

Dell™ OpenManage™ Server Administratorバージョン 6.0.1 ユーザーズガイド

[はじめに](#)

[バージョン 6.0.1 の新機能](#)

[設定と管理](#)

[Server Administrator の使用](#)

[Server Administrator サービス](#)

[Remote Access Controller の操作](#)

[Server Administrator ログ](#)


[警告処置の設定](#)

[トラブルシューティング](#)

[よくあるお問い合わせ \(FAQ\)](#)

[用語集](#)

メモおよび警告

 **メモ:** メモは、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:** 警告は、ハードウェアの損傷またはデータの損失の可能性を示唆し、問題を回避する方法を説明しています。

本書の内容は予告なく変更されることがあります。

© 2008 Dell Inc. All rights reserved.

Dell Inc. の書面による許可のない複製は、いかなる形態においても厳重に禁じられています。

本書で使用されている商標: Dell, DELL ロゴ, PowerEdge, PowerVault, および OpenManage は Dell Inc. の商標です。Microsoft, Windows, Internet Explorer, Active Directory, Windows Server, および Windows NT は 米国およびその他の国における Microsoft Corporation の商標または登録商標です。Java は米国およびその他の国における Sun Microsystems, Inc. の商標または登録商標です。Novell は Novell, Inc. の登録商標です。SUSE は米国およびその他の国における Novell, Inc. の登録商標です。Intel および Pentium は Intel Corporation の登録商標で、Intel386 は同社の商標です。Red Hat および Red Hat Enterprise Linux は 米国およびその他の国における Red Hat, Inc. の登録商標です。UNIX は米国およびその他の国における The Open Group の登録商標です。

Server Administrator には、Apache Software Foundation(www.apache.org)によって開発されたソフトウェアが含まれています。Server Administrator は OverLIB JavaScript ライブラリを利用しています。このライブラリは www.bosrup.com から入手できます。

商標または製品の権利を主張する事業体を表すためにその他の商標および社名が使用されていることがあります。Dell Inc. はデル以外の商標や社名に対する所有権を一切否認します。

2008 年 11 月

[目次ページに戻る](#)

警告処置の設定

Dell™ OpenManage™ Server Administratorバージョン 6.0.1 ユーザーズガイド

- [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を稼動するシステム上で警告処置を設定する](#)
- [Microsoft Windows Server 2003、Windows Server 2008 で警告処置を設定する](#)
- [BMC/iDRAC プラットフォームイベントフィルタ警告メッセージ](#)
- [サービス名を理解する](#)

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を稼動するシステム上で警告処置を設定する

イベントの警告処置を設定する場合、**サーバーで警告を表示する**処置を指定できます。この処置を実行するため、Server Administrator は `/dev/console` にメッセージを書き込みます。Server Administrator で X Window System を実行している場合、デフォルトではメッセージは表示されません。X Window System の実行中に Red Hat ® Enterprise Linux ® システムで警告メッセージを参照するには、イベント発生前に `xconsole` または `xterm -C` を起動する必要があります。X Window System の実行中に SUSE ® Linux Enterprise Server システムで警告メッセージを参照するには、イベント発生前に `xterm -C` を起動する必要があります。

イベントの警告処置を設定する場合、**メッセージをブロードキャスト**するように処置を指定できます。この処置を実行するために、Server Administrator はメッセージ権限が **はい** に設定された状態でログインしているユーザー全員にメッセージを送信する `wall` コマンドを実行します。Server Administrator で X Window System を実行している場合、デフォルトではメッセージは表示されません。X Window System の実行中にブロードキャストメッセージを表示するには、イベント発生前に `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。

イベントに警告処置を設定する場合、**アプリケーションを実行する**ように処置を指定できます。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、次のガイドラインに従ってください。

- 1 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。
- 1 Server Administrator はユーザーからの入力が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、ユーザーからの入力が必要とするアプリケーションを指定しないでください。
- 1 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。
- 1 警告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** ボックスに入力してください。

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、`/tmp/alertmsg.txt` ファイルに含まれているメッセージを Red Hat Enterprise Linux ユーザーまたは SUSE Linux Enterprise Server ユーザーまたはシステム管理者 に**サーバー警告**という件名で送信します。イベントが発生する前に、ユーザーはファイル `/tmp/alertmsg.txt` を作成する必要があります。さらに `stdout` と `stderr` は、エラーが起きた場合、ファイル `/tmp/mailout.txt` にリダイレクトされます。

Microsoft Windows Server 2003、Windows Server 2008 で警告処置を設定する


警告処置を指定するとき `.cmd`、`.com`、`.bat`、`.exe` ファイルを警告処置として実行できますが、Visual Basic スクリプトはアプリケーションの実行機能によって自動的に解釈されません。

