説明されています。
- 『*Dell OpenManage 管理ステーションソフトウェアインストールガイド*』では、Dell OpenManage 管理ステーションソフトウェアのインストール手順が説明されています。
- 『*Dell OpenManage Server Administrator SNMP リファレンスガイド*』には、シンプルネットワーク管理プロトコル（SNMP）管理情報ベース（MIB）について記載されています。

- 『*Dell OpenManage Server Administrator CIM リファレンスガイド*』では、標準の管理オブジェクトフォーマット（MOF）ファイルの拡張である、共通情報モデル（CIM）プロバイダについて説明しています。
- 『*Dell OpenManage Server Administrator メッセージリファレンスガイド*』には、Server Administrator ホームページのアラートログまたはオペレーティングシステムのイベントビューアに表示されるメッセージ一覧が掲載されています。
- 『*Dell OpenManage Server Administrator コマンドラインインターフェースガイド*』には、Server Administrator のコマンドラインインターフェースがすべて記載されています。
- 『Dell Remote Access Controller 5 ユーザーズガイド』は、DRAC 5 を設定するための RACADM コマンドラインユーティリティの使用についての包括的な情報を提供しています。
- 『Dell Chassis Management Controller ユーザーズガイド』は、お使いの Dell システムを含むシャーシの全モジュールを管理するコントローラの使用についての、包括的な情報を提供しています。
- 『iDRAC6 および CMC 用コマンドラインリファレンスガイド』は、iDRAC6 および CMC 向けの RACADM サブコマンド、対応インタフェース、プロパティデータベースグループ、およびオブジェクト定義についての情報を提供しています。
- 『Integrated Dell Remote Access Controller 7（iDRAC7）ユーザーズガイド』は、ネットワークを介してお使いのシステムとその共有リソースをリモートで管理および監視するため、第 12 世代ラック、タワー、およびブレードサーバー用に iDRAC7 を設定および使用することについての情報を提供しています。
- 『ブレードサーバー用 Integrated Dell Remote Access Controller 6（iDRAC6）Enterprise ユーザーガイド』は、ネットワークを介してお使いのシステムとその共有リソースをリモートで管理および監視するため、第 11 世代ブレードサーバー用に iDRAC6 を設定および使用することについての情報を提供しています。
- 『Integrated Dell Remote Access Controller 6（iDRAC6）ユーザーガイド』は、ネットワークを介してお使いのシステムとその共有リソースをリモートで管理および監視するため、第 11 世代タワーおよびラックサーバー用に iDRAC6 を設定および使用することについての完全な情報を提供しています。
- 『*Dell Online Diagnostics ユーザーズガイド*』では、システムでのオンライン診断のインストールおよび使用に関する情報を完全に網羅しています。
- 『*Dell OpenManage Baseboard Management Controller ユーティリティ ユーザーズガイド*』は Server Administrator を使ったシステムの BMC 設定および管理についての追加情報を提供します。
- 『*Dell OpenManage Server Administrator Storage Management ユーザーズガイド*』は、システムに接続されているローカルおよびリモートのストレージを設定、管理するための包括的なリファレンスガイドです。
- 『*Dell Remote Access Controller Racadm ユーザーズガイド*』では、racadm コマンドラインユーティリティの使い方についての情報を提供します。
- 『*Dell Remote Access Controller 5 ユーザーズガイド*』では、DRAC 5 コントローラのインストールと設定方法、および DRAC 5 を使用した作動不能システムへのリモートでのアクセス方法について詳しく説明しています。
- 『*Dell Update Packages ユーザーズガイド*』は、システムアップデート対策の一環としての Dell Update Packages の入手方法と使い方を説明しています。
- 『*Dell OpenManage Server Update Utility ユーザーズガイド*』では、Dell システムをアップデートしたり、リポジトリに登録されているシステムに適用可能なアップデートを表示できる、サーバーアップデートユーティリティ（SUU）の入手方法と使用法に関する情報が記載されています。
- 『*Dell Management Console ユーザーズガイド*』は、Dell 管理コンソールのインストール、設定、使用について説明しています。
- 『*Dell Lifecycle Controller ユーザーズガイド*』は、システムのライフサイクルに渡って、システムおよびストレージ管理タスクを行うための、Unified Server Configurator の設定および使用に関する情報を提供しています。
- 『Dell License Manager ユーザーズガイド』は Dell 第 12 世代サーバーのコンポーネントサーバーライセンスの管理に関する情報を提供しています。
- 『*用語集*』では、本書で使用される用語について説明されています。

## デルサポートサイトからの文書へのアクセス

デルサポートサイトから文書にアクセスするには、次の手順を実行します。

1. **dell.com/support/manuals** にアクセスします。
2. **サービスタグまたはエクスプレスサービスコードをお持ちですか?** セクションの **いいえ** で **すべてのデル製品のリストから選択する** を選択し、**続行** をクリックします。

3. **お使いの製品タイプを選択してください** セクションで、**ソフトウェアとセキュリティ** をクリックします。
4. **お使いのデル製システムを選択してください - Software** セクションで、次の中から必要なリンクをクリックします。
   - **クライアントシステム管理**
   - **エンタープライズシステム管理**
   - **リモートエンタープライズシステム管理**
   - **Serviceability Tools**
5. マニュアルを表示するには、必要な製品バージョンをクリックします。

**メモ:** または、次のリンクを使用してマニュアルに直接アクセスすることもできます。

- エンタープライズシステム管理マニュアル — **dell.com/openmanagemanuals**
- リモートエンタープライズシステム管理マニュアル — **dell.com/esmmanuals**
- Serviceability Tools マニュアル — **dell.com/serviceabilitytools**
- クライアントシステム管理マニュアル — **dell.com/OMConnectionsClient**
- OpenManage Connections エンタープライズシステム管理マニュアル — **dell.com/OMConnectionsEnterpriseSystemsManagement**
- OpenManage Connections クライアントシステム管理マニュアル — **dell.com/OMConnectionsClient**

# テクニカルサポートの利用法

ガイドに説明されている手順を理解できない、あるいは製品が予想通り動作しない場合は、ヘルプツールをご利用ください。これらのヘルプツールに関しては、お使いのシステムの『*ハードウェアオーナーズマニュアル*』の「**ヘルプが必要な場合**」を参照してください。

さらに、Dell Enterprise Training および Certification もご利用いただけます。詳細に関しては **dell.com/training** を参照してください。このサービスをご利用いただけない地域もあります。

# デルへのお問い合わせ

**メモ:** デルでは、オンラインおよび電話ベースのサポートとサービスオプションをいくつかご用意しています。アクティブなインターネット接続がない場合は、 ご購入時の納品書、出荷伝票、請求書、またはデル製品カタログで連絡先をご確認いただけます。これらのサービスは国および製品によって異なり、お住まいの地域では一部のサービスがご利用いただけない場合があります。

デルのセールス、テクニカルサポート、またはカスタマーサービスへは、次の手順でお問い合わせいただけます。

1. **dell.com/contactdell** にアクセスします。
2. インタラクティブな世界地図からお住まいの国または地域を選択します。
   地域を選択すると、選択した地域内の国が表示されます。
3. 選択した国の下にある適切な言語を選択します。
4. 管轄の営業セグメントを選択します。
   選択したセグメントのメインサポートページが表示されます。
5. 必要に応じて、適切なオプションを選択します。

**メモ:** Dell システムをご購入いただいた場合は、サービスタグを要求される場合があります。

2

# 設定と管理

Dell OpenManage Server Administrator は、ウェブをベースとするインタフェースとコマンドラインインタフェースの両方に対し、役割をベースとしたアクセス制御（RBAC）、認証、および暗号化を使ってセキュリティを提供します。

## 役割ベースのアクセスコントロール

RBAC は特定の役割内のユーザーが実行できる操作を決定して、セキュリティを管理します。各ユーザーには 1 つ、または複数の役割が割り当てられており、各役割にはその役割内のユーザーが使用できるユーザー権限が 1 つまたは複数割り当てられています。RBAC によってセキュリティ管理は組織の構造に密接に対応しています。

### ユーザー特権

Server Administrator は割り当てられたユーザーのグループ権限に応じて、異なるアクセス権を与えます。ユーザー権限には、ユーザー、パワーユーザー、管理者、昇格管理者の 4 つのレベルがあります。

**表 2. ユーザー特権**

| ユーザー権限のレベル | アクセスタイプ | | 説明 |
|---|---|---|---|
| | 表示 | 管理 | |
| ユーザー | はい | 不可 | *ユーザー*はほとんどの情報を表示できます。 |
| パワーユーザー | はい | はい | *パワーユーザー*は、警告しきい値の設定、警告またはエラーイベントが発生した場合のアラート処置を設定できます。 |
| システム管理者 | はい | はい | *管理者*は、シャットダウン処理の設定と実行、システムでオペレーティングシステムが応答しない場合の自動回復処置の設定、ハードウェアログ、イベントログ、およびコマンドログのクリアなどを行います。管理者はまた、電子メールを送信するシステムも設定可能です。 |
| 昇格理者（Linux のみ） | はい | はい | *昇格管理者*は情報を表示および管理できます。 |

#### *Server Administrator サービスにアクセスするための権限レベル*

次の表は、Server Administrator サービスへのアクセスと管理ができるユーザーをまとめたものです。

Server Administrator では、ユーザー権限でログインしたユーザーには読み取り専用のアクセス権、パワーユーザー権限でログインしたユーザーには読み取りと書き込みのアクセス権、*管理者* または *昇格管理者* 権限でログインしたユーザーには読み取り、書き込み、管理のアクセス権が与えられます。

**表 3. Server Administrator サービスの管理に必要な権限**

| サービス | 必要なユーザー権限レベル | |
|---|---|---|
| | 表示 | 管理 |

| | | |
|---|---|---|
| 計装 | ユーザー、パワーユーザー、管理者、昇格管理者 | パワーユーザー、管理者、昇格管理者 |
| リモートアクセス | ユーザー、パワーユーザー、管理者、昇格管理者 | 管理者、昇格管理者 |
| ストレージ管理 | ユーザー、パワーユーザー、管理者、昇格管理者 | 管理者、昇格管理者 |

# 認証

Server Administrator 認証スキームを使用すると、正しいアクセスタイプが正しいユーザー権限に割り当てられます。さらに、コマンドラインインタフェース（CLI）が起動すると、Server Administrator 認証スキームが現在のプロセスが実行されているコンテキストを検証します。この認証スキームを使うことにより、Server Administrator ホームページと CLI のいずれからアクセスした場合でもすべての Server Administrator 機能が正しく認証されます。

## Microsoft Windows 認証

対応 Microsoft Windows オペレーティングシステムの場合、Server Administrator の認証に、統合 Windows 認証（旧称 NTLM）が使用されます。この認証システムは、Server Administrator のセキュリティをネットワークの全体的なセキュリティスキームに組み込むことができます。

## Red Hat Enterprise Linux および SUSE Linux Enterprise Server 認証

対応 Red Hat Enterprise Linux および SUSE Linux Enterprise Server オペレーティングシステムでは、Server Administrator がプラグ認証可能モジュール（PAM）ライブラリに基づいてさまざまな認証方法を使用します。ユーザーは、異なるアカウント管理プロトコル（LDAP、NIS、Kerberos、および Winbind）を使って、ローカルまたはリモートに Server Administrator にログインできます。

## VMware ESX Server 4.X 認証

ESX Server は、ユーザーが ESX Server ホストにアクセスする際、認証に PAM（Pluggable Authentication Modules）の仕組みを使用します。VMware の PAM は、**/etc/pam.d/vmware-authd** にある認証モジュールにパスを保管します。

ESX Server のデフォルトインストールでは、Linux と同様に、**/etc/passwd** 認証を用いますが、他の認証メカニズムを使用するように ESX Server を設定することも可能です。

**メモ:** VMware ESX Server 4.x オペレーティングシステムが稼動しているシステム上で Server Administrator にログインするには、どのユーザーも管理者権限が必要です。役割の割り当てについては、VMware のマニュアルを参照してください。

## VMware ESXi Server 5.X 認証

ESXi Server は、vSphere/VI Client またはソフトウェア開発キット（SDK）を使って ESXi ホストにアクセスするユーザーを認証します。ESXi のデフォルト認証には、ローカルパスワードデータベースが使用されます。Server Administrator の ESXi 認証トランザクションも、**vmware-hostd** プロセスとの直接インタラクションです。お使いのサイトで認証が効率的に機能するよう、ユーザー、グループ、許可、および役割の設定、ユーザー属性の設定、自分の証明書の追加、および SSL を使用するかどうかの決定などの基本タスクを実行します。

**メモ:** VMware ESXi Server 5.0 オペレーティングシステムを実行中のシステムでは、Server Administrator にログインする際、ユーザー全員に管理者権限が必要です。役割の割り当てについては、VMware マニュアルを参照してください。

# 暗号化

管理下システムを識別し保護するため、Server Administrator には SSL（Secure Socket Layer）技術を使用したセキュア HTTPS 接続を使ってアクセスします。対応の Microsoft Windows、Red Hat Enterprise Linux、および SUSE Linux Enterprise Server オペレーティングシステムでは、ユーザーが **Server Administrator** ホームページにアクセスしたときに、ソケット接続を介して転送されるユーザー資格情報やその他の機密データを、JSSE（Java Secure Socket Extension）を使用して保護します。

# ユーザー特権の割り当て

重要なシステムコンポーネントを確実にセキュリティ保護するため、Dell OpenManage ソフトウェアをインストールする前に、すべての Dell OpenManage ユーザーにユーザー権限を割り当てます。新しいユーザーは、オペレーティングシステムのユーザー権限を使って Dell OpenManage ソフトウェアにログインできます。

**注意: 重要なシステムコンポーネントに対するアクセスを保護するため、Dell OpenManage ソフトウェアにアクセスできる各ユーザーアカウントに対してパスワードを割り当てます。パスワードが割り当てられていないユーザーは、オペレーティングシステムの設計により、Windows Server 2003 を実行中の Dell OpenManage ソフトウェアにはログインできません。**

**注意: サポートされている Windows オペレーティングシステムに対するゲストアカウントを無効にして、重要なシステムコンポーネントへのアクセスを保護します。リモートスクリプトがデフォルトのゲストアカウント名を使ってアカウントを有効にできないよう、ゲストアカウントの名前を変更することを検討してください。**

**メモ:** 各対応オペレーティングシステムで、ユーザーの作成とユーザー特権の割り当てる手順は、オペレーティングシステムのマニュアルを参照してください。

**メモ:** OpenManage ソフトウェアにユーザーを追加するには、オペレーティングシステムにユーザーを追加してください。OpenManage ソフトウェア内から新規ユーザーを作成する必要はありません。

## Windows オペレーティングシステム上でのドメインへのユーザーの追加

**メモ:** 以下の手順を実行するには、Microsoft Active Directory がシステムにインストールされている必要があります。Active Directory の使用の詳細については、「Active Directory ログインの使用方法」を参照してください。

1. **コントロールパネル** → **管理ツール** → **Active Directory ユーザーとコンピュータ** の順に移動します。
2. コンソールツリーで、**ユーザー** を右クリックするか新規ユーザーを追加するコンテナを右クリックして、**新規作成** → **ユーザー** の順に選択します。
3. ダイアログボックスに適切なユーザー名情報を入力し、**次へ** をクリックします。
4. **次へ** をクリックしてから **終了** をクリックします。
5. 作成したユーザーを表すアイコンをダブルクリックします。
6. **所属するグループ** タブをクリックします。
7. **追加** をクリックします。
8. 該当するグループを選択し、**追加** をクリックします。
9. **OK** をクリックしてから、**OK** を再度クリックします。

   新しいユーザーは、割り当てられたグループとドメインへのユーザー権限で Dell OpenManage ソフトウェアにログインできます。

## 対応の Red Hat Enterprise Linux および SUSE Linux Enterprise Server オペレーティングシステムでの Server Aministrator ユーザーの作成

システム管理者のアクセス権限は、ルートでログインしているユーザーに割り当てられます。ユーザー権限とパワーユーザー権限を持つユーザーを作成するには、以下の手順に従います。

**メモ:** これらの手順を実行するには、ルート ユーザーまたはそれと同等の権限を有するユーザーとしてログインする必要があります。

**メモ:** これらの手順を実行するには、システムに **useradd** ユーティリティがインストールされている必要があります。

### ユーザーの作成

**メモ:** ユーザーとユーザーグループの作成の詳細については、オペレーティングシステムのマニュアルを参照してください。

### ユーザー特権を持つユーザーの作成

1. コマンドラインから次のコマンドを実行します: `useradd -d <home-directory> -g <group> <username>`（`<group>` はルートでない）

   **メモ:** `<group>` が存在しない場合は、**groupadd** コマンドを使ってグループを作成してください。
2. `passwd<username>`を入力し、<Enter> を押します。
3. プロンプトが表示されたら、新しいユーザーのパスワードを入力します。

   **メモ:** 重要なシステムコンポーネントのアクセスを保護するには、Server Administrator にアクセスできる各ユーザーアカウントにパスワードを割り当てます。

   新しいユーザーはユーザーというグループ特権を使って Server Administrator にログインできます。

### パワーユーザー特権を持つユーザーの作成

1. コマンドラインから次のコマンドを実行します: `useradd -d <home-directory> -g <group> <username>`

   **メモ:** ルートをプライマリグループとして設定します。
2. `passwd<username>`を入力し、<Enter> を押します。
3. プロンプトが表示されたら、新しいユーザーのパスワードを入力します。

   **メモ:** 重要なシステムコンポーネントのアクセスを保護するには、Server Administrator にアクセスできる各ユーザーアカウントにパスワードを割り当てます。

   新しいユーザーはユーザーというグループ特権を使って Server Administrator にログインできます。

### Linux オペレーティングシステムでの Server Administrator ユーザー権限の編集

**メモ:** これらの手順を実行するには、ルート ユーザーまたはそれと同等の権限を有するユーザーとしてログインする必要があります。

1. **/opt/dell/srvadmin/etc/omarolemap** にある **omarolemap** ファイルを開きます。
2. 以下をファイルに追加します。 `<User_Name>[Tab]<Host_Name>[Tab]<Rights>`

   次の表は、`omarolemap` ファイルへの役割定義の追加に使用する凡例を示しています。

表 4. OpenManage Server Administrator に役割の定義を追加する凡例

| <User_Name> | <Host_Name> | <Rights> |
|---|---|---|
| ユーザー名 | ホスト名 | システム管理者 |
| （+）グループ名 | ドメイン | ユーザー |
| ワイルドカード（*） | ワイルドカード（*） | ユーザー |
| [Tab] = \t （tab 文字） | | |

次の表は、omarolemap ファイルへの役割定義の追加例を示しています。

表 5. OpenManage Server Administrator に役割の定義を追加する例

| <User_Name> | <Host_Name> | <Rights> |
|---|---|---|
| Bob | Ahost | パワーユーザー |
| + ルート | Bhost | システム管理者 |
| + ルート | Chost | システム管理者 |
| Bob | *.aus.amer.com | パワーユーザー |
| Mike | 192.168.2.3 | パワーユーザー |

3. ファイルを保存して閉じます。

### *omarolemap ファイル使用に際するベストプラクティス*

omarolemap ファイルの使用時に考慮すべきベストプラクティスを、次に示します。

- **omarolemap** ファイルの次のデフォルトエントリは削除しないでください。

  root * Administrator

  +root * Poweruser

  * * User

- **omarolemap** ファイルの許可とファイル形式は変更しないでください。
- localhost や 127.0.0.1 といった、*<ホスト名>* のループバックアドレスは使用しないでください。
- 接続サービスを再起動したときに **omarolemap** ファイルの変更が反映されない場合は、コマンドログでエラーを調べてください。
- **omarolemap** ファイルを別のコンピュータに移動したとき、ファイル許可とファイルのエントリを再確認する必要があります。
- *グループ名* に + を前付けします。
- 次の場合、Server Administrator はデフォルトのオペレーティングシステムのユーザー権限を使用します。
  - ユーザーの権限が **omarolemap** ファイルで降格された。
  - 同じ*<ホスト名>*に重複したユーザー名またはユーザーグループのエントリがある。
- [タブ] の代わりに スペース を列の区切り文字として使うこともできます。

## VMware ESX 4.X、ESXi 4.X、および ESXi 5.X 用の Server Administrator ユーザーの作成

ユーザーテーブルにユーザーを追加するには次の手順を行います。

1. vSphere クライアントを使用してホストにログインします。
2. **ユーザーとグループ** タブをクリックし、**ユーザー** をクリックします。
3. ユーザー テーブルを右クリックし、**追加** をクリックして、**新規ユーザーの追加** ダイアログボックスを開きます。

4. ログイン、ユーザー名、数字から成るユーザー ID（UID）、パスワードを入力します。ユーザー名と UID の指定はオプションです。UID を指定しない場合、vSphere クライアントが利用可能な UID を割り当てます。
5. コマンドシェルを通じてユーザーが ESX/ESXi ホストにアクセスできるようにするには、**このユーザーにシェルアクセスを許可する** を選択します。vSphere クライアントからのみホストにアクセスするユーザーは、シェルアクセスを必要としません。
6. ユーザーをグループに追加するには、**グループ** ドロップダウンメニューからグループ名を選択し、**追加** をクリックします。
7. **OK** をクリックします。

## 対応 Windows オペレーティングシステム上でのゲストアカウントと匿名アカウントの無効化

**メモ:** この手順を実行するには、システム管理者権限でログインしている必要があります。

1. **コンピュータの管理** ウィンドウを開きます。
2. コンソールツリーで、**ローカルユーザーとグループ** を展開し、**ユーザー** をクリックします。
3. これらのユーザーのプロパティを表示するには、**ゲスト** または **IUSR_system** 名ユーザーアカウントをダブルクリック、または **ゲスト** または **IUSR_***システム名*ユーザーアカウントを右クリックし、**プロパティ** を選択します。
4. **アカウントが無効** を選択し、**OK** をクリックします。

アカウントが無効であることを示す、X の付いた赤い丸がユーザー名の上に表示されます。

## SNMP エージェントの設定

Server Administrator は、簡易ネットワーク管理プロトコル（SNMP—すべての対応オペレーティングシステムにおけるシステム管理標準）をサポートします。SNMP サポートは、お使いのオペレーティングシステムおよびインストール方法によってインストールされている場合とそうでない場合があります。ほとんどの場合、SNMP はオペレーティングシステムのインストールの一貫としてインストールされています。Server Administrator をインストールする前に、SNMP などのインストールされた対応システム管理プロトコルが必要です。

SNMP エージェントを設定して、コミュニティ名を変更し、設定操作を可能にし、管理ステーションにトラップを送信できます。SNMP エージェントが Dell OpenManage IT Assistant などの管理アプリケーションと正しくインタラクションを取れるように設定するには、次のセクションに説明されている手順を実行します。

**メモ:** デフォルトの SNMP エージェント設定には通常、パブリックのような SNMP コミュニティ名が含まれます。セキュリティ上の理由から、デフォルト SNMP コミュニティ名を変更する必要があります。残りの SNMP コミュニティ名に関する詳細については、「SNMP コミュニティ名の変更」を参照してください。

**メモ:** SNMP 設定操作は、デフォルトで Server Administrator バージョン 5.2 以降で無効にされます。プリファレンスまたは Server Administrator コマンドラインインタフェース（CLI）の下にある Server Administrator SNMP 設定ページを使って SNMP 設定操作を有効または無効にできます。Server Administrator CLI の詳細に関しては、『*Dell OpenManage Server Administrator コマンドラインインターフェースユーザーズガイド*』（**dell.com/support/manuals**）を参照してください。

**メモ:** IT Assistant が Server Administrator を実行しているシステムからの管理情報を取得するには、IT Assistant が使用するコミュニティ名が Server Administrator を実行しているシステムのコミュニティ名と一致する必要があります。IT Assistant が Server Administrator を実行中のシステムで情報を変更するか、またはアクションを実行するには、IT Assistant で使用しているコミュニティ名が Server Administrator を実行中のシステムで設定操作を許可するコミュニティ名と一致する必要があります。IT Assistant が Server Administrator を実行中のシステムからトラップ（非同期イベント通知）を受け取るには、Server Administrator を実行中のシステムが、IT Assistant を実行中のシステムにトラップを送信するよう設定する必要があります。