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警告処置の値は次のようになります。

```
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のフルパスです。

アプリケーションフィールドの絶対パス内ではインタラクティブアプリケーション(グラフィカルユーザーインターフェイスを持つアプリケーションまたはユーザー入力が必要とするアプリケーション)のパスは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インタラクティブアプリケーションは予想通りに動作しないことがあります。

 **メモ:** `cmd.exe` ファイルとスクリプトファイルは両方共、フルパスを指定してください。

BMC/iDRAC プラットフォームイベントフィルタ警告メッセージ

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 [表 8-1](#) に示します。

表 8-1 PEF 警告イベント

イベント	説明
ファンロープエラー	ファンの稼動速度が遅すぎるかまったく稼動していません。

電圧ブロープエラー	電圧が低すぎて適切な操作が行えません。
離散的電圧ブロープエラー	電圧が低すぎて適切な操作が行えません。
温度ブロープ警告	温度が高温、低温の限界に近づいています。
温度ブロープエラー	温度が高すぎるか低すぎて適切な操作が行えません。
シャーシイントリージョンが検出されました	シャーシが開けられました。
冗長性 (PS またはファン) が低下しています。	ファンおよび / または電源装置の冗長性が少なくなりました。
冗長性 (PS またはファン) が低下しています。	システムのファンおよび / または電源装置の冗長性が残っていません。
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実行されています。
プロセッサエラー	プロセッサが失敗しました。
PPS/VRM/DcToDc 警告	電源装置、電圧調整モジュールまたは DC ツー DC 変換機でエラー条件が保留になっています。
電源装置 / VRM/D2D エラー	電源装置、電圧調整モジュールまたは DC ツー DC 変換機が失敗しました。
ハードウェアログが一杯または空です。	ハードウェアログがいっぱいか空のため、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。
システム電源ブロープ警告	電力消費量がエラーしきい値に近づいています。
システム電源ブロープエラー	電力消費量が許容上限を超え、エラーが発生しました。

サービス名を理解する

次のサービスのサービス実行ファイルおよび表示名が変更されました。

表 8-2 サービス名

目的	サービス名	旧リリース (5.0 以前)	現在のリリース
Web Server			
	表示名	セキュリティ保護されたポートサーバー	DSM SA 接続サービス
	実行ファイル名	Omaaws[32 64]	dsm_om_connsvc[32 64]
			dsm_om_connsvc
スケジュールまたは通知			
	表示名	OM 一般サービス	DSM SA 共有サービス
	実行ファイル名	Omsad[32 64]	dsm_om_shrsvc[32 64]
			dsm_om_shrsvc

[目次ページに戻る](#)

[目次ページに戻る](#)

トラブルシューティング

Dell™ OpenManage™ Server Administratorバージョン 6.0.1 ユーザーズガイド

- [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](#)
- [OpenManage Server Administrator サービス](#)

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、Server Administrator のアンインストールを実行することによりインストールエラーを修正することができます。

再インストールを強制するには:

1. 過去にインストールされた Server Administrator のバージョンを検索します。
2. そのバージョンのインストールパッケージを Dell™ サポートサイト support.dell.com からダウンロードします。
3. `srvadmin\windows\SystemManagement` ディレクトリから `SysMgmt.msi` を指定します。
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、インストールされていた機能をすべて選択します。どの機能がインストールされているか定かでない場合は、すべての機能を選択してから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る場合は、必ず**カスタムセットアップ**においてもこれを変更するようにしてください。

6. 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機能を使って Server Administrator をアンインストールすることができます。

OpenManage Server Administrator サービス

この表には、システム管理情報を提供するために OMSA で使用されるサービスとこれらのサービスの失敗による影響を示します。

サービス名	説明	失敗の影響	回復の仕組み	Severity
Windows: DSM SA 接続サービス Linux: dsm_om_connsvc	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 OMSA にリモート / ローカルアクセスが可能です。	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 OMSA にリモート / ローカルアクセスが可能です。	再起動サービス	重要
共通サービス				
Windows: DSM SA 共有サービス Linux: dsm_om_shrsvc	起動時にインベントリコレクタを実行して、OMSA 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システムソフトウェアのインベントリを実行します。	ソフトウェアアップデートは ITA を使って行うことはできません。ただし、個々の Dell アップデートパッケージを使って OMSA のローカルおよび外部でアップデートを行うことはできます。アップデートはサードパーティツール (MSSMS、Altiris、Novell ZENworks など) を使って行うことができます。	再起動サービス	警告
計装サービス				
Windows: DSM SA データマネージャ Linux: dsm_sa_datamgr32d (dataeng サービス下でホスト)	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。	再起動サービス	重要
DSM SA イベントマネージャ (Windows) Linux: dsm_sa_eventmgr32d (dataeng サービス下でホスト)	OS 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。	再起動サービス	警告

ト)				
Linux: dsm_sa_snmp32d (dataeng サービス下でホスト)	データエンジン Linux SNMP インタフェース	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。	再起動サービス	重要
Storage Management Service				
Windows: mr2kserv	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。	ユーザーは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を実行するわけではありません。	再起動サービス	重要


[目次ページに戻る](#)

[目次ページに戻る](#)

よくあるお問い合わせ(FAQ)

Dell™ OpenManage™ Server Administratorバージョン 6.0.1 ユーザーズガイド

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

 **メモ:** これらの質問はこのリリースの Server Administrator のみに関するものではありません。

1. OMSA をインストールするために最小限必要な権限レベルは何ですか。

OMSA をインストールするには最小限、**システム管理者**の権限レベルが必要です。パワーユーザーやユーザーは OMSA をインストールする権限を持ちません。

2. OMSA 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。

バージョン 4.3 がインストールされているシステムでは、アップグレードパスは必要ありません。バージョン 4.3 より古いバージョンがインストールされているシステムでは、まずバージョン 4.3 にアップグレードしてから、バージョン 5.x (x はアップグレードしたい OMSA のバージョン番号)にアップグレードする必要があります。

3. システムで使用可能な OMSA の最新バージョンを知るにはどうしますか。

support.dell.com ->製品サポート->製品マニュアル->ソフトウェア->Systems Management ->Dell OpenManage Server Administrator の順にアクセスします。

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。

4. システムでどのバージョンの OMSA が実行されているか知るにはどうしますか。

回答:Server Administrator にログインした後、**プロパティ**->**概要** にアクセスします。Systems Management 行にシステムにインストールされている Server Administrator のバージョンが表示されます。

5. 1311 以外にユーザーが使用できるポートはありますか。

回答:はい、任意の https ポートを使用するように設定できます。**プリファランス** ->**一般設定**->**Web Server**->**HTTPS ポート** の順にアクセスします。

デフォルトの使用 の代わりに**ラジオボタン**の使用をクリックして任意のポートに設定します。

ポート番号を、無効な番号または使用中のポート番号に変更すると、その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。デフォルトポートの一覧は、『Dell OpenManage インストールとセキュリティユーザーズガイド』を参照してください。

6. OMSA を Fedora, College Linux, Mint, Ubuntu, Sabayon, PCLinux にインストールできますか。

回答: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。

7. OMSA に問題があった場合に電子メールを送信できますか。

回答: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。

8. PowerEdge™ システム上での ITA 検出、インベントリ、ソフトウェアアップデートを行うには SNMP が必要ですか。CIM だけで検出、インベントリ、アップデートできますか、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。

Dell 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、その動作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引き継がれません。

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を実行しているシステム)では、ITA による検出用に SNMP や CIM が設定されているとは限りません。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。その後 WMI 関数が呼び出されてソフトウェアアップデートが実行されます。

クライアント / ワークステーションでは OMSA はインストールされていないので、ターゲットが OpenManage クライアントの計装を実行するとき 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)にはいまだに SNMP 規格が使用されています。

EMC ストレージなどのデバイスでは専用プロトコルが使用されています。この環境についての情報は、OpenManage マニュアルの使用ポートの表を参照してください。

9. SNMP v3 をサポートする予定はありますか。

いいえ、このリリースでは SNMP v3 をサポートする予定はありません。

10. **ドメイン名に下線を含めると Server Admin へのログインに問題が生じますか。**

はい、ドメイン名には下線は使用できません。その他の特殊文字(ハイフン以外)もすべて無効です。英数字のみを使用してください。なお、大文字と小文字は区別されます。

[目次ページに戻る](#)

[目次ページに戻る](#)

用語集

Dell™ OpenManage™ Server Administratorバージョン 6.0.1 ユーザーズガイド

以下に、システムドキュメントで使用される技術用語、略語、頭字語の定義を示します。

BMC

ベースボード管理コントローラの省略。このコントローラは IPMI 構造にインテリジェンスを提供します。

BTU

英国熱量単位 (British thermal unit) の略語。

CA

認証局 (Certification authority) の略語。

CHAP

Challenge-Handshake Authentication Protocol の略語。PPP サーバーが使用している認証スキームで、接続時またはそれ以降に、接続元の一致を確認します。

CIM

DMTF からの管理情報について説明したモデル、Common Information Model の頭字語。CIM は実装に依存しないため、異なる管理アプリケーションでさまざまなソースから必要なデータを収集できます。CIM にはシステム、ネットワーク、アプリケーションおよびデバイスのスキーマが含まれ、新しいスキーマが追加されます。CIM は、CIM データを SNMP エージェントの MIB データで置き換えるためのマッピング方法を提供します。

CLI

コマンドラインインタフェース (Command Line Interface) の略語。

CMC

シャーシ管理 コントローラの頭字語

DBPM

デマンドベースの電源管理 (Demand Based Power Management) の略語。

DHCP

ダイナミックホスト設定プロトコル (Dynamic Host Configuration Protocol) の略語。このプロトコルは IP アドレスをローカルエリアネットワーク (LAN) のコンピュータに動的に割り当てる手段を提供します。

DIMM

デュアルインラインメモリモジュール (Dual in-line memory module) の略語。DRAMチップを持つ小さな回路基板で、システム基板に接続します。

DMTF

分散管理タスクフォース (Distributed Management Task Force) の略語。企業およびインターネット環境でシステム管理の標準規格を開発、保守するためにハードウェアとソフトウェアプロバイダが集まって形成した企業コンソーシアム。

DRAC 4

Dell™ Remote Access Controller 4 の頭字語。

DRAC 5

Dell™ Remote Access Controller 5 の頭字語。

DRAM

ダイナミックランダムアクセスメモリ (Dynamic random-access memory) の頭字語。通常、システムの RAM は DRAM チップのみで構成されます。DRAM チップは無限に充電状態を保存できないため、システムは各 DRAM チップを継続的にリフレッシュします。

DSM SA 接続サービス

Dell Systems Management Server Administration の頭字語。HTTPS プロトコルを使って、ウェブページをウェブブラウザで表示可能にするアプリケーション。「[ウェブサーバー](#)」を参照してください。

ECC

誤り検出訂正 (Error checking and correction) の略語。

EMC

電磁環境適合性 (Electromagnetic Compatibility) の略語。

EMI

電磁妨害 (Electromagnetic interference) の略語。

EMM

拡張メモリマネージャ (Expanded memory manager) の略語。Intel386? 以上のマイクロプロセッサで拡張メモリをエミュレートする拡張メモリを使用するユーティリティ。

ERA

埋め込みリモートアクセス (Embedded Remote Access) の略語。

ERA/MC

埋め込みリモートアクセスモジュラーコンピュータ (Embedded Remote Access Modular Computer) の略語。[モジュラシステム](#)を参照してください。

ERA/O

埋め込みリモートアクセスオプション (Embedded Remote Access Option) の略語。

ESM

埋め込みシステム管理 (Embedded systems management) の略語。

FRU

フィールド置換可能ユニット (Field Replaceable Unit) の略語。

HPFS

Windows NTオペレーティングシステムの、高性能ファイルシステム (High Performance File System) オプションの略語。

HTTP

ファイル転送プロトコル(File transfer protocol)の略語。HTTP は Web 上で HTML 文書のやり取りに使用されるクライアントサーバー TCP/IP プロトコルです。

HTTPS

ハイパーテキスト転送プロトコル、セキュリティ(HyperText Transmission Protocol, Secure)の略語。HTTPS は HTTP のセキュリティ強化版で、ウェブブラウザがセキュリティ保護されたトランザクションを処理するのに使用されます。HTTPS は、SSL が HTTP下にある固有のプロトコルです。HTTP URL で SSL を持つものには "https://" を、SSL のない HTTP URL には引き続き "http://" を使用する必要があります。

iDRAC

Integrated Dell Remote Access Controller の頭字語。

iDRAC6 Enterprise

高度な機能と iDRAC への専用ネットワーク通信用の SD カードを含むオプションカードです。

iDRAC6 Express

オプションのストレージカードです。その存在は、AMEA カードの詳細情報の一部としてスロットページに表示されます。

IP アドレス

インターネットプロトコルアドレス(Internet protocol address)の略語。「TCP/IP」を参照してください。

IPMI

Intel アーキテクチャに基づいた企業用コンピュータの周辺機器管理の業界標準である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(Intelligent Platform Management Interface)の略語。IPMI の主な特徴は、インベントリ、モニター、ログおよび回復制御機能が、メインのプロセッサ、BIOS、およびオペレーティングシステムと関係なく提供されていることです。

IPv6

Internet Protocol version 6.

IRQ

割り込み信号(Interrupt request)の略語 周辺デバイスによってデータ送受信される信号は、IRQ 回線を通じてマイクロプロセッサに送られます。各周辺接続には IRQ 番号が割り当てられる必要があります。たとえば、システムの最初のシリアルポート(COM1)はデフォルトで IRQ4 に割り当てられます。2 つの機器が同じ IRQ 番号を共有することはできませんが、両方の機器を同時に動作させることはできません。

iSCSI

インターネット SCSI の頭字語。データストレージ機能にリンクする IP ベースストレージネットワーク基準。IP ネットワーク上に SCSI コマンドを実行すると、iSCSI を使用して、インターネット上のデータ転送および離れた場所のストレージの管理が行われます。

JSSE

Java? Secure Socket Extension の略語。

Kerberos

ネットワーク認証プロトコル。秘密鍵暗号を用いて、クライアント / サーバーアプリケーションのための強固な認証システムを提供するように設計されています。

LDAP

軽量ディレクトリアクセスプロトコル(Lightweight Directory Access Protocol)の略語。TCP/IP 上で実行しているディレクトリサービスを検索したり、変更したりするためのネットワークプロトコル。

LPT n

システム上にある1～3番目のパラレルポートのデバイス名は、LPT1、LPT2、LPT3です。

LRA

ローカルレスポンスエージェント(local response agent)の略語。

MIB

管理情報ベース(management information base)の頭字語。MIB を使用して、SNMP管理デバイスに状態/コマンドの詳細を送受信します。

MOF

Managed Object Format の頭字語。これは ASCII ファイルで、CIM スキーマの正式な定義が含まれます。

NIC

network interface controller の頭字語。

NTFS

NT File System(NTファイルシステム)。Windows NTオペレーティングシステムのオプションです。NTFS は、Windows NT オペレーティング システム内で使用するよう特別に設計された高度なファイルシステムです。ファイルシステムの回復、大きなストレージ メディア、および長いファイル名をサポートしています。また、ユーザー定義アトリビュートとシステム定義アトリビュートを使ってすべてのファイルをオブジェクトとして処理することにより、オブジェクト指向のアプリケーションもサポートしています。FAT と FAT32 も参照してください。

NTLM

Windows NT LAN Manager の略語。NTLM は、Windows NT オペレーティング システムのセキュリティ プロトコルです。

NUMA

Non-Uniform Memory Architecture の略語。

OID

object identifier の略語。オブジェクトを一意に識別する、実装固有の整数またはポインタ。

PAM

Pluggable Authentication Modules の頭字語 PAM を使うと、システム管理者は認証プログラムをコンパイルし直さずに、認証ポリシーを設定することができます。

PERC

Expandable RAID controller の頭字語。

PKCS #7

公開鍵暗号標準(Public Key Cryptography Standard)#7 の略語。PKCS #7 は、認証チェーンなどの署名データをカプセル化した、RSA Data Security, Inc.の標準です。

PMBus

電源管理バス(Power Management Bus)の略語。

ppm

1分あたりのページ数(pages per minute)の略語。

PPP

Point-to-Point Protocol の略語。

PS

電源装置(power supply)の略語。

RAC

Remote Access Controller の頭字語。

RAID

Redundant Array of Independent Disks の頭字語

RBAC

Role-based access control の略語。

ROM

読み取り専用メモリ(read-only memory)の頭字語。コンピュータのプログラムの中には、ROM コードで実行しなければならないものがあります。RAM と違って ROM チップの内容は、システムの電源を切った後も保持されます。ROM コードの例として、コンピュータのブートルーチンと POST を起動するプログラムなどが挙げられます。

RPM

Red Hat® Package Manager の略語。

SAS

セキュア認証サービス(Secure Authentication Services)またはシリアル付き SCSI(Serial-attached SCSI)の頭字語。セキュリティプロトコルまたは認証について言及している場合、SAS はセキュア認証サービスを意味します。細径ケーブルでのデジタルデータ転送にシリアル(1 回につき 1 ビット)方法を使用するコンピュータ周辺機器について言及している場合、SAS は、シリアル付き SCSIを意味します。

SCSI

小型コンピュータシステムインタフェース(small computer system interface)の頭字語。通常のポートよりも速いデータ転送レートを持つ I/O バスインタフェース。1 つの SCSI インタフェースに最大 7 個(新しいSCSIタイプによっては15個)のデバイスを接続できます。

SEL

システムイベントログ(system event log)の略語。

SMART

Self-Monitoring Analysis and Reporting Technology。ハードディスクドライブにエラーや障害があった場合に、システム BIOS が報告し、画面にエラーメッセージを表示するための技術です。この技術を利用するには、SMART 準拠のハードディスクドライブおよびシステム BIOS のサポートが必要です。

SMTP

Simple Mail Transfer Protocol の略語。

SNMP

シンプルネットワーク管理プロトコル(Simple Network Management Protocol)の略語。一般的なネットワーク管理 / 監視プロトコルである SNMP は、TCP/IP プロトコル スイートの一部です。SNMP は、ネットワークサーバーやルータなど異なるネットワークデバイスについての重要な情報を管理アプリケーションに送る形式を提供します。

SSL

secure socket layer の略語。

TCP/IP

Transmission Control Protocol/Internet Protocol の略語。実行中の Windows と UNIX など、異なるシステムを含むコンピュータ ネットワークで情報を転送するシステム。

TFTP

Trivial File Transfer Protocol の略語。TFTP は TCP/IP FTP プロトコルのバージョンの 1 つで、ディレクトリ機能もパスワード機能もありません。

TPM

Trusted Platform Module の頭字語

UART

Universal asynchronous receiver transmitter の頭字語。シリアルポートを構成する電子回路。

URL

Uniform Resource Locator(以前の名称は Universal Resource Locator)の略語。

USB

Universal Serial Bus の略語。USB コネクタは、マウス、キーボード、プリンタ、スピーカなど、USB 準拠の複数のデバイスに対応しています。また、USB デバイスはシステムの 実行中に取り付けたり取り外したりすることができます。

UUID

ユニバーサル固有識別(Universal Unique Identification)の略語。

VRM

電圧変換モジュール(Voltage Regulator Module)の略語。

WH

watt-hour(s)(1 時間当たりのワット数)の略語。

WMI

Windows Management Instrumentation の略語。WMI は CIM オブジェクトマネージャサービスを提供します。

X Window System

Linux® ベースのディストリビューションで使用するグラフィックユーザーインターフェース。

X.509 証明書

X.509 証明書は公開暗号鍵を ID またはその他の主体の属性に結合します。主体は人々、アプリケーションコード(署名アプレットなど)または一意に識別されたその他のエンティティ(DSM SA Connection Service またはウェブサーバーなど)である可能性があります。

Xen

Xen は x86 システム用の仮想マシンモニタです。

XMM

拡張メモリアネージャ(eXtended Memory Manager)の略語。XMM は、アプリケーションプログラムやオペレーティングシステムで、XMS に準拠する拡張メモリを使用できるようにするユーティリティです。

XMS

拡張メモリ仕様(eXtended Memory Specification)の略語。

ZIF

ゼロ圧力(zero insertion force)の頭字語。一部のコンピュータでは、ZIF ソケットや ZIF コネクタを使用して、デバイス(プロセッサチップなど)の取り付けや取り外しを行うときにデバイスに圧力が加からないようにします。

ZIP

Imega? 提供の 3.5 インチのリムーバブルディスクドライブ。基本的に 100 MB のリムーバブル カートリッジを使用します。ドライブは、ディスクをカタログ化してセキュリティのためにファイルをロックするソフトウェアとバンドルされています。250 MB バージョンの Zip ドライブも 100 MB の Zip カートリッジに読み書きします。

ウェブサーバー

HTTP プロトコルを使って、ウェブページをウェブブラウザで表示可能にするアプリケーション。

コントローラ

マイクロプロセッサとメモリ間、マイクロプロセッサとディスクドライブやキーボードなど、周辺デバイス間のデータ転送を管理するチップ。

コントロールパネル

電源スイッチ、ハードドライブアクセスインジケータ、および電源インジケータなど、インジケータとコントロールを含むシステムの一部。

サーバーモジュール

ローカルシステムとして機能するモジュラスシステム部品。システムとして機能するには、サーバーモジュールは、電源装置、ファン、システム管理モジュール、および最低 1 つのネットワークスイッチモジュールを含んだシャーシに挿入されます。電源装置、ファン、システム管理モジュール、およびネットワークスイッチモジュールは、シャーシにあるサーバーモジュールの共有リソースです。[モジュラスシステム](#)を参照してください。

しきい値

温度、電圧、電流およびファン速度などを監視するセンサーを備えたシステム。センサーのしきい値は、センサーが通常、非重要、重要または危険状態で稼働しているかを決定する範囲(最小値と最大値)を指定します。Server Administrator 対応のしきい値は次のとおりです。

- 1 致命的しきい値上限
- 1 重要しきい値上限
- 1 非重要しきい値上限
- 1 標準
- 1 非重要しきい値下限
- 1 重要しきい値下限
- 1 致命的しきい値下限

システムメモリ

RAM の同義語。

システム基板

コンピュータの主要な回路ボードであるシステム基板には、次に示すような、ほとんどの集積コンポーネントが搭載されています。

- 1 マイクロプロセッサ
- 1 RAM
- 1 標準的な周辺機器(キーボードなど)のコントローラ
- 1 さまざまな ROM チップ

システム基板は、マザーボード および論理ボード と呼ばれることもあります。

シリアル ポート

一般的には、モデムをコンピュータに接続するのに使用される I/O ポート。コンピュータのシリアルポートは、9 ピンのコネクタが使用されていることで識別できます。

シンタックス(構文)

コンピュータによって正しく認識されるように、コマンドや命令を入力する方法を指示する規則。変数のシンタックスはそのデータタイプを示します。

スイッチ

コンポーネントのシステム基板のスイッチは、コンピュータシステムでのさまざまな回路機能を制御します。これらのスイッチは DIP スイッチ として知られています。通常、DIP スイッチは 2 つ以上のスイッチがパッケージ化されており、プラスチックのケースに入っています。システム基板には、スライド スイッチとロッカー スイッチの 2 個の DIP スイッチが使われています。スイッチの名前は、設定(オン/オフ)の変更方法に基づいています。

ステータス

オブジェクトの健康や機能の状態を指します。たとえば、プローブが許容温度内の場合には、温度プローブは正常状態です。ユーザーが設定した制限温度をこえた値がプローブによって読み取られると、重要ステータスが報告されます。

セットアップユーティリティ

コンピュータのハードウェアを構成し、パスワード保護機能や省電力設定などを設定することでコンピュータの動作をカスタマイズするための BIOS プログラム。セットアップユーティリティのオプションの中には、コンピュータを再起動しないと(自動的に再起動する場合があります)ハードウェア設定の変更が有効にならないものがあります。セットアップユーティリティは NVRAM に保存されるため、設定は再度変更しない限り有効に維持されます。

タイムアウト

省電力機能が起動されるまでのシステムのアイドル時間。

テーブル

SNMP MIB では、テーブルは管理オブジェクトを構成する変数について説明した 2D の配列です。

パラメータ

プログラムに対して指定する値またはオプション。パラメータは、スイッチまたは引数 と呼ばれることもあります。

ピークヘッドルーム

電源装置によって使用された論理最大電力からピーク電力消費量を差し引いたもの。

ヒートシンク

熱を発散させるための金属釘または金属リブが付いた金属板。ほとんどのマイクロプロセッサは、このヒートシンクを装備しています。

ファームウェア

読み取り専用メモリ (ROM) に書き込まれたソフトウェア (プログラムまたはデータ)。ファームウェアはデバイスの起動や操作を実行できます。各コントローラにはコントローラの機能提供に役立つファームウェアが含まれています。

ファイバーチャネル

1 つの接続技術で高速 I/O およびネットワーク機能を実現したデータ転送インタフェース技術。ファイバ チャネル標準では、ファイバチャネルポイントツーポイント、ファイバチャネルファブリック (汎用スイッチポロジ)、およびファイバチャネル調停ループ (FC_AL) などを含むいくつかのトポロジをサポートしています。

フラッシュ BIOS

ROM ではなくフラッシュメモリに保存される BIOS。ROM BIOS が新しいチップと交換しなければならないのに対し、フラッシュ BIOS チップはアップデートすることができます。

フラッシュメモリ

コンピュータに取り付けただけのまま、ディスク内のユーティリティを使って再プログラミングできる EEPROM チップ。一般の EEPROM チップは、特別なプログラミング用の装置を使わなければ書き換えはできません。

プロバイダ

プロバイダは管理オブジェクトと通信してさまざまなソースからデータとイベント通知にアクセスする CIM スキーマの拡張機能です。プロバイダはこの情報を CIM オブジェクト マネージャに転送して統合と解釈を行います。

ボーレート

データ伝送速度の尺度。たとえば、モデムはシステムの COM (シリアル) ポートを通して、数種類の特定のボーレートでデータを転送します。

ホットプラグ

システム使用中に、冗長部分を削除または置換できる機能。「ホット スペア」とも呼ばれます。

マイクロプロセッサ

コンピュータ内にある主要コンピュータ計算チップで、演算および論理機能の解釈と実行を制御します。1 つのマイクロプロセッサに書き込まれたソフトウェアは、別のマイクロプロセッサで実行するためには改訂する必要があります。CPU は、マイクロプロセッサの同義語です。

メモリモジュール

DRAMチップを持つ小さな回路基板で、システム基板に接続します。

モジュラシステム

複数のサーバーモジュールを含んだシステム。各サーバーモジュールはローカルシステムとして機能します。システムとして機能するには、サーバーモジュールは、電源装置、ファン、システム管理モジュール、および最低 1 つのネットワークスイッチモジュールを含んだシャーシに挿入されます。電源装置、ファン、システム管理モジュール、およびネットワークスイッチモジュールは、シャーシにあるサーバーモジュールの共有リソースです。[サーバーモジュール](#)を参照してください。

ユーティリティ

システム資源 (メモリ、ディスクドライブ、プリンタなど) を管理するためのプログラム。

ユーティリティパーティション

ハードドライブ上のブート可能なパーティションで、ハードウェアとソフトウェアにユーティリティと診断を提供します。有効にすると、パーティションが起動して、パーティションのユーティリティに実行可能環境を提供します。

リモート管理システム

リモート管理システムは対応するウェブブラウザを使って、リモートから管理下システム上の Server Administrator ホームページにアクセスするシステムです。「管理したシステム」を参照してください。

内蔵 USB

内蔵 USB フラッシュドライブとデバイスは追加のストレージです。内蔵 USB は仮想化を強化します。

内蔵されたハイパーバイザ

内蔵 USB を参照してください。

冷却ユニット

システムシャーシにあるファンまたはその他の冷却デバイス。

名前

オブジェクトまたは変数の名前は、SNMP Management Information Base (MIB) ファイル、または CIM Management Object File (MOF) で識別されるのと同じ文字列です。

周辺デバイス

プリンタ、ディスクドライブまたはキーボードなど、コンピュータに接続されている内部または外部デバイス。

変数

管理オブジェクトの一部。たとえば温度プローブには、機能、正常性またはステータス、および正しい温度プローブを見つけるのに役立つ特定の指標などの変数があります。

機能

オブジェクトが実行できる動作、または管理オブジェクトで実行できる動作を示します。たとえば、カードがホットプラグ対応の場合、システム電源がオンの状態でカードを取り替えることができます。

状況 (状態)

1 つ以上の条件を持つオブジェクトの状況を指します。たとえば、オブジェクトは「準備中」状況である場合があります。

瞬時ヘッドルーム

電源装置によって使用された論理最大電力から瞬時電力消費量を差し引いたもの。

管理下システム

管理下システムは Server Administrator を使ってモニタされ管理されるシステムです。Server Administrator を実行中のシステムは、対応するウェブブラウザを使ってローカル、またはリモートから管理できます。リモート管理システム を参照してください。

設定

設定は、コンポーネントに特定の値が検出されたときにどうするかを決定する、管理可能オブジェクトヘルプの条件です。たとえばユーザーは、温度プローブの上限しきい値を摂氏 75 度に設定できます。プローブがその温度に達すると、ユーザーが介入できるように管理システムに警告が送られます。設定の中には、値に達するとシステムのシャットダウンやシステム損傷を防ぐその他の反応を引き起こすものがあります。

認証 (authentication)

Server Administrator Remote Access Controller には、ユーザーアクセスを認証する 方法として、

RAC 認証と、ローカルオペレーティングシステム認証の 2 つの方法があります。RAC 認証は常に有効になっています。システム管理者は、RAC へのアクセスを許可する、特定のユーザーアカウントおよびパスワードを設定することができます。

オペレーティングシステムでは、システム管理者は異なるレベルのユーザーおよびユーザーアカウントを定義する必要があります。ユーザーの各レベルには、それぞれの異なる特権があります。RAC におけるローカルオペレーティングシステム認証は、オペレーティングシステムのユーザーに 1 組の権限を定義し、RAC に別のユーザーとアカウントを設定することを希望しないシステム管理者が使用

できるオプションです。RAC のローカルオペレーティングシステム認証を有効にすると、オペレーティングシステム上でシステム管理者権限を持つすべてのユーザーが RAC へログインできるようになります。

電源ユニット

壁コンセントからの AC 電流をコンピュータ回路が必要とする DC 電流に変換する電気システム。パーソナルコンピュータの電源装置は通常、いくつもの電圧を生成します。

[目次ページに戻る](#)

[目次ページに戻る](#)

Server Administrator サービス

Dell™ OpenManage™ Server Administratorバージョン 6.0.1 ユーザーズガイド

- [システムの管理](#)
- [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 ホームページシステムツリー オブジェクト](#)
- [プリファランス:ホームページ設定オプションの管理](#)

概要

Server Administrator Instrumentation Service (計装サービス) 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ます。報告機能と表示機能を使うと、システムを構成する各シャーシの全般的な正常性の状態を把握することができます。サブシステム レベルでは、電圧、温度、電流、ファン回転数/分、およびシステムの主要点におけるメモリ機能についての情報を表示できます。システムの各関連所有コスト (COO) のアカウント詳細は概要ビューで参照できます。BIOS、ファームウェア、オペレーティング システム、およびインストールされているすべての Systems Management Software のバージョン情報も簡単に取得できます。

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

- 1 特定の重要コンポーネントの最大値と最小値を指定します。この値はしきい値と呼ばれ、そのコンポーネントの危険イベント発生範囲を決定します (故障最大値と最小値は、システム メーカーによって指定されます)。
- 1 危険イベントまたは故障イベントが発生したときのシステムの応答方法を指定します。ユーザーは危険および故障イベントの通知を受けたときにシステムが取る対応を設定できます。また、24 時間監視を行っているユーザーは、イベント発生に対して何も処置を取らずに責任者の裁量に任せるよう選択することができます。
- 1 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:** Microsoft® Windows Server® 2003 環境の管理下システムとネットワーク管理ステーションで SNMP パケットを受け入れるには、Simple Network Management Protocol (SNMP) サービスを設定する必要があります。詳細については、「[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 ホームページには、デフォルトでシステムツリービューの **システム** オブジェクトが表示されます。**システム** オブジェクトのデフォルトでは、**プロパティ** タブの **正常性** コンポーネントが開かれます。

プリファランス ホームページのデフォルトウィンドウは、**プリファランス** タブにある **アクセス設定** です。

プリファランス ホームページから、「ユーザー」と「パワーユーザー」の権限を持つユーザーへのアクセスを制限、SNMP パスワードを設定、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。グローバルナビゲーションバーの **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 サービスのさまざまな要素を実行するのに必要な特定の操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とユーザー特権レベルに従って、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。

 **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、アクションタブ、およびデータ領域機能を表示するには、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 タブに含まれている **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-「[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](#)」を展開すると、システムコンポーネントのメジャーカテゴリとして「[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](#)」が表示されることがあります。


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、以下のオブジェクトが表示されません。

Storage Management Service コンポーネントの詳細については、『[Dell Systems Management tools and Documentation DVD](#)』またはデル サポートサイト support.dell.com 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

 **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、アクションタブ、およびデータ領域機能を表示するには、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 タブに含まれている **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では別々のサーバーモジュールとして表示される 1 つまたは複数のモジュラーシステムを含むシステムを指します。スタンドアロンのサーバーモジュールと同様、モジュラーエンクロージャにはシステムに不可欠のコンポーネントが含まれます。唯一の違いは、大きいエンクロージャ内に最低 2 つのサーバーモジュール用のスロットがあり、それぞれが完全なサーバーモジュールである点です。

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

プロパティ

サブタブ: 情報

プロパティ タブでは、以下のことができます。

- 1 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。
- 1 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 から Chassis Management Controller の **ログイン** ウィンドウにリンクするには、**モジュラエンクロージャ** オブジェクト、**CMC 情報** タブ、**CMC ウェブインタフェースの起動** の順にクリックします。CMC **ログイン** ウィンドウが表示されます。CMC に接続すると、モジュラエンクロージャの監視と管理を行うことができます。

システム / サーバーモジュール

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含まれます。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**オブジェクトのアクション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**オブジェクトのアクションウィンドウには、**プロパティ**、**シャットダウン**、**ログ**、**警告管理**、**セッション管理**のタブがあります。

 **メモ:** Server Administrator バージョン 2.0 またはそれ以前のバージョンではアップデート機能がサポートされています。Dell™ サーバーアップデートユーティリティと Dell アップデートパッケージはデルサポートサイト support.dell.com からダウンロードできます。これらは 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サポートされています。

 **メモ:** Dell サーバーアップデートユーティリティまたは Dell アップデートパッケージは、アップデートするシステムから始動する必要があります。


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、以下のことができます。

- 1 **メインシステムシャーシ / メインシステム**オブジェクトのハードウェアおよびソフトウェアコンポーネントと**ストレージ**オブジェクトの現在の正常性警告状態を表示します。
- 1 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。
- 1 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。
- 1 監視中のシステムの自動システム回復(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:** BIOS で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有効になっているので自動システム回復オプションは使用できません。自動回復オプションを設定するには、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する必要があります。

 **メモ:** 応答していないシステムをウォッチドッグが識別している場合は、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可能性があります。処置の実行時間は $n-h+1 \sim n+1$ 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 $n \leq 30$ 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エVENTが発生した場合に、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エVENT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ので、この機能は正常に作動しません。この問題が起こった場合は、手でシステムを再起動する必要があります。

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 シャットダウン**

シャットダウン タブでは、以下のことができます。

- 1 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。
- 1 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、センサーによって報告された温度が温度しきい値を超えた場合にのみ発生します。サーマルシャットダウンは、センサーによって報告された温度が温度しきい値を超えない場合はサーマルシャットダウンは起こりません。



- 1 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いる場合でも、Server Administrator はコマンドラインインタフェース(CLI)を使って使用できます。CLI 機能では、DSM SA 接続サービスが実行されている必要はありません。


ログ

サブタブ: **ハードウェア** | **警告** | **コマンド**

ログ タブでは、以下のことができます。

- 1 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一覧の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)を表示できます。ログファイルの使用量が 80% に到達すると、ログ名の隣にある状態インジケータアイコンは、正常状態()から非重要状態()に変わります。Dell™ PowerEdge? x8xx, x9xx, xx1x システムでは、ログファイ


ルの容量が 100 % に到達すると、ログ名の隣にある状態インジケータアイコンは、重要状態(✖)に変わります。

 **メモ:** 容量が 80 % に達したら、ハードウェアログをクリアすることをお勧めします。ログの容量が 100 % に達してしまうと、最新のイベントはログから破棄されます。

- 1 センサーやその他の監視されてい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警告ログを表示します。

 **メモ:** 各警告イベント ID の説明、重大レベルおよび原因などの完全な説明は、『Server Administrator メッセージリファレンスガイド』を参照してください。

- 1 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、保存および電子メール送付手順の詳細については、『Server Administrator ログ』を参照してください。

警告管理


サブタブ: 警告処置 | プラットフォームイベント | SNMP トラップ

警告管理 タブでは以下のことができます。

- 1 現在の警告処置設定の表示と、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警告処置を設定します。
- 1 現在のプラットフォームイベントフィルタ設定の表示と、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プラットフォームイベントフィルタ処置を設定します。また、**送信先の設定** オプションを使用して、プラットフォームイベントの警告を送信する送信先 (IPv4 または IPv6) を選択します。

 **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。

- 1 現在の SNMP トラップ警告しきい値を表示し、計装されたシステムコンポーネントの警告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で生成された場合に、選択したトラップがトリガされます。


 **メモ:** すべての潜在的なシステムコンポーネントのセンサーに対する警告処置は、システム上になくても **警告処置** ウィンドウに一覧表示されます。システム上にないシステムコンポーネントセンサーに対して警告処置を設定しても、効果はありません。

セッション管理

サブタブ: セッション

セッション管理 タブでは以下のことができます。

- 1 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。
- 1 ユーザーセッションを終了する。


 **メモ:** セッション管理ページの表示およびログインユーザーのセッション終了は、システム管理者の権限をもつユーザーのみ行うことができます。


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。


- | | |
|---------------------------------|----------------------------|
| 1 AC スイッチ | 1 ポート |
| 1 バッテリー | 1 電源管理 |
| 1 BIOS | 1 電源ユニット |
| 1 ファン | 1 プロセッサ |
| 1 ファームウェア | 1 リモートアクセス |
| 1 ハードウェアパフォーマンス | 1 スロット |
| 1 イントルージョン | 1 温度 |
| 1 メモリ | 1 電圧 |
| 1 ネットワーク | |

 **メモ:** **AC スイッチ** は限られたシステムでサポートされています。

 **メモ:** **バッテリー** は Dell PowerEdge x9xx と Dell xx0x システムでのみサポートされています。

 **メモ:** **ハードウェアパフォーマンス** は Dell xx0x システムでのみサポートされています。

 **メモ:** **電源** は Dell PowerEdge 1900 システムでは使用できません。

 **メモ:** **電源管理** は限られた Dell xx0x システムでのみサポートされています。

システム / サーバーには、1 つのメインシステムシャーシが含まれることもあれば、複数のシャーシが含まれることもあります。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ています。**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 **プロパティ** タブがあります。


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、以下のことができます。


- ハードウェアコンポーネントおよびセンサーの正常性および状態を表示します。リスト内の各コンポーネント名の隣に「[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](#)」アイコンが表示されます。緑のチェックマーク(✓)は、コンポーネントが正常であることを示します。感嘆符が入った黄色の三角形(⚠)は、コンポーネントは危険(重要ではない)状態で、速やかな対応が必要なことを示します。赤い X マーク(✗)は、コンポーネントが故障(重要)状態にあり、早急に対応が必要なことを示します。ブランクスペース()は、コンポーネントの正常性が不明であることを示します。使用できるモニタコンポーネントには次のようなものがあります。

1 AC スイッチ	1 ネットワーク
1 バッテリー	1 電源管理
1 ファン	1 電源ユニット
1 ハードウェアログ	1 プロセッサ
1 イントルージョン	1 温度
1 メモリ	1 電圧

 **メモ:** **AC スイッチ** は限られたシステムでサポートされています。

 **メモ:** **バッテリー** は Dell PowerEdge x9xx と Dell xx0x システムでのみサポートされています。

 **メモ:** **電源** は Dell PowerEdge 1900 システムでは使用できません。

 **メモ:** **電源管理** は限られた Dell xx0x システムでのみサポートされています。

- メインシステムシャーシの属性についての情報を表示します。
- 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)。
- フロントパネルボタンすなわち電源ボタン、およびシステムに存在する場合は NMI (非マスキ割り込み) ボタンと呼ばれる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。

AC スイッチ

AC スイッチ オブジェクトをクリックすると、システムの AC フェールオーバースイッチの主要機能を表示できます。**AC スイッチ** 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従って、**プロパティ** タブが表示されます。

プロパティ

サブタブ: 情報

プロパティ タブでは、AC スイッチの冗長性と AC 電源供給ラインについて情報を表示できます。

バッテリー

バッテリー 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**バッテリー**の情報を表示できます。システムの電源がオフのときも、バッテリーは時間および日付を維持します。バッテリーは、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。**バッテリー** 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従って、**プロパティ** タブと **警告管理** タブが表示されます。

プロパティ

サブタブ: 情報

プロパティ タブでは、システムバッテリー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。

警告管理

警告管理 タブでは、バッテリー警告または重要 / エラーイベントが発生した時に有効にする警告を設定できます。

BIOS

BIOS オブジェクトをクリックすると、システムの BIOS の主要機能を管理できます。システムの BIOS には、フラッシュメモリチップセットに保存されて、プロセッサと周辺機器(キーボードやビデオアダプタ)間の通信と、システムメッセージなどその他の機能を制御するプログラムが含まれています。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従って、**プロパティ** タブと **設定** タブが表示されます。

プロパティ


サブタブ: 情報

プロパティタブでは BIOS 情報を表示できます。

セットアップ


サブタブ: BIOS


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。

 **メモ:** セットアップタブで起動順序を **デバイスリスト** に設定すると、起動順序は ディスケット、IDE CD ドライブ、ハードドライブ、オプションの ROM(デバイスを使用できる場合)となります。

シリアルポート、ネットワークインタフェースコントローラカード、起動順序、ユーザーのアクセスが可能な USB ポート、CPU 仮想化テクノロジー、CPU ハイパースレディング、AC 電源回復モード、内蔵 SATA コントローラ、コンソールリダイレクト、コンソールリダイレクト Failsafe ポーレート等の多数の BIOS 設定機能の状態を変更できます。また、内蔵 USB デバイス、トラステッドプラットフォームモジュール (TPM)、光学式ドライブコントローラ、自動システムリカバリ (ASR) ウォッチドッグタイマー、組み込みハイパーバイザ、マザーボード上の追加の LAN ネットワークポートを設定することもできます。

特定のシステム構成ではその他の設定アイテムが表示される場合もありますが、BIOS 設定オプションによっては、Server Administrator ではアクセス不能な F2 BIOS 設定画面に表示されるものがあります。

 **メモ:** Server Administrator 内の NIC 設定情報 BIOS 設定が内蔵型の NIC では不正確な場合があります。BIOS 設定画面で NIC を有効または無効にすると、予想外の結果が生じる可能性があります。内蔵型の NIC では実際の **システムセットアップ** 画面(システムの起動中に <F2> を押してアクセス)からすべての設定を実行することをお勧めします。

 **メモ:** システムの BIOS 設定タブは、システムでサポートされる BIOS 機能のみを表示します。

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 の測定によって各システムファンの状態を監視します。Server Administrator は rpm の測定によって各システムファンの状態を監視します。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従って、**プロパティ**と **警告管理** タブが表示されます。

プロパティ

サブタブ:ファンプローブ | ファンコントロール

プロパティタブでは、以下のことができます。

- 1 システムのファンプローブの電流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 ベースのシステムでは編集できません。

- 1 ファンコントロールオプションを選択します。

警告管理

サブタブ:警告処置 | SNMPトラップ

警告管理タブでは以下のことができます。

- 1 現在の警告処置設定の表示と、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警告処置を設定します。
- 1 現在の SNMP トラップ警告しきい値を表示し、ファンの警告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で生成された場合に、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の起動や操作を実行できます。各コントローラには、コントローラの機能提供を円滑にする 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、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劣化の状態と原因を表示されます。ハードウェアパフォーマンス 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よっては、**プロパティ**タブが表示されることがあります。

表 5-1 には、ステータスの一覧とプローブの原因が表示されます。

状態値	原因値
低下	ユーザー設定

	不十分な電源容量
	原因不明
標準	該当せず

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、システムのシャールイントルージョンの状態を管理できます。Server Administrator では、システムの重大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ルイントルージョンの状態をモニタします。シャールイントルージョンは、誰かがシステムのシャールを開いているか、開いたことを示します。**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よっては、**プロパティ** タブと **警告管理** タブが表示されることがあります。

プロパティ

サブタブ: イントルージョン

プロパティ タブでシャールイントルージョンの状態を表示できます。

警告管理

サブタブ: 警告処置 | SNMP トラップ

警告管理 タブでは以下のことができます。

- 現在の警告処置設定の表示と、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警告処置の設定を行います。
- 現在の SNMP トラップ警告しきい値を表示し、イントルージョンセンサーの警告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で生成された場合に、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、モニタ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モニタします。メモリデバイスの事前故障センサーは、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モニタします。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モニタします。**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よっては、**プロパティ** タブと **警告管理** タブが表示されることがあります。

プロパティ

サブタブ: メモリ