以下の手順は、対応している各オペレーティングシステムで SNMP エージェントを設定する方法を説明しています。

- Microsoft Windows オペレーティングシステム環境のシステムでの SNMP エージェントの設定
- 対応 Red Hat Enterprise Linux 環境のシステムでの SNMP エージェントの設定
- 対応 SUSE Linux Enterprise Server が実行されるシステムでの SNMP エージェントの設定
- VMware MIB をプロキシするために対応 VMware ESX 4.0 オペレーティングシステムが稼動するシステムにおいて SNMP エージェントを設定する
- 対応 VMware ESXi 4.X および ESXi 5.X オペレーティングシステムが実行されるシステムにおける SNMP エージェントの設定

## 対応 Windows オペレーティングシステムが稼動するシステムでの SNMP エージェントの設定

Server Administrator は、Windows SNMP エージェントが提供する SNMP サービスを使用します。SNMP エージェントを設定すると、コミュニティ名を変更したり、Set 操作を有効にしたり、管理ステーションにトラップを送信することができます。IT Assistant などの管理アプリケーションと正しく連携するように SNMP エージェントを設定するには、次項で説明する手順に従ってください。

**メモ:** SNMP 設定の詳細については、ご利用のオペレーティングシステムのマニュアルを参照してください。

### リモートホストで SNMP アクセスを有効にするには（Windows Server 2003 のみ）

Windows Server 2003 はデフォルトでは、リモートホストから SNMP パケットを受け入れません。リモートホストから SNMP 管理アプリケーションを使ってシステムを管理する場合、2003 を実行中のシステムでは、SNMP サービスが SNMP パケットを受け入れるよう設定する必要があります。

Windows Server 2003 オペレーティングシステムが稼動するシステムでリモートホストから SNMP パケットを受信できるようにするには、次の手順を実行します。

1. **コンピュータの管理** ウィンドウを開きます。
2. 必要に応じて、同ウィンドウの **コンピュータの管理** アイコンを展開します。
3. **サービスとアプリケーション** アイコンを展開して、**サービス** をクリックします。
4. リストを下にスクロールして **SNMP サービス** を見つけ、**SNMP サービス** を右クリックして、**プロパティ** をクリックします。

   **SNMP サービスプロパティ** ウィンドウが表示されます。
5. **セキュリティ** タブをクリックします。
6. **任意のホストから SNMP パケットを受け入れる** を選択するか、**リモートホストを これらのホストの SNMP パケットを受け入れる** リストに追加します。

### SNMP コミュニティ名の変更

SNMP コミュニティ名を設定することで、どのシステムが SNMP を使用してシステムを管理できるかが決まります。管理アプリケーションが Server Administrator から管理情報を取得するには、管理アプリケーション

で使用される SNMP コミュニティ名が、Server Administrator のシステムで設定されている SNMP コミュニティ名と一致する必要があります。

1. **コンピュータの管理** ウィンドウを開きます。
2. 必要に応じて、同ウィンドウの **コンピュータの管理** アイコンを展開します。
3. **サービスとアプリケーション** アイコンを展開して、**サービス** をクリックします。
4. サービスのリストを下にスクロールして **SNMP サービス** を見つけ、**SNMP サービス** を右クリックしてから、**プロパティ** をクリックします。

   **SNMP サービスプロパティ** ウィンドウが表示されます。
5. **セキュリティ** タブをクリックして、コミュニティ名を追加または編集します。

   コミュニティ名を追加するには、次を行います。
   a. **受理されたコミュニティ名** リストで **追加** をクリックします。

      **SNMP サービス設定** ウィンドウが表示されます。
   b. **コミュニティ名** ボックスで、システムを管理できるシステムのコミュニティ名（デフォルトは public）を入力して、**追加** をクリックします。

      **SNMP サービスプロパティ** ウィンドウが表示されます。

   コミュニティ名を編集するには、次を行います。
   a. **受理されたコミュニティ名** リストでコミュニティ名を選択して、**編集** をクリックします。

      **SNMP サービス設定** ウィンドウが表示されます。
   b. **コミュニティ名** のボックスで、コミュニティ名を編集し、**OK** をクリックします。

      **SNMP サービスプロパティ** ウィンドウが表示されます。
6. **OK** をクリックして、変更を保存します。

### SNMP Set 操作を有効にする

IT Assistant を使って Server Administrator の属性を変更するには、Server Administrator で SNMP Set 操作が有効になっている必要があります。

1. **コンピュータの管理** ウィンドウを開きます。
2. 必要に応じて、同ウィンドウの **コンピュータの管理** アイコンを展開します。
3. **サービスとアプリケーション** アイコンを展開して、**サービス** をクリックします。
4. サービスのリストを下にスクロールして **SNMP サービス** を見つけ、**SNMP サービス** を右クリックしてから、**プロパティ** をクリックします。

   **SNMP サービスプロパティ** ウィンドウが表示されます。
5. **セキュリティ** タブをクリックして、コミュニティのアクセス権限を変更します。
6. **受理されたコミュニティ名** リストでコミュニティ名を選択して、**編集** をクリックします。

   **SNMP サービス設定** ウィンドウが表示されます。
7. **コミュニティ権限** を **読み取り / 書き込み** または **読み取り / 作成** に設定して、**OK** をクリックします。

   **SNMP サービスプロパティ** ウィンドウが表示されます。
8. **OK** をクリックして、変更を保存します。

### SNMP トラップを管理ステーションに送信するためのシステム設定

Server Administrator は、センサーおよびその他の監視パラメータの状態の変更に応じて、SNMP トラップを生成します。管理ステーションに SNMP トラップを送信するには、Server Administrator が稼動しているシステム上で 1 つ以上のトラップ先を設定する必要があります。

1. **コンピュータの管理** ウィンドウを開きます。
2. 必要に応じて、同ウィンドウの **コンピュータの管理** アイコンを展開します。
3. **サービスとアプリケーション** アイコンを展開して、**サービス** をクリックします。

4. サービスのリストを下にスクロールして **SNMP サービス** を見つけ、**SNMP サービス** を右クリックしてから、**プロパティ** をクリックします。

   **SNMP サービスプロパティ** ウィンドウが表示されます。

5. **トラップ** タブをクリックしてトラップのコミュニティを追加するか、トラップコミュニティのトラップ送信先を追加します。
   a. トラップのコミュニティを追加するには、**コミュニティ名** ボックスにコミュニティ名を入力し、**コミュニティ名** ボックスの横にある **リストに追加** をクリックします。
   b. トラップコミュニティのトラップ送信先を追加するには、**コミュニティ名** ドロップダウンボックスからコミュニティ名を選択して、**トラップ送信先** ボックスの下の **追加** をクリックします。

      **SNMP サービス設定** ウィンドウが表示されます。
   c. **ホスト名、IP または IPX アドレスボックス** 内で、トラップ送信先を入力し、**追加** をクリックします。

      **SNMP サービスプロパティ** ウィンドウが表示されます。
6. **OK** をクリックして、変更を保存します。

### 対応 Red Hat Enterprise Linux 環境のシステムでの SNMP エージェントの設定

Server Administrator は、SNMP **net-snmp** エージェントにより提供された SNMP サービスを使用します。 SNMP エージェントを設定して、コミュニティ名を変更し、設定操作を可能にし、管理ステーションにトラップを送信できます。SNMP エージェントが IT Assistant などの管理アプリケーションと正しくインタラクションを取れるように設定するには、次のセクションに説明されている手順を実行します。

**メモ:** SNMP 設定の詳細については、オペレーティングシステムのマニュアルを参照してください。

### SNMP エージェントのアクセスコントロールの設定

Server Administrator によって実装されている管理情報ベース（MIB）ブランチは、オブジェクト識別子（OID）1.3.6.1.4.1.674 で識別されます。Server Administrator を実行しているシステムを管理するには、管理アプリケーションがこの MIB ツリーのブランチへのアクセス権を確保している必要があります。

Red Hat Enterprise Linux および VMware ESXi 4.0 オペレーティングシステムの場合、デフォルトの SNMP エージェント設定では、MIB ツリーの MIB-II システムブランチ（1.3.6.1.2.1.1 の OID で識別）にのみ *public* コミュニティへの読み取り専用アクセスが与えられます。この設定では、管理アプリケーションを使用して、Server Administrator や MIB-II システムブランチ外の他のシステム管理情報を取得したり変更することはできません。

### Server Administrator SNMP エージェントのインストール処置

Server Administrator がインストール中にデフォルトの SNMP 設定を検知した場合、SNMP エージェント設定を変更して、パブリックコミュニティは MIB ツリー全体で読み取り専用アクセスを提供するようにしようとします。Server Administrator は、次の手順で SNMP エージェント設定ファイル **/etc/snm, p/snmpd.conf** を変更します。

- 存在しない場合は、次のラインを追加することにより、MIB ツリー全体のビューを作成します: `view all included`
- デフォルトのアクセスラインを変更すると、パブリックコミュニティは MIB ツリー全体に読み取り専用アクセスのみを付与されます。Server Administrator は次のラインを探します: `access notConfigGroup "" any noauth exact systemview none none`
- Server Administrator が上記のラインを見つけると、次のラインに変更します: `access notConfigGroup "" any noauth exact all none none`

  **メモ:** Server Administrator が確実に SNMP エージェント設定を変更し、システム管理データに正しくアクセスできるようにするには、Server Administrator のインストール後にその他の SNMP エージェント設定を変更することをお勧めします。

Server Administrator SNMP は、SNMP 多重化（SMUX）プロトコルを使って SNMP エージェントと通信します。Server Administrator SNMP が SNMP エージェントと接続すると、SNMP エージェントにオブジェクト識別子を送信して、自身を SMUX ピアと識別します。オブジェクト識別子は SNMP エージェントとして設定する必要

があるため、存在しない場合は、インストール中に Server Administrator は SNMP エージェント設定ファイル **/etc/snmp/snmpd.conf** に次のラインを追加します:

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

### SNMP コミュニティ名の変更

SNMP コミュニティ名を設定すると、どのシステムが SNMP を使用してシステムを管理できるかが決まります。管理アプリケーションが Server Administrator から管理情報を取得するには、管理アプリケーションで使用される SNMP コミュニティ名が、Server Administrator のシステムで設定されている SNMP コミュニティ名と一致する必要があります。

Server Administrator のシステムから管理情報を取得するために使用される SNMP コミュニティ名を変更するには、以下の手順を行います。

1. SNMP エージェント設定ファイル、**/etc/snmp/snmpd.conf** を開きます。
2. `com2sec publicsec default public` または `com2sec notConfigUser default public` の行を探します。

   **メモ:** IPv6 には、`com2sec6 notConfigUser default public` の行を探し、ファイルに `agentaddress udp6:161` と追加します。
3. この行の `public` を新しい SNMP コミュニティ名と置き換え編集します。編集後の行は、`com2sec publicsec default community_name` または `com2sec notConfigUser default community_name` となります。
4. SNMP 設定の変更を有効にするには、`service snmpd restart` と入力して SNMP エージェントを再起動します。

### SNMP Set 操作を有効にする

IT Assistant を使って Server Administrator の属性を変更するには、SNMP Set 操作を Server Administrator を実行中のシステムで有効にする必要があります。

Server Administrator を実行中のシステムで SNMP Set 操作を有効にするには、SNMP エージェント設定ファイル、**/etc/snmp/snmpd.conf** を編集して、次の手順を実行します。

1. 次の行、`access publicgroup "" any noauth exact all none none` または、`access notConfigGroup "" any noauth exact all none none` を見つけます。
2. 最初の `none` を `all` と置き換えてこの行を編集します。編集完了後の新しい行は、`access publicgroup "" any noauth exact all all none` または `access notConfigGroup "" any noauth exact all all none` となります。
3. SNMP 設定の変更を有効にするには、`service snmpd restart` と入力して SNMP エージェントを再起動します。

### SNMP トラップを管理ステーションに送信するためのシステム設定

Server Administrator は、センサーおよびその他の監視パラメータのステータス変更に対して、SNMP トラップを生成します。管理ステーションに SNMP トラップを送信するには、Server Administrator を実行しているシステム上で 1 つ、または複数のトラップ先を設定する必要があります。

Server Administrator を実行しているシステムで管理ステーションにトラップを送信するように設定するには、SNMP エージェント設定ファイル、 **/etc/snmp/snmpd.conf** を編集して次の 手順を実行します。

1. 次のラインをファイルに追加します: `trapsink IP_address community_name`（`IP_address` は管理ステーションの IP アドレスで、`community_name` は SNMP コミュニティ名）。
2. SNMP 設定の変更を有効にするには、次のように入力して SNMP エージェントを再起動します: `service snmpd restart`。

### 対応 SUSE Linux Enterprise Server が実行されるシステムでの SNMP エージェントの設定

Server Administrator は、net-snmp エージェントにより提供される SNMP サービスを使用します。 SNMP エージェントを設定して、リモートホストから SNMP へのアクセスの有効化、コミュニティ名の変更、Set 操作の

有効化、管理ステーションへのトラップ送信ができます。 IT Assistant などの管理アプリケーションと適切に対話できるよう SNMP エージェントを設定するには、次のセクションの手順を実行します。

**メモ:** SNMP 設定の詳細については、オペレーティングシステムのマニュアルを参照してください。

### Server Administrator SNMP インストールアクション

Server Administrator SNMP は、SMUX プロトコルを使って SNMP エージェントと通信します。 Server Administrator SNMP が SNMP エージェントと接続すると、SNMP エージェントにオブジェクト識別子を送信して自身を SMUX ピアとして識別します。 このオブジェクト識別子は、SNMP エージェントと設定する必要があるため、Server Administrator は次のラインが存在しない場合は、インストール中に SNMP エージェント設定ファイル **/etc/snmp/snmpd.conf** に追加します。

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

### リモートホストからの SNMP アクセスの有効化

SUSE Linux Enterprise Server オペレーティングシステムのデフォルトの SNMP エージェント設定では、public コミュニティに対して、ローカルホストからのみ、MIB ツリー全体への読み取り専用アクセス権を与えます。Server Administrator システムを正しく検知し、管理するために、この設定では他のホストで実行される IT Assistant などの SNMP 管理アプリケーションが許可されていません。インストール中、Server Administrator がこの設定を検知すると、メッセージをオペレーティングシステムのログファイル **/var/log/messages** に記録し、SNMP アクセスがローカルホストに制限されていることを示します。リモートホストから SNMP 管理アプリケーションを使用してシステムを管理する場合は、リモートホストからの SNMP アクセスを有効にするように SNMP エージェントを設定する必要があります。

**メモ:** セキュリティ上の理由から、可能であれば、SNMP アクセスは、特定のリモートホストに制限することをお勧めします。

特定のリモートホストから Server Administrator を実行中のシステムへの SNMP アクセスを有効にするには、SNMP エージェント設定ファイル **/etc/snmp/snmpd.conf** を編集し、次の手順を実行してください。

1. 次の行を見つけます。`rocommunity public 127.0.0.1`
2. この行の 127.0.0.1 の部分をリモートホストの IP アドレスに書き換えます。編集後の行は、次のようになります。 `rocommunity public IP アドレス`

   **メモ:** 各リモートホストに対し `rocommunity` 指令を追加することにより、複数の特定リモートホストからの SNMP アクセスを有効にできます。
3. SNMP 設定の変更を有効にするには、次のように入力して SNMP エージェントを再起動します。 `/etc/init.d/snmpd restart`

   すべてのリモートホストから Server Administrator を実行中のシステムへの SNMP アクセスを有効にするには、SNMP エージェント設定ファイル **/etc/snmp/snmpd.conf** を編集し、次の手順を実行してください。
4. 次の行を見つけます。`rocommunity public 127.0.0.1`
5. 127.0.0.1 を削除してこの行を編集します。編集後の行は、次のようになります。 `rocommunity public`
6. SNMP 設定の変更を有効にするには、次のように入力して SNMP エージェントを再起動します。 `/etc/init.d/snmpd restart`

### SNMP コミュニティ名の変更

SNMP コミュニティ名の設定により、どの管理ステーションが SNMP を使用してシステムを管理できるかが決まります。管理アプリケーションが Server Administrator から管理情報を取得するには、管理アプリケーションで使用される SNMP コミュニティ名が、Server Administrator のシステムで設定されている SNMP コミュニティ名と一致する必要があります。

Server Administrator を実行するシステムから、管理情報を取得するために使用されるデフォルトの SNMP コミュニティ名を変更するには、以下の手順を行います。

1. SNMP エージェント設定ファイル、**/etc/snmp/snmpd.conf** を開きます。
2. 次の行を見つけます。`rocommunity public 127.0.0.1.`

3. この行の public を新しい SNMP コミュニティ名と置き換え編集します。編集後の行は、次のようになります。rocommunity コミュニティ名 127.0.0.1.
4. SNMP 設定の変更を有効にするには、**/etc/init.d/snmpd restart** と入力して SNMP エージェントを再起動します。

### SNMP Set 操作を有効にする

IT Assistant を使って Server Administrator の属性を変更するには、SNMP Set 操作を Server Administrator を実行中のシステムで有効にする必要があります。 IT Assistant からシステムのリモートシャットダウンを有効にするには、SNMP 設定操作を有効にする必要があります。

**メモ:** 管理機能を変更するためにシステムを再起動する場合、SNMP Set 操作は不要です。

Server Administrator を実行中の SNMP 設定操作を有効にするには、次の手順を実行します。

1. SNMP エージェント設定ファイル **/etc/snmp/snmpd.conf** を開きます。
2. 次のラインを探します: rocommunity public 127.0.0.1。
3. rocommunity を rwcommunity に変更してこのラインを編集します。編集後、新しいラインは次のようになります: rwcommunity public 127.0.0.1。
4. SNMP 設定の変更を有効にするには、次のように入力して SNMP エージェントを再起動します: **/etc/init.d/snmpd restart**。

### VMware MIB をプロキシするために対応 VMware ESX 4.0 オペレーティングシステムが稼動するシステムにおいて SNMP エージェントを設定する

ESX 4.X サーバーは、SNMP プロトコルを使って単一デフォルトポート 162 経由で管理できます。 このためには、snmpd はデフォルトポート 162 を、vmwarehostd は 167 のように異なる（未使用の）ポートを使うように設定されます。 VMware MIB ブランチの SNMP 要求は、**snmpd** デーモンのプロキシ機能を使って **vmware-hostd** に送信されます。

VMware SNMP 設定ファイルは、ESX サーバー上、またはリモートシステム（Windows または Linux）から VMware Remote Command-Line Interface (RCLI) コマンド、vicfg-snmp を実行することにより、手動で変更できます。 RCLI ツールは、VMware ウェブサイト **vmware.com/download/vi/drivers_tools.html** からダウンロードできます。

SNMP エージェントを設定するには、次の手順を行います。

1. VMware SNMP 設定ファイル、**/etc/vmware/snmp.xml** を手動で編集するか、または次の vicfg-snmp コマンドを実行して SNMP 設定を変更します。 これには、SNMP リッスンポート、コミュニティ文字列、およびトラップターゲット ipaddress/port、およびトラップコミュニティ名が含まれ、次に VMware SNMP サービスを有効にします。
   a. `vicfg-snmp.pl --server <ESX IP addr> --username root --password <password> -c <community name> -p X -t <Destination_IP_Address>@162/ <community name>`

      未使用ポートを示します。 未使用ポートを見つけるには、定義済みシステムサービスのポート割り当てについて **/etc/services** ファイルをチェックします。 また、選択したポートがどのアプリケーションまたはサービスでも使用されていないことを確認するため、ESX サーバーで次のコマンドを実行します： netstat –a command

      **メモ:** カンマ区切りで複数の IP アドレスを入力することも可能です。

      VMware SNMP サービスを有効にするには、次のコマンドを実行します。
   b. `vicfg-snmp.pl --server <ESX IP addr> --username root --password <password> - E`

      設定を表示するには、次のコマンドを実行します。
   c. `vicfg-snmp.pl --server <ESX_IP_addr> --username root --password <password> -s`

      変更後の設定ファイルの例は次の通りです：

      ```
      <?xml version="1.0">
      ```

```
<config>
<snmpSettings>
<enable> true </enable>
<communities> public </communities>
<targets> 143.166.152.248@162/public </targets>
<port> 167 </port>
</snmpSettings>
</config>
```

2. システムで SNMP サービスが既に起動している場合は、次のコマンドを入力して停止させます：`service snmpd stop`
3. **/etc/snmp/snmpd.conf** ファイルの最後に次のラインを追加します：`proxy -v 1 -c public udp: 127.0.0.1:X .1.3.6.1.4.1.6876`

   ここで、X は、上記の SNMP 設定時に指定された未使用ポートを表します。
4. 次のコマンドを使用してトラップの送信先を設定します：`<Destination_IP_Address> <community_name>`

   専用 MIB で定義されたトラップを送信するには、trapsink 仕様が必要です。
5. 次のコマンドを使って mgmt-vmware サービスを再スタートします：`service mgmt-vmware restart`
6. 次のコマンドを使って snmpd サービスを再スタートします：`service snmpd start`

   **メモ:** このサービスは **snmpd** サービスに依存するため、srvadmin がインストールされ、サービスがすでに開始されている場合はサービスを再起動してください。
7. 再起動ごとに snmpd デーモンが開始されるようにするため、次のコマンドを実行します：`chkconfig snmpd on`
8. 管理ステーションにトラップを送信する前に、次のコマンドを実行して、SNMP ポートが開かれていることを確認します：`esxcfg-firewall -e snmpd`。

### 対応 VMware ESXi 4.X および ESXi 5.X オペレーティングシステムが稼動するシステムにおける SNMP エージェントの設定

Server Administrator は、VMware ESXi 4.X および ESXi 5.X 上の SNMP トラップをサポートしています。ライセンスがスタンドアロンライセンスのみの場合は、VMware ESXi オペレーティングシステムの SNMP 設定はできません。必要な SNMP サポートがないため、Server Administrator は VMware ESXi 4.x および ESXi 5.X での SNMP Get および Set 操作をサポートしていません。VMware ESXi 4.X および ESXi 5.X が稼動するシステムで、管理ステーションに SNMP トラップを送信させるように設定するには、VMware vSphere コマンドラインインタフェース（CLI）を使用します。

**メモ:** VMware vSphere の CLI 使用方法については、 **vmware.com/support** を参照してください。

### SNMP トラップを管理ステーションに送信するためのシステム設定

Server Administrator は、センサーおよびその他の監視パラメータのステータス変更に対して、SNMP トラップを生成します。管理ステーションに SNMP トラップを送信するには、Server Administrator を実行しているシステム上で 1 つ、または複数のトラップ先を設定する必要があります。

管理ステーションにトラップを送信するように Server Administrator を実行するお使いの ESXi システムを設定するには、次の手順を実行します。

1. VMware vSphere CLI をインストールします。
2. VMware vSphere CLI をインストールしたシステム上で、コマンドプロンプトを開きます。
3. VMware vSphere CLI がインストールされたディレクトリを変更します。Linux のデフォルトロケーションは **/usr/bin** です。Windows のデフォルトロケーションは **C:\Program Files\VMware\VMware vSphere CLI\bin** です。

4. 次のコマンドを実行します: `vicfg-snmp.pl --server <server> --username <username> --password <password> -c <community> -t <hostname> @162/<community>`

   ここで、<server> は ESXi システムのホスト名または IP アドレス、<username> は ESXi システム上のユーザー、<community> は SNMP コミュニティ名、<hostname> は管理ステーションのホスト名または IP アドレスを指します。

   **メモ:** .pl の拡張子は、Linux では必要ありません。

   **メモ:** ユーザー名とパスワードを指定しないと、入力を求めるプロンプトが表示されます。

SNMP のトラップ設定は、サービスを再起動する必要なく、直ちに反映されます。

## 対応 Red Hat Enterprise Linux オペレーティングシステム と SUSE Linux Enterprise Server が稼動するシステム上でのファイアウォールの設定

Red Hat Enterprise Linux/SUSE Linux のインストール中にファイアウォールのセキュリティを有効にする場合は、デフォルトですべての外部ネットワークインタフェース上の SNMP ポートが閉じます。Server Administorator から情報を検出、取得するための IT Assistant などの SNMP 管理アプリケーションを有効にするには、外部ネットワークインタフェースの SNMP ポートが最低 1 つ開いている必要があります。外部ネットワークインタフェースのファイアウォールで SNMP が 1 つも開いていないことを Server Administrator が検知すると、Server Administrator は警告メッセージを表示し、システムログにそのメッセージを記録します。

ファイアウォールを無効にして SNMP ポートを開いたり、ファイアウォールですべての外部ネットワークインタフェースを開く、または、ファイアウォールで外部ネットワークインタフェースの SNMP ポートを 1 つ開くことができます。この操作は Server Administrator の開始前または開始後に行うことができます。

以前に説明した方法のいずれかを使用して Red Hat Enterprise Linux 上の SNMP ポートを開くには、次の手順を実行します。

1. Red Hat Enterprise Linux コマンドプロンプトで、`setup` と入力して <Enter> を押し、テキストモードセットアップユーティリティを起動します。

   **メモ:** このコマンドは、オペレーティングシステムでデフォルトのインストールを実行した場合にのみ使用できます。

   **ツールの選択** メニューが表示されます。
2. 下矢印を使用して **ファイアウォールの設定** を選択し、<Enter> を押します。

   **ファイアウォールの設定** 画面が表示されます。
3. <Tab> を押して **セキュリティレベル** を選択し、スペースキーで設定するセキュリティレベルを選びます。選択した **セキュリティレベル** に星印が表示されます。

   **メモ:** ファイアウォールのセキュリティレベルの詳細については、<F1> を押します。SNMP のデフォルトでのポート番号は、161 となっています。X Window System グラフィックユーザーインタフェースを使用している場合は、<F1> を押しても新しいバージョンの Red Hat Enterprise Linux ではファイアウォールのセキュリティレベルが表示されないことがあります。

   a. ファイアウォールを無効にするには、**ファイアウォールなし** または **無効** を選択して手順 7 に進みます。
   b. ネットワークインタフェース全体または SNMP ポートを開くには、**高、中** または **有効** を選択して手順 4 に進みます。
4. <Tab> を押して カスタマイズ へ移動し、<Enter> を押します。

   **ファイアウォールの設定-カスタマイズ** 画面が表示されます。
5. ネットワークインタフェース全体を開放するか、すべてのネットワークインタフェースの SNMP ポートだけを開放するかを選択します。
   a. すべてのネットワークインタフェースを開くには、<Tab> を押して信頼されたデバイスに移動し、スペースキーを押します。すべてのインタフェースが開いていると、デバイス名の左にあるボックスに星印が表示されます。

b. すべてのネットワークインタフェースの SNMP ポートを開くには、<Tab> を押して その他のポートに進み snmp:udp と入力します。

6. <**Tab**> を押して **OK** を選択し、<**Enter**> を押します。
   **ファイアウォールの設定** 画面が表示されます。
7. <**Tab**> を押して **OK** を選択し、<**Enter**> を押します。
   **ツールの選択** メニューが表示されます。
8. <**Tab**> を押して **終了** を選択し、<**Enter**> を押します。

### ファイアウォール設定

SUSE Linux Enterprise Server で SNMP ポートを開くには、次の操作を実行します。

1. コンソールで次のコマンドを実行して SuSEfirewall2 を設定します：`a.# yast2 firewall`
2. 矢印キーを使用して、**許可サービス**に移動します。
3. <Alt><d> を押して、**追加の許可ポート** ダイアログボックスを開きます。
4. <Alt><T> を押して、カーソルを **TCP ポート** テキストボックスに移動します。
5. テキストボックスに **snmp** と入力します。
6. <Alt><O> <Alt><N> を押して、次の画面に進みます。
7. <Alt><A> を押して、変更を受け入れ、適用します。

# 3

# Server Administrator の使用

Server Administrator セッションを開始するには、デスクトップ上の **Dell OpenManage Server Administrator** アイコンをダブルクリックします。

**Server Administrator ログイン** 画面が表示されます。Dell OpenManage Server Administrator のデフォルトポートは 1311 となっています。必要に応じてポートを変更できます。システムのプリファレンスの設定については、『Dell Systems Management Server Administration』を参照してください。

**メモ:** XenServer 6.0 上で動作しているサーバーは、コマンドラインインターフェース（CLI）または別のマシンにインストールされている Central Web Server によって管理することができます。

## ログインおよびログアウト

OpenManage Server Administrator では、以下の種類のログインが可能です。

- Server Administrator ローカルシステムログイン
- Server Administrator 管理下システムログイン — デスクトップアイコンを使用
- Server Administrator 管理システムログイン — ウェブブラウザを使用した場合
- Central Web Server ログイン

### Server Administrator ローカルシステムログイン

このログインは、ローカルシステム上に Server Instrumentation および Server Administrator Web Server コンポーネントをインストールした場合にのみ、利用可能です。

このオプションは、XenServer 6.0 上で動作しているサーバーでは使用できません。

ローカルシステムで Server Administrator にログインするには、次の手順を行います。

1. System Management の **ログイン** ウィンドウの該当するフィールドに、あらかじめ割り当てられた **ユーザー名** および **パスワード** を入力します。

   定義されたドメインから Server Administrator にアクセスするには、正しいドメイン 名も指定する必要があります。
2. Microsoft Active Directory を使用してログインするには、**Active Directory ログイン** のチェックボックスにチェックを入れます。Active Directory ログインの使用 を参照してください。
3. **Submit**（送信）をクリックします。

Server Administrator セッションを終了するには、それぞれの **Server Administrator** ホームページ右上の角にある **ログアウト** をクリックします。

**メモ:** CLI を使用してシステムの Active Directory を設定する方法に関する情報 は、**dell.com/support/manuals** にある『*Dell OpenManage 管理ステーションソフトウェアインストールガイド*』を参照してください。

## Server Administrator 管理下システムログイン — デスクトップアイコンを使用

このログインは、Server Administrator Web Server コンポーネントがシステムにインストールされている場合にのみ使用できます。Server Administrator にログインしてリモートシステムを管理するには、次の手順を実行します。

1. デスクトップ上の **Dell OpenManage Server Administrator** アイコンをダブルクリックします。
2. 管理下システムの IP アドレス、システム名、または完全修飾ドメイン名（FQDN）をタイプします。

   **メモ:** システム名または FQDN を入力した場合、 Dell OpenManage Server Administrator Web Server ホストはシステム名または FQDN を管理システムの IP アドレスに変換します。 管理システムのポート番号も入力できます。 たとえば、Hostname:Port number、または IP address:Port number です。 Citrix XenServer 6.0 管理ノードに接続している場合、フォーマット Hostname:Port number、または IP address:Port number でポート 5986 を使用します。
3. イントラネット接続を使用している場合、**証明書の警告を無視する**を選択します。
4. **Active Directory ログイン** を選択して、Microsoft Active Directory 認証を使用してログインします。 Active Directory ソフトウェアがネットワークへのアクセスを制御するのに使用されていない場合、**Active Directory ログイン** を選択しないでください。「Active Directory ログインの使用」を参照してください。
5. **送信** をクリックします。

## Server Administrator 管理システムログイン — ウェブブラウザを使用した場合

**メモ:** Server Administrator にログインするには、事前に割り当てられたユーザー権限が必要です。新しいユーザーを設定する方法については、「設定と管理「を参照してください。

1. ウェブブラウザを開きます。
2. アドレスフィールドに、次のいずれかを入力します。

   - `https://hostname:1311` は管理ノードシステムに割り当てられた名前、1311 はデフォルトのポート番号を表します。
   - `https://IP address:1311` の IP address は管理下システムの IP アドレスで、1311 はデフォルトのポート番号を表します。

   **メモ:** アドレスフィールドには必ず `https://`（`http://`ではない）と入力してください。
3. <Enter>を押します。

## Central Web Server ログイン

このログインは、Server Administrator Web Server コンポーネントがシステムにインストールされている場合にのみ使用できます。 このログインを使って、OpenManage Server Administrator Central Web Server を管理します:

1. デスクトップ上の **Dell OpenManage Server Administrator** アイコンをダブルクリックします。 リモートログインページが表示されます。

   **注意: ログイン画面には、証明書の警告を無視する チェックボックスが表示されます。このオプションは慎重に使用してください。信頼できるイントラネット環境でのみ使用することをお勧めします。**
2. 画面の右上角の **ウェブサーバーの管理** リンクをクリックします。
3. **ユーザー名、パスワード** および **ドメイン名**（定義されたドメインから Server Administrator にアクセスしている場合）を入力し、 **送信** をクリックします。
4. **Active Directory Login** を選択して、Microsoft Active Directory を使用してログインします。「Active Directory ログインの使用」を参照してください。

5. **送信** をクリックします。

   Server Administrator セッションを終了するには、グローバルナビゲーションバーで **ログアウト** をクリックします。

   **メモ:** Mozilla Firefox バージョン 3.0 および 3.5 または Microsoft Internet Explorer version 7.0 または 8.0 を使って Server Administrator を起動すると、中程度の警告ページにセキュリティ証明書に関する問題が表示されます。システムセキュリティを確保するには、新しい X.509 証明書を生成する、既存 X.509 証明書を再使用するか、または認証局（CA）からルート証明書または証明書チェーンをインポートすることが推奨されます。証明書に関するそのようなメッセージを表示しないようにするには、使用する証明書が信頼できる CA からのものである必要があります。X.509 証明書管理の詳細に関しては、「X.509 証明書管理」を参照してください。

   **メモ:** システムセキュリティを確保するために、認証局（CA）からルート証明書または証明書チェーンをインポートすることが推奨されます。詳細に関しては、VMware マニュアルを参照してください。

   **メモ:** 管理下システムの認証局が有効であるにもかかわらず、Server Administrator ウェブサーバーが信頼できない証明書のエラーをレポートしてくる場合、**certutil.exe** ファイルを使うことにより管理下システムの CA を信頼できるものとすることができます。この .exe ファイルにアクセスする方法の詳細に関しては、オペレーティングシステムのマニュアルを参照してください。対応する Windows オペレーティングシステムの場合、証明書スナップを使って証明書をインポートすることもできます。

## Active Directory ログインの使用

Active Directory で Dell 拡張スキーマソリューションを使用してログインする場合は、**Active Directory ログイン** チェックボックスを選択します。

このソリューションにより、Server Administrator にアクセスできるようになり、Server Administrator ユーザーおよび権限を Active Directory ソフトウェアに追加/制御できます。詳細に関しては、『*Dell OpenManage Server Administrator インストールおよびセキュリティユーザーズガイド*』の「Microsoft Active Directory の使用」（**dell.com/support/manuals**）を参照してください。

## シングルサインオン

Windows オペレーティングシステムでシングルサインオンオプションを使用すると、ログインをしているすべてのユーザーはログインページを介さずに、デスクトップの **Dell OpenManage Server Administrator** アイコンをクリックするだけで Server Administrator Web アプリケーションにアクセスできます。

**メモ:** シングルサインオンの詳細については、**support.microsoft.com/default.aspx?scid=kb;en-us;Q258063** でサポート技術情報の記事を参照してください。

ローカルのマシンへのアクセスには、そのマシンに合った権限のあるアカウント（ユーザー、パワーユーザー、管理者）が必要です。他のユーザーは、Microsoft Active Directory に対して認証されます。Microsoft Active Directory へのシングルサインオン認証を使用して Server Administrator を起動する場合は、次のパラメータを渡す必要があります。

```
authType=ntlm&application=[プラグイン名]
```

ここで、 プラグイン名 = omsa、ita 等となります。
たとえば、次のとおりです。

```
https://localhost:1311/?authType=ntlm&application=omsa
```

ローカルマシンのユーザーアカウントに対してシングルサインオン認証を使用して Server Administrator を起動するには、次のパラメータも渡す必要があります。

```
authType=ntlm&application=[プラグイン名]&locallogin=true
```

ここで、 プラグイン名 = omsa、ita 等となります。
たとえば、次のとおりです。
`https://localhost:1311/?authType=ntlm&application=omsa&locallogin=true`

また、Server Administrator は他の製品（Dell OpenManage IT Assistant など）もログインページを介さずに直接 Server Administrator の Web ページにアクセスできるように機能が拡張されています（既にログインしており、適切な権限を持っている場合）。

## 対応 Microsoft Windows オペレーティングシステムが稼動するシステム上のセキュリティ設定

対応の Microsoft Windows オペレーティングシステムが稼動するリモート管理システムから Server Administrator にログインするには、ブラウザのセキュリティオプションを設定する必要があります。

ブラウザのセキュリティ設定によっては、Server Administrator が使用するクライアント側のスクリプトを実行できない場合があります。クライアント側のスクリプトを使用できるようにするには、リモート管理下システムで次の手順を実行します。

**メモ:** クライアント側のスクリプトを使用できるようにブラウザを設定していない場合、Server Administrator にログインするときに空白の画面が表示される場合があります。この場合は、エラーメッセージが表示され、ブラウザを設定するように指示されます。

### Internet Explorer でクライアントサイドスクリプトの使用を有効にする

1. ご利用の Web ブラウザで、**ツール → インターネットオプション → セキュリティ** を順にクリックします。
   **インターネットオプション** ウィンドウが表示されます。
2. **セキュリティ設定を表示または変更するゾーンを選択** の下で、**信頼されたサイト** をクリックして、**サイト** をクリックします。
3. **この Web サイトをゾーンに追加する** フィールドで、リモート管理下システムにアクセスするのに使用する Web アドレスをペーストします。
4. **追加** をクリックします。
5. ブラウザのアドレスバーからリモート管理下システムにアクセスするために使用する Web アドレスをコピーし、**この Web サイトをゾーンに追加する** フィールドに貼り付けます。
6. **このゾーンのセキュリティのレベル** で、**カスタム** レベルをクリックします。
   Windows Server 2003 の場合：
   a. **その他** で、**メタ更新を許可する** を選択します。
   b. **アクティブスクリプト** で、**有効にする** を選択します。
   c. **アクティブスクリプト** の下の **Internet Explorer web ブラウザコントローラのスクリプトを許可する** を選択します。
7. **OK** をクリックし新しい設定を保存します。
8. ブラウザを閉じて Server Administrator にログインします。

### Internet Explorer での Server Administrator のシングルサインオンの有効化

Server Administrator へのシングルサインオンをユーザー認証情報のプロンプトなしに許可するには、以下の手順を行います。

1. お使いのウェブブラウザで、**ツール → インターネットオプション → セキュリティ** の順にクリックします。
2. **表示するゾーンの選択またはセキュリティ設定の変更** で、**信頼済みサイト** をクリックし、**サイト** をクリックします。
3. **このウェブサイトをゾーンに追加する** フィールドに、リモート管理下システムにアクセスする際に使用するウェブアドレスを貼り付けます。

4. **追加** をクリックします。
5. **カスタムレベル** をクリックします。
6. **ユーザー認証** で、**現在のユーザー名とパスワードで自動ログイン** を選択します。
7. **OK** をクリックし新しい設定を保存します。
8. ブラウザを閉じて Server Administrator にログインします。

### Mozilla Firefox でのクライアント側スクリプト使用の有効化

1. ブラウザを開きます。
2. **編集** → **プリファレンス** の順にクリックします。
3. **詳細設定** → **スクリプトおよびプラグイン** をクリックします。
4. Javascript を有効にする でナビゲータが選択されていることを確認します。**次の JavaScript を有効にする** で、**ナビゲータ** のチェックボックスにチェックを入れます。
5. **OK** をクリックし新しい設定を保存します。
6. ブラウザを閉じます。
7. Server Administrator にログインします。

# Server Administrator ホームページ

**メモ:** Server Administrator 使用中に、ウェブブラウザのツールバーボタン（**戻る** および **更新** など）は使用しないでください。Server Administrator のナビゲーションツールのみを使用してください。

いくつか例外がありますが、Server Administrator のホームページには 3 つの主な領域があります。

- グローバルナビゲーションバー は一般的なサービスへのリンクを提供します。
- システムツリーは、ユーザーのアクセス権限に基づいて、可視のシステムオブジェクトをすべて表示します。
- 処置ウィンドウには、ユーザーのアクセス権限に基づいて、選択されたシステムツリーオブジェクトに使用できる管理処置が表示されます。処置ウィンドウには、3 つの機能領域が含まれます：
  - 処置タブは、ユーザーのアクセス権限に基づいて、選択オブジェトに利用できるプライマリ処置または処置カテゴリを表示します。
  - 処置タブは、ユーザーのアクセス特権に基づいて、処置タブで使用可能な二次オプションのサブカテゴリに分かれています。
  - データ領域は、ユーザーのアクセス権限に基づいて、選択システムツリーオブジェクト、処置タブそしてサブタブの情報を表示します。

さらに **Server Administrator** ホームページにログインすると、システムモデル、システムに割り当てられた名前、および現在のユーザーのユーザー名とユーザー権限がウィンドウの右上隅に表示されます。

次の表は、Server Administrator がインストールされている場合の **GUI** フィールド名と該当システムの一覧です。

**表 6. GUI フィールド名と該当システム**

| GUI フィールド名 | 該当システム |
|---|---|
| モジュラーエンクロージャ | モジュラーシステム |
| サーバーモジュール | モジュラーシステム |
| メインシステム | モジュラーシステム |
| システム | 非モジュラーシステム |
| メインシステムシャーシ | 非モジュラーシステム |

次の図は、非モジュラーシステムに管理者特権でログインしたユーザー用の、サンプル Server Administrator ホームページのレイアウトを示します。

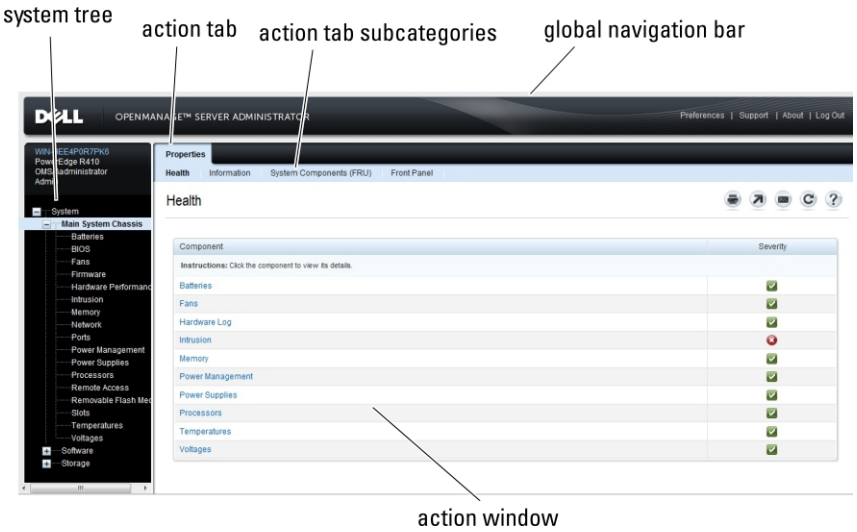


**図 1. Server Administrator ホームページの例 — 非モジュラーシステム**

次の図は、モジュラーシステムに管理者特権でログインしたユーザー用の、サンプル Server Administrator ホームページのレイアウトを示します。

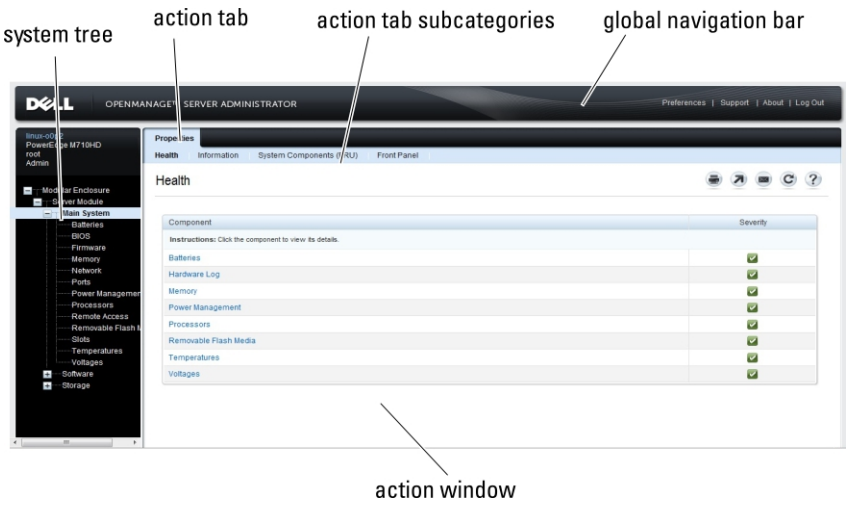


**図 2. Server Administrator ホームページの例 — モジュラーシステム**

システムツリーでオブジェクトをクリックすると、そのオブジェクトに対応する処置ウィンドウが開きます。処置ウィンドウは、処置タブをクリックして主なカテゴリを選択し、処置タブのサブカテゴリをクリックして詳しい情報またはより絞り込んだ処置を選択することにより、ナビゲーションすることができます。 処置ウィンドウのデータ領域に表示された情報は、システムログ、ステータスインジケータ、システムプローブゲージまでさまざまなものがあります。 処置ウィンドウのデータ領域で下線がついているアイテムは、機能レベルがさらにあることを示しています。 下線付きのアイテムをクリックすると、処置ウィンドウに新しいデータ領域が作成され、より詳しい情報が含まれます。 たとえば、**プロパティ**処置タブの **正常性** サブカテゴリの下にある **メインシステムシャーシ/メインシステム** をクリックすると、正常性がモニタされているメインシステムシャーシ/メインシステムオブジェクトに含まれる、すべてのコンポーネントの正常性ステータスが表示されます。

**メモ:** 設定可能なシステムのツリーオブジェクト、システムコンポーネント、処置タブ、およびデータ領域機能の大部分を表示するには、管理者またはパワーユーザーの権限が必要です。 さらに、管理者権限でログインしているユーザーのみが、**シャットダウン** タブに含まれるシャットダウン機能のような、重要なシステム機能にアクセスできます。

## モジュラーおよび非モジュラーシステムにおける Server Administrator ユーザーインタフェースの違い

以下の表では、モジュラーおよび非モジュラーシステムにおいて利用できる Server Administrator 機能を記載しています。

**表 7. モジュラーおよび非モジュラーシステムにおける Server Administrator ユーザーインタフェースの違い**

| 機能 | モジュラーシステム | 非モジュラーシステム |
|---|---|---|
| バッテリ | ✓ | ✓ |
| 電源装置 | ✗ | ✓ |
| ファン | ✗ | ✓ |
| ハードウェアパフォーマンス | ✗ | ✓（第 10 世代以降） |
| イントルージョン | ✗ | ✓ |
| メモリ | ✓ | ✓ |
| ネットワーク | ✓ | ✓ |
| ポート | ✓ | ✓ |
| 電源管理 | ✓ | ✓（第 10 世代以降） |
| プロセッサ | ✓ | ✓ |
| リモートアクセス | ✓ | ✓ |
| リムーバブルフラッシュメディア | ✓ | ✓ |
| スロット | ✓ | ✓ |
| 温度 | ✓ | ✓ |
| 電圧 | ✓ | ✓ |
| モジュラーエンクロージャ（シャーシ情報および CMC 情報） | ✓ | ✗ |

## グローバルナビゲーションバー

グローバルナビゲーションバーとそのリンクは、プログラム内のすべてのユーザーレベルで使用可能です。

- **プリファランス** をクリックして **プリファランス** ホームページを開きます。「プリファランスホームページの使い方」を参照してください。
- **サポート** をクリックして、デルサポートサイトに接続します。
- **バージョン情報** をクリックすると、Server Administrator のバージョン情報と著作権情報が表示されます。
- **ログアウト** をクリックすると、現在の Server Administrator プログラムセッションが終了します。