プロパティ タブでは、メモリの属性、メモリデバイスの詳細、およびメモリデバイスの状態を表示できます。

 **メモ:** スベ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 **検出されたスベ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。

警告管理

サブタブ: 警告処置 | SNMP トラップ

警告管理 タブでは以下のことができます。

- 現在の警告処置設定の表示と、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警告処置の設定を行います。
- 現在の SNMP トラップ警告しきい値を表示し、メモリモジュール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で生成された場合に、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すると、システムの NIC を管理できます。Server Administrator は、システムに存在する各 NIC の状態をモニタして、リモート接続が続いていることを確認します。**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権限によっては、**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、システムに設置されている NIC 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モニタします。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、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

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。

$BTU/hr = Watt \times 3.413$ (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。

システムの瞬時ヘッドルームとシステムのピークヘッドルームも表示できます。値はワットと BTU/hr (英サーマルユニット) で表示されます。電力しきい値はワットと BTU/hr 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、システムアイドル電力やシステム最大電力予測値などの電力インベントリ属性をワットと BTU/hr で表示できます。また、電力キャップを有効にしたり、システムの電力キャップを設定する電力バジェットオプションも使用できます。

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。

警告管理

サブタブ: 警告処置 | SNMP トラップ

警告処置 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警告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。

電源ユニット

電源装置 オブジェクトをクリックすると、電源装置を管理できます。Server Administrator は、冗長性を含めた電源装置の状態をモニタして、システムに存在する各電源装置が正しく機能しているか確認します。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っては、**プロパティ** タブと **警告管理** タブが表示されることがあります。

プロパティ

サブタブ: 要素

プロパティ タブでは、以下のことができます。


- 1 電源装置の冗長性属性についての情報を表示します。
- 1 定格入力ワット数や最大出力ワット数など電源装置の各要素の状態をチェックします。定格入力ワット数の属性は xxTx で始まる PMBus システムでのみ表示されます。

警告管理

サブタブ: 警告処置 | SNMP トラップ

警告管理 タブでは以下のことができます。

- 1 現在の警告処置設定の表示と、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警告処置の設定を行います。
- 1 IPv6 アドレスのプラットフォームイベント警告先を設定します。
- 1 現在の SNMP トラップ警告しきい値を表示し、システム電力の警告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で生成された場合に、選択したトラップがトリガされます。

 **メモ:** システムのピーク電力トラップは重要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すると、システムのプロセッサを管理できます。プロセッサはシステム内にある主要計算チップで、演算関数と論理関数の解釈と実行を制御します。**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よっては、**プロパティ** タブと **警告管理** 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、システムのプロセッサについての情報を表示して、詳細な機能およびキャッシュ情報にアクセスできます。

警告管理

サブタブ: 警告処置 | SNMPトラップ


警告管理 タブでは以下のことができます。


- 現在の警告処置設定の表示と、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警告処置の設定を行います。
- 現在の SNMP トラップ警告しきい値を表示し、プロセッサの警告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で生成された場合に、選択したトラップがトリガされます。

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)機能および統合 Dell リモートアクセスコントローラ(iDRAC)機能を管理できます。

リモートアクセス タブを選択すると、BMC/iDRAC の一般情報など BMC/iDRAC の機能管理ができます。また、ローカルエリアネットワーク(LAN)上の BMC/iDRAC 設定、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 接続の BMC/iDRAC、BMC/iDRAC ユーザーなども管理できます。

 **メモ:** BMC は Dell PowerEdge x8xx と x9xx システムでサポートされており、iDRAC は Dell xx0x と xx1x システムでのみサポートされています。

 **メモ:** Server Administrator 以外のアプリケーションを使用して Server Administrator を実行中に BMC/iDRAC を設定すると、Server Administrator によって表示される BMC/iDRAC 設定データが BMC/iDRAC と非同期になることがあります。Server Administrator の実行中は Server Administrator を使用して BMC/iDRAC を設定されることをお勧めします。

DRAC を使うと、システムのリモートシステム管理機能にアクセスできます。Server Administrator DRAC は、操作不能なシステムへのリモートアクセス、システムダウン発生時の警告通知、そしてシステムを再起動する能力を提供します。

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よっては、**プロパティ**タブ、**設定**タブ、**ユーザー** 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、リモートアクセスデバイスの一般情報を表示できます。IPv4 と IPv6 のアドレスの属性も表示できます。

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。


構成

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

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。

DRAC を設定する場合、**設定** タブで、次の設定を実行できます。

- ネットワークのプロパティ設定

 **メモ:** NIC を有効にする、NIC の選択、および暗号化キー フィールドは、Dell PowerEdge x9xx 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 / 無効は、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 リモートアクセスユーザー設定を変更できます。Remote Access Controller ユーザーについての情報を追加、設定、表示できます。

 **メモ:** Dell PowerEdge x9xx システム上。

- 10 個のユーザー ID が表示されます。DRAC カードがインストールされている場合は、16 個のユーザー ID が表示されます。
- シリアルオーバー LAN ベイロード列が表示されます。

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すると、システム温度を管理して、システムの内部コンポーネントへの熱損傷を防ぐことができます。Server Administrator は、システムのシャーシのさまざまな場所で温度をモニタして、シャーシ内部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応じて、**プロパティ** タブ、**警告管理** タブが表示されます。

プロパティ

サブタブ: 温度プローブ

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と状況を表示したり、温度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:** 一部の温度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 ベースのシステムでは編集できません。プローブしきい値を割り当てるとき、入力した最小値または最大値が割り当て可能な値に自動的に四捨五入される場合があります。

警告管理

サブタブ: 警告処置 | SNMP トラップ

警告管理 タブでは以下のことができます。

- 1 現在の警告処置設定の表示と、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警告処置を設定します。
- 1 現在の SNMP トラップ警告しきい値を表示し、温度プローブの警告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で生成された場合に、選択したトラップがトリガされます。

 **メモ:** ユーザーは外部シャーシの最小温度プローブしきい値と最大温度プローブしきい値を整数でのみ設定できます。ユーザーが最小温度プローブしきい値または最大温度プローブしきい値を小数点が含まれる値に設定すると、小数点の前の整数だけ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、監視されているシステム内のさまざまなシャーシの場所において、重要なコンポーネントの電圧をモニタします。**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 **警告管理** タブが表示されます。

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と状況を表示したり、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:** 一部の電圧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 ベースのシステムでは編集できません。

警告管理

サブタブ: 警告処置 | SNMP トラップ

警告管理 タブでは以下のことができます。

- 1 現在の警告処置設定の表示と、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警告処置の設定を行います。
- 1 現在の SNMP トラップ警告しきい値を表示し、電圧センサーの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で生成された場合に、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: 概要

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

ストレージ

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

Storage Management Service はストレージデバイスの設定機能を提供します。ほとんどの場合、Storage Management Service は 標準セットアップを使用してインストールします。

Storage Management 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使用可能です。

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よっては、**プロパティ** タブが表示されます。

プロパティ

サブタブ: 正常性

プロパティ タブでは、アレイレージシステム、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: ホームページ設定オプションの管理

プリファランスホームページの左ウィンドウ枠(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。表示されるオプションは、管理下システムにインストールされているシステム管理ソフトウェアによって異なります。

使用可能なプリファランスホームページオプションについては、[表 5-2](#) を参照してください。

表 5-2 プリファランスホームページ設定オプション

	*****	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** オブジェクトウィンドウには、ユーザーのグループ権限によっては、**ユーザー** タブと **Web Server** タブが表示されることがあります。

ユーザー

サブタブ: プロパティ

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 プでは以下のことができます。

- 1 DSM SA 接続サービスプリファランスの設定。サーバー設定の指定方法については、「[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。
- 1 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。
- 1 新しい X.509 証明書を作成したり、既存の X.509 証明書を再利用したり、認証機関 (CA) からルート認証や認証チェーンをインポートして X.509 証明書を管理します。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、ユーザー権限とパワーユーザー権限のあるユーザーの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よっては、**プリファランス** タブが表示されることがあります。

プリファランス


サブタブ: アクセス設定 | SNMP 設定

プリファランス タブでは、以下のことができます。

- 1 ユーザー権限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。
- 1 SNMP ルートパスワードを設定します。

 **メモ:** デフォルト SNMP ユーザーは root、デフォルトパスワードは calvin です。

- 1 SNMP Set 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を実行しているシステムでは、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を実行しているシステムでは、`srvadmin-services.sh restart` 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。

[目次ページに戻る](#)

[目次ページに戻る](#)


はじめに

Dell™ OpenManage™ Server Administratorバージョン 6.0.1 ユーザーズガイド

- [概要](#)
- [組み込み機能](#)
- [Server Administrator ホームページ](#)
- [その他の参考ドキュメント](#)
- [テクニカルサポートの利用法](#)


概要

Server Administrator には、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ーフェイス (GUI)、および OS を通じて使用するコマンドラインインターフェイス (CLI) の 2 つの形式で、包括的な 1 対 1 のシステム管理ソリューションが備わっています。Server Administrator は、システム管理者がネットワーク上のシステムをローカルおよびリモートで管理できるように設計されています。Server Administrator は包括的な 1 対 1 のシステム管理を提供することにより、システム管理者がネットワーク全体の管理に集中できるようにします。

 **メモ:** Server Administrator を使用するには、システムはスタンドアロン、別のシャーシ内にネットワークストレージ ユニートを接続したサーバー、1 つのモジュラーエンクロージャ内に 1 つまたは複数のサーバーモジュールを組み込んだモジュラーシステムのいずれでもかまいません。

Server Administrator は次の情報を提供します。

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

 **メモ:** リモート回復するには、Dell™ Remote Access Controller カードが実装されていなければなりません。


組み込み機能

Server Administrator は、統合管理サービスの総合セットを利用した使い易いローカルおよびリモートシステムの管理制御を提供します。Server Administrator のみを管理下システムにインストールするだけで、Server Administrator ホームページからローカルおよびリモートにアクセスできます。リモートで監視しているシステムには、ダイヤルイン、LAN、またはワイヤレス接続を使ってアクセスできます。Server Administrator では、ロールベースアクセス制御 (RBAC)、認証、および業界標準セキュアソケットレイヤ (SSL) 暗号化を使って管理接続のセキュリティを確保します。

インストール

『Dell™ Systems Management Tools and Documentation DVD』を使って Server Administrator をインストールできます。この DVD には、Server Administrator およびその他のシステム管理ソフトウェアのコンポーネントをお使いの管理下システムにインストール、アップグレード、アンインストールするためのセットアッププログラムが用意されています。この DVD には、管理ステーションに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、アンインストールするためのセットアッププログラムも収録されています。また、ネットワークを介して Server Administrator を複数のシステムに無人インストールすることもできます。

Server Administrator のインストール / アンインストールの詳細については、『Dell OpenManage ソフトウェアクイックインストールガイド』 and the 『Dell OpenManage? インストールとセキュリティユーザーズガイド』を参照してください。これらのマニュアルには、『Dell Systems Management Tools and Documentation DVD 』またはデルサポートサイト support.dell.com からアクセスできます。

 **メモ:** モジュラーシステムがある場合、シャーシでインストールさ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、コンポーネント専用の Dell アップデートパッケージを使用してください。『Dell Server Update DVD』を使用すると、完全なバージョンレポートを表示して、システム全体をアップデートすることができます。Server Update Utility は、アップデートを見つけてサーバーに適用する DVD-ROM ベースのアプリケーションです。このユーティリティは support.dell.com からダウンロードできます。

『Server Update Utility ユーザーズガイド』では、Dell サーバーをアップデートしたり、リポジットに登録されているサーバー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) の入手方法と使用方法に関する情報を参照してください。

Storage Management Service

Storage Management Service は、統合グラフィカル 表示でストレージ管理情報を提供します。

Server Administrator の Storage Management Service:

- 1 モニタされるシステムに接続しているローカルおよびリモートのストレージのステータスを表示できます。
- 1 SCSI、SATA、ATA、および SAS をサポートしています。ファイバチャネルはサポートしていません。
- 1 対応するすべての RAID および RAID 以外のコントローラとエンクロージャについて、コントローラ BIOS ユーティリティを使用せず、単一のグラフィカルインターフェイスまたはコマンドラインインターフェイスから、コントローラおよびエンクロージャ機能を実行できます。
- 1 データ冗長性の設定、ホットスワップ割り当て、または障害発生ドライブの再構成によってデータを保護します。


- 1 ストレージ設定機能を提供します。

Storage Management Serviceの詳細については、『*Dell Systems Management tools and Documentation DVD*』またはデルサポートサイト support.dell.com 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。

Instrumentation Service(計装サービス) :

Instrumentation Service 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モニタシステムのリモート管理を実現します。

Remote Access Controller

 **メモ:** Remote Access Controller はモジュラーシステムでは使用できません。モジュラーシステムの Dell Embedded Remote Access/Modular Chassis Controller(ERA/MC) に直接接続する必要があります。詳細については、『*Dell Embedded Remote Access/MC ユーザーズガイド*』を参照してください。

Remote Access Controller は、Dell Remote Access Controller (DRAC) または Baseboard Management Controller (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提供するため、迅速なシステム起動と実行を実現できます。Remote Access Controller は、システムがダウンしたときに警告を通知し、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 には、システム、モニタハードウェアイベントおよびシステム警告などに発行されたコマンドのログが表示されます。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、指定のサービス担当者に電子メールで送信できます。

Server Administrator ホームページ

Server Administrator ホームページは、管理下システムから、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を使用したりリモートホストから、セットアップと使用が簡単なウェブブラウザベースのシステム管理タスクを提供します。Dell Systems Management Server Administrator 接続サービス (DSM SA 接続サービス) が管理下システムにインストールおよび設定されている場合は、サポートされているウェブブラウザおよび接続機能をもつすべてのシステムからリモート管理機能を実行することができます。さらに Server Administrator ホームページは、包括的なオンラインコンテンツヘルプを提供します。

その他の参考ドキュメント

このユーザーズガイドのほか、以下のガイドをデル サポートサイト support.dell.com または『*Dell Systems Management Tools and Documentation DVD*』からご利用いただけます。

- 1 『*Dell システムソフトウェアサポートマトリックス*』には、各種の 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が記載されています。
- 1 『*Dell OpenManage インストールとセキュリティユーザーズガイド*』では、インストール方法に関する包括的な情報と、サポートしている各オペレーティングシステム別に Server Administrator のインストール、アップグレード、およびアンインストールの詳しい手順を説明しています。
- 1 『*Dell OpenManage ソフトウェアクイックインストールガイド*』では、管理ステーション(コンソール)および管理下システムにインストールできるアプリケーションの概要と、対応オペレーティングシステムを実行しているコンソールおよび Managed System アプリケーションのインストール手順について説明しています。
- 1 『*Dell OpenManage Server Administrator 互換性ガイド*』では、Microsoft Windows、Red Hat Enterprise Linux、SUSE Linux Enterprise Server などの対応オペレーティングシステムを実行している各種ハードウェアプラットフォーム(またはシステム)での Server Administrator のインストールと運用に関する互換性情報を提供しています。
- 1 『*Dell OpenManage Server Administrator SNMP リファレンスガイド*』は、管理ネットワーク管理プロトコル(SNMP)管理情報ベース(MIB)について文書化したものです。SNMP MIB はシステム管理エージェントの機能を行うよう標準 MIB を拡張する変数を定義します。
- 1 『*Dell OpenManage Server Administrator CIM リファレンスガイド*』は、標準管理オブジェクト形式(MOF)ファイルの拡張機能である Common Information Model(CIM)プロバイダについて文書化したものです。CIM プロバイダの MOF のマニュアルでは、管理オブジェクトのサポートされているクラスについて説明しています。
- 1 『*Dell OpenManage Server Administrator メッセージリファレンスガイド*』は、Server Administrator ホームページの警告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を掲載しています。このガイドは Server Administrator が発行する各警告メッセージのテキスト、重大度、および原因について説明しています。
- 1 『*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*』は、システムの状態の表示、ログへのアクセス、レポートの作成、コンポーネントの各種パラメータの設定、重要なしきい値の設定などを CLI コマンドを使って実行する方法のほか、Server Administrator のコマンドラインインタフェースについても詳しく説明しています。
- 1 iDRAC の設定と使用の詳細については、『*Dell Integrated Remote Access Controller ユーザーズガイド*』を参照してください。
- 1 CNC のインストール、設定、使用の詳細については、『*Dell Chassis Management Controller ユーザーズガイド*』を参照してください。
- 1 『*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。
- 1 『*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*』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。
- 1 『*Dell OpenManage Server Administrator Storage Management ユーザーズガイド*』は、システムに接続し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。
- 1 『*Dell Remote Access Controller インストールおよびセットアップガイド*』では、DRAC III、DRAC III/XT および ERA/O コントローラのインストールと設定方法、ERA コントローラの設定方法、および RAC を使用した作動不能のシステムへのアクセス方法に関する情報を完全に網羅しています。

- 1 『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。
- 1 『Dell Remote Access Controller 4 ユーザーズガイド』では、DRAC 4 コントローラのインストールと設定方法、および DRAC 4 を使用した作動不能システムへのアクセス方法に関する情報を完全に網羅しています。
- 1 『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アクセス方法に関する情報を完全に網羅しています。
- 1 『Dell Embedded Remote Access/MC Controller ユーザーズガイド』では、モジュール式システムとその共有リソースをネットワークを介してリモートから管理、モニタするための ERA/MC の設定と使用法を説明しています。
- 1 『Dell OpenManage リモートインストールユーザーズガイド』では、イメージベースのテクノロジーを活用し、ネットワークを介した無人の同時配備と設定のソリューションに関する情報を提供しています。
- 1 『Dell アップデートパッケージユーザーズガイド』では、システムアップデートの対策として、Dell アップデートパッケージの入手方法と使用方法に関する情報を掲載しています。
- 1 『Dell OpenManage サーバーアップデートユーティリティユーザーズガイド』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)の入手方法と使用方法に関する情報を掲載しています。

『Dell Systems Management Tools and Documentation DVD』には、Server Administrator の readme ファイルおよびその他のアプリケーションのほとんどが収録されています。

テクニカルサポートの利用法

このガイドに記載された手順がよくわからない場合や、お使いの製品が予想通りに実行されない場合は、ヘルプツールを使用してください。ヘルプツールの詳細については、システムの『ハードウェアオーナーズマニュアル』の「困ったときは」を参照してください。

さらに、Dell エンタープライズのトレーニングと検定もご利用いただけます。詳細については、www.dell.com/training を参照してください。このサービスが提供されていない地域もあります。

[目次ページに戻る](#)

[目次ページに戻る](#)

Server Administrator ログ

Dell™ OpenManage™ Server Administratorバージョン 6.0.1 ユーザーズガイド

- [概要](#)
- [組み込み機能](#)
- [Server Administrator ログ](#)

概要

Server Administrator を使用すると、ハードウェア、警告、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システム管理者特権でログインし、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システム管理者特権またはパワーユーザー特権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の情報は、『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』を参照してください。