## システムツリー

システムツリーは Server Administrator ホームページの左側に表示され、システムの表示可能なコンポーネントを一覧表示します。システムコンポーネントはコンポーネントの種類によって分類されています。**モジュラエンクロージャ → システム / サーバーモジュール** のメインオブジェクトを展開したときに表示されるシステム / サーバーモジュールコンポーネントの主要カテゴリは、**メインシステムシャーシ / メインシステム**、**ソフトウェア**、および **ストレージ** です。

ツリーを展開するには、オブジェクトの左側にあるプラス記号（  ）をクリックするか、オブジェクトをダブルクリックします。マイナス記号（  ）が付いているものは、展開済みのエントリでそれ以上展開できないことを意味します。

## 処置ウィンドウ

システムツリーのアイテムをクリックすると、コンポーネントまたはオブジェクトについての詳細がウィンドウのデータ領域に表示されます。処置タブをクリックすることにより、利用可能なユーザーオプションのすべてが、サブカテゴリのリストとして表示されます。

システム/モジュールツリーのオブジェクトをクリックすると、そのコンポーネントの処置ウィンドウが開き、使用可能な処置タブが表示されます。データ領域には、選択したオブジェクトの最初の処置タブの事前選択サブカテゴリがデフォルト表示されます。

事前選択サブカテゴリは通常最初のオプションです。たとえば、**メインシステムシャーシ / メインシステム** オブジェクトは処置ウィンドウを開き、そのデータ領域には **プロパティ** 処置タブと **正常性** サブカテゴリが表示されます。

## データ領域

データ領域はホームページ右側、処置タブの下にあります。データ領域では、タスクを実行しシステムコンポーネントの詳細を表示します。ウィンドウ内の表示内容は、システムのツリーオブジェクトおよび現在選択されている処置タブによって異なります。例えば、システムツリーから **BIOS** を選択している場合は、デフォルトで **プロパティ** タブが選択されており、システム BIOS のバージョン情報がデータ領域に表示されます。処置ウィンドウのデータ領域には、状態インジケータ、タスクボタン、下線項目、ゲージインジケータなどの多数の共通機能が表示されます。

Server Administrator ユーザーインタフェースでは、<mm/dd/yyyy> の形式で日付を表示します。

### システム / サーバーモジュールコンポーネントステータスインジケータ

コンポーネント名の横のアイコンはそのコンポーネントの状態を表します（ページの最終更新時点）。

表 8. システム / サーバーモジュールコンポーネントステータスインジケータ

| 説明 | アイコン |
|---|---|
| コンポーネントは正常（通常通り）です。 | |
| コンポーネントには、警告（重要でない）状態が含まれています。警告状態は、プローブまたはその他のモニタリングツールが、特定の最小および最大値に入るコンポーネントの値を検知する場合に発生します。警告状態が発生すると迅速に対応する必要があります。 | |
| コンポーネントには、障害または重要な状態が含まれています。警告状態は、プローブまたはその他のモニタリングツールが、特定の最小および最大値に入るコンポーネントの値を検知する場合に発生します。重要状態が発生すると直ちに対応する必要があります。 | |
| コンポーネントの正常性が不明です。 | |

## タスクボタン

Server Administrator ホームページから開いたほとんどのウィンドウには、少なくとも次の 5 つのタスクボタンが含まれます: **印刷**、 **エクスポート**、**電子メール**、**ヘルプ** および **更新**。他のタスクボタンは、特定の Server Administrator ウィンドウに含まれます。たとえば、**ログ** ウィンドウには、**名前をつけて保存** および **ログのクリア** タスクボタンが含まれます。

- **印刷**（  ）をクリックすると、開いているウィンドウのコピーをデフォルトプリンタに印刷します。
- **エクスポート**（  ）をクリックすると、開いているウィンドウの各データフィールドの値が表示されたテキストファイルが生成されます。エクスポートファイルは指定したロケーションに保存されます。データフィールドを区切る区切り文字のカスタマイズに関しては、「ユーザーの設定」および「システムプリファレンス」を参照してください。
- **電子メール**（  ）をクリックすると、指定した電子メール受信者宛ての電子メールメッセージが作成されます。電子メールサーバーおよびデフォルトの電子メール受信者を設定する方法については、「ユーザーの設定」および「システムプリファレンス」を参照してください。
- **更新**（  ）をクリックすると、処置ウィンドウのデータ領域のシステムコンポーネント状態の情報が再ロードされます。
- **名前を付けて保存** をクリックすると、処置ウィンドウの HTML ファイルが **.zip** ファイルに保存されます。
- **ログのクリア** をクリックすると、処置ウィンドウのデータ領域に表示されたログからすべてのイベントが消去されます。
- **ヘルプ**（  ）をクリックすると、表示中の特定のウィンドウやタスクボタンの詳細が表示されます。

**メモ: エクスポート**、**電子メール**、および **名前をつけて保存** ボタンは、パワーユーザーまたは管理者権限でログインしているユーザーにのみ表示されます。**ログのクリア** ボタンは、管理者権限を持つユーザーにのみ表示されます。

## 下線付きアイテム

処置ウィンドウのデータ領域の下線付きアイテムをクリックすると、そのアイテムの詳細が表示されます。

## ゲージインジケータ

温度プローブ、ファンプローブ、電圧プローブはそれぞれゲージインジケータによって示されます。例えば、次の図はシステムの CPU のファンプローブの読み取り値の例を示しています。

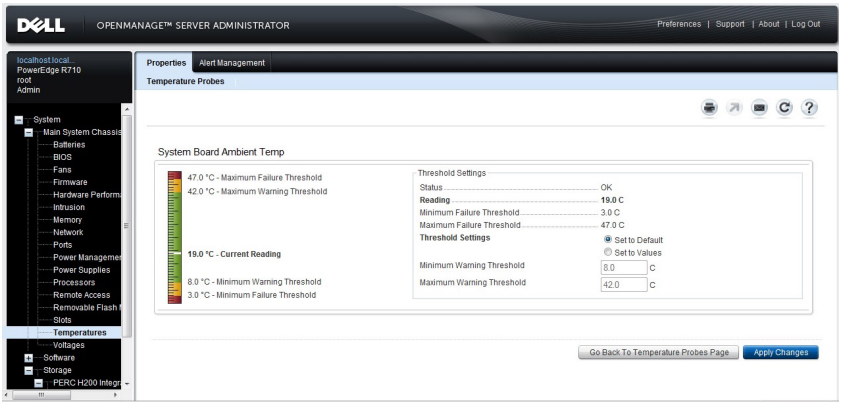


**図 3. ゲージインジケータ**

# オンラインヘルプの使用

Server Administrator ホームページの各ウィンドウでは、状況に応じたオンラインヘルプを使用できます。**ヘルプ** をクリックすると、表示中のウィンドウについて詳しい情報が掲載されたヘルプウィンドウが開きます。オンラインヘルプは、Server Administrator サービスの各要素を実行するのに必要な、特定の動作について説明するように設計されています。Server Administrator が検出するシステムのソフトウェアとハードウェアのグループおよび、ユーザー権限レベルに応じて表示可能なすべてのウィンドウにオンラインヘルプが用意されています。

# プリファランスホームページの使い方

プリファランス ホームページの左ペイン（システムツリーが Server Administrator ホームページで表示されている）には、システムツリーウィンドウの使用可能な設定オプションがすべて表示されます。

使用可能なプリファランスホームページオプションは次の通りです。

- 一般設定
- Server Administrator

リモートシステムの管理のためにログインした後、**プリファランス** タブを表示できます。このタブは、Server Administrator Web サーバー、またはローカルシステムを管理するためにログインした際にも表示されます。

Server Administrator ホームページ同様、**プリファランス** ホームページには 3 つの主な領域があります。

- グローバルナビゲーションバー は一般的なサービスへのリンクを提供します。
  - **ホーム** をクリックすると、Server Administrator のホームページに戻ります。
- **プリファランス** ホームページの左ペイン（システムツリーが Server Administrator ホームページで表示されている）には、管理下システムまたは Server Administrator ウェブサーバーのプリファランスカテゴリが表示されます。
- 処置ウィンドウには、管理下システムまたは Server Administrator ウェブサーバー用に利用可能な、設定およびプリファレンスが表示されます。

次の図は、プリファランス ホームページレイアウトの例を示しています。

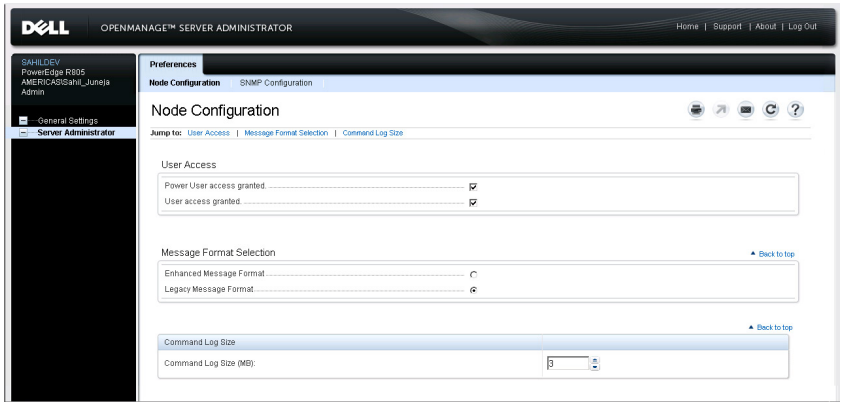


**図 4. プリファランス ホームページの例 - 管理下システム**

## 管理下システムのプリファレンス

リモートシステムにログインするとき、プリファレンスホームページにはデフォルトで **プリファレンス** タブにノード設定ウィンドウが表示されます。

Server Administrator オブジェクトをクリックして、ユーザーまたはパワーユーザー権限を持つユーザーへのアクセスを有効または無効にします。ユーザーのグループ権限によって、Server Administrator オブジェクト処置ウィンドウに **プリファレンス** タブが表示されない場合があります。

プリファランスタブでは、次の操作が可能です。

- ユーザーまたはパワーユーザー特権を持つユーザーのアクセスを有効または無効にします。
- アラートメッセージのフォーマットを選択します。

  **メモ:** 考えられるフォーマットは、**従来** と **拡張** のいずれかです。 デフォルトのフォーマットは **従来** で、レガシーフォーマットです。
- コマンドログサイズの設定
- SNMP の設定

## Server Administrator ウェブサーバーのプリファレンス

Server Administrator ウェブサーバーを管理するためにログインするとき、**プリファレンス** ホームページには、デフォルトでプリファレンスに ユーザープリファレンスウィンドウが表示されます。

管理下システムから Server Administrator ウェブサーバーの分離により、ウェブサーバーの管理 リンクを使用して Server Administrator ウェブサーバーにログインすると、次のオプションが表示されます。

- ウェブサーバープリファレンス
- X.509 証明書管理

これらの機能へのアクセスの詳細に関しては、「Server Administrator サービスの概要」を参照してください。

## Dell Systems Management Server Administration 接続サービスおよびセキュリティ設定

### ユーザーとシステムのプリファランスの設定

**プリファランス** ホームページから、ユーザーとセキュアポートシステムのプリファランスを設定します。

**メモ:** ユーザーまたはシステムのプリファランスをリセットするには、システム管理者権限でログインする必要があります。

ユーザープリファランスをセットアップするには、次の手順を実行します。

1. グローバルナビゲーションバーの **プリファランス** をクリックします。
   プリファランス ホームページが表示されます。
2. **一般設定** をクリックします。
3. 事前に選択されている電子メールの受取人を追加するには、指定するサービス連絡先の電子メールアドレスを **宛先：** フィールドに入力し、**適用** をクリックします。

   **メモ:** 任意のウィンドウで電子メール（  ）をクリックし、そのウィンドウの HTML ファイルが添付された電子メールを、指定したアドレスに送信します。

   **メモ:** OpenManage Server Administrator サービスまたは Server Administrator がインストールされているシステムを再起動すると、Web Server の URL は失われます。omconfig コマンドを使用して、再度 URL を入力します。

### セキュアポートシステム

次の手順を実行して、セキュアポートシステムの環境を設定します。

1. グローバルナビゲーションバーの **プリファランス** をクリックします。
   **プリファランス** ホームページが表示されます。
2. **一般設定** をクリックします。
3. **サーバープリファランス** ウィンドウで、必要に応じてオプションを設定します。

   - **セッションタイムアウト（分）** 機能を使うと、Server Administrator セッションがアクティブな状態でいられる時間制限を設定することができます。**有効にする** を選択すると、指定した分数の間ユーザーインタラクションがない場合にタイムアウトできます。セッションがタイムアウトしたユーザーは、ログインしなおさないと続行できません。**無効にする** を選択すると、Server Administrator **セッションタイムアウト（分）** 機能が無効になります。
   - **HTTPS ポート** フィールドは、Server Administrator にセキュアポートを指定します。Server Administrator のデフォルトセキュアポートは 1311 です。

     **メモ:** ポート番号を無効または使用中のポート番号に変更すると、他のアプリケーションまたはブラウザが管理下システムの Server Administrator にアクセスできなくなる場合があります。デフォルトポートのリストに関しては、*Dell OpenManage Installation およびセキュリティユーザーガイド* を参照してください。
   - **IP アドレスのバインド先** フィールドは、セッション開始時に Server Administrator がバインドする先の管理下システムの IP アドレスを指定します。システムに該当するすべての IP アドレスにバインドするには、**すべて** を選択します。**特定** を選択すると、特定の IP アドレスにバインドされます。

     **メモ: IP アドレスのバインド先** の値を **すべて** 以外の値に変更すると、他のアプリケーションまたはブラウザが管理下システムの Server Administrator にアクセスできなくなる可能性があります。
   - **宛先：** フィールドは、アップデートについてデフォルトで送信する電子メールアドレスを指定します。複数の電子メールアドレスをコンマで区切って設定することができます。
   - **SMTP Server Name（または IP アドレス）** および **DNS Suffix for SMTP Server** フィールドは、会社の SMTP およびドメイン名サーバー（DNS）サフィックスを指定します。Server Administrator が電子メールを送信できるようにするには、該当するフィールドに会社または組織の SMTP Server の IP アドレスおよび DNS suffix for the SMTP Server を入力する必要があります。

     **メモ:** セキュリティ上の理由から、SMTP サーバーから外部アカウントへの電子メール送信を許可していない会社や組織もあります。
   - **コマンドログサイズ** フィールドは、コマンドログファイル の最大ファイルサイズを MB 単位で指定します。

     **メモ:** Server Administrator Web Server を管理するためにログインした場合にのみ、このフィールドが表示されます。

- **サポートリンク** フィールドでは、管理下システムのサポートを提供する事業体の URL を指定します。
- **カスタム区切り文字** フィールドは、**エクスポート** ボタンを使用して作成されるファイルの、データフィールドを区切るために使用される文字を指定します。**;** 文字がデフォルトの区切り文字です。この他のオプションは **!**、**@**、**#**、**$**、**%**、**^**、*****、**~**、**?**、**|** および **,** です。
- **SSL 暗号化** フィールドは、セキュア HTTPS セッションの暗号化レベルを指定します。使用可能な暗号化レベルには、**自動ネゴシエート** および **128 ビット以上** が含まれます。

  – **自動ネゴシエート** — 暗号化強度に関係なくブラウザからの接続を許可します。ブラウザは Server Administrator Web Server と自動ネゴシエートし、セッションに使用可能な暗号化のうち最高のレベルを使用します。暗号化が弱いレガシーブラウザも、Server Administrator に接続できます。

  – **128 ビット以上** — 128 ビット以上の暗号化強度を持つブラウザからの接続を許可します。次の暗号スイートのうち 1 つが、任意の確立済みセッションのブラウザに基づいて適用できます:

```
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_RC4_128_MD5
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

  **メモ: 128 ビット以上** オプションでは、40 ビットおよび 56 ビットなど低い SSL 暗号レベルのブラウザからの接続はできません。

- **キー署名アルゴリズム（自己署名の証明書向け）** — 対応する署名アルゴリズムを選択できます。**SHA 512** または **SHA 256** を選択する場合、お使いのオペレーティングシステム/ブラウザがこのアルゴリズムをサポートすることを確認してください。必要なオペレーティングシステム/ブラウザがサポートしていないのにこれらのオプションのいずれかを選択すると、Server Administrator には ウェブページを表示できません というエラーが表示されます。このフィールドは、Server Administrator 自動生成自己署名向けです。新しい証明書を Server Administrator にインポートまたは生成した場合、ドロップダウン リストがグレーアウトされます。

- **Java ランタイム環境** — 次のオプションのいずれかを選択できます:
- **バンドル JRE** — System Administrator に付属する JRE を使用できます。
- **システム JRE** — システムにインストールされた JRE を使用できます。ドロップダウン リストから必要なバージョンを選択します。

  **メモ:** Server Administrator 実行中のシステムに JRE が存在しない場合、Server Administrator に付属の JRE が使用されます。

  **メモ:** 暗号化レベルを **128 ビット以上** に設定している場合は、同レベルまたはより高い暗号レベルのブラウザを使用して、Server Administrator の設定にアクセスしたり、その設定を変更したりすることができます。

4. **サーバープリファレンス** ウィンドウのオプション設定が完了したら、**適用** をクリックします。

   **メモ:** 変更を適用するには、Server Administrator Web Server を再起動する必要があります。

## *X.509 証明書管理*

**メモ:** 証明書を管理するには、システム管理者権限でログインする必要があります。

リモートシステムの身元を確認し、そのリモートシステムと交換する情報を他人が閲覧したり変更したりできないことを確実にするには、ウェブ証明書が必要です。システムのセキュリティを確保するには、以下を行うことが推奨されています。

- 新しい X.509 証明書の生成、既存の X.509 証明書の再使用、あるいは認証局（CA） からのルート証明書または証明書チェーンのインポートを行う。
- Server Administrator がインストールされているすべてのシステムがそれぞれ固有のホスト名を持つ。

**プリファランス** ホームページを使って X.509 証明書を管理するには、**一般設定** をクリックし、**ウェブサーバー** タブをクリックしてから **X.509 証明書** をクリックします。

使用できるオプションは次のとおりです。

- **新規証明書の生成** — Server Administrator を実行するサーバーとブラウザ間の SSL 通信のための、新しい自己署名証明書を生成します。

  **メモ:** 自己署名証明書の使用時は、この証明書がオペレーティングシステムが信頼する証明局（CA）によって署名されていないことから、多くのブラウザが *信頼できません* という警告を表示します。一部のセキュアブラウザ設定によって、自己署名 SSL 証明書がブロックされることもあります。OMSA ウェブ GUI では、そのようなセキュアブラウザのために CA 署名済み証明書を必要とします。
- **証明書メンテナンス** — 信頼済み SSL ウェブ証明書の作成を自動化するために CA が必要とする、ホストに関する証明書情報のすべてが含まれる証明書署名要求（CSR）を生成することを可能にします。必要な CSR ファイルは、証明書署名要求（CSR）ページの手順から、または CSR ページのテキストボックス内にあるテキスト全体をコピーし、CA 送信フォームにペーストすることによって取得できます。テキストは Base64 エンコードフォーマットである必要があります。

  **メモ:** また、証明書情報を表示して、使用されている証明書を他のウェブサービスへのインポートが可能なユニバーサル Base–64 エンコードフォーマットにエクスポートするオプションもあります。
- **ルート証明書のインポート** — 証明局は通常、ルート証明書ファイル（ホストのドメインネームに基づく）と、CA、ホストのルート証明書、およびリモートユーザーのウェブブラウザとオペレーティングシステム間における信頼を確立する証明書チェーンファイルの両方を発行します。大型のドメインでは、チェーンファイルは中間 CA を定義できます。まず最初にホストのルート証明書ファイル（一般的に .CER ファイルタイプ）をインポートします。次に、トップレベル CA から、オペレーティングシステムによって信頼されるあらゆる中間 CA を通して信頼チェーンを確立する、CA 発行 PKCS#7 証明書チェーン（一般的に .P7B ファイルタイプ）、最後にルートをインポートします。
- **証明書チェーンのインポート** — 信頼済み CA から PKCS#7 フォーマットでの証明書応答をインポートすることができます。

### Server Administrator Web Server の処置タブ

Server Administrator Web Server を管理するためにログインすると、次の処置タブが表示されます。

- プロパティ
- シャットダウン
- ログ
- アラート管理
- セッション管理

## Server Administrator コマンドラインインタフェースの使い方

Server Administrator コマンドラインインタフェース（CLI）を使うと、ユーザーはモニタしているシステムのオペレーティングシステムのコマンドプロンプトから必要なシステム管理タスクを実行できます。

CLI を使うと、タスクがきちんと定義されているユーザーが、システムに関する情報を迅速に取得できます。CLI を使うと、たとえば管理者がコマンドを使って、特定の時刻に実行するバッチプログラムまたはスクリプトを書くことができます。これらのプログラムを実行すると、ファン RPM のような関心のあるコンポーネントに関するレポートをキャプチャできます。さらにスクリプトを書くことにより、CLI を使ってシステム利用率が高い期間中のデータをキャプチャし、システム利用率が低い期間の同じ測定と比較できます。コマンドの結果は、ファイルに保存して後に分析できます。レポートにより、管理者は、使用パタンを調整し、新しいシステムリソースの購入を正当化し、問題のコンポーネントの正常性に焦点を当てるのに役立つ情報を入手することができます。

CLI の機能と使い方の詳細については、『*Dell OpenManage Server Administrator コマンドラインインタフェースユーザーズガイド*』（**dell.com/support/manuals**）を参照してください。

# 4

# Server Administrator サービス

Dell OpenManage Server Administrator Instrumentation Service は、システムの正常性をモニタし、業界標準システム管理エージェントにより収集された詳しい障害およびパフォーマンス情報への迅速なアクセスを提供します。レポートおよび表示機能により、システムを構成する各シャーシの総合的正常性ステータスを取得できます。サブシステムレベルでは、システムのキーポイントにおける電圧、温度、ファン RPM、およびメモリ機能を表示できます。システムの関連する各所有コスト（COO）詳細の明細アカウントは、概要ビューで表示できます。BIOS、ファームウェア、オペレーティングシステム、およびすべてのインストールされたシステム管理ソリューションのバージョン情報も取得することができます。

さらに、システム管理者は Instrumentation Service を使用して次の重要タスクを実行することができます。

- 特定の重要なコンポーネントについて最小および最大値を指定します。この値はしきい値と呼ばれ、そのコンポーネントの警告イベントが発生する値を決定します（最小および最大エラー値はシステム製造元によって指定されます）。
- 警告またはエラーイベントが発生したときのシステムの応答を指定します。ユーザーは、警告およびエラーイベントの通知に対してシステムが取る処置を設定できます。または、無休のモニタリングを使っているユーザーは、処置を指定せずに、イベントに対する最良の処置について担当者の判断に任せることもできます。
- システム名、システムのプライマリユーザー電話番号、減価償却方法、システムがリースか所有かなど、システムにユーザー指定できる値をすべて作成します。

**メモ:** 簡易ネットワーク管理プロトコル（SNMP）サービスを設定して、Microsoft Windows Server 2003 を実行中の管理下システムおよびネットワーク管理システムの両方について SNMP パケットを受け入れる必要があります。SNMP 設定の詳細に関しては、「Microsoft Windows オペレーティングシステム環境のシステムでの SNMP エージェントの設定」を参照してください。

## システムの管理

Server Administrator ホームページでは、デフォルトでシステムツリービューにシステムオブジェクトが表示されます。デフォルトで、**システム** オブジェクトは **プロパティ** タブの下に **正常性** コンポーネントが表示されます。

デフォルトでは、**プリファレンス** ホームページは **ノード設定** を開きます。

**プリファレンス** ホームページから、ユーザーとパワーユーザーの特権を持つユーザーへのアクセスの制限、SNMP パスワードの設定、ユーザーと DSM SA 接続サービスの設定ができます。

**メモ:** Server Administrator ホームページの各ウィンドウでは、状況に応じたオンラインヘルプを使用できます。 **ヘルプ**（  ）をクリックすると、表示中の特定ウィンドウについての詳しい情報を含む、独立したヘルプウィンドウが開きます。オンラインヘルプは、Server Administrator サービスの全局面を実行するのに必要な、特定の処置をガイドするよう設計されています。オンラインヘルプは、Server Administrator がお使いのシステムで検知するソフトウェアとハードウェアグループおよびユーザー権限レベルに基づいて、表示できるすべてのウィンドウで利用できます。

**メモ:** 設定可能なシステムツリーオブジェクト、システムコンポーネント、処置タブ、およびデータ領域機能の多くを表示するには、管理者またはパワーユーザー権限が必要です。さらに、管理者権限でログインしたユーザーのみが、**シャットダウン** タブに含まれるシャットダウン機能などの重要なシステム機能にアクセスできます。

# システム / サーバーモジュールツリーオブジェクトの管理

Server Administrator のシステム / サーバーモジュールツリーには、管理下システムとユーザーのアクセス権限で Server Administrator が検出するソフトウェアとハードウェアのグループに基づいて、表示可能なシステムオブジェクトがすべて表示されます。システムコンポーネントはコンポーネントの種類によって分類されています。メインオブジェクトである モジュラエンクロージャ、システム / サーバーモジュール を展開すると、システムコンポーネントの主要なカテゴリとして メインシステムシャーシ/メインシステム、ソフトウェア、ストレージ などが表示されます。

Storage Management Service がインストールされると、システムに実装されているコントローラやストレージに応じて、ストレージツリーのオブジェクトが展開され、様々なオブジェクトが表示されます。

Storage Management Service コンポーネントの詳細については、**dell.com/support/manuals** にある『*Dell OpenManage Server Administrator Storage Management ユーザーズガイド*』を参照してください。

# Server Administrator ホームページシステムツリーオブジェクト

このセクションでは、Server Administrator のホームページのシステムツリーにあるオブジェクトについて説明しています。VMware ESX および ESXi バージョン 4.X および 5.X オペレーティングシステムの制限により、OpenManage Server Administrator の前バージョンで使用可能であった機能がこのリリースで使用できない場合があります。例として次の機能があります:

- FCoE（Fibre Channel over Ethernet）機能および iSoE（iSCSI over Ethernet）機能情報
- FCoE 機能および iSoE 機能情報
- アラート管理 – アラート処置
- ネットワークインタフェース — 管理ステータス、DMA、インターネットプロトコル（IP）アドレス、
- ネットワークインタフェース — 操作ステータス
- プリファランス — SNMP の設定
- リモートシャットダウン — 先にオペレーティングシステムをシャットダウンしてからシステムをパワーサイクル
- 詳細情報 — **詳細** タブに表示されない Server Administrator コンポーネントの詳細
- 役割マップ

**メモ:** Server Administrator は、常に <mm/dd/yyyy> 形式で日付を表示します。

**メモ:** 設定可能なシステムツリーオブジェクト、システムコンポーネント、処置タブ、およびデータ領域機能の多くを表示するには、管理者またはパワーユーザー権限が必要です。さらに、管理者権限でログインしたユーザーのみが、**シャットダウン** タブに含まれるシャットダウン機能などの重要なシステム機能にアクセスできます。

## モジュラーエンクロージャ

**メモ:** Server Administrator では、モジュラーエンクロージャとは、システムツリーに個別のサーバーモジュールとして表示される 1 台、または複数台のモジュラーシステムで構成されるシステムを指します。スタンドアロンサーバーモジュールと同様に、モジュラーエンクロージャにはシステムの必須コンポーネントのすべてが装備されています。唯一の違いは、より大型のコンテナ内に少なくとも 2 つのサーバーモジュール用のスロットがあり、それぞれがサーバーモジュールと同様に完全なシステムであることです。

モジュラーシステムのシャーシ情報と Chassis Management Controller（CMC）情報を表示するには、**モジュラーエンクロージャ** オブジェクトをクリックします。

- **タブ: プロパティ**
- **サブタブ: 情報**

プロパティ タブでは、次の操作が可能です。

- 監視下のモジュラーシステムのシャーシ情報を表示する。
- 監視下のモジュラーシステムの Chassis Management Controller（CMC）に関する詳細情報を表示する。

## Chassis Management Controller にアクセスして使用する

Server Administrator ホームページから Chassis Management Controller **ログイン** ウィンドウを起動するには次の操作を行います。

1. **モジュラーエンクロージャ** オブジェクトをクリックします。
2. **CMC 情報タブ**、次に **CMC ウェブインタフェースの起動** をクリックします。CMC **ログイン** ウィンドウが表示されます。

CMC に接続すると、モジュラーエンクロージャを監視および管理することができます。

## システム/サーバーモジュールプロパティ

**システム / サーバーモジュール** オブジェクトには、メインシステムシャーシ / メインシステム、ソフトウェア、ストレージ の 3 つの主要システムコンポーネントグループがあります。Server Administrator のホームページではデフォルトでシステムツリーの **システム** オブジェクトが表示されます。ほとんどの管理機能は、**システム / サーバーモジュール** オブジェクトの処置ウィンドウから管理できます。**システム / サーバーモジュール** オブジェクトの処置ウィンドウには、ユーザーのグループ権限に応じて、**ライセンス管理**、**プロパティ**、**シャットダウン**、**ログ**、**アラート管理**、**セッション管理** などのタブがあります。

**ライセンス**

**サブタブ：情報 | ライセンス**

ライセンスのサブタブでは、次の操作が可能です。

- iDRAC（Integrated Dell Remote Access Controller）を使用して、ハードウェアのデジタルライセンスを、インポート、エクスポート、削除、交換できるようにプリファランスを設定。
- 使用中のデバイスの詳細表示。詳細には、ライセンスの状態、ライセンスの説明、資格 ID、ライセンスの有効期限があります。

  **メモ:** Server Administrator は PowerEdge 第 12 世代システム以降のライセンス機能をサポートします。この機能は、iDRAC の必要最低限のバージョンである、iDRAC 1.30.30 がインストールされている場合にのみ利用可能です。

**プロパティ**

**サブタブ：正常性 | 概要 | 資産情報 | 自動回復**

**プロパティ** タブでは、次の操作が可能です。

- **メインシステムシャーシ/メインシステム** オブジェクトおよび **ストレージ** オブジェクト内のハードウェアおよびソフトウェアコンポーネントの現在の正常性アラート状態を表示します。
- 監視されているシステムのすべてのコンポーネントの詳細な概要情報を表示します。
- 監視されているシステムの資産情報を表示および設定します。
- 監視中のシステムの自動システム回復（オペレーティングシステムのウォッチドッグタイマー）処置の表示と設定を行います。

  **メモ:** オペレーティングシステムのウォッチドッグタイマーが BIOS で有効になっていると、自動回復オプションが使えない場合があります。自動回復オプションを設定するには、必ずオペレーティングシステムのウォッチドッグタイマーを無効にしてください。

  **メモ:** 応答していないシステムをウォッチドッグが認識している場合は、設定したタイムアウト時間（n 秒）に従って自動システム回復処置が実行されないことがあります。処置の実行時間は n-h+1 ～ n+1 秒で、n は設定したタイムアウト時間、h はハートビート間隔です。ハートビート間隔の値は n < 30 の場合は 7 秒、n > 30 の場合は 15 秒です。

  **メモ:** システム DRAM Bank_1 で修復できないメモリイベントが発生した場合は、ウォッチドッグタイマー機能の動作を保証できません。修復できないメモリイベントがこの場所で発生すると、この領域の BIOS コードレジデントが破損する場合があります。ウォッチドッグ機能は BIOS への呼び出しを使ってシャットダウンまたは再起動の動作を実行するため、この機能は正常に作動しない場合があります。この問題が発生した場合は、手動でシステムを再起動する必要があります。ウォッチドッグタイマーの最大設定値は 720 秒です。

### シャットダウン

**サブタブ：リモートシャットダウン | サーマルシャットダウン | Web Server のシャットダウン**

**シャットダウン** タブでは、次の操作が可能です。

- オペレーティングシステムのシャットダウンとリモートシャットダウンのオプションを設定します。
- 温度センサーが警告またはエラー値を返したときにシステムをシャットダウンするサーマルシャットダウンの重大度レベルを設定します。

  **メモ:** サーマルシャットダウンは、センサーがレポートする温度が温度しきい値を超えた場合にのみ発生します。センサーがレポートする温度が温度しきい値を下回っても、サーマルシャットダウンは発生しません。
- DSM SA 接続サービス（Web server）をシャットダウンします。

  **メモ:** DSM SA 接続サービスがシャットダウンしても、Server Administrator はコマンドラインインタフェース（CLI）を通じて使用することができます。CLI 機能の実行に、DSM SA 接続サービスは必要ありません。

### ログ

**サブタブ：ハードウェア | アラート | コマンド**

**ログ** タブでは、次の操作が可能です。

- お使いのシステムのハードウェアコンポーネントに関連したすべてのイベントを一覧表示する、組み込みシステム管理（ESM）ログまたはシステムイベントログ（SEL）の表示。ログファイルが容量の 80 パーセントに達すると、ログ名の隣にある状態インジケータアイコンが、正常状態（  ）から非重要状態（  ）に変わります。Dell PowerEdge 第 9 および 11 世代システムでは、ログファイルの容量の 100 パーセントに達すると、ログ名の隣にある状態インジケータアイコンが、重要状態（  ）に変わります。

  **メモ:** ハードウェアのログが容量の 80 パーセントに達した際には、ログをクリアすることをお勧めします。ログが容量の 100 パーセントに達したままにしておくと、最新のイベントはログに記録されなくなります。
- センサーやその他の監視するパラメータの変更に対する応答として、Server Administrator Instrumentation Service が生成したすべてのイベント一覧のアラートログを表示します。

メモ: 各アラートイベント ID およびその説明、重大度レベル、および原因については、**dell.com/support/manuals** で、『Server Server Administrator のメッセージリファレンスガイド』を参照してください。

- **Server Administrator** ホームページまたはコマンドラインインタフェースから実行した、各コマンド一覧が入ったコマンドログを表示します。

  メモ: ログの表示、印刷、保存、E-メールでの送信方法については、「Server Administrator ログ」を参照してください。

### アラート管理

**サブタブ：アラート処置 | プラットフォームイベント | SNMP トラップ**

**アラート管理** タブでは、次の操作が可能です。

- 現在のアラート処置設定の表示と、システムコンポーネントセンサーが警告値またはエラー値を返したときに実行するアラート処置を設定します。
- 現在のプラットフォームイベントフィルタ設定を表示し、システムコンポーネントセンサーが警告値またはエラー値を返したときに実行するプラットフォームイベントフィルタ処置を設定します。**送信先の設定** オプションを使って、プラットフォームイベントのアラートが送信される先（IPv4 または IPv6 アドレス）を選択することもできます。

  メモ: Server Administrator は、グラフィカルユーザーインタフェースの IPv6 アドレスのスコープ ID を表示しません。
- インストルメント化されたシステムコンポーネントに対して現行の SNMP トラップを表示して、アラートしきい値レベルを設定します。選択したトラップは、システムが選択した重大度レベルで対応イベントを生成した場合にトリガーされます。

  メモ: すべての潜在的システムコンポーネントセンサーのアラート処置は、お使いのシステムに存在しない場合でも、**アラート処置** ウィンドウに表示されています。お使いのシステムに存在しないシステムコンポーネントセンサーに対してアラート処置を設定しても効果はありません。

  メモ: Microsoft Windows オペレーティングシステムでは、オペレーティンシステム上の **詳細システム設定 → アドバンスリカバリ** オプションを無効にして、Server Administrator 自動システム回復アラートが確実に生成されるようにする必要があります。

### セッション管理

**サブタブ：セッション**

**セッション管理** タブでは、次の操作が可能です。

- 現在 Server Administrator にログインしているユーザーのセッション情報を表示する。
- ユーザーセッションを終了する。

  メモ: 管理者権限のあるユーザーのみが **セッション管理** ページを表示したり、ログインしているユーザーのセッションを終了したりできます。

## メインシステムシャーシ / メインシステム

**メインシステムシャーシ / メインシステム** オブジェクトをクリックすると、システムの主要なハードウェアおよびソフトウェアコンポーネントを管理できます。

使用可能なコンポーネントは以下のとおりです。

- バッテリ
- BIOS
- ファン
- ファームウェア
- ハードウェアパフォーマンス
- イントルージョン
- メモリ
- ネットワーク

- ポート
- 電源管理
- 電源装置
- プロセッサ
- リモートアクセス
- リムーバブルフラッシュメディア
- スロット
- 温度
- 電圧

**メモ:** ハードウェアパフォーマンスは、Dell PowerEdge 第 10 世代以降のシステムのみでサポートされています。**電源装置** オプションは、Dell PowerEdge 1900 で使用できません。電源管理は、一部の Dell PowerEdge 第 10 世代以降のシステムでサポートされています。電源装置監視および電源監視機能は、複数のホットスワップ可能な冗長電源装置が取り付けられているシステムでのみ使用可能です。これらの機能は、電源管理回路がない恒久的に取り付けられた非冗長の電源装置には使用できません。

### メインシステムシャーシ / メインシステムプロパティ

システム / サーバーモジュールは、1 つのメインシステムシャーシで構成される場合と複数のシャーシで構成される場合があります。メインシステムシャーシ / メインシステムには、システムに不可欠なコンポーネントが含まれます。**メインシステムシャーシ / メインシステム** オブジェクト処置ウィンドウには、次の項目が含まれます:

**プロパティ**

**サブタブ：正常性 | 情報 | システムコンポーネント（FRU）| フロントパネル**

**プロパティ** タブでは、次の操作が可能です。

- ハードウェアコンポーネントおよびセンサーの正常性または状態を表示します。各表示コンポーネントの名前の横には、システム / サーバーモジュールコンポーネント状態インジケータ アイコンが表示されています。はコンポーネントが正常（通常の状態）であることを示します。はコンポーネントは警告（非重要）状態で、早急な対応が必要であることを示します。 コンポーネントがエラー（重要）状態にあり、即座な対応が必要なことを示します。 は、コンポーネントの正常性状態が不明であることを示します。監視対象にすることが可能なコンポーネントは次の通りです。

- バッテリ
- ファン
- ハードウェアログ
- イントルージョン
- ネットワーク
- 電源管理
- 電源装置
- プロセッサ
- 温度
- 電圧

**メモ:** バッテリは、Dell PowerEdge 第 9 世代および Dell PowerEdge 第 10 世代システムのみでサポートされています。**電源装置** は Dell PowerEdge 1900 では使用できません。電源管理は一部の Dell PowerEdge 第 10 世代のみでサポートされています。**電源装置監視** および **電源監視** 機能は、複数のホットスワップ可能な冗長電源装置が取り付けられているシステムでみ使用可能です。これらの機能は、電力管理回路がない恒久的に取り付けられた非冗長の電源装置には使用できません。

**メモ:** QLogic QLE2460 4Gb シングルポートファイバチャネル HBA、QLogic QLE2462 4Gb デュアルポートファイバチャネル HBA、Qlogic QLE2562 デュアルポート FC8 アダプタ、または Qlogic QLE2560 シングルポート FC8 アダプタカードが第 12 世代システムに取り付けられている場合、**システムコンポーネント（FRU）**画面は表示されません。

- ホスト名、iDRAC バージョン、Lifecycle Controller バージョン、シャーシモデル、シャーシロック、シャーシサービスタグ、Express Service Code、およびシャーシ資産タグなどのメインシステムのシャーシ属性についての情報を表示します。Express Service Code（ESC）属性は、Dell システムのサービスタグを 11 桁の数値のみのコードに変換したものです。Dell テクニカルサポートに電話する際は、この ESC を入力することにより自動的に適切な担当者が応答します。
- システムに設置されているフィールド交換可能装置（FRU）についての詳細情報を表示します（**システムコンポーネント（FRU）**サブタブ内）。
- 電源ボタンおよび非マスキング中断（NMI）ボタン（システムにある場合）という、管理下システムのフロントパネルボタンを有効または無効にします。または、管理下システムの LCD セキュリティアクセスレベルをセキュリティします。管理下システムの LCD 情報は、ドロップダウンメニューからセキュリティできます。また、**フロントパネル** サブタブからリモート KVM の標示セッションを有効にすることもできます。

### *バッテリ*

**バッテリ** オブジェクトをクリックすると、システムに取り付けられているバッテリの情報を表示できます。システムの電源がオフのときも、バッテリは時間および日付を維持します。バッテリは、システムが効率的に再起動できるよう、システムの BIOS 設定を保存します。バッテリ オブジェクト処置ウィンドウには、ユーザーのグループ権限に応じて、**プロパティ** タブおよび **アラート管理** タブなどが表示されます。

**プロパティ**

**サブタブ：情報**

**プロパティ** タブでは、システムバッテリについての現在の読み取り値および状態を表示できます。

**アラート管理**

**アラート管理** タブでは、バッテリ警告あるいは重要イベントまたは、エラーイベントが発生した時に有効にするアラートを設定できます。

### *BIOS*

**BIOS** オブジェクトをクリックして、システムの BIOS の主要機能を管理します。システムの BIOS には、キーボードとビデオアダプタなどのマイクロプロセッサと周辺デバイス間の通信、およびシステムメッセージのようなその他の機能を制御するプログラムが、フラッシュメモリチップセットに保存されています。**BIOS** オブジェクト処置ウィンドウには、ユーザーのグループ権限によって次のようなタブが表示されます。

**プロパティ** および **セットアップ**

**プロパティ**

**サブタブ：情報**

**プロパティ** タブでは BIOS 情報を表示できます。

**セットアップ**

**サブタブ：BIOS**

**メモ:** システムの BIOS セットアップタブは、システムでサポートされる BIOS 機能のみを表示します。

**セットアップ** タブでは各 BIOS セットアップオブジェクトの状態を設定できます。

多くの BIOS セットアップ機能の状態を変更できます。これにはシリアルポート、ハードディスクドライブシーケンス、ユーザーアクセス可能 USB ポート、CPU 仮想化テクノロジ、CPU ハイパースレッディング、AC 電力リカバリモード、内蔵 SATA コントローラ、システムプロファイル、コンソールリダイレクション、およびコンソールリダイレクションフェールセーフボーレートなどがありますが、これに限定されません。また、内部 USB デバイス、光学式ドライブコントローラ設定、自動システムリカバリ（ASR）ウォッチドッグタイマー、内蔵ハイパーバイザー、およびマザーボード情報の追加 LAN ネットワークポートも設定できます。さらに、トラステッドプラットフォームモジュール（TPM）およびトラステッド暗号化モジュール（TCM）設定も設定できます。

特定のシステム構成によっては、その他のセットアップ項目が表示される場合があります。ただし、いくつかの BIOS セットアップオプションは、Server Administrator でアクセスできない BIOS セットアップ画面について表示される可能性があります。

第 12 世代システムの場合、設定可能な BIOS 機能は特定のカテゴリにグループ化されています。カテゴリには、システム情報、メモリ設定、システムプロファイル設定、Unified Extensible Firmware Interface（UEFI）起動設定、ネットワークインタフェースコントローラカード、1 回限りの起動、およびスロット無効化などがあります。例えば、**システム BIOS 設定** ページで、**メモリ設定** リンクをクリックすると、システムメモリに関連する機能が表示されます。それぞれのカテゴリに移動することにより、設定を表示または変更することができます。

BIOS セットアップパスワードは、**BIOS セットアップ - システムセキュリティ** ページで設定できます。BIOS 設定を有効にして変更するには、パスワードを入力する必要があります。そうしないと、BIOS 設定は読み取り専用モードで表示されます。パスワード設定後にシステムを再起動できます。

前回のセッションからの保留値が残っている場合や、帯域外インターフェースから帯域内設定が無効化されている場合は、Server Administrator は BIOS セットアップ設定を許可しません。

**メモ:** Server Administrator BIOS セットアップ内の NIC 設定情報が、内蔵 NIC について正しくない可能性があります。BIOS セットアップ画面を使って NIC を有効/無効化すると、予期されない結果となる場合があります。内蔵 NIC の設定はすべて、システム起動中に <F2> を押すと表示される実際のシステムセットアップ画面で行うことが推奨されます。

### *ファン*

**ファン** オブジェクトをクリックしてシステムのファンを管理します。Server Administrator は rpm（毎分回転数）の測定によって各システムファンの状態を監視します。ファンプローブは rpm を Server Administrator Instrumentation Service に報告します。デバイスツリーから ファン を選択すると、Server Administrator ホームページの右側ペインのデータ領域に詳細が表示されます。ファンオブジェクト処置ウィンドウには、ユーザーのグループ権限に応じて、**プロパティ** タブおよび **アラート管理** タブなどが表示されます。

#### プロパティ

#### サブタブ：ファンプローブ

**プロパティ** タブでは、次の操作が可能です。

- システムのファンプローブの現在の読み取り値を表示して、ファンプローブ警告しきい値の最大値と最小値を設定します。

**メモ:** 一部のファンプローブフィールドは、システムで使用されているファームウェアの種類が BMC か ESM かによって異なります。一部のしきい値は BMC をベースとしたシステムでは編集できません。

- ファンコントロールオプションを選択します。

#### アラート管理

#### サブタブ：アラート処置 | SNMP トラップ

**アラート管理** タブでは、次の操作が可能です。

- 現在のアラート処置設定の表示と、ファンが警告値またはエラー値を返したときに実行するアラート処置を設定します。
- 現在の SNMP トラップアラートしきい値を表示し、ファンのアラートしきい値のレベルを設定します。選択した重大度レベルでシステムがイベントを生成した場合に、選択したトラップがトリガされます。

### *ファームウェア*

**ファームウェア** オブジェクトをクリックしてシステムファームウェアを管理します。ファームウェアは、ROM に書き込まれたプログラムまたはデータから構成されています。ファームウェアはデバイスを起動して実行できます。各コントローラには、コントローラの機能発揮を円滑にする ファームウェアが入っています。**ファームウェア** オブジェクト処置ウィンドウには、ユーザーのグループ権限に応じて、**プロパティ** タブなどが表示されます。

#### プロパティ

**サブタブ：情報**

**プロパティ** タブでは、システムのファームウェア情報を表示できます。

### *ハードウェアパフォーマンス*

**ハードウェアのパフォーマンス** オブジェクトをクリックすると、システムパフォーマンスの低下状態とその原因が表示されます。**ハードウェアのパフォーマンス** オブジェクト処置ウィンドウには、ユーザーのグループ権限に応じて、**プロパティ** タブなどが表示されます。

次の表には、状態の一覧とプローブの原因が示されています。

**表 9. 状態の可能値とプローブの原因値**

| 状態値 | 原因値 |
|---|---|
| 劣化 | ユーザー設定<br>不十分な電力容量<br>不明の原因 |
| 正常 | 該当なし |

- **プロパティ**
- **サブタブ：情報**

**プロパティ** タブで、システムのパフォーマンス低下の詳細を表示できます。

### *イントルージョン*

**イントルージョン** オブジェクトをクリックすると、システムのシャーシイントルージョンの状態を管理できます。 Server Administrator では、システム内の重要なコンポーネントへの不正アクセスを防ぐセキュリティ対策として、シャーシへのイントルージョンの状態をモニタします。シャーシイントルージョンは、システムのシャーシが開かれている、あるいは開かれたことを示します。**イントルージョン** オブジェクト 処置ウィンドウには、ユーザーのグループ権限に応じて、 **プロパティ** タブおよび **アラート管理** タブなどが表示されます。

**プロパティ**

**サブタブ：イントルージョン**

**プロパティ** タブでシャーシイントルージョンの状態を表示できます。

**アラート管理**

**サブタブ：アラート処置 | SNMP トラップ**

**アラート管理** タブでは、次の操作が可能です。

- 現在のアラート処置設定の表示と、イントルージョンセンサーが警告値またはエラー値を返したときに実行する、アラート処置の設定を行います。
- 現在の SNMP トラップアラートしきい値を表示し、イントルージョンセンサーのアラートしきい値のレベルを設定します。選択した重大度レベルのイベントをシステムが生成した場合に、選択したトラップがトリガされます。

### *メモリ*

**メモリ** オブジェクトをクリックすると、システムのメモリデバイスを管理できます。 Server Administrator では、監視中のシステムに存在する各メモリモジュールのメモリデバイス状態を監視します。 メモリデバイスの事前エラーセンサーは、ECC メモリ修正数のカウントによってメモリモジュールを監視します。また、システムでサポートされていれば、メモリ冗長性情報も監視します。**メモリ** オブジェクト処置ウィンドウには、ユーザーのグループ権限に応じて、 **プロパティ** タブや **アラート管理** タブなどが表示されます。

**プロパティ**

**サブタブ：メモリ**

**プロパティ** のタブで、メモリの冗長性状態、メモリアレイの属性、総容量、詳細、メモリデバイスの詳細、状態を表示できます。メモリデバイスの詳細では、デバイスの状態、デバイス名、サイズ、種類、速度、ラ

ンク、エラーなどのコネクタ上のメモリデバイスの詳細がわかります。ランクとは、ダイナミックランダムアクセスメモリ（DRAM）デバイスの列であり、各デュアルインラインメモリモジュール（DIMM）ごとに 64 ビットのデータで構成されています。ランクの可能な値は、シングル、デュアル、クアッド、オクタル、ヘキサ です。ランクでは、DIMM のランクを表示し、サーバー上の DIMM の保守に役立ちます。

**メモ:** スペアバンクメモリが有効になっているシステムが冗長性喪失状態に入った場合、どのメモリモジュールが原因か明らかでない場合があります。交換する DIMM を特定できない場合は、ESM システムログの検出されたスペアメモリバンクに *切り替え* というエントリを参照し、 エラーが発生したメモリモジュールを見つけてください。

**アラート管理**

**サブタブ：アラート処置 | SNMP トラップ**

**アラート管理** タブでは、次の操作が可能です。

- 現在のアラート処置設定の表示と、メモリモジュールが警告値またはエラー値を返したときに実行する、アラート処置の設定を行います。
- 現在の SNMP トラップアラートしきい値を表示し、メモリモジュールのアラートしきい値レベルを設定します。選択した重大度レベルのイベントをシステムが生成した場合に、選択したトラップがトリガされます。

## *ネットワーク*

**ネットワーク** オブジェクトをクリックして、システムの NIC を管理します。Server Administrator はシステム内の各 NIC のステータスをモニタして、リモート接続が切断されないようにします。Dell OpenManage Server Administrator は NIC の FCoE と iSoE 機能をレポートします。また、システム上ですでに設定済みの場合は、NIC チーム詳細をレポートします。複数の物理 NIC をチームにして 1 つの論理 NIC にし、管理者はこれに IP アドレスを割り当てることができます。チーム作成は NIC ベンダーツールで設定できます。たとえば、Broadcom - BACS などがあります。物理 NIC のいずれかに障害が発生しても、IP アドレスは単一の物理 NIC ではなく論理 NIC にバウンドするため、アクセスできます。チームインタフェースが設定された場合、詳しいチームプロパティが表示されます。これらの物理 NIC がチームインタフェースのメンバーである場合、物理 NIC とチームインタフェースの関係、またはその逆はもレポートされます。

Windows 2008 ハイパーバイザーオペレーティングシステムでは、Server Administrator は仮想マシンに IP を割り当てるために使用される、物理 NIC ポートの IP アドレスを報告しません。

**メモ:** デバイスが検知される順序は、デバイスの物理ポート順と一致するとは限りません。インタフェース名の下にあるハイパーリンクをクリックして、NIC 情報を表示します。

オペレーティングシステムが ESX と ESXi の場合、ネットワークデバイスはグループとみなされます。例えば、サービスコンソールによって使用される仮想イーサネットインタフェース（vswif）ならびに、ESX の VMKernel（vmknic）デバイスで使用される仮想ネットワークインタフェースおよび ESXi の vmknic デバイスなどです。

**ネットワーク** オブジェクト処置ウィンドウには、ユーザーのグループ特権によっては、**プロパティ** タブが表示されることがあります。

**プロパティ**

**サブタブ：情報**

**プロパティ** タブでは、物理 NIC インタフェースとシステムに取り付けられている チームインタフェースについての情報を表示できます。

**メモ:** Server Administrator は IPv6 アドレス セクションにリンクのローカルアドレスに加えて 2 つのアドレスのみを表示します。

## *ポート*

**ポート** オブジェクトをクリックすると、システムの外部ポートを管理できます。 Server Administrator は、システムに存在する各外部ポートの状態を管理します。

**メモ:** ブレードサーバーが取り付けられた CMC USB ポートは、OMSA では列挙されません。

**ポート** オブジェクト処置ウィンドウには、ユーザーのグループ権限に応じて、**プロパティ** タブなどが表示されます。

**サブタブ：情報**

**プロパティ**

**プロパティ** タブでは、システムの内部および外部ポート情報を表示できます。

### *電源管理*

**メモ:** 電源モニタリングおよび電源モニタリング機能は、複数の冗長、ホットスワップ可能な電源装置が取り付けられているシステムにのみ対応します。これらの機能は、電力管理回路がない永久的に取り付けられた非冗長の電源装置には使用できません。

**監視**

**サブタブ：消費量 | 統計**

**消費量** タブでは、システムの電力消費量情報をワットと BTU/hr で表示できます。

**BTU/hr=Watt X 3.413**（最も近い整数に切り捨て）

Server Administrator は消費電力とアンペアを監視し、電源の統計情報の詳細を追跡します。

また、システム瞬間的ヘッドルームとシステムピークヘッドルームも表示できます。値は、ワットと BTU/時（英国の温度単位）の両方で表示されます。電力しきい値はワットと BTU/時 で設定できます。

統計 タブでは、エネルギー消費量、システムピーク電力、システムピークアンペアなどシステムの電力追跡統計値の表示とリセットが可能です。

**管理**

**サブタブ：バジェット | プロファイル**

**バジェット** タブでは、システムアイドリング電力およびシステム最大潜在電力などの電力インベントリ属性ををワットと BTU/時 で表示できます。また、電力バジェットオプションを使って、電力キャップを有効にして、お使いのシステムに電力キャップを設定することもできます。

**プロファイル** タブでは、システムの性能を最大化し、エネルギーを節約するための電源プロファイルを選択できます。

**アラート管理**

**サブタブ：アラート処置 | SNMP トラップ**

**アラート処置** タブでは、システム電源プローブ警告やシステムピーク電力など各種のシステムイベントに対するシステムアラート処置を設定できます。

**SNMP トラップ**タブは、システムの SNMP トラップを設定するために使用します。

一部の電源管理機能は、電力管理バス（PMBus）が有効になっているシステムでしか利用できません。

### *電源装置*

**電源装置** オブジェクトをクリックして、システムの電源装置を管理します。Server Administrator は、冗長性を含む電源ステータスをモニタし、システム内の各電源装置が正しく機能していることを確認します。電源装置オブジェクト処置ウィンドウには、ユーザーのグループ権限により次のいずれかのタブが表示されます: **プロパティ** および **アラート管理**。

**メモ:** 電源装置モニタリングおよび電源モニタリング機能は、複数の冗長、ホットスワップ可能な電源装置が取り付けられているシステムにのみ対応します。これらの機能は、電力管理回路がない永久的に取り付けられた非冗長の電源装置には使用できません。

**プロパティ**

**サブタブ：要素**

**プロパティ** タブでは、次の操作が可能です。

- 電源装置の冗長性属性についての情報を表示します。
- 各電源装置要素について、ファームウェアバージョン、定格入力ワット数、および最大出力ワット数などの状態をチェックします。定格入力ワット数属性は、第 11 世代以降の PMBus システムでのみ表示されます。

**アラート管理**

**サブタブ：アラート処置 | SNMP トラップ**

アラート管理タブでは、次の操作が可能です。

- 現在のアラート処置設定の表示と、システム電源が警告値またはエラー値を返したときに実行するアラート処置の設定を行います。
- IPv6 アドレスのプラットフォームイベントアラートの宛先を設定します。
- システム電力ワット数に対して現行の SNMP トラップを表示して、アラートしきい値レベルを設定します。選択したトラップは、システムが選択した重大度レベルで対応イベントを生成した場合にトリガーされます。

**メモ:** システムのピーク電力トラップは重大度が情報のイベントのみを生成します。

*プロセッサ*

**プロセッサ** オブジェクトをクリックして、システムのマイクロプロセッサを管理します。プロセッサとは、システム内で計算を担う主要なチップであり、計算やロジック機能の実行、その解釈を統括しています。プロセッサオブジェクト処置ウィンドウには、ユーザーのグループ権限に応じて、**プロパティ** および **アラート管理** タブなどが表示されます。

**サブタブ：情報**

**プロパティ**

**プロパティ** タブでは、システムのプロセッサの情報を表示し、詳細な機能およびキャッシュ情報にアクセスできます。

**アラート管理**

**サブタブ：アラート処置**

**アラート管理** タブでは、現在のアラート処置設定の表示と、プロセッサが警告値またはエラー値を返したときに実行する、アラート処置の設定を行います。

*リモートアクセス*

**リモートアクセス** オブジェクトをクリックすることにより、ベースボード管理コントローラ（BMC）機能または統合 Dell リモートアクセスコントローラ（iDRAC）機能およびリモートアクセスコントローラ機能を管理できます。

リモートアクセスタブを選択して、BMC/iDRAC の一般情報などを管理します。また、LAN 上にある BMC/iDRAC、BMC/iDRAC のシリアルポート、シリアルポートのターミナルモード設定、シリアルオーバー LAN 接続をしている BMC/iDRAC、および BMC/iDRAC のユーザー管理などを行います。

**メモ:** BMC は Dell PowerEdge 第 9 世代システムでサポートされており、iDRAC は Dell PowerEdge 第 10 および 11 世代システムのみでサポートされています。

**メモ:** Server Administrator の稼動中に、Server Administrator 以外のアプリケーションを使用して、BMC/iDRAC を設定している場合は、Server Administrator に表示される BMC/iDRAC の設定データは、BMC/iDRAC と同期していない場合があります。Server Administrator の稼働中は、Server Administrator を使用して BMC/iDRAC の設定を行うことをお勧めします。

DRAC では、システムのリモート管理機能へのアクセスができます。Server Administrator DRAC では、操作不能なシステムへのリモートアクセス、システムがダウンした際のアラート通知、システムの再起動が可能です。