Server Administrator ログを表示する場合、グローバルナビゲーションバーの **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、ユーザー特権レベルと、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群に応じてアクセスできるすべてのウィンドウでご利用いただけます。

組み込み機能

列見出しをクリックすると、列ごとに並べ替えられるか、列の並べ替えの方向が変わります。さらに、各ログ ウィンドウには、システム管理とサポートに使用できるいくつかのタスクボタンがあります。

ログウィンドウタスクボタン

- 1 ログのコピーをデフォルトのプリンタに印刷するには、**印刷** をクリックします。
- 1 (各データフィールドをカスタマイズ可能な区切り文字で区切った値を持つ)ログデータが含まれたテキストファイルを指定の場所に保存するには、**エクスポート** をクリックします。
- 1 ログのコンテンツを添付に含む電子メールメッセージを作成するには、**電子メール** をクリックします。
- 1 ログからすべてのイベントを消去するには、**ログのクリア** をクリックします。
- 1 ログのコンテンツを .zip ファイルに保存するには、**名前を付けて保存** をクリックします。
- 1 アクションウィンドウデータ領域にログのコンテンツを再度ロードするには、**更新** をクリックします。

タスクボタンの使用方法についての詳細は、「[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。

- 1 [「ハードウェアログ」](#)
- 1 [「警告ログ」](#)
- 1 [「コマンドログ」](#)

ハードウェアログ

ハードウェアコンポーネントに問題があると考えられる場合、ハードウェアログを使用します。Dell PowerEdge? x8xx、x9xx、および xx1x システムでは、ログファイルの容量が 100% に達するとハードウェアログ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、Embedded System Management (ESM) ログと System Event Log (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 状態 メッセージを送ることができる一組の組み込み命令です。ログに一覧表示された各コンポーネントには、名前の横にステータス インジケータアイコンがあります。緑のチェック マーク (✅) は、コンポーネントが正常であることを示します。感嘆符が入った黄色の三角形 (⚠️) は、コンポーネントは危険 (重要ではない) 状態で、速やかな対応が必要であることを示します。赤い X マーク (❌) は、コンポーネントが故障 (重要) 状態にあり、早急に対応が必要であることを示します。ブランクスペース () は、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 には次のような情報が含まれます。

- 1 イベントの重大度
- 1 イベントがキャプチャされた日時
- 1 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は、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% に達してしまうと、最新のイベントはログから破棄されます。

警告ログ


 **メモ:** 警告ログで無効な XML データ(たと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。

警告ログを使用すると、さまざまなシステムイベントをモニタできます。Server Administrator では、センサーやその他のモニタパラメータの状態変化に応じてイベントが生成されます。警告ログに記録される各状態変更イベントは、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 ID と、そのイベントについて説明したイベントメッセージから構成されています。イベント ID とメッセージは、個々のイベントの重大度と原因を説明し、イベントの場所やモニタ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。

警告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、**警告** をクリックします。


警告ログには次のような情報が含まれます。

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

 **メモ:** ログ履歴は、今後のトラブルシューティングや診断目的で必要になることがあります。したがって、ログファイルを保存することをお勧めします。

警告メッセージの詳細については、『*Server Administrator Messages リファレンスガイド*』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(たと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。

Server Administrator ユーザーが発行したすべてのコマンドをモニタするには、コマンドログを使用します。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始動したシャットダウンなどを追跡し、最後にログがクリアされた日時を記録します。コマンドログファイルのサイズは、必要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。

コマンドログには次のような情報が含まれます。

- 1 コマンドが起動された日時
- 1 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
- 1 コマンドと関連値の説明

 **メモ:** ログ履歴は、今後のトラブルシューティングや診断目的で必要になることがあります。したがって、ログファイルを保存することをお勧めします。


[目次ページに戻る](#)

[目次ページに戻る](#)

Remote Access Controller の操作

Dell™ OpenManage™ Server Administratorバージョン 6.0.1 ユーザーズガイド

- [概要](#)
- [基本情報の表示](#)
- [リモートアクセスデバイスで LAN 接続を使用するように設定する](#)
- [リモートアクセスデバイスでシリアルポート接続を使用するように設定する](#)
- [リモートアクセスデバイスでシリアルオーバー LAN 接続を使用するように設定する](#)
- [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警告の設定](#)

 **メモ:** ベースボード管理コントローラ(BMC)は Dell™ PowerEdge™ x8xx および x9xx システムでサポートされ、Integrated Dell Remote Access Controller (iDRAC) は Dell xx0x および xx1x システムでサポートされています。

概要

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 システムベースボード管理コントローラ(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モニタし、一定のパラメータがプリセットしきい値を超えたときに警告とログイベントを送信します。BMC/iDRAC は、業界標準の Intelligent Platform Management Interface(IPMI)仕様をサポートし、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。


DRAC 5 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。


システムのベースボード管理コントローラ(BMC)/ Integrated Dell Remote Access Card (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を電子メール警告として送信されるように DRAC 4 および DRAC 5 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助けるために、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を実行するシステムのみで利用可) を記録します。

Remote Access Controller は、動作不能のシステムへのリモートアクセスを提供するため、迅速なシステム起動と実行を実現できます。Remote Access Controller は、システムがダウンしたときに警告を通知し、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、最近のクラッシュ 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。

Remote Access Controller を使用する場合、グローバルナビゲーションバーの **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詳しい説明が表示されます。Remote Access Controller のヘルプは、ユーザーの特権レベルと、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 についての詳細は、『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 4 の使用方法については『Dell Remote Access Controller 4 ユーザーズガイド』を、DRAC 5 の使用方法については『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、『Integrated Dell Remote Access Controller ユーザーズガイド』を参照してください。

[表 6-1](#) システムに Server Administrator がインストールされたときに GUI フィールド名と該当システムが一覧表示されます。

表 6-1 以下の GUI フィールド名に対するシステムの可用性

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 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の帯域内アクセスが可能で、BMC/iDRAC を設定する機能も提供します。BMC/iDRAC と DRAC 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て、Server Administrator グラフィカルユーザーインターフェイスから管理できます。以下のタスクを実行できます。


- 1 基本情報の表示
- 1 LAN 接続上のリモートアクセスデバイスの設定
- 1 シリアルオーバーLAN 接続上のリモートアクセスデバイスの設定
- 1 シリアルポート接続上のリモートアクセスデバイスの設定
- 1 追加のリモートアクセスデバイスプロパティの設定
- 1 リモートアクセスデバイス上でのユーザーの設定

1. プラットフォームイベントフィルタ警告の設定

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、リモートアクセスの `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)パラメータと警告の宛先を管理できます。

 **メモ:** BMC データは、Dell PowerEdge x8xx および x9xx 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、BMC 設定をデフォルト値に設定することもできます。これには、次の操作を行います。

 **メモ:** BMC 設定をリセットするには、「システム管理者」特権でログインする必要があります。

1. **モジュラエンクロージャ → 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** オブジェクトをクリックします。

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


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

IPv4 アドレス


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

IPv6 アドレス

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

リモートアクセスデバイスで LAN 接続を使用するように設定する


 **メモ:** **LAN 設定** フィールドは、インバンドユーザーに **無効** と設定されていれば、読み取り専用として表示されます。

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できます。これには、次の操作を行います。

1. **モジュラエンクロージャ → 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** オブジェクトをクリックします。
2. **設定** タブをクリックします。


- 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ム構成されている場合、BMC/iDRAC 管理トラフィックは正しく機能しません。

- 次の NIC 設定詳細を設定します。


- NIC を有効にする(このオプションは DRAC がインストールされている Dell PowerEdge x9xx システムで使用可能です。NIC のチーム構成にこのオプションを選択します。Dell PowerEdge x9xx システムでは、追加冗長性用に NIC をチーム構成できます。)

 **メモ:** DRACI には統合 10BASE-T/100BASE-T Ethernet NIC があり、TCP/IP をサポートしています。NIC には、192.168.20.1 のデフォルト アドレスと 192.168.20.1 のデフォルト ゲートウェイが設定されています。

 **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 の選択

 **メモ:** NIC の選択は、モジュラーシステムでは設定できません。

- 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
- チャンネル権限レベルの制限
- 新しい暗号化キー(このオプションは Dell PowerEdge x9xx システムで使用可能です。)

- 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

- 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

- 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
- プレフィックスの長さ
- 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 アドレスプロパティを有効にした場合にのみ IPv4 と IPv6 アドレスの詳細を設定できます。

- 変更の適用 をクリックします。

リモートアクセスデバイスでシリアルポート接続を使用するように設定する

シリアルポート接続を介して通信用に BMC を設定できます。これには、次の操作を行います。

1. **モジュラエンクロージャ**→ **システム / サーバモジュール**→ **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** オブジェクトをクリックします。
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。
 - 1 接続モード設定
 - 1 ボーレート
 - 1 フロー制御
 - 1 チャネル権限レベルの制限

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、Intelligent Platform Interface Management (IPMI) のメッセージをシリアルポートから ASCII 文字で出力するために使用します。ターミナルモードは限定数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。

- 1 ライン編集
- 1 削除制御
- 1 エコー制御
- 1 ハンドシェイク制御
- 1 新しいラインシーケンス
- 1 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。

リモートアクセスデバイスでシリアルオーバー LAN 接続を使用するように設定する

シリアルオーバー LAN (SOL) 接続を介して通信用に BMC/iDRAC を設定できます。これには、次の操作を行います。

1. **モジュラエンクロージャ**→ **システム / サーバモジュール**→ **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** オブジェクトをクリックします。
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。
 - 1 シリアルオーバー LAN を有効にする
 - 1 ボーレート
 - 1 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 をさらに細かく設定できます。

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。
 - 1 文字累積間隔

- 1 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 プロパティを設定できます。これには、次の操作を行います。

1. **モジュラエンクロージャ** → **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** オブジェクトをクリックします。
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。

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のユーザーを設定できます。このページにアクセスするには、次の手順に従います。


1. **モジュラエンクロージャ** → **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** オブジェクトをクリックします。
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。
 - 1 **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。
 - 1 **ユーザー名** フィールドにユーザーの名前を入力します。
 - 1 **パスワードの変更** チェックボックスを選択します。
 - 1 **新しいパスワード** フィールドに新しいパスワードを入力します。
 - 1 **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. 次のユーザー特権を指定します。
 - 1 最大 LAN ユーザー特権レベル制限を選択します。
 - 1 許可する最大シリアルポートユーザー特権を選択します。
 - 1 Dell PowerEdge x9xx システムでは、シリアルオーバー LAN を有効にするを選択してシリアルオーバー LAN を有効化します。
6. 次の iDRAC ユーザー特権を指定します。
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警告の設定


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)パラメータや警告の宛先など最も適切な BMC 機能を設定できます。これには、次の操作を行います。


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に個別の処置をとることができます。シャットダウン処置を行うイベントを選択して、選択し処置の警告を生成することができます。また、選択した IP アドレスの宛先に警告を送信することもできます。

 **メモ:** BMC プラットフォームのイベントフィルタ警告を設定するには、「システム管理者」特権でログインする必要があります。

 **メモ:** プラットフォームのイベントフィルタ警告を有効にする 設定では、プラットフォームのイベントフィルタ警告の生成を有効または無効にできます。個々のプラットフォームイベント警告設定とは関係なく設定できます。

 **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、PMBus サポートのない Dell システムではサポートされていませんが、Server Administrator を使用して設定できます。

 **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 電源装置がありません のプラットフォームイベントフィルタは、Server 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警告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。


1 なし
オペレーティングシステムがハングまたはクラッシュした場合に、何もしません。

1 システムを再起動する
オペレーティングシステムをシャットダウン後、システムを起動し、BIOS チェックを実行してオペレーティングシステムを再ロードします。


1 システムの電源を入れ直す
システムの電源を切り、一時停止後に電源を入れて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したいときなどに便利です。

1 システムの電源を切る
システムの電源をオフにします。

1 電力低減
CPU をスロットルします。

 **注意:** なし または 電力低減 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した場合には、指定したイベントが発生するとシステムが強制的にシャットダウンします。このシャットダウンはファームウェアによって実行され、オペレーティングシステムおよび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。

6. 送信する警告の 警告の生成 チェックボックスを選択します。

 **メモ:** 警告を生成するには、警告の生成 と プラットフォームイベント警告を有効にする 設定の両方を選択する必要があります。

7. 変更の適用 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戻る 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警告送信先の設定

プラットフォームのイベントフィルタ ウィンドウでは、プラットフォームイベントの警告を送信する宛先を選択することもできます。表示されている宛先の数によっては、各宛先アドレスの IP アドレスを個別に設定することもできます。設定した各宛先 IP アドレスにプラットフォームイベント警告が送信されます。

1. プラットフォームのイベントフィルタ ウィンドウで、宛先の設定 をクリックします。

宛先の設定 ウィンドウに宛先の数が表示されます。

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宛先の数はシステムによって異なります。

3. 送信先を有効にする 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警告が送信される IP アドレスです。

5. コミュニティ文字列 フィールドに、管理ステーションと管理下システムの間で送信されるメッセージの認証にシステムパスワードとして使う値を入力します。コミュニティ文字列(別名コミュニティ名)が管理ステーションと管理下システム間の各バケットに送信されます。

6. 変更の適用 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、**プラットフォームのイベントフィルタ** ウィンドウに戻ります。

[目次ページに戻る](#)

[目次ページに戻る](#)

設定と管理

Dell™ OpenManage™ Server Administratorバージョン 6.0.1 ユーザーズガイド

- [セキュリティ管理](#)
- [ユーザー特権の割り当て](#)
- [対応するWindows オペレーティングシステムでゲストアカウントと匿名アカウントを無効にする](#)
- [SNMP Agent の設定](#)
- [対応 Red Hat Enterprise Linux オペレーティングシステムと SUSE Linux Enterprise Server を実行しているシステム上でのファイアウォールの設定](#)

セキュリティ管理

Server Administrator は、ウェブベースの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、ロールベースのアクセス制御 (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特定して、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特権が 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関連しています。

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特権に応じて、異なるアクセス権を与えます。ユーザー特権には、ユーザー、パワーユーザー、システム管理者、昇格システム管理者の 4 つのレベルがあります。

- 1 ユーザー はほとんどの情報を表示できます。
- 1 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ときの警告処置を設定できます。
- 1 システム管理者 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無応答の場合の自動回復処理の設定、ハードウェア / イベント / およびコマンドログのクリアなどを実行できます。システム管理者はまた、電子メールを送信するシステムも設定可能です。
- 1 昇格システム管理者は情報を表示および管理できます。

Server Administrator は、ユーザー特権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、パワーユーザー特権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、システム管理者または昇格システム管理者特権でログインしたユーザーには読み取り、書き込み、管理のアクセス権を与えます。表 3-1 を参照してください。

表 3-1 ユーザー特権

ユーザー特権	アクセスタイプ	
	ビュー	管理
ユーザー	○	×
パワーユーザー	○	○
システム管理者	○	○
昇格システム管理者 (Linux のみ)	○	○

Server Administrator サービスにアクセスするための特権レベル

表 3-2 は、Server Administrator サービスにアクセスして管理できるユーザーレベルをまとめたものです。

表 3-2 Server Administrator ユーザー特権レベル

サービス	必要なユーザー特権レベル	
	ビュー	管理
計装	U、P、A、EA	P、A、EA
リモートアクセス	U、P、A、EA	A、EA
Storage Management (ストレージ管理)	U、P、A、EA	A、EA

表 3-3 は、表 3-2 で使用した特権レベルの略語の意味を説明しています。

表 3-3 Server Administrator ユーザー特権レベルの凡例

U	ユーザー
P	パワーユーザー
A	システム管理者
EA	昇格システム管理者

認証


Server Administrator 認証スキームは、正しいアクセスタイプが正しいユーザー特権に割り当てられていることを確認します。さらに、コマンドラインインタフェース(CLI)を起動したとき、現在のプロセスが実行しているコンテキストを Server Administrator 認証スキームが検証します。この認証スキームは、アクセス元が Server Administrator ホームページか CLI かを問わず、すべての Server Administrator 機能が正しく認証されていることを確認します。

Microsoft Windows 認証

対応する Microsoft® Windows® オペレーティングシステムでは、Server Administrator 認証に Integrated Windows Authentication(旧名称:NTLM)が使われます。この認証システムによって、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は、Server Administrator 認証は PAM(Pluggable Authentication Modules)ライブラリに基づいた様々な認証方法を用いています。ユーザーは、LDAP、NIS、Kerberos、Winbind などの異なるアカウント管理プロトコルを使用して、ローカルまたはリモートで Server Administrator にログインすることができます。


 **メモ:** Winbind の 32 ビット互換ライブラリが、オペレーティングシステムに存在しないため、SUSE Linux Enterprise Server(バージョン 9 Service Pack 3)上での Winbind および Kerberos を使用した Server Administrator 認証はサポートされません。

暗号化


管理下システムの身元を確認して保護するため、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のセキュリティを確保するには、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™ に正しくユーザー特権を割り当てる必要があります。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特権で 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へのアクセスを保護するには、Dell OpenManage ソフトウェアにアクセスできるユーザーアカウントのすべてにパスワードを割り当てる必要があります。パスワードを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制約を受けるため、Windows Server 2003 を実行しているシステムでは Dell OpenManage ソフトウェアにログインできません。

 **注意:** 重要なシステムコンポーネントへのアクセスを保護するには、対応 Windows オペレーティングシステムのゲストアカウントを無効にします。リモートスクリプトがその名前を使ってアカウントを有効にすることを防ぐために、アカウントの名前を変更することをお勧めします。

 **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したいときは、まず新規ユーザーをオペレーティングシステムに追加します。OpenManage ソフトウェア内で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 の使用方法に関する詳細は、「Microsoft Active Directory」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 へ移動します。
2. コンソールツリーで **ユーザー** を右クリックするか、新しいユーザーを追加するコンテナを右クリックし、**新規** → **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** をクリックしたら、**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のユーザー特権で 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 Administrator ユーザーの作成

Administrator(システム管理者)のアクセス権限が、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。ユーザー特権とパワーユーザー特権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保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 <ホームディレクトリ> -g <グループ> <ユーザー名>
```