**リモートアクセス** オブジェクト処置ウィンドウには、ユーザーのグループ権限に応じて、**プロパティ** タブ、設定 タブ、**ユーザー** タブ などが表示されます。

**サブタブ：情報**

**プロパティ**

**プロパティ** タブで、リモートアクセスデバイスの一般情報を表示します。IPv4 および IPv6 アドレスの属性を表示することもできます。

**デフォルトにリセット** をクリックすると、すべての属性がシステムのデフォルト値にリセットされます。

**サブタブ：LAN | シリアルポート | シリアルオーバー LAN | 追加設定**

**構成**

BMC/iDRAC を設定する場合、設定 タブで、LAN 上の BMC/iDRAC、BMC/iDRAC のシリアルポート、およびシリアルオーバー LAN 接続の BMC/iDRAC を設定できます。

**メモ:** 追加設定 タブは、iDRAC 搭載システムでのみ表示されます。

DRAC が設定されている場合、**設定** タブでネットワークプロパティを設定できます。

**メモ:** NIC の有効化、NIC 選択、および暗号化キーフィールドは、Dell PowerEdge 第 9 世代システム上でのみ表示されます。

**追加設定** タブでは、IPv4/IPv6 プロパティを有効または無効にできます。

**メモ:** IPv4/IPv6 の有効化または無効化は、デュアルスタック環境でのみ可能です（IPv4 と IPv6 スタックがロードされている場合）。

**ユーザー**

**サブタブ：ユーザー**

**ユーザー** タブでは、リモートアクセスユーザーの設定を変更できます。Remote Access Controller ユーザーの情報の表示、ユーザーの追加、設定が可能です。

**メモ:** Dell PowerEdge 第 9 世代システムでは、次が表示されます。

- 10 個のユーザー ID の表示。DRAC カードが取り付けてある場合は、16 個のユーザー ID が表示されます。
- シリアルオーバー LAN ペイロード 列の表示。

### *リムーバブルフラッシュメディア*

内蔵 SD モジュールおよび vFlash メディアの正常性と冗長性の状態を表示するには、**リムーバブルフラッシュメディア** オブジェクトをクリックします。リムーバブルフラッシュメディアの処置ウィンドウには、**プロパティ** タブがあります。

**プロパティ**

**サブタブ：情報**

**プロパティ** タブでは、リムーバブルフラッシュメディアおよび内蔵 SD モジュールに関する情報を表示できます。この情報には、コネクタ名、その状況、そしてストレージサイズの詳細が含まれます。

**アラート管理**

**サブタブ：アラート処置 | SNMP トラップ**

**アラート管理** タブでは、次の操作が可能です。

- 現在のアラート処置設定の表示と、リムーバブルフラッシュメディアプローブが警告値またはエラー値を返したときに実行する、アラート処置を設定できます。
- 現在の SNMP トラップアラートしきい値を表示し、リムーバブルフラッシュメディアプローブのアラートしきい値のレベルを設定できます。選択した重大度レベルのイベントをシステムが生成した場合に、選択したトラップがトリガされます。

アラート管理は、内蔵 SD モジュールおよび vFlash で共通となります。SD モジュールまたは vFlash のアラート処置/SNMP/PEF を設定すると、その両方に対してこれらが自動的に設定されます。

### *スロット*

**スロット** オブジェクトをクリックすると、拡張カードなど、プリント回路基板を使用するシステム基板のコネクタまたはソケットを管理できます。スロット オブジェクト処置ウィンドウには **プロパティ** タブがあります。

**プロパティ**

**サブタブ：情報**

**プロパティ** タブでは、各スロットと取り付けられたアダプタについての情報を表示できます。

### *温度*

**温度** オブジェクトをクリックして、システムの内部コンポーネントが高温により破損しないよう、システム温度を管理します。Server Administrator は、システムのシャーシのさまざまなロケーションの温度をモニタして、シャーシ内の温度が高くなりすぎないようにします。**温度** オブジェクト処置ウィンドウには、ユーザーのグループ権限により、**プロパティ** と **アラート管理**のいずれかのタブが表示されます。

**サブタブ：温度プローブ**

**プロパティ**

- 
- 

**プロパティ** タブで、システムの温度プローブの現在の読み取り値と状況を表示したり、温度プローブの警告しきい値の最大および最小値を設定することができます。

**メモ:** いくつかの温度プローブフィールドは、システムにあるファームウェアタイプ（BMC や ESM など）によって異なります。BMC ベースのシステムでは、編集できないしきい値があります。プローブしきい値を割り当てる際、Server Administrator は入力する最小または最大値を最も近い割当可能値に四捨五入する場合があります。

**アラート管理**

**サブタブ：アラート処置 | SNMP トラップ**

**アラート管理** タブでは、次の操作が可能です。

- 現在のアラート処置設定の表示と、温度プローブが警告値またはエラー値を返したときに実行する、アラート処置を設定します。
- 温度プローブに対して現行の SNMP トラップを表示して、アラートしきい値レベルを設定します。選択したトラップは、システムが選択した重大度レベルで対応イベントを生成した場合にトリガーされます。

**メモ:** 外付けシャーシの最小および最大温度プローブしきい値は、整数のみに設定できます。最小または最大温度プローブしきい値を小数を含む値に設定しようとすると、小数点前の整数部分のみがしきい値設定として保存されます。

### *電圧*

**電圧** オブジェクトをクリックすると、システムの電圧レベルを管理できます。Server Administrator は、監視下のシステム内のシャーシの様々な位置で、重要なコンポーネントの電圧を監視します。**電圧** オブジェクト処置ウィンドウには、ユーザーのグループ権限に応じて、 **プロパティ** タブおよび **アラート管理** タブなどが表示されます。

**プロパティ**

**サブタブ：電圧プローブ**

**プロパティ** タブで、システムの電圧プローブの現在の読み取り値と状態を表示したり、電圧プローブ警告しきい値の最大および最小値を設定することができます。

**メモ:** 一部のファンプローブフィールドは、BMC または ESM など、システムで使用されているファームウェアの種類によって異なります。一部のしきい値は BMC をベースとしたシステムでは編集できません。

**アラート管理**

**サブタブ：アラート処置 | SNMP トラップ**

**アラート管理** タブでは、次の操作が可能です。

- 現在のアラート処置設定の表示と、システム電圧センサーが警告値またはエラー値を返したときに実行する、アラート処置の設定を行います。

- 現在の SNMP トラップアラートしきい値を表示し、電圧センサーのアラートしきい値レベルを設定します。選択した重大度レベルのイベントをシステムが生成した場合に、選択したトラップがトリガされます。

### ソフトウェア

**ソフトウェア** オブジェクトをクリックすると、オペレーティングシステムやシステム管理ソフトウェアなど、管理下システムの重要なソフトウェアコンポーネントの詳しいバージョン情報が表示できます。 ソフトウェア オブジェクト処置ウィンドウには、ユーザーのグループ権限に応じて、 **プロパティ** タブなどが表示されます。

**サブタブ：概要**

**プロパティ**

**プロパティ** タブでは、モニタされているシステムのオペレーティングシステムとシステム管理ソフトウェアの概要を表示できます。

### オペレーティングシステム

**オペレーティングシステム** オブジェクトをクリックすると、お使いのオペレーティングシステムに関する基本情報が表示されます。オペレーティングシステムオブジェクト処置ウィンドウには、ユーザーのグループ権限に基づいて次のタブが表示されます: **プロパティ**。

**プロパティ**

**サブタブ：情報**

**プロパティ** タブでは、オペレーティングシステムの情報を表示できます。

### 保管時

Server Administrator は、Storage Management Service を提供します。

Storage Management Service には、ストレージデバイスの設定機能があります。ほとんどの場合、Storage Management Service は、**標準的なセットアップ** を使用してインストールされています。Storage Management Service は、Microsoft Windows、Red Hat Enterprise Linux、および SUSE Linux Enterprise Server オペレーティングシステムで利用可能です。

Storage Management Service がインストールされている場合、**ストレージ** オブジェクトをクリックすると、接続している各種のアレイストレージデバイス、システムディスクなどの状態および設定が表示されます。

Storage Management Service の場合、ストレージ オブジェクト処置ウィンドウには、ユーザーのグループ権限に応じて、**プロパティ** タブなどが表示されます。

**プロパティ**

**サブタブ： 正常性**

**プロパティ** タブでは、アレイサブシステム、オペレーティングシステムディスクなど、接続しているストレージコンポーネントやセンサーの正常性や状態を表示できます。

# プリファランスの管理：ホームページ設定オプション

**プリファランス** ホームページの左ペイン（システムツリーが Server Administrator ホームページで表示されている）には、システムツリーウィンドウの使用可能な設定オプションがすべて表示されます。

使用可能な **プリファランス** ホームページ設定オプションは次の通りです。

- 一般設定
- Server Administrator

## 一般設定

**一般設定** オブジェクトをクリックすると、選択した Server Administrator 機能のユーザーと DSM SA 接続サービス（Web Server）の環境を設定できます。一般設定 オブジェクト処置ウィンドウには、ユーザーのグループ権限に応じて、**ユーザー** タブおよび **Web Server** タブなどが表示されます。

**サブタブ：プロパティ**

**ユーザー**

**ユーザー** タブでは、ホームページの外観や **電子メール** ボタン用のデフォルト電子メールアドレスなどのユーザー設定を設定できます。

- **Web Server**
- **サブタブ： プロパティ | X.509 証明書**

Web Server タブでは、次の操作が可能です。

- DSM SA 接続サービスプリファランスの設定。サーバー環境の設定方法については、「Dell Systems Management Server Administration 接続サービスおよびセキュリティ設定」を参照してください。
- IPv4 または IPv6 アドレス指定モードでの SMTP サーバーアドレスと バインド IP アドレスの設定。
- 新しい X.509 証明書の作成、既存の X.509 証明書の再利用、認証機関（CA）からルート認証や認証チェーンのインポートによる X.509 証明書の管理。証明書管理の詳細については、「X.509 証明書管理」 を参照してください。

## Server Administrator

**Server Administrator** オブジェクトをクリックすると、ユーザーまたはパワーユーザーの権限を持つユーザーによるアクセスを有効または無効にして、SNMP ルートパスワードを設定できます。**Server Administrator** オブジェクト処置ウィンドウには、ユーザーのグループ権限に応じて、**プリファランス** タブなどが表示されます。

**サブタブ：アクセス設定 | SNMP 設定**

**プリファランス**

**プリファランス** タブでは、次の操作が可能です。

- ユーザーまたはパワーユーザー権限を持つユーザーのアクセスを有効または無効にします。
- SNMP ルートパスワードを設定します。

  **メモ:** デフォルト SNMP 設定ユーザーは root、デフォルトパスワードは calvin です。
- SNMP 設定操作を設定します。

  **メモ:** SNMP Set 操作を設定した後で変更を有効にするには、サービスを再起動する必要があります。対応 Microsoft Windows オペレーティングシステムが稼動するシステムでは、Windows SNMP サービスを再起動する必要があります。対応 Red Hat Enterprise Linux および SUSE Linux Enterprise Server オペレーティングシステムが稼動するシステムでは、`srvadmin-services.sh` 再起動コマンドを実行して Server Administrator サービスを再起動する必要があります。

5

# Remote Access Controller の操作

本章では、BMC/iDRAC と DRAC のリモートアクセス機能へのアクセスおよび使用方法を説明します。

Dell Sytems Baseboard Management Controller（BMC）/Integrated Dell Remote Access Controller（iDRAC）は、システムボード上のさまざまなセンサーと通信して重要なイベントを監視し、一定のパラメータが事前設定されたしきい値を超えたときにアラートとログイベントを送信します。BMC/iDRAC は、業界標準のインテリジェントプラットフォーム管理インタフェース（IPMI）仕様に対応しており、システムをリモートで設定、監視および復旧することができます。

**メモ:** Baseboard Management Controller（BMC）は Dell PowerEdge 第 9 世代システムでサポートされ、Integrated Dell Remote Access Controller（iDRAC）は Dell PowerEdge 第 10 および 11 世代システムでサポートされています。

DRAC は、Dell システムのリモート管理機能、クラッシュしたシステムのリカバリ、電源制御機能などを提供するシステム管理ハードウェアおよびソフトウェアソリューションです。

Dell Sytems Baseboard Management Controller（BMC）/Integrated Dell Remote Access Controller（iDRAC）との通信によって、電圧、温度、およびファン速度に関連した警告やエラーが E-メールアラートとして送信されるように DRAC を設定できます。DRAC は、システムクラッシュの原因の診断を容易にするため、イベントデータのログと最近のクラッシュ画面（Microsoft Windows オペレーティングシステムが稼動するシステムのみで利用可）を記録します。

リモートアクセスコントローラは、動作不能のシステムへのリモートアクセスを行い、迅速なシステムの立ち上げ実現します。リモートアクセスコントローラは、システムがダウンしたときにアラートで通知し、システムをリモートで再起動できるようにします。さらに、リモートアクセスコントローラはシステムクラッシュの推定原因をログに記録し、*前回のクラッシュ画面*を保存します。

Remote Access Controller へは Server Administrator ホームページからログインできるほか、対応ブラウザを使ってコントローラの IP アドレスに直接アクセスすることもできます。

リモートアクセスコントローラを使用する場合、**ヘルプ** をクリックすると、表示中のウィンドウの詳細な説明が表示されます。リモートアクセスコントローラのヘルプは、ユーザーの権限レベルと、Server Administrator が管理下システムで検出する特定のハードウェアとソフトウェアのグループに基づいて、アクセス可能なすべてのウィンドウで使用できます。

**メモ:** BMC の詳細については、**dell.com/support/manuals** にある『*Dell OpenManage ベースボード管理コントローラユーティリティユーザーズガイド*』を参照してください。

**メモ:** DRAC 5 の使用方法については、**dell.com/support/manuals** にある『*Dell Remote Access Controller 5 ユーザーズガイド*』を参照してください。

**メモ:** iDRAC の設定と使用の詳細については、**dell.com/support/manuals** にある『*Integrated Dell Remote Access Contoller ユーザーズガイド*』を参照してください。

次の表は、システムに Server Administrator がインストールされている際の GUI フィールド名およびその該当システムの一覧です。

**表 10. GUI フィールド名および該当するシステム**

| GUI フィールド名 | 該当システム |
|---|---|
| モジュラーエンクロージャ | モジュラーシステム |
| サーバーモジュール | モジュラーシステム |
| メインシステム | モジュラーシステム |

| | |
|---|---|
| **システム** | 非モジュラーシステム |
| **メインシステムシャーシ** | 非モジュラーシステム |

リモートアクセスデバイスのシステムサポートの詳細については、**dell.com/support/manuals** にある『*Dell* システムソフトウェアサポートマトリックス』を参照してください。

Server Administrator では、イベントログ、電源制御、センサー状況情報へのリモートでの帯域内アクセスにより、BMC/iDRAC の設定が可能です。BMC/iDRAC と DRAC を Server Administrator グラィカルユーザーインタフェースから管理するには、**メインシステムシャーシ / メインシステム** グループのサブコンポーネントである **リモートアクセス** オブジェクトをクリックします。

次のタスクを実行できます。

- 基本情報の表示
- リモートアクセスデバイスの LAN 接続使用の設定
- リモートアクセスデバイスのシリアルオーバー LAN 接続使用の設定
- シリアルポート接続用リモートアクセスデバイスの設定
- iDRAC の追加設定
- リモートアクセスデバイスユーザーの設定
- プラットフォームのイベントフィルタアラートの設定

システムでリモートアクセス機能を提供しているハードウェアに基づいて、BMC/iDRAC または DRAC の情報を表示できます。

BMC/iDRAC と DRAC のレポートおよび設定は、`omreport/omconfig chassis remoteaccess` CLI コマンドを使って管理することもできます。

さらに Server Administrator Instrumentation Service を使用して、プラットフォームのイベントフィルタ（PEF）パラメータとアラートの送信先を管理できます。

**メモ:** BMC データは、Dell PowerEdge 第 9 世代システムのみで表示できます。

# 基本情報の表示

BMC/iDRAC、IPv4 アドレス、DRAC についての基本情報を表示できます。また、リモートアクセスコントローラの設定をデフォルト値にリセットすることもできます。リセットをするには、次の操作を行います。

**メモ:** BMC 設定をリセットするには、管理者権限でログインする必要があります。

**モジュラーエンクロージャ → システム / サーバーモジュール → メインシステムシャーシ / メインシステム → リモートアクセス** の順にクリックします。

**リモートアクセス** ページには、システムの BMC に関する次の基本情報が表示されます。

**リモートアクセスデバイス**

- デバイスの種類
- IPMI バージョン
- システム GUID
- アクティブ可能なセッション数
- 現在アクティブなセッション数
- LAN 有効
- SOL 有効
- MAC アドレス

**IPv4 アドレス**

- IP アドレスソース
- IP アドレス
- IP サブネット
- IP ゲートウェイ

**IPv6 アドレス**

- IP アドレスソース
- IPv6 アドレス 1
- デフォルトゲートウェイ
- IPv6 アドレス 2
- リンクのローカルアドレス
- DNS アドレスソース
- 優先 DNS サーバー
- 代替 DNS サーバー

**メモ: リモートアクセス** タブの **追加設定** で IPv4 と IPv6 アドレスプロパティを有効にした場合にのみ、IPv4 と IPv6 アドレスの詳細を表示できます。

# リモートアクセスデバイスの LAN 接続使用の設定

LAN 接続を通して通信するリモートアクセスデバイスを設定するには、次の操作を行います。

1. **モジュラーエンクロージャ → システム / サーバーモジュール → メインシステムシャーシ / メインシステム → リモートアクセス** オブジェクトの順にクリックします。
2. **設定** タブをクリックします。
3. **LAN** をクリックします。
   **LAN 設定** ウィンドウが表示されます。

   **メモ:** マザーボード上の LAN がネットワークアダプタのアドインカードとチーミングされている場合、BMC/iDRAC 管理トラフィックは正しく機能しません。
4. 次の NIC 設定詳細を設定します。

   - NIC の有効化（このオプションは DRAC がインストールされている場合に Dell PowerEdge 第 9 世代システムで使用可能です。NIC チーミングにはこのオプションを選択します。Dell PowerEdge 第 9 世代システムでは、冗長性を追加するために NIC をチーミングすることができます。）

     **メモ:** DRAC には内蔵 10BASE-T/100BASE-T Ethernet NIC があり、TCP/IP に対応しています。NIC のデフォルトアドレスとデフォルトゲートウェイは、それぞれ 192.168.20.1、192.168.20.1 となっています。

     **メモ:** DRAC が同一ネットワーク上の別の NIC と同じ IP アドレスに設定されていると、IP アドレスの競合が発生します。DRAC は、IP アドレスが DRAC で変更されるまで、ネットワークコマンドへの応答を中止します。DRAC は、その他の NIC の IP アドレスを変更して IP アドレスの競合が解決されても、リセットする必要があります。

     **メモ:** DRAC の IP アドレスを変更すると、DRAC がリセットされます。SNMP が DRAC が初期化される前に DRAC をポーリングすると、初期化されるまで正しい温度が伝送されないため、温度警告がログ記録されます。

     - NIC 選択

メモ: NIC 選択は、モジュラーシステムでは設定できません。

メモ: NIC 選択オプションは第 11 世代、およびそれ以前のシステムでのみ使用できます。

- プライマリーネットワークおよびフェイルオーバーネットワークのオプション

第 12 世代システムでは、リモート管理（iDRAC7）**NIC** のプライマリネットワークオプションは、**LOM1**、**LOM2**、**LOM3**、**LOM4**、および **Dedicated** (専用) となっており、フェイルオーバーネットワークオプションは、**LOM1**、**LOM2**、**LOM3**、**LOM4**、**All LOMs** (すべての LOM) および **None** (なし) となっています。
専用のオプションは iDRAC7 エンタープライズの有効なライセンスがある場合にのみ使用できます。

メモ: LOM の数はシステムまたはハードウェアの構成によって異なります。

- IPMI オーバー LAN を有効にする
- IP アドレスソース
- IP アドレス
- サブネットマスク
- ゲートウェイアドレス
- チャネル特権レベルの制限
- 新しい暗号化キー（このオプションは Dell PowerEdge 第 9 世代システムで使用可能です。）

5. 次の VLAN 設定詳細を設定します。

   メモ: VLAN 設定は iDRAC のシステムには該当しません。

   - VLAN ID を有効にする
   - VLAN ID
   - 優先順位

6. 次の IPv4 プロパティを設定します。

   - IP アドレスソース
   - IP アドレス
   - サブネットマスク
   - ゲートウェイアドレス

7. 次の IPv6 プロパティを設定します。

   - IP アドレスソース
   - IP アドレス
   - プレフィックス長
   - デフォルトゲートウェイ
   - DNS アドレスソース
   - 優先 DNS サーバー
   - 代替 DNS サーバー

   メモ: **追加設定** で IPv4 と IPv6 プロパティを有効にした場合にのみ IPv4 と IPv6 アドレスの詳細を設定できます。

8. **変更の適用** をクリックします。

# シリアルポート接続用リモートアクセスデバイスの設定

シリアルポート接続を介した通信に BMC を設定するには、次の操作を行います。

1. **モジュラーエンクロージャ → システム / サーバーモジュール → メインシステムシャーシ / メインシステム → リモートアクセス** の順にクリックします。
2. **設定** タブをクリックします。
3. **シリアルポート** をクリックします。
   **シリアルポート設定** ウィンドウが表示されます。
4. 次の詳細を設定します。
   - 接続モード設定
   - ボーレート
   - フロー制御
   - チャネル特権レベルの制限
5. **変更の適用** をクリックします。
6. **ターミナルモード設定** をクリックします。
   ターミナルモード設定 ウィンドウでは、シリアルポートのターミナルモード設定を指定できます。
   ターミナルモードは、インテリジェントプラットフォームインタフェース管理（IPMI）のメッセージ用に、シリアルポートで ASCII 文字によって出力するために使用します。ターミナルモードは、限られたいくつかのテキストコマンドにも対応して、テキストベースのレガシー環境をサポートしています。この環境は、単純なターミナルやターミナルエミュレータを使用できるように設計されています。
7. 既存のターミナルとの互換性を強化するには、次のカスタマイズを指定します。
   - ライン編集
   - 削除制御
   - エコー制御
   - ハンドシェイク制御
   - 新しいラインシーケンス
   - 新しいラインシーケンスの入力
8. **変更の適用** をクリックします。
9. **シリアルポート設定ウィンドウに戻る** をクリックすると、**シリアルポート設定** ウィンドウに戻ります。

# シリアルオーバー LAN 接続用リモートアクセスデバイスの設定

シリアルオーバー LAN（SOL）接続を介する通信用に BMC/iDRAC を設定するには、次の操作を行います。

1. **モジュラーエンクロージャ → システム / サーバーモジュール → メインシステムシャーシ / メインシステム → リモートアクセスオブジェクト** の順にクリックします。
2. **設定** タブをクリックします。
3. **シリアルオーバー LAN** をクリックします。
   **シリアルオーバー LAN 設定** ウィンドウが表示されます。
4. 次の詳細を設定します。
   - シリアルオーバー LAN を有効にする
   - ボーレート

- 必要とされる最小特権

5. **変更の適用** をクリックします。
6. **詳細設定** をクリックすると、BMC をさらに詳細に設定できます。
7. **シリアルオーバー LAN 詳細設定** ウィンドウ では、次の情報の設定が可能です。

   - 文字累積間隔
   - 文字送信しきい値

8. **変更の適用** をクリックします。
9. **シリアルオーバー LAN 設定に戻る** をクリックすると、**シリアルオーバー LAN 設定** ウィンドウに戻ります。

# iDRAC の追加設定

**追加設定** タブを使って IPv4 と IPv6 プロパティを設定するには、次の操作を行います。

1. **モジュラーエンクロージャ → システム / サーバーモジュール → メインシステムシャーシ / メインシステム → リモートアクセスオブジェクト** とクリックします。
2. **設定** タブをクリックします。
3. **追加設定** をクリックします。
4. IPv4 と IPv6 のプロパティを **有効** または **無効** に設定します。
5. **変更の適用** をクリックします。

   **メモ:** ライセンス管理についての詳細は、**dell.com/support/manuals** で『*Dell License Manager ユーザーズガイド*』を参照してください。

# リモートアクセスデバイスユーザーの設定

リモートアクセスページを使ってリモートアクセスデバイスユーザーの設定をするには、次の操作を行います。

1. **モジュラーエンクロージャ → システム / サーバーモジュール → メインシステムシャーシ / メインシステム → リモートアクセスオブジェクト** の順にクリックします。
2. **ユーザー** タブをクリックします。

   **リモートアクセスユーザー** ウィンドウには、BMC/iDRAC ユーザーとして設定できるユーザーについての情報が表示されます。
3. **ユーザー ID** をクリックすると、新規または既存の BMC/iDRAC ユーザーを設定できます。

   **リモートアクセスユーザー設定** ウィンドウでは、特定の BMC/iDRAC ユーザーを設定できます。
4. 次の一般情報を指定します。

   - **ユーザーを有効にする** を選択すると、ユーザーが有効になります。
   - **ユーザー名** フィールドにユーザーの名前を入力します。
   - **パスワードの変更** チェックボックスを選択します。
   - **新規パスワード** フィールドに新しいパスワードを入力します。
   - **新規パスワードの確認** フィールドに新しいパスワードを再入力します。

5. 次のユーザー権限を指定します。

   - LAN ユーザー権限レベルの上限を選択します。
   - 許可するシリアルポートユーザー権限の上限を選択します。
   - Dell PowerEdge 第 9 世代システムでは、**シリアルオーバー LAN の有効化** を選択してシリアルオーバー LAN を有効化します。

6. DRAC/iDRAC ユーザー権限のユーザーグループを指定します。
7. **変更の適用** をクリックして変更を保存します。
8. **リモートアクセスユーザーウィンドウに戻る** をクリックすると、**リモートアクセスユーザー** ウィンドウに戻ります。

**メモ:** DRAC がインストールされている場合、6 つの追加ユーザーエントリが設定可能です。これによりユーザー合計数は 16 になります。BMC/iDRAC および RAC ユーザーに対しても同じユーザー名およびパスワードの規定が適用されます。DRAC/iDRAC6 がインストールされると、16 のユーザーエントリすべては DRAC に割り当てられます。

# プラットフォームのイベントフィルタアラートの設定

Server Administrator Instrumentation Service を使用してプラットフォームイベントフィルタ（PEF）のパラメータやアラートの宛先などの最も関連のある BMC 機能を設定するには、次の操手順を行います。

1. **システム** オブジェクトをクリックします。
2. **警告管理** タブをクリックします。
3. **プラットフォームイベント** をクリックします。

   **プラットフォームイベント** ウィンドウでは、特定のプラットフォームイベントで個別の処置を取ることができます。シャットダウン処置を取るイベントを選択し、選択した処置に関するアラートを生成できます。また、希望する特定の送信先 IP アドレスにアラートを送信することもできます。

   **メモ:** BMC PEF アラートを設定するには、管理者特権でログインする必要があります。

   **メモ:** **プラットフォームイベントアラートの有効化** 設定で、PEF アラート生成を有効または無効にします。これは、個別のプラットフォームイベントアラート設定に依存します。

   **メモ:** **システム電源プローブ警告** と **システム電源プローブエラー** は、Server Administrator を使用して設定できますが、PMBus サポートのない Dell PowerEdge システムではサポートされていません。

   **メモ:** Dell PowerEdge 1900 システムでは、PS/VRM/D2D 警告、PS/VRM/D2D エラー、および 電源装置不在プラットフォームイベントフィルタは、Sever Administrator で設定することができますが、実際に使用することはできません。
4. シャットダウン処置を実行するか選択した処置のアラートを生成するプラットフォームイベントを選択し、**プラットフォームイベントの設定** をクリックします。

   **プラットフォームイベントの設定** ウィンドウでは、システムがプラットフォームイベントに反応してシャットダウンした場合の処置を指定できます。
5. 次の処置の 1 つを選択します。

   - **なし**
   - **システムの再起動**

     オペレーティングシステムをシャットダウンし、システムのスタートアップを開始して、BIOS チェックを行い、オペレーティングシステムをリロードします。
   - **システムの電源を切る**

     システムの電源をオフにします。
   - **システムの電源を入れ直す**

     電源のシステムをオフにしたり、一時停止したり、電源をオンにするほか、システムを再起動します。パワーサイクルは、ハードドライブなどのシステムコンポーネントを再初期化する場合に便利です。
   - **電源の低減**

     CPU をスロットルします。

**注意: なしまたは電源の低減以外のプラットフォームイベントシャットダウン処置を選択すると、指定したイベントが発生した場合にシステムが強制的にシャットダウンされます。このシャットダウンはファームウェアによって開始され、最初にオペレーティングシステムまたは実行中のアプリケーションをシャットダウンせずに行われます。**

**メモ:** 電源の低減はすべてのシステムでサポートされているわけではありません。電源モニタリングおよび電源モニタリング機能は、複数の冗長、ホットスワップ可能な電源装置が取り付けられているシステムにのみ対応します。これらの機能は、電力管理回路がない永久的に取り付けられた非冗長の電源装置には使用できません。

6. 送信するアラートの **アラートの生成** チェックボックスを選択します。

   **メモ:** アラートを生成するには、**アラートの生成** と **プラットフォームイベントアラートの有効化** 設定の両方を選択する必要があります。

7. **適用** をクリックします。
8. **プラットフォームイベントページに適用する** をクリックすると、**プラットフォームのイベントフィルタ** ウィンドウに戻ります。

## プラットフォームイベントアラート送信先の設定

プラットフォームイベントフィルタのウィンドウを使用して、プラットフォームイベント用のアラートが送信される宛先を選択します。お使いのシステムに表示される送信先の数に応じて、各送信先アドレスに個別の IP アドレスを設定することができます。プラットフォームイベントアラートは、ユーザーが設定する送信先 IP アドレスそれぞれに送信されます。

1. プラットフォームイベントフィルタのウィンドウで、**宛先の設定** をクリックします。
2. 設定する宛先の番号をクリックします。

   **メモ:** 特定のシステムで設定できる送信先の数は、システムによって異なる場合があります。

3. **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。
4. **宛先番号** をクリックして、その宛先の個々の IP アドレスを入力します。この IP アドレスは、プラットフォームイベントのアラートが送信される IP アドレスです。

   **メモ:** iDRAC7 固有のバージョンがある第 12 世代システムでは、プラットフォームイベント宛先を IPv4、IPv6、または FQDN として設定することができます。

5. 管理ステーションと管理下システム間で送信されるメッセージの認証に使用するパスワードとして機能する値を **コミュニティ文字列** フィールドに入力します。コミュニティ文字列（コミュニティ名とも呼ばれます）は、管理ステーションと管理下システム間におけるパケットごとに送信されます。
6. **適用** をクリックします。
7. **プラットフォームイベントページに戻る** をクリックすると、**プラットフォームイベントフィルタ** ウィンドウに戻ります。

6

# Server Administrator ログ

Server Administrator を使用すると、ハードウェア、アラート、およびコマンドなどのログを表示して管理できます。すべての ユーザーが Server Administrator ホームページまたはコマンドラインインタフェースからログにアクセスして、レポートを印刷できます。ログをクリアするには管理者権限でログインし、ログを指定のサービス連絡先に電子メールで送信するには管理者権限またはパワーユーザー権限でログインする必要があります。

コマンドラインからのログの表示およびレポートの作成については、**dell.com/support/manuals** にある『*Dell OpenManage Server Administrator コマンドラインインタフェースユーザーズガイド*』を参照してください。

Server Administrator ログを表示している際に、**ヘルプ**（  ）をクリックすると、表示中の特定のウィンドウについての詳細を表示できます。Server Administrator ログヘルプは、ユーザーの権限レベルと、Server Administrator が管理下システム 上で検出する特定のハードウェアおよびソフトウェアグループに応じてアクセスできる、すべてのウィンドウで利用できます。

## 組み込み機能

列見出しをクリックして、列を並べ替えるか、または列の並べ替え方法を変更します。さらに、各ログウィンドウには、システムの管理とサポートに使用できるタスクボタンがいくつか含まれます。

### ログウィンドウタスクボタン

次の表は、ログウィンドウのタスクボタンを表しています。

**表 11. ログウィンドウタスクボタン**

| Name（名前） | 説明 |
|---|---|
| 印刷 | ログのコピーをデフォルトのプリンタで印刷します。 |
| エクスポート | 各データフィールドがカスタマイズ可能な区切り文字で区切られた値を持つ、ログデータを含むテキストファイルを、指定の場所に保存します。 |
| 電子メール | ログのコンテンツが添付された電子メールメッセージを作成します。 |
| ログのクリア | ログからすべてのイベントを消去します。 |
| 名前を付けて保存 | ログの内容を **.zip** ファイル形式で保存します。 |
| 更新 | アクションウィンドウデータ領域で、ログのコンテンツを再度ロードします。 |

**メモ:** タスクボタンの使用方法については、「タスクボタン」を参照してください。

## Server Administrator ログ

Server Administrator では次のログを提供しています。

- ハードウェアログ

- アラートログ
- コマンドログ

## ハードウェアログ

Dell PowerEdge 第 9 世代および第 11 世代システムでは、システムのハードウェアコンポーネントに存在する可能性のある問題を探知するために、ハードウェアログを使用します。ログファイルの容量が 100% に達すると、ハードウェアログの状態インジケータが重要状態（  ）に変わります。システムによって、組み込みシステム管理（ESM）ログとシステムイベントログ（SEL）の 2 種類の異なるハードウェアログがあります。ESM ログと SEL はそれぞれ、システム管理ソフトウェアにハードウェアの状態メッセージを送ることができる、一組の組み込み指示です。ログに一覧表示された各コンポーネントには、名前の横に状態インジケータアイコンがあります。 次の表は状態インジケータを表しています。

**表 12. ハードウェアログの状態インジケータ**

| 状態 | 説明 |
|---|---|
| 緑のチェックマーク（  ） | コンポーネントが正常（通常の状態）であることを示します。 |
| 感嘆符のある黄色の三角形（  ） | コンポーネントは警告（非重要）状態で、早急な対応が必要であることを示します。 |
| 赤色の X 印（  ） | コンポーネントがエラー（重要）状態にあり、即座の対応が必要なことを示します。 |
| クエスチョンマーク（  ） | コンポーネントの正常性が不明であることを示します。 |

ハードウェアログにアクセスするには、**システム** をクリックし、**ログ** タブをクリックしてから、**ハードウェア** をクリックします。

ESM および SEL ログに表示される情報は次のとおりです。

- イベントの重大度
- イベントがキャプチャされた日時
- イベントの説明

### ハードウェアログの維持

ログファイルの容量が 80 % に到達すると、Server Administrator ホームページにあるログ名の隣にある状態インジケータアイコンが、正常状態（  ）から非重要状態（  ）に変わります。容量が 80 % に達したら、ハードウェアログを必ずクリアしてください。ログの容量が 100 % に達すると、最新のイベントはログに記録されなくなります。

ハードウェアログをクリアするには、**ハードウェアログ** ページで、**ログのクリア** リンクをクリックします。

## アラートログ

**メモ:** アラートログで無効な XML データ（例えば選択されたデータ用に生成された XML データの形式が正しくない場合）が表示された場合、**ログのクリア** をクリックするとログ情報が再度表示されます。

アラートログを使って、さまざまなシステムイベントをモニタします。サーバー管理者はセンサーおよびその他のモニタされたパラメータの変化に対応してイベントを生成します。アラートログに記録された各ステータス変更イベントは、特定のイベントソースカテゴリのイベント ID と呼ばれる固有の識別子と、そのイベントを説明するイベントメッセージで構成されています。イベント ID とメッセージはイベントの重大度と原因を個別に解説し、イベントのロケーションおよびモニタされたコンポーネントの以前の状態などの関連情報を提供します。

アラートログにアクセスするには、**システム** をクリックし、**ログ** タブをクリックしてから、**アラート** をクリックします。
アラートログに表示される情報は次のとおりです。

- イベントの重大度
- イベント ID
- イベントがキャプチャされた日時
- イベントのカテゴリ
- イベントの説明

**メモ:** 将来のトラブルシューティングおよび診断目的でログ履歴が必要となる場合があります。そのため、ログファイルを保存しておくことをお勧めします。

アラートメッセージの詳細については、『*Server Administrator メッセージリファレンスガイド*』（**dell.com/support/manuals**）を参照してください。

## コマンドログ

**メモ:** コマンドログで無効な XML データ（例えば選択されたデータ用に生成された XML データの形式が正しくない場合）が表示された場合、**ログのクリア** をクリックするとログ情報が再度表示されます。

コマンドログを使って、Server Administrator ユーザーが発行したすべてのコマンドをモニタします。コマンドログはログイン、ログアウト、システム管理ソフトウェアの初期化、システム管理ソフトウェアが開始したシャットダウンをトラッキングし、前回のログのクリアを記録します。コマンドログファイルのサイズは、要件に応じて指定できます。
コマンドログにアクセスするには、**システム** をクリックし、**ログ** タブをクリックしてから、**コマンド** をクリックします。
コマンドログに表示される情報は次のとおりです。

- コマンドが呼び出された日時
- Server Administrator ホームページまたは CLI に現在ログインしているユーザー
- コマンドと関連値の説明

**メモ:** 将来のトラブルシューティングおよび診断目的でログ履歴が必要となる場合があります。そのため、ログファイルを保存しておくことをお勧めします。

# 7

# アラート処置の設定

## 対応 Red Hat Enterprise Linux および SUSE Linux Enterprise Server オペレーティングシステムが実行されるシステムにおけるアラート処置の設定

イベントにアラート処置を設定する場合は、処置でサーバにアラートを表示するよう指定できます。この処置を実行するには、Server Administrator がメッセージを **/dev/console** に送信します。Server Administrator システムが X Window System を実行している場合、メッセージは表示されません。X Windows System を実行中の Red Hat Enterprise Linux システムでアラートメッセージを表示するには、イベントが発生する前に **xconsole** または **xterm -C** を起動する必要があります。X Windows System を実行中の SUSE Linux Enterprise Server システムでアラートメッセージを表示するには、イベント発生前に **xterm -C** などの端末を起動する必要があります。

イベントにアラート処置を設定する場合は、アラート処置で **メッセージをブロードキャストする** よう指定できます。このアラート処置を実行するために、Server Administrator は wall コマンドを実行します。このコマンドは、メッセージ許可が **はい** に設定されている状態でログインしているすべてのユーザーにメッセージを送信します。Server Administrator が実行されているシステムで X Window System を実行している場合、このメッセージはデフォルトで表示されません。X Window System を実行しているときにブロードキャストメッセージを表示するには、イベントが発生する前に **xterm** または **gnome-terminal** などのターミナルを起動する必要があります。

イベントにアラート処置を設定する場合は、処置で **アプリケーションを実行する** よう指定できます。Server Administrator が実行できるアプリケーションには制限があります。正しく実行するためには次の操作を行います:

- Server Administrator は X Window System ベースのアプリケーションを正しく実行できないため、この種類のアプリケーションは指定しないでください。
- Server Administrator はユーザーからの入力を必要とするアプリケーションを正しく実行できないため、そのようなアプリケーションを指定しないでください。
- 出力やエラーメッセージが見えるように、アプリケーション指定時に、**stdout** と **stderr** をファイルにリダイレクトしてください。
- アラートに対して複数のアプリケーション（またはコマンド）を実行する場合、それを実行するスクリプトを作成し、その完全パスを **アプリケーションの絶対パス** ボックスに入力します。

例 1 : `ps -ef >/tmp/psout.txt 2>&1`

例 1 のコマンドは、ps のアプリケーションを実行し、stdout を **/tmp/psout.txt** ファイルにリダイレクトして、**stderr** を **stdout** と同じファイルにリダイレクトします。

例 2 : `mail -s "Server Alert" admin </tmp/alertmsg.txt>/tmp/mailout.txt 2>&1`

例 2 のコマンドは、メールアプリケーションを実行してファイル **/tmp/alertmsg.txt** に含まれるメッセージを Red Hat Enterprise Linux ユーザーまたは SUSE Linux Enterprise Server ユーザー、および管理者に **サーバーアラート** という件名で送信します。ファイル **/tmp/alertmsg.txt** は、イベントが発生する前にユーザーが作成する必要があります。さらに、エラーの発生に備えて **stdout** および **stderr** はファイル **/tmp/mailout.txt** にリダイレクトされます。

# Microsoft Windows Server 2003 および Windows Server 2008 におけるアラート処置の設定

アラート処置を指定する場合、アプリケーションの実行機能は Visual Basic スクリプトを自動的に解釈しませんが、ファイルをアラート処置として指定するだけで、cmd、.com、.bat、または .exe ファイルを実行できます。

この問題を解決するには、まずコマンドプロセッサ cmd.exe を呼び出してスクリプトを起動します。たとえば、アプリケーションを実行するアラート処置の値は次のように設定できます。