<グループ>は `root` 以外のものとします。

 **メモ:** <グループ> 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<ユーザー名>`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る必要があります。

新しいユーザーはユーザーというグループ権限を使って 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 <ホームディレクトリ> -g root <ユーザー名>
```

 **メモ:** ルートをプライマリグループとして設定する必要があります。

2. `passwd<ユーザー名>`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る必要があります。

新しいユーザーはユーザーというグループ権限を使って 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 Server Administrator ユーザー権限を編集する

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保有するユーザーとしてログインする必要があります。

1. /etc にある `omarolemap` ファイルを開きます。
2. 以下をこのファイルに追加します。

<ユーザー名>[Tab]<ホスト名>[Tab]<権限>

表 3-4 に、ロールの定義を `omarolemap` に追加する凡例を示します。

表 3-4 OpenManage Server Administrator にロールの定義を追加する凡例

<ユーザー名>	<ホスト名>	<権限>
ユーザー名	ホスト名	Administrator
(+)グループ名	Domain(ドメイン)	User
ワイルドカード (*)	ワイルドカード (*)	User
[Tab] = \t (tab 文字)		

表 3-5 に、ロールの定義を `omarolemap` に追加する凡例を示します。

表 3-5 OpenManage Server Administrator にロールの定義を追加する例

<ユーザー名>	<ホスト名>	<権限>
Bob	Ahost	Poweruser
+ルート	Bhost	Administrator
+ルート	Chost	Administrator
Bob	*.aus.amer.com	Poweruser
Mike	192.168.2.3	Poweruser

3. ファイルを保存して閉じます。
4. コマンドラインから次のコマンドを実行して、接続サービスを再起動します。

```
service dsm_om_connsvc restart
```

メモ: 変更を反映するには、接続サービスを再起動する必要があります。

omarolemap ファイル使用の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以下に示します。

1. `omarolemap` ファイルの以下のデフォルトエントリは削除しないでください。

1	root	*	Administrator
1	+ルート	*	Poweruser
1	*	*	User

1. `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。
1. `omarolemap` ファイルでユーザーの権限が低下した場合、Server Administrator はデフォルトのオペレーティングシステムでのデフォルトユーザー権限を使用します。
1. localhost や 127.0.0.1 といった、<Host_Name>、のループバックアドレスは使用しないでください。
1. 接続サービスを再起動したときに /etc/omarolemap ファイルの変更が有効にならない場合は、コマンドログでエラーを調べてください。
1. `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。
1. グループ名に + を前付けします。
1. 同じ <Host_Name> 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と、Server Administrator はオペレーティングシステムのデフォルトユーザー権限を使用します。
1. [Tab] の代わりに空白文字を列の区切り文字として使うこともできます。

対応するWindowsオペレーティングシステムでゲストアカウントと匿名アカウントを無効にする

 **メモ:** この手順を実行するには、システム管理者でログイン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. 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. **ゲスト**または**USR_システム名**ユーザーアカウントをクリックします。
4. **処置**をクリックし、**プロパティ**を選択します。
5. **アカウントを無効にする**を選択し、OK をクリックします。


X の付いた赤い丸がユーザー名の上に表示されます。アカウントは無効になります。


SNMP Agent の設定

Server Administrator は、対応するすべてのオペレーティングシステムで管理ネットワーク管理プロトコル(SNMP)システム管理規格をサポートしています。SNMP サポートは、オペレーティングシステム、またオペレーティングシステムの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されてい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過程で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 などの対応システム管理プロトコル規格がインストールされている必要があります。

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ることができます。Dell OpenManage? IT Assistant や Array Manager などの管理アプリケーションと正しく相互作用するように 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:** デフォルトの SNMP エージェント設定には、通常、**public** のような SNMP コミュニティ名が含まれています。セキュリティを強化するため、この SNMP コミュニティ名は、デフォルト値でないものに変更します。SNMP コミュニティ名の変更に関しては、該当する下記の項を参照してください。詳細なガイドラインは、『Dell Power Solutions (Dell パワースリュージョン)』誌の 2003 年 5 月号にある「Securing an SNMP Environment (SNMP 環境のセキュリティ)」の記事を参照してください。このマガジンは www.dell.com/powersolutions から入手できます。

 **メモ:** SNMP Set 操作は、Server Administrator バージョン 5.2 以降ではデフォルトで無効になっています。Server Administrator は SNMP Set 操作を有効または無効にする機能をサポートしています。**プリファランス** 下の **Server Administrator SNMP 設定** ページを使うか、Server Administrator コマンドラインインタフェース (CLI) を使って、Server Administrator での SNMP Set 操作を有効または無効にできます。Server Administrator CLI 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*』を参照してください。


 **メモ:** IT Assistant で Server Administrator を実行中のシステムから管理情報を取得するには、IT Assistant で使用するコミュニティ名が Server Administrator を実行中の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 で Server Administrator を実行しているシステムの情報を変更したり処置を実行するには、IT Assistant で使用するコミュニティ名が Server Administrator を実行中のシステムで Set 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 で 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できるように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。

1. 「[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](#)」
1. 「[対応 Red Hat Linux 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](#)」
1. 「[対応SUSE Linux Enterprise Server オペレーティングシステムを実行しているシステムでの SNMP エージェントの設定](#)」

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

Server Administrator は、Windows SNMP エージェントによって提供される 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相互作用するように 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、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。

リモートホストによる SNMP アクセスを有効にする

Windows Server 2003 はデフォルトではリモートホストからの SNMP パケットを受け入れません。Windows Server 2003 を実行しているシステムで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したい場合は、リモートホストから SNMP パケットを受け入れるように SNMP サービスを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を実行しているシステムでリモートホストから SNMP パケットを受け取れるようにするには、次の手順を実行してください。

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、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 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** ウィンドウを閉じます。
2. 必要に応じて、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。
 - a. コミュニティ名を追加するには、**受け付けるコミュニティ名** リストから **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. システムを管理できるコミュニティ名 (デフォルトは public) を **コミュニティ名** テキストボックスに入力して、**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。
 - c. コミュニティ名を変更するには、**受け付けるコミュニティ名** 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。
 - d. **コミュニティ名** テキストボックスで、システムを管理できるシステムのコミュニティ名を変更し、**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 アトリビュートを変更するには、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** ウィンドウを閉じます。
2. 必要に応じて、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** タブをクリックして、コミュニティのアクセス権限を変更します。
6. **受け付けるコミュニティ名** 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システム設定

Server Administrator は、センサーや他の監視パラメータのステータスの変化に応じて SNMP トラップを生成します。SNMP トラップが Management Station に送信されるためには、Server Administrator のトラップ送信先を 1 つまたは複数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、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. **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。
 - c. **SNMP サービス設定** ウィンドウが表示されます。


トラップ送信先を入力して、**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。

6. **OK** をクリックして、変更を保存します。

対応 Red Hat Linux 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

Server Administrator は ucd-snmp または net-snmp SNMP エージェントによって提供された 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相互作用するように 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、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、1.3.6.1.4.1.674 の OID 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 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「パブリック」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 Systems Management 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 はインストール中にデフォルト SNMP 設定を検出すると、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の MIB ツリー全体に読み取り専用アクセスを与えます。Server Administrator は、`/etc/snmp/snmpd.conf` SNMP エージェント設定ファイルを 2 つの方法で変更します。

まず、次の行がない場合は、それを追加して MIB ツリー全体の表示を作成します。