```
c:\winnt\system32\cmd.exe /c d:\example\example1.vbs
```

ここで、d:\example\example1.vbs はスクリプトファイルへの完全パスです。

アプリケーションへの絶対パスフィールドには、対話型アプリケーション（グラフィカルユーザーインタフェースを備えたアプリケーションまたはユーザーの入力が必要なアプリケーション）のパスを設定しないでください。一部のオペレーティングシステムでは、対話型アプリケーションが意図したように動作しないことがあります。

**メモ: cmd.exe** およびスクリプトファイルの両方で完全パスを指定する必要があります。

**メモ:** Microsoft Windows 2003 は第 12 世代システムではサポートされていません。

# Windows Server 2008 でアプリケーションを実行するアラート処置の設定

セキュリティ上の理由により、Microsoft Windows Server 2008 は対話型サービスを許可しないよう設定されています。サービスが Microsoft Windows Server 2008 に対話型サービスとしてインストールされると、オペレーティングシステムは、そのサービスが対話型サービスとしてマークされたことを示すエラーメッセージを Windows System ログに記録します。

Server Administrator を使用してイベントにアラート処置を設定する場合は、処置がアプリケーションを実行するよう指定できます。アラート処置が対話型アプリケーションで適切に実行されるには、Dell Systems Management Server Administrator（DSM SA）Data Manager サービスを対話型サービスとして設定する必要があります。対話型アプリケーションの例としては、グラフィカルユーザーインタフェース（GUI）を備えたアプリケーションまたはユーザーによる入力（バッチファイルでの pause コマンドなど）を促すアプリケーションなどが挙げられます。

Server Administrator を Microsoft Windows Server 2008 にインストールした場合、DSM SA Data Manager サービスはデフォルトで非対話型サービスとしてインストールされ、デスクトップと対話できないように設定されます。したがって、アラート処置を実行する際、対話型アプリケーションは適切に実行されません。この状態でアラート処置により対話型アプリケーションが実行された場合、アプリケーションは一時停止し、入力を待ちます。アプリケーションインタフェース / プロンプトはユーザーには見えず、対話型サービス検出サービスが開始された後も見えないままとなります。タスクマネージャの **プロセス** タブには、対話型アプリケーションが実行されるたびにアプリケーションプロセスエントリが表示されます。

Microsoft Windows Server 2008 でアラート処置に対して対話型アプリケーションを実行する必要がある場合、DSM SA Data Manager サービスをデスクトップとの対話を許可するように設定し、対話サービスを有効化する必要があります。

デスクトップとの対話を許可するには、次の手順を実行します。

- **サービス**コントロールパネル で DSM SA Data Manager サービスを右クリックし、**プロパティ** を選択します。
- **ログオン** タブで、**デスクトップとの対話をサービスに許可** を選択し、**OK** をクリックします。
- 変更を適用するには、DSM SA Data Manager サービスを再起動します。
- **対話型サービス検出** が動作していることを確認します。

DSM SA Data Manager サービスがこの変更によって再起動されると、サービスコントロールマネージャは次のメッセージをシステムログに記録します。

DSM SA Data Manager サービスは、対話型サービスとしてマークされます。対話型サービス検出サービスを有効にすると、DSM SA Data Manager サービスがアラート処置に対して対話型アプリケーションを適切に実行できます。

これらの変更が適用されると、オペレーティングシステムにより、**対話型サービスダイアログ検出** ダイアログボックスが表示され、対話型アプリケーションのインタフェース / プロンプトにアクセスできるようになります。

# BMC/iDRAC プラットフォームイベントフィルタアラートメッセージ

次の表では、使用可能なすべてのプラットフォームイベントフィルタ（PEF）メッセージと、各イベントの説明を示します。

**表 13. PEF アラートイベント**

| イベント | 説明 |
|---|---|
| ファンプローブエラー | ファンの稼動速度が遅すぎるかまったく動作していません。 |
| 電圧プローブ障害 | 電圧が低すぎて適切な操作が行えません。 |
| バッテリプローブ警告 | バッテリが推奨されている充電レベル未満で稼動しています。 |
| バッテリプローブ障害 | バッテリが故障しました。 |
| 外付け電圧プローブ障害 | 電圧が低すぎて適切な操作が行えません。 |
| 温度プローブ警告 | 温度が過度の高低の限度に近づいています。 |
| 温度プローブエラー | 温度が高すぎるか低すぎて正しく動作できません。 |
| 検出されたシャーシイントルージョン | シャーシが開けられました。 |
| 冗長性（PS またはファン）が劣化 | ファンや電源装置の冗長性が低下しています。 |
| 冗長性（PS またはファン）喪失 | システムのファンおよび / または電源装置には冗長性がありません。 |
| プロセッサ警告 | プロセッサがピークパフォーマンスまたは速度以下で動作しています。 |
| プロセッサ障害 | プロセッサが故障しました。 |
| プロセッサ不在 | プロセッサが取り外されました。 |
| PS/VRM/D2D 警告 | 電源装置、電圧調整モジュールまたは DC から DC への変換機は障害が差し迫った状態です。 |
| PS/VRM/D2D エラー | 電源装置、電圧調整モジュールまたは DC から DC への変換機が故障しました。 |
| ハードウェアログが一杯または空 | ハードウェアログが満杯か空であり、システム管理者の注意が必要です。 |
| 自動システム回復 | システムがハングしているか、応答しておらず、自動システム回復によって設定された処置を実行しています。 |
| システム電源プローブ警告 | 電力消費量が障害しきい値に近づいています。 |
| システム電源プローブ障害 | 電力消費量が許容上限を超え、障害が発生しました。 |
| リムーバブルフラッシュメディア不在 | リムーバブルフラッシュメディアが取り外されました。 |

| イベント | 説明 |
| --- | --- |
| リムーバブルフラッシュメディア障害 | リムーバブルフラッシュメディアは障害が差し迫った状態です。 |
| リムーバブルフラッシュメディア警告 | リムーバブルフラッシュメディアは障害が差し迫った状態です。 |
| 内蔵デュアル SD モジュールカード重要 | 内蔵デュアル SD モジュールカードが故障しました。 |
| 内蔵デュアル SD モジュールカード警告 | 内蔵デュアル SD モジュールカードは障害が差し迫った状態です。 |
| 内蔵デュアル SD モジュールの冗長性損失 | 内蔵デュアル SD モジュールカードの冗長性が失われました。 |
| 内蔵デュアル SD モジュールカード不在 | 内蔵デュアル SD モジュールカードが取り外されました。 |

8

# トラブルシューティング

## 接続サービスエラー

Red Hat Enterprise Linux では、SELinux が強制モードに設定されている場合、Dell Systems Management Server Administrator（SM SA）接続サービスが起動できません。次の手順のいずれかを実行して、このサービスを起動してください。

- SELinux を無効モードまたは許可モードに設定する。
- SELinux の **allow_execstack** プロパティを **ON** 状態に変更します。次のコマンドを実行します:

  a. setsebool allow_execstack on
- SM SA 接続サービスのセキュリティコンテキストを変更します。次のコマンドを実行します:

```
chcon -t unconfined_execmem_t
```

**/opt/dell/srvadmin/sbin/dsm_om_connsvcd**

## ログイン失敗のシナリオ

次のような場合に、管理下システムにログインできないことがあります。

- 無効 / 誤った IP アドレス を入力した。
- 誤った資格情報 （ユーザー名およびパスワード）を入力した。
- 管理下システムがオフになっている。
- 無効な IP アドレスまたは DNS エラーにより、管理下システムに到達できない。
- 管理下システムが信頼されていない証明書を持ち、ログインページで **証明書の警告を無視する** が選択されていない。
- VMware ESX/ESXi システム上で Server Administrator サービスが有効になっていない。VMware ESXi/ESXi システム上で Server Administrator サービスを有効にする方法については、**dell.com/support/manuals** にある『*Dell OpenManage Server Administrator インストールガイド*』を参照してください。
- VMware ESX/ESXi システム上で、SFCBD（small footprint CIM broker daemon）サービスが実行されていない。
- 管理下システム上で Web Server Management サービスが実行されていない。
- **証明書の警告を無視する** チェックボックスが選択されていないにも関わらず、ホスト名ではなく管理下システムの IP アドレスを入力した。
- 管理下システムにおいて、WinRM 認証機能（リモート有効化）が設定されていない。この機能の詳細については、**dell.com/support/manuals** にある『*Dell OpenManage Server Administrator インストールガイド*』を参照してください。
- VMware ESX ESXi 4.1/5.0 オペレーティングシステムに接続中に認証エラーがある。次のいずれかの原因が考えられます。

  a. サーバーにログイン中または Server Administrator にログイン中に ロックダウン モードが有効になった。ロックダウン モードの詳細については、VMware マニュアルを参照してください。

  b. Server Administrator にログイン中にパスワードが変更された。

c. システム管理者権限なしで普通のユーザーとして Server Administrator にログインした。詳細については、VMware マニュアルで役割の割り当てに関する説明を参照してください。

# 対応 Windows オペレーティングシステムで Server Administrator のインストールエラーを修正する

再インストールを強制し、次に Server Administrator のアンインストールを実行するとインストールの不具合を修正できます。
再インストールを強制するには：

1. インストールされている Server Administrator のバージョンを特定します。
2. **support.dell.com** から、該当するバージョンのインストールパッケージをダウンロードします。
3. **srvadmin\windows\SystemsManagement** ディレクトリから **SysMgmt.msi** を見つけます。
4. コマンドプロンプトに次のコマンドを入力して、再インストールを強制します。
   ```
   msiexec /i SysMgmt.msi REINSTALL=ALL
   REINSTALLMODE=vamus
   ```
5. **カスタムセットアップ** を選択し、最初にインストールされていたすべての機能を選択します。インストールされていた機能が不明な場合は、すべての機能を選択してインストールを実行します。

   **メモ:** Server Administrator をデフォルトでないディレクトリにインストールしていた場合は、**カスタムセットアップ**においても必ずこれを変更するようにしてください。

   **メモ:** アプリケーションがインストールされた後、**プログラムの追加と削除** を使って Server Administrator をアンインストールことができます。

# OpenManage Server Administrator サービス

次の表には、システム管理情報を提供するために Server Administrator で使用されるサービスと、これらのサービスの障害による影響を示します。

**表 14. OpenManage Server Administrator サービス**

| サービス名 | 説明 | 障害の影響 | リカバリメカニズム | 重大度 |
|---|---|---|---|---|
| Windows: SM SA 接続サービス Linux: `dsm_om_connsvc`（このサービスは、Server Administrator ウェブサーバーでインストールされます。） | 対応ウェブブラウザとネットワーク接続を持つどのシステムからでも、Server Administrator にリモート / ローカルアクセスが可能です。 | ユーザーは、Server Administrator にログインできず、ウェブユーザーインタフェースで操作を実行できません。ただし、CLI は引き続き使用できます。 | サービスの再起動 | 重要 |
| Windows: SM SA 共有サービス Linux: `dsm_om_shrsvc`（このサービスは管理下システム上で実行されます。） | 起動時にインベントリコレクタを実行して、Server Administrator の SNMP と CIM プロバイダが Dell System Management Console と Dell IT Assistant（ITA）を使ってリモートソフトウェアアップデートを行うために消費する、 | ソフトウェアアップデートは ITA を使って実行できません。ただし、個別の Dell アップデートパッケージを使えば、Server Administrator 外でローカルに実行できます。アップデートは、サードパーティのツール（たとえば、 | サービスの再起動 | 警告 |

| サービス名 | 説明 | 障害の影響 | リカバリメカニズム | 重大度 |
|---|---|---|---|---|
| | システムソフトウェアのインベントリを実行します。 | MSSMS、Altiris および Novell ZENworks など）を使って行うことができます。 | | |

**メモ:** 32 ビット互換性ライブラリが 64 ビット Linux システムにインストールされていない場合、共有サービスはインベントリコレクタを起動できず、インベントリコレクタを実行するには `libstdc++.so.5` が必要です。というエラーメッセージが表示されます。 **srvadmin-cm.rpm** は、インベントリコレクタにバイナリを提供します。srvadmin-cm が依存する RPM のリストについては、*『Dell OpenManage Server Administrator インストールガイド』*（**dell.com/support/manuals**）を参照してください。

**メモ:** インベントリコレクタは、Dell Update パッケージを使った Dell コンソールをアップデートするのに必要です。

**メモ:** インベントリコレクタ機能のいくつかは、OMSA（64 ビット）でサポートされていません。

| | | | | |
|---|---|---|---|---|
| Windows: SM SA Data Manager Linux: `dsm_sa_datamgrd`（dataeng サービス下でホストされています）（このサービスは管理下システム上で実行されます。） | システムの監視、詳細なエラーとパフォーマンス情報への迅速なアクセスの提供、シャットダウン、起動、セキュリティを含む監視下システムのリモート管理の許可。 | ユーザーはこれらのサービスを実行することなく GUI/CLI 上でハードウェアレベルの詳細を設定、表示することはできません。 | サービスの再起動 | 重要 |
| SM SA Data Manager（Windows）Linux: `dsm_sa_datamgrd`（dataeng サービス下でホストされています）（このサービスは管理下システム上で実行されます。） | オペレーティングシステムとシステム管理用のファイルイベントログサービスを提供し、イベントログアナライザによっても使用されます。 | このサービスが停止されると、イベントログ機能は正しく動作しなくなります。 | サービスの再起動 | 警告 |
| Linux: `dsm_sa_datamgrd`（dataeng サービス下でホストされています）（このサービスは管理下システム上で実行されます。） | データエンジン Linux SNMP インターフェース | SNMP get/set /trap 要求は管理ステーションからは実行できません。 | サービスの再起動 | 重要 |
| Windows: `mr2kserv`（このサービスは管理下システム上で実行されます。） | ストレージ管理サービスはストレージ管理情報と、システムに接続されたローカルまたはリモートストレージを設定するための高度な機能を提供します。 | サポートされているすべての RAID および非 RAID コントローラのストレージ機能の一部には、ユーザーが実行できないものもあります。 | サービスの再起動 | 重要 |

# 9

# よくあるお問い合わせ

本項には、OpenManage Server Administrator に関してのよくあるお問い合わせ（FAQ）を掲載しています。

**メモ:** 以下の質問は、このリリースの Server Administrator に特定のものではありません。

1. **OpenManage Server Administrator から ESXi 4.x（4.0 U3）および ESXi 5.x ホスト再起動機能を実行すると失敗するのはなぜですか？**

   この問題は VMware スタンドアロンライセンス（SAL）キーに原因があります。詳細に関しては、**kb.vmware.com/kb/kb1026060** のサポート技術情報の記事を参照してください。

2. **VMware ESX 4.0 U3 または ESX 4.1 U2 オペレーティングシステムを Active Directory ドメイン に追加した後に実行する必要のあるタスクは何ですか？**

   VMware ESX 4.0 U3 および ESX 4.1 U2 オペレーティングシステムを Active Directory ドメインに追加した後、Active Directory ユーザーは次の操作を行う必要があります。

   a. VMware ESX 4.0 U3 and ESX 4.1 U2 オペレーティングシステムを実行中のシステムで Server Administrator にログインし、DSM SA 接続サービスを再起動します。

   b. リモート有効化エージェントとして VMware ESX 4.0 U3 および ESX 4.1 U2 オペレーティングシステムを使用している間に、リモートノードにログインします。sfcbd プロセスが新しいユーザーに許可を追加するまで約 5 分間待ちます。

3. **Server Administrator をインストールするのに必要な最低許可レベルは何ですか?**

   Server Administrator をインストールするには、管理者レベル権限が必要です。パワーユーザーおよびユーザーには、Server Administrator をインストールする権限がありません。

4. **Server Administrator をインストールするにはアップグレードパスが必要ですか?**

   Server Administrator バージョン 4.3 を実行しているシステムの場合、バージョン 6.*x* にアップグレードしてから、バージョン 7.*x.* にアップグレードする必要があります。4.3 以前のバージョンを実行しているシステムの場合、バージョン 4.3 にアップグレードしてから、バージョン 6.*x*、そしてバージョン 7.*x* にアップグレードする必要があります（*x* はアップグレード目標の Server Administrator バージョンを示します）。

5. **自分のシステムに適用できる Server Administrator の最新バージョンを知るにはどうしたらいいですか?**

   次の順にログインします: **support.dell.com** → Enterprise IT → マニュアル → ソフトウェア → システム管理 → OpenManage Server Administrator。

   最新ドキュメントバージョンは、利用可能な OpenManage Server Administrator のバージョンを反映しています。

6. **システムでどのバージョンの Server Administrator が実行されているかを知るにはどうしたらいいですか?**

   Server Administrator にログインした後、**プロパティ → 概要** と進みます。**システム管理** 列で、システムにインストールされている Server Administrator のバージョンがわかります。

7. **1311 以外にユーザーが使用できるポートはありますか?**

   はい、優先 https ポートを設定できます。**プリファレンス → 一般設定 → ウェブサーバー →HTTPS ポート** と進みます。

   **デフォルトを使用** の代わりに **使用** ラジオボタンを選択して、希望のポートを設定します。

**メモ:** ポート番号を無効または使用中のポート番号に変更すると、他のアプリケーションまたはブラウザが管理下システムの Server Administrator にアクセスできなくなる場合があります。デフォルトポートのリストに関しては、『*Dell OpenManage Installation およびセキュリティユーザーズガイド*』（**dell.com/support/manuals**）を参照してください。

8. **Server Administrator を Fedora、College Linux、 Mint、 Ubuntu、Sabayon、または PClinux にインストールできますか?**

   いいえ、Server Administrator はこれらのオペレーティングシステムをサポートしていません。

9. **Server Administrator に問題があった場合に電子メールを送信できますか?**

   いいえ、Server Administrator は問題があった場合に電子メールを送信するようには設計されていません。

10. **PowerEdge の ITA 検出、インベントリおよびソフトウェアアップデートに SNMP は必要ですか? 検出、インベントリ、およびアップデートに CIM 実行体を使用できますか、それとも SNMP が必要ですか?**

    ITA が *Linux システムと通信する場合* :

    検出、状態ポーリング、インベントリを行うには、Linux システム上に SNMP が必要です。

    ソフトウェアアップデートは、SSH セッションとセキュア FTP を介して行われ、それぞれの動作にルートレベルの権限 / 資格情報が必要であり、その処置を設定または要求するときにその提示を求められます。検出範囲からの資格情報は前提となりません。

    ITA が *Windows システムと通信する場合* :

    サーバー（Windows Server オペレーティングシステムが稼動するシステム）では、ITA による検出用に SNMP および CIM のいずれかまたは両方が設定されている可能性があります。インベントリには CIM が必要です。

    Linux の場合と同様に、ソフトウェアのアップデートは検出、ポーリングおよび使用プロトコルとは無関係に行われます。

    アップデートのスケジュール時または実行時に求められる管理者レベルの資格情報を使って、ターゲットシステム上のドライブに管理者（ドライブ）共有が確立され、他の場所（他のネットワーク共有など）からのファイルがターゲットシステムにコピーされます。そうすると、WMI 関数が呼び出されて、ソフトウェアアップデートを実行します。

    クライアント / ワークステーションには Server Administrator がインストールされていないため、ターゲットで OpenManage Client Instrumentation を実行するときには CIM 検出が使用されます。

    ネットワークプリンタやその他の多くのデバイスでは、デバイスとの通信（主として検出）には SNMP が標準として使用されています。

    EMC ストレージなどのデバイスには、独自のプロトコルがあります。この環境に関する情報の一部は、OpenManage マニュアルの表にある使用ポートを参照して収集できます。

11. **SNMP v3 をサポートする予定はありますか?**

    いいえ、SNMP v3 をサポートする予定はありません。

12. **ドメイン名に下線文字を含めると Server Admin へのログインに問題が生じますか?**

    はい、下線文字を含むドメイン名は無効です。その他すべての特殊文字（ハイフン以外）も無効です。大文字と小文字が区別されるアルファベットおよび数値のみを使用してください。

13. **Server Administrator のログインページ上で「Active Directory」をチェックまたはチェック解除することで、特権レベルにどのような影響がありますか?**

    Active Directory チェックボックスを選択しない場合、Microsoft Active Directory で設定したアクセス権のみを使用できます。Microsoft Active Directory で拡張スキーマソリューションを使用してログインすることはできません。

    このソリューションにより、Server Administrator にアクセスできるようになり、Server Administrator ユーザーおよび権限を Active Directory ソフトウェアに追加/制御できます。詳細に関しては、『*Dell OpenManage Server Administrator インストールガイド*』の「Microsoft Active Directory の使用」（**dell.com/support/manuals**）を参照してください。

14. **Kerberos 認証を行ってウェブサーバーからログインするときに必要な操作は何ですか?**

    認証に関して、管理下ノードの **/etc/pam.d/openwsman** と **/etc/pam.d/sfcb** ファイルの内容を以下で置き換える必要があります。

    32 ビットの場合

    ```
    auth required pam_stack.so service=system-auth auth required /lib/security/
    pam_nologin.so account required pam_stack.so service=system-auth
    ```

    64 ビットの場合

    ```
    auth required pam_stack.so service=system-auth auth required /lib64/
    security/pam_nologin.so account required pam_stack.so service=system-auth
    ```