```
view all included .1
```


次に、デフォルトの「アクセス」行を変更して、「パブリック」コミュニティの MIB ツリー全体に読み取り専用アクセス権を与えます。Server Administrator は次の行を探します。

```
access notConfigGroup "" any noauth exact systemview none none
```

Server Administrator で上の行が見つかったら、次のように変更されます。

```
access notConfigGroup "" any noauth exact all none none
```

デフォルト SNMP エージェント設定をこのように変更すると、パブリックコミュニティの MIB ツリー全体に読み取り専用アクセスが与えられます。

 **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 Multiplexing(SMUX)プロトコルを使って SNMP エージェントと通信を行います。Server Administrator SNMP は SNMP エージェントに接続するとき、自らを SMUX ピアとして識別するオブジェクト識別子を SNMP エージェントに送信します。オブジェクト識別子は SNMP エージェントとともに設定される必要があるため、Server Administrator はインストール中、SNMP エージェント設定ファイルに `/etc/snmp/snmpd.conf` が存在しない場合、これを追加します。

```
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 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 を実行中のシステムから管理情報を取得するのに使う SNMP コミュニティ名を変更し、SNMP エージェント設定ファイル `/etc/snmp/snmpd.conf` を編集するには、次の手順を実行します。

1. 次の行を見つけてください。

```
com2sec publicsec default public
```

または

```
com2sec notConfigUser default public
```

2. `public` の部分を SNMP コミュニティ名に置き換えて、この行を編集します。編集後の行は次のようになります。

```
com2sec publicsec default <コミュニティ名>
```

または

```
com2sec notConfigUser default <コミュニティ名>
```

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。

```
service snmpd restart
```

SNMP Set 操作を有効にする

IT Assistant を使って Server Administrator アトリビュートを変更するには、Server Administrator を実行しているシステムで SNMP Set 操作が有効になっている必要があります。

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. 次の行を見つけてください。

```
access publicgroup "" any noauth exact all none none
```

または

```
access notConfigGroup "" any noauth exact all none none
```

2. 最初の `none` を `all` に置き換えて行を編集します。編集後の行は次のようになります。

```
access publicgroup "" any noauth exact all all none
```

または

```
access notConfigGroup "" any noauth exact all all none
```

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。

```
service snmpd restart
```

SNMP トラップを管理ステーションに送信するシステム設定

Server Administrator は、センサーや他の監視パラメータのステータスの変化に応じて SNMP トラップを生成します。SNMP トラップが管理ステーションに送信されるためには、Server Administrator を実行するシステムでトラップ送信先を 1 つまたは複数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. ファイルに次の行を追加します。

```
trapsink <IPアドレス> <コミュニティ名>
```



<IPアドレス> は 管理ステーションの IP アドレスを表し、<コミュニティ名> は、SNMP コミュニティ名を表します。

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 オペレーティングシステムを実行しているシステムでの SNMP エージェントの設定

Server Administrator は ucd-snmp または net-snmp エージェントによって提供された SNMP サービスを使用します。リモートホストからの SNMP アクセスを有効にするための SNMP エージェントの設定、コミュニティ名の変更、セット操作の有効化、および管理ステーションへのトラップの送信が可能です。IT Assistant などの管理アプリケーションと正しく相互作用するように 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:** SUSE Linux Enterprise Server (バージョン 10) では、SNMP エージェントの設定ファイルは `/etc/snmpd.conf` に配置されています。
-  **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 インストール処置

Server Administrator SNMP は、SNMP Multiplexing (SMUX) プロトコルを使って SNMP エージェントと通信を行います。Server Administrator SNMP は SNMP エージェントに接続するとき、自らを SMUX ピアとして識別するオブジェクト識別子を SNMP エージェントに送信します。このオブジェクト識別子は SNMP エージェントとともに設定される必要があるため、Server Administrator はインストール中、SNMP エージェント設定ファイル (`/etc/snmpd.conf` または `/etc/snmp/snmpd.conf`) が存在しない場合、これを追加します。

```
smuxpeer .1.3.6.1.4.1.674.10892.1
```

リモートホストからの SNMP アクセスを有効にする

SUSE Linux Enterprise Server オペレーティングシステムのデフォルトの SNMP エージェント設定は、「パブリック」コミュニティに対してローカルホストからのみによる MIB ツリー全体へ読み取り専用のアクセスを与えます。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` にログし、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っ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 を実行しているシステムへの 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/snmpd.conf` または `/etc/snmp/snmpd.conf` を編集し、次の手順を実行します。

1. 次の行を見つけます。

```
rocommunity public 127.0.0.1
```

2. 127.0.0.1 をリモートホストの IP アドレスに書き換えてこの行を編集またはコピーします。編集後の行は次のようになります。

```
rocommunity public IP_address
```

-  **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
```

特定のリモートホストから Server Administrator を実行しているシステムへの 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/snmpd.conf` または `/etc/snmp/snmpd.conf` を編集し、次の手順を実行します。

1. 次の行を見つけます。

```
rocommunity public 127.0.0.1
```

2. 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
```

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
```

SNMP コミュニティ名の変更

SNMP コミュニティ名の設定によって、SNMP を使ってシステムを管理できる管理ステーションが決まります。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 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 を実行中のシステムから管理情報の取得に使うデフォルトの SNMP コミュニティ名を変更するには、SNMP エージェント設定ファイル `/etc/snmpd.conf` また

は `/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. `public` を新しい SNMP コミュニティ名に置き換えて、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 <コミュニティ名> 127.0.0.1
```

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
```

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 Set 操作が有効化されている必要があります。

 **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 を実行中のシステムにおいて 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/snmpd.conf` または `/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. `rocommunity` を `rwcommunity` に置き換え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。

```
rwcommunity public 127.0.0.1
```

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
```

SNMP トラップを管理ステーションに送信するシステム設定

Server Administrator は、センサーや他の監視パラメータのステータスの変化に応じて SNMP トラップを生成します。SNMP トラップが管理ステーションに送信されるためには、Server Administrator を実行するシステムでトラップ送信先を 1 つまたは複数設定する必要があります。

管理ステーションへトラップを送信するように Server Administrator を実行しているシステムを設定するには、SNMP エージェント設定ファイル `/etc/snmpd.conf` または `/etc/snmp/snmpd.conf` を編集し、次の手順を実行してください。

1. ファイルに次の行を追加します。

```
trapsink <IP アドレス> <コミュニティ名>
```

<IP アドレス>は 管理ステーションの IP アドレスを表し、<コミュニティ名> は、SNMP コミュニティ名を表します。

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。

```
/etc/init.d/snmpd restart
```


対応 Red Hat Enterprise Linux オペレーティングシステム と SUSE Linux Enterprise Server を実行してい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 をインストールしているときにファイアウォールセキュリティを有効にすると、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。IT Assistant などの SNMP 管理アプリケーションを有効にして Server Administrator からの情報を検出して取得するには、少なくとも 1 つの外部ネットワークインタフェースの SNMP ポートが開いている必要があります。Server Administrator によって外部ネットワークインタフェースの SNMP ポートがファイアウォールで開かれていないことが検出されたら、Server Administrator は警告メッセージを表示してメッセージをシステムログに記録します。

SNMP ポートを開くには、ファイアウォールを無効にし、ファイアウォールの外部ネットワークインタフェース全体を開くか、ファイアウォールで少なくとも 1 つの外部ネットワークインタフェースの SNMP ポートを開きます。この処理は、Server Administrator が起動する前か後で行うことができます。

前に説明した方法のいずれかを使用して RHEL 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。

Choose a Tool(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 Firewall Configuration(ファイアウォール設定)を選択し、<Enter> を押します。

Firewall Configuration(ファイアウォール選択)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てからスペースバーを押して希望のセキュリティレベルを選択します。選択したセキュリティレベル にアスタリスクが付きます。

 **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> を押してください。デフォルトの SNMPポート番号は 161 です。X Window System グラフィカルユーザーインターフェースを使用している場合は、新しいバージョンの Red Hat Enterprise Linux では <F1> を押してもファイアウォールのセキュリティレベルに関する情報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、No firewall(ファイアウォールなし)か Disabled(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。

Firewall Configuration - Customize(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くか、すべてのネットワークインタフェースの SNMP ポートだけを開くかを選択します。

- a. ネットワークインタフェース全体を開くには、<Tab>を押して信頼できるデバイスの 1 つに進んでスペースバーを押します。デバイス名の左側のボックスにアスタリスクが付いたら、インタフェース全体が開くことを示します。
- 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 他のポート に進んで 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。

Firewall Configuration(ファイアウォール選択)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。

Choose a Tool(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。

SUSE Linux Enterprise Server 上の SNMP ポートを開くには、次の手順を実行します。

1. コンソール: a で次を実行し、SuSEfirewall2 を設定します。# 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 と 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。

[目次ページに戻る](#)

[目次ページに戻る](#)

Server Administrator の使用

Dell™ OpenManage™ Server Administratorバージョン 6.0.1 ユーザーズガイド

- [Server Administrator セッションの開始](#)
- [ログインとログアウト](#)
- [Server Administrator ホームページ](#)
- [オンラインヘルプの使い方](#)
- [ユーザー設定ホームページの使い方](#)
- [Server Administrator コマンドラインインタフェースの使い方](#)
- [Dell Systems Management Server Administration 接続サービスおよびセキュリティ設定](#)
- [Server Administrator の制御](#)

Server Administrator セッションの開始

ローカルシステムで Server Administrator セッションを開始するには、デスクトップの Dell™ OpenManage™ Server Administrator アイコンをクリックします。

リモートシステムで Server Administrator セッションを開始するには、Webブラウザを開いて次の 1 つをアドレスフィールドに入力し、<Enter> を押します。

https://ホスト名:1311


ホスト名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。


または


https://IP アドレス:1311

IP アドレスは、管理下システムの IP アドレス、1311 はデフォルトのポート番号を表します。

Server Administrator ログイン ウィンドウが表示されます。


 **メモ:** ブラウザで有効な応答を受信するために、アドレスフィールドに https:// (http:// ではない) と入力します。

 **メモ:** Dell™ OpenManage™ Server Administrator のデフォルトポートは 1311 です。ポート番号は必要に応じて変更できます。システムプリファランスの設定手順は、「[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。


 **メモ:** Internet Explorer® バージョン 7.0 を使って Server Administrator を起動する場合、セキュリティ証明書の問題を表示する警告のページが表示される場合があります。システムセキュリティを確保するには、新しい X.509 証明書を生成し、既存の X.509 証明書を再利用するか、証明機関 (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をお勧めします。このような証明に関する警告メッセージを受けることのないよう、使用する証明書は信頼できる CA から受ける必要があります。X.509 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。

ログインとログアウト

Server Administrator にログインするには、事前にも割り当てられた **ユーザー名** と **パスワード** をシステム管理 **ログイン** ウィンドウの該当するフィールドに入力します。ログインページをバイパスし、デスクトップの **Dell OpenManage Server Administrator** アイコンをクリックして Server Administrator ウェブアプリケーションにアクセスする方法については、「[シングルサインオン](#)」を参照してください。

 **メモ:** Server Administrator にログインするには、事前にも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手順は、「[設定と管理](#)」を参照してください。

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。


 **メモ:** **アプリケーション** ドロップダウンメニューは、1 つの Dell OpenManage Server Administrator コンポーネントにしかアクセスできない、システムでは選択不能フィールドとして表示されます。2 つ以上の Dell OpenManage Server Administrator コンポーネントが管理下システムで使用できる場合にのみ、ドロップダウンメニューは機能します。

Microsoft® Active Directory® を使用してログインするには、**Active Directory** ログイン チェックボックスを選択します。

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](#)」上の **ログアウト** をクリックします。**ログアウト** ボタンは、各 Server Administrator ホームページの右上隅にあります。

シングルサインオン

Microsoft Windows® 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、十分な権限を持つログインユーザーはすべてログインページをバイパスし、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、<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q258063> の Knowledge Base の記事を参照してください。

ローカルマシンアクセスの場合は、マシンに適切な権限 (ユーザー、パワーユーザー、または管理者) のあるアカウントを持っていることが必要です。他のユーザーは Microsoft Active Directory と照合して認証されます。

Microsoft Active Directory 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、次の追加パラメータを渡す必要があります。

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

プラグイン名は *omsa*、*ita* などになります。

次に、例を示します。

```
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
```

プラグイン名は *omsa*、*ita* などになります。

次に、例を示します。


```
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 (現在ログインしており、適切な権限を持っている場合)。

対応 Microsoft Windows Server 2003 オペレーティングシステム環境のシステム

対応の Windows Server® 2003 オペレーティングシステム環境のリモート管理下システムから 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が出ます。

Internet Explorer

1. ご利用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** をクリックします。
2. **信頼済みサイト** のアイコンをクリックします。
3. **サイト** をクリックします。
4. 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。
5. **カスタムレベル** をクリックします。

Windows 2000 の場合

- **その他** の下の、**ページの自動読み込み** のラジオボタンを選択します。
- **Active Scripting** の下の、**有効** ラジオボタンを選択します。

Windows 2003 の場合

- **その他** の下の、**ページの自動読み込み** のラジオボタンを選択します。
- **Active Scripting** の下の、**有効** ラジオボタンを選択します。
- **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** ラジオボタンを選択します。

1. **OK** をクリックし新しい設定を保存します。ブラウザを閉じて Server Administrator にログインします。

Server Administrator に、ユーザーの資格情報のプロンプトを表示せずにシングルサインオンするには、次の手順を実行してください。


1. ご利用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** をクリックします。
2. **信頼済みサイト** のアイコンをクリックします。
3. **サイト** をクリックします。
4. 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。
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的にログオンする** のラジオ ボタンを選択してください。

7. OK をクリックし新しい設定を保存します。ブラウザを閉じて Server Administrator にログインします。

Mozilla

1. ブラウザを起動します。
2. **編集**→**プリファランス** をクリックします。
3. **詳細設定**→**スクリプトとプラグイン** をクリックします。
4. **ナビゲータ** チェックボックスで **JavaScript を有効にする** が選択されていることを確認します。
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 を使用中は、Web ブラウザのツールバーボタン(**戻る**、**更新**)を使用しないでください。Server Administrator のナビゲーションツールだけを使用してください。

いくつか例外がありますが、Server Administrator には 3 つの主な領域があります。

1. [グローバルナビゲーションバー](#) は一般サービスへのリンクを提供します。
1. [システムツリー](#)には、ユーザーのアクセス特権に基づいて、表示可能なすべてのシステムオブジェクトが表示されます。
1. [処置 ウィンドウ](#)には、ユーザーのアクセス特権に基づいて、選択したシステムツリーオブジェクトで使用可能な管理処置が表示されます。処置ウィンドウには 3 つの機能領域があります。
 - 処置タブには、ユーザーのアクセス特権に基づいて、選択したオブジェクトで使用可能な一次処置または処置のカテゴリが表示されます。
 - 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](#) には、ユーザーのアクセス特権に基づいて、選択したシステムツリーオブジェクト、処置タブ、およびサブカテゴリの情報が表示されます。

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特権 がウィンドウの右上隅に表示されます。

[表 4-1](#) システムに Server Administrator がインストールされたときに GUI フィールド名と該当システムが一覧表示されます。

表 4-1 以下の GUI フィールド名に対するシステムの可用性

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

[図 4-1](#) は、非モジュラーシステムに管理者権限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 4-1 サンプル Server Administrator ホームページ - 非モジュラーシステム



処置 ウィンドウ

図 4-2 は、モジュラーシステムに管理者権限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 4-2 サンプル Server Administrator ホームページ - モジュラーシステム



処置 ウィンドウ

システムツリーの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。主なカテゴリを選択するには処置タブをクリックし、詳細情報や特定の処置にアクセスするには処置タブのサブカテゴリをクリックして、処置ウィンドウを移動します。処置ウィンドウのデータ領域に表示される情報は、システムログから、状態インジケータ、システムプローブページまでさまざまです。処置ウィンドウのデータ領域で下線が付いたアイテムには、さらに詳細レベルの機能があります。下線が付いたアイテムをクリックすると、処置ウィンドウに詳細レベルを持つ新しいデータ領域が作成されます。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、正常性状態をモニタした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状態が表示されます。

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 タブに含まれてい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。

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から使用可能です。

- 1 **プリファランス** をクリックすると、**プリファランス** ホームページが開きます。「[ユーザー設定ホームページの使い方](#)」を参照してください。
- 1 **サポート** をクリックすると、Dell サポートの Web サイトに接続します。
- 1 **ヘルプ** をクリックすると、オンラインヘルプのウィンドウが開きます。「[オンラインヘルプの使い方](#)」を参照してください。
- 1 **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。
- 1 **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を終了します。

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リストにします。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。モジュラー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**、**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、展開されていてそれ以上展開できないエントリを指します。

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処置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と、使用できるすべてのユーザーオプションがサブカテゴリのリストとして表示されます。

システム / サーバーモジュールツリーのオブジェクトをクリックすると、コンポーネントの処置ウィンドウが開き、使用できる処置タブが表示されます。データ領域にはデフォルトでは、選択したオブジェクトの最初の処置 タブから事前選択されたサブカテゴリが表示されます。事前選択された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

をクリックすると処置ウィンドウが開き、そのウィンドウのデータ領域に **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の処置タブの下にあります。データ領域は、システムコンポーネントのタスクを実行したり詳細を表示したりする場所です。ウィンドウに表示される内容は、現在選択されているシステムツリーオブジェクトと処置 タブによって異なります。たとえばシステムツリーから **BIOS** を選択すると、デフォルトでは **プロパティ** タブが選択され、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、下線アイテム、およびゲージインジケータなど多くの共通機能があります。

システム / サーバ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 4-2 システム / サーバモジュールコンポーネントステータスインジケータ

	緑のチェックマークは、コンポーネントが健全(正常)であることを示します。
	感嘆符が入った黄色の三角形は、コンポーネントが警告(非重大)状態にあることを示します。警告状態は、プローブまたはその他のモニタツールによって特定の最小値や最大値を満たさないコンポーネントが検出された場合に発生します。警告状態は早めの対処を要します。
	赤い X は、コンポーネントがエラー(重要)状態にあることを示します。重要な状態は、プローブまたはその他のモニタツールによって特定の最小値や最大値を満たさないコンポーネントが検出された場合に発生します。重要な状態は早急な対処を要します。
	ブランクスペースは、コンポーネントの正常性が不明であることを示します。

タスクボタン

Server Administrator ホームページから開いたウィンドウのほとんどには、少なくとも **印刷**、**エクスポート**、**電子メール**、**更新** の 4 つのボタンが表示されます。一部のウィンドウにはその他のタスクボタンも含まれています。たとえば、ログ ウィンドウには、**名前を付けて保存** ボタンと **ログのクリア** ボタンもあります。各タスクボタンに固有の情報は、Server Administrator ホームページの **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詳細が表示されます。

- 1 **印刷** をクリックすると、開いているウィンドウのコピーがデフォルトのプリンタに印刷されます。
- 1 **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を一覧にしたテキストファイルが作成されます。エクスポートファイルは指定の場所に保存されます。データフィールド値を区切り文字をカスタマイズする手順は、「[ユーザーとシステムのプリファランスの設定](#)」を参照してください。
- 1 **電子メール** をクリックすると、指定の電子メール受取人に宛てた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とデフォルトの電子メール 受取人を設定する手順は、「[ユーザーとシステムのプリファランスの設定](#)」を参照してください。
- 1 **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。
- 1 **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。
- 1 **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。

 **メモ:** エクスポート、電子メール、名前を付けて保存、および ログのクリア ボタンは、パワーユーザー特権または管理者権限でログインしたユーザーにのみ表示されます。

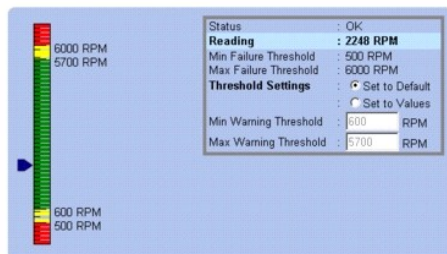
下線付きアイテム

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、および電圧プローブはそれぞれゲージインジケータで表されます。たとえば、[図 4-3](#)には、システムの CPU ファンプローブからの読み取り値が表示されています。

図 4-3 ゲージインジケータ



オンラインヘルプの使い方

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。グローバルナビゲーションバーの **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とユーザー特権レベルに従って、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。

ユーザー設定ホームページの使い方

プリファランス ホームページのデフォルトウィンドウは、**プリファランス** タブにある **アクセス設定** です。

プリファランスホームページから、「ユーザー」と「パワーユーザー」特権を持つユーザーへのアクセスを制限したり、Simple Network Management Protocol(SNMP)パスワードを設定したり、ユーザーとセキュリティ保護されたポートシステムのプリファランスを設定できます。

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。

- 1 グローバルナビゲーションバーは一般サービスへのリンクを提供します。
 - **Server Administrator に戻る** をクリックすると、Server Administrator のホームページに戻ります。
- 1 プリファランスホームページの左ウィンドウ枠(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、Managed System のプリファランスカテゴリが表示されません。
- 1 処置ウィンドウでは、Managed System で使用できる設定とプリファランスを表示します。

図 4-4 にサンプルプリファランスホームページのレイアウトを示します。



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

Server Administrator コマンドラインインターフェース(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 は、特定のタスクを念頭に置いたユーザーがシステム情報を迅速に取得するのに役立ちます。たとえば CLI を使用すると、管理者は特定の時間に実行されるバッチプログラムやスクリプトを作成できます。これらのプログラムが実行されると、ファン RPM などの対象コンポーネントについてレポートを入手できます。追加のスクリプトと共に CLI を使用することで、システム使用状況が高いときにデータをキャプチャし、システム使用状況が低いときの測定値と比較できます。コマンド結果はファイルに転送して、あとで分析できます。レポートは、管理者が使用パターンを調整したり、新しいシステムリソース購入を裏証したり、問題のあるコンポーネントの正常性に注目する場合に役立ちます。

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ーフェースユーザーズガイド』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

この項には以下のトピックがあります。

- 1 [ユーザーとシステムのプリファランスの設定](#)
- 1 [X.509 証明書管理](#)

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を設定します。

 **メモ:** ユーザー、またはシステム設定をリセットするには、「システム管理者」特権でログインする必要があります。

次の手順を実行して、ユーザープリファランスを設定します。

- 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. 事前に選択されている電子メール受信者を追加するには、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、**変更の適用** をクリックします。

 **メモ:** 任意のウィンドウで **電子メール** をクリックすると、そのウィンドウの添付 HTML ファイルと一緒に電子メールアドレスに送信するメッセージが送信されます。

4. ホームページの外観を変更するには、**スキン** または **スキーム** フィールドで別の値を選択して **変更の適用** をクリックします。

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** と **Webサーバー** タブをクリックします。


3. **サーバー一般設定** ウィンドウで、必要に応じてオプションを設定します。

1. **セッションのタイムアウト** 機能を使うと、セッションがアクティブでいられる時間を制限できます。指定の時間(分)、ユーザー操作がない場合に Server Administrator をタイムアウトにするには、**有効** ラジオボタンを選択します。セッションがタイムアウトしたユーザーは、セッションを続行するにはログインし直す必要があります。Server Administrator セッションタイムアウト機能を無効にするには、**無効** ラジオボタンを選択します。


1. **HTTPS ポート** フィールドでは、Server Administrator のセキュアポートを指定します。Server Administrator のデフォルトのセキュアポートは 1311 です。

 **メモ:** ポート番号を、無効な番号または使用中のポート番号に変更すると、その他のアプリケーションまたはブラウザが Managed System の Server Administrator にアクセスできなくなる可能性があります。デフォルトポートの一覧については、『Dell OpenManage インストールとセキュリティユーザーズガイド』を参照してください。

1. **IP アドレスのバインド先** フィールドで、セッション開始時に Server Administrator がバインドする管理下システムの 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 アドレスをバインドする場合は、**すべて** ラジオボタンを選択します。特定の IP アドレスにバインドする場合は、**特定** ラジオボタンを選択します。

 **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。

1. **SMTP サーバー名** フィールドと **SMTP サーバーの DNS サフィックス** フィールドでは、所属会社または組織の SMTP とドメイン名サーバー(DNS)のサフィックスを指定します。Server Administrator で電子メールを送信できるようにするには、適切なフィールドに所属会社または組織の SMTP サーバーの IP アドレスと DNS サフィックス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。

1. **コマンドログサイズ** フィールドに、**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。

1. **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者の URL を指定します。

1. **カスタム区切り文字** フィールドでは、**エクスポート** ボタンを使用して作成されたファイルでデータフィールドを区切る文字を指定します。; 文字はデフォルトの区切り文字です。その他のオプションは !、@、#、\$、%、^、*、-、@、:、|、および、です。

1. **SSL 暗号化** フィールドで、セキュリティ保護された 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、**オートネゴシエート** および **128 ビット以上** があります。

- **オートネゴシエート:** ブラウザの暗号化のレベルに関係なく接続できます。ブラウザは、Server Administrator web server と自動的にネゴシエーションして、そのセッションで使用可能な最も高い暗号化レベルを選択します。暗号化レベルの低いレガシーブラウザでも、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レベルを持つブラウザからの接続を可能にします。すべての確立されたセッションに、使用されるブラウザに基づいて次の暗号スイートのうちの 1 つが適用されます。

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 ビットまたは 56 ビットなど低い SSL 暗号レベルのブラウザでは接続できません。

 **メモ:** 変更を適用するには、Server Administrator web server を再起動します。


 **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. **サーバー一般設定** ウィンドウのオプション設定が完了したら、**変更の適用** をクリックします。

X.509 証明書管理

リモートシステムの身元を確認し、リモートシステムとやり取りする情報を他の人が閲覧したり変更したりできないようにするには、Web 証明書が必要です。システムのセキュリティを確保するために、以下の励行を推奨します。

- 1 新しい X.509 証明書の生成、既存の X.509 証明書の再利用、あるいはルート証明書または証明書チェーンの認証局 (CA) からのインポートを行う。
- 1 Server Administrator がインストールされているすべてのシステムが一意的なホスト名を持つ。

 **メモ:** 証明書管理を実行するには、Administrator (管理者) 権限でログインする必要があります。


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、**Web Server** タブをクリックしてから **X.509 証明書** をクリックします。

次のオプションを使用できます。

- 1 **新しい X.509 証明書の作成** - このオプションは、Server Administrator にアクセスするための証明書を作成するのに使用します。
- 1 **既存の X.509 証明書の再利用** - このオプションは、あなたの会社が所有権を持つ既存の証明書を選択して、この証明書を使って Server Administrator へのアクセスを制御します。
- 1 **ルート証明書のインポート** - このオプションは、信頼される認証局から受け取ったルート証明書と証明書の応答 (PKCS#7 形式) をインポートできるようにします。
- 1 **CA からの証明書チェーンのインポート** - このオプションは、信頼される認証局から証明書の応答 (PKCS#7 形式) をインポートできるようにします。信頼される認証局には、Verisign、Thawte、Entrust があります。

Server Administrator の制御

Server Administrator は、Managed System を再起動するたびに自動的に起動します。Server Administrator の手動起動、停止、再起動を行うには、次の手順を使用します。

 **メモ:** Server Administrator を制御するには、管理者権限でログインする必要があります (対応の Red Hat® Enterprise Linux® または SUSE® Linux Enterprise Server オペレーティングシステムでは root でログイン)。

Server Administrator の起動

Microsoft Windows オペレーティングシステム

Server Administrator を開始するには、サポートしている Microsoft Windows オペレーティングシステム環境のシステムで、以下の手順で実行します。

1. **サービス** ウィンドウを開きます。
2. **Dell Systems Management Server Administration (DSM SA) 接続サービス** アイコンを右クリックします。
3. **Start (開始)** をクリックします。

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

対応の Red Hat Enterprise Linux または SUSE Linux Enterprise Server オペレーティングシステム環境のシステムで Server Administrator を起動するには、コマンドラインから次のコマンドを実行します。

```
dsm_om_connsvc start
```

Server Administrator の停止

Microsoft Windows オペレーティングシステム

Server Administrator を停止するには、次の手順を実行します。

1. **サービス** ウィンドウを開きます。
2. **DSM SA Connection Service** アイコンを右クリックします。
3. **停止** をクリックします。

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

対応の Red Hat Enterprise Linux または SUSE Linux Enterprise Server オペレーティングシステム環境のシステムで Server Administrator を停止するには、コマンドラインから次のコマンドを実行します。

```
dsm_om_connsvc stop
```

Server Administrator の再起動

対応 Microsoft Windows オペレーティングシステム

Server Administrator を停止するには、次の手順を実行します。

1. **サービス** ウィンドウを開きます。
2. **DSM SA Connection Service** アイコンを右クリックします。
3. **再起動** をクリックします。

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

対応の Red Hat Enterprise Linux または SUSE Linux Enterprise Server オペレーティングシステム環境のシステムで Server Administrator を再起動するには、コマンドラインから次のコマンドを実行します。

```
dsm_om_connsvc restart
```

[目次ページに戻る](#)


[目次ページに戻る](#)

バージョン 6.0.1 の新機能

Dell™ OpenManage™ Server Administratorバージョン 6.0.1 ユーザーズガイド

OpenManage Server Administrator の新リリースに新しく追加された主な機能について説明します。

- 1 新しい xx1x システムのサポート。
- 1 以下のシステムコンポーネントのサポート:
 - o 追加属性の前面パネル LCD 表示の設定(システム名、MAC アドレス、IP アドレスなど)
 - o iDRAC6 Enterprise の存在、および存在する場合はストレージサイズの表示
 - o xx1x システムの一部である新しい PCI デバイスの表示
 - o CPU ターボモードの表示
 - o 新しいメモリアイプの表示(DDR3 Registered、DDR3 Unregistered)
 - o 新しいスロットタイプの表示(PCIe Gen1/2)
 - o 導入時に NUMA(Non-Uniform Memory Architecture)の有効化 / 無効化
 - o すべての LOM に対し個別にネットワークコントローラ - サイドバンドインタフェースのサポートを有効化
 - o メモリ動作モードの表示(オプティマイザ、ミラー、アドバンスド ECC)
 - o AC 電源回復遅延時間の設定
 - o xx1x システムを起動する該当プラットフォームのシリアル接続用 COM ポートの設定
 - o 物理 NIC 属性と送信 / 受信統計情報の表示
- 1 強化された電源監視のサポート:
 - o 電力消費量(BTU と W)の表示
 - o ピーク電力ヘッドルームと瞬時ヘッドルームのサポート
 - o ユーザー定義可能な電力バジェットキャップのサポート
 - o 最大および最小予測電力消費量の表示をサポート
 - o 電源装置の定格入力電力の表示をサポート
 - o ピーク電力消費量のイベント警告機能のサポート
 - o 電源プロファイルオプションのサポート - 省電力モードと高性能モード
- 1 Internet Protocol Version 6 のサポート:
 - o このリリースでは、IPv4 と IPv6 がサポートされています。

 **メモ:** 対応オペレーティングシステムのリストについては、デル提供メディアまたはデルサポートサイト support.dell.com 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。

[目次ページに戻る](#)