

Dell OpenManage Server Administrator バージョン 6.4 ユーザーズガイド

[はじめに](#)

[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\(FAQ\)](#)

メモおよび注意

 **メモ:** コンピュータを使いやすくするための重要な情報を説明しています。

 **注意:** ハードウェアの損傷やデータの損失の可能性を示し、その危険を回避するための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。
© 2010 すべての著作権は Dell Inc. にあります。

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®、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。EMC® は EMC Corporation の登録商標です。Java® は米国における Sun Microsystems, Inc. の商標または登録商標です。Novell® および SUSE® は、米国およびその他の国における Novell, Inc. の登録商標です。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。VMware® は米国およびその他の管轄域における VMware, Inc. の登録商標で、ESX Server™ は同社の商標です。Mozilla® および Firefox® は Mozilla Foundation の登録商標です。Citrix®、XenServer®、XenMotion® は米国およびその他の国における Citrix System, Inc. の登録商標または商標です。

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。

本書では、上記記載以外の商標および会社名が使用されている場合があります。それらの商標や会社名は、一切 Dell Inc. に帰属するものではありません。

2010 年 12 月

[目次に戻る](#)

警告処置の設定

Dell OpenManage Server Administrator バージョン 6.4 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が稼動するシステムにおける警告処置の設定](#)
- [Microsoft Windows Server 2003 および Windows Server 2008 における警告処置の設定](#)
- [Windows Server 2008 における警告処置の実行アプリケーションの設定](#)
- [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が稼動するシステムにおける警告処置の設定

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` にメッセージを送信します。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 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、`/tmp/mailout.txt` のファイルにリダイレクトされます。

Microsoft Windows Server 2003 および Windows Server 2008 における警告処置の設定


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ー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。

Windows Server 2008 における警告処置の実行アプリケーションの設定

セキュリティ上の理由から、Microsoft Windows Server 2008 は対話型サービスを許可するように設定されていません。Microsoft Windows Server 2008 で対話型サービスとしてサービスがインストールされると、オペレーティングシステムは、このことを知らせるエラーメッセージを Windows システムログに記録します。

Server Administrator を使用してイベントに対する警告処置を設定する際、同処置で**アプリケーションを実行する**ように指定できます。警告処置の対話型アプリケーションを正常に実行させるようにするには、Dell Systems Management Server Administrator (DSM SA) Data Manager サービスが対話型サービスとして設定されている必要があります。対話型アプリケーションの例としては、グラフィカルユーザーインターフェース(GUI)を含むアプリケーション、またはパッチファイルの `pause` コマンドのように、ユーザーの入力を求めるアプリケーションなどが挙げられます。

Microsoft Windows Server 2008 に Server Administrator がインストールされると、DSM SA Data Manager サービスは、非対話型のサービスとしてインストールされます。これは、デフォルトにより、同サービスがデスクトップ対話できないように設定されていることを意味します。したがって、対話型アプリケーションは、警告処置に対して正常に実行されません。この状況で、警告処置

に対してインタラクティブなアプリケーションが実行されると、アプリケーションは一時停止の状態になり、ユーザーの入力を待つこととなります。アプリケーションインタフェース / プロンプトは非表示になっており、Interactive Services Detection (対話型サービスの検出) サービスが開始されても、その状態が続きます。**タスクマネージャ**の**プロセス**タブでは、対話型アプリケーションの各実行に対して、アプリケーションプロセスのエントリが表示されます。

Microsoft Windows Server 2008 で警告処置に対して対話型アプリケーションを実行する必要がある場合、DSM SA Data Manager サービスとデスクトップとの対話を許可するように設定しなければなりません。

デスクトップとの対話を許可するには:

1. **サービスコントロール パネル** で DSM SA Data Manager サービスを右クリックし、[プロパティ] を選択します。
2. **ログオン** タブで、**デスクトップとの対話をサービスに許可** を選択し、OK をクリックします。
3. **変更を適用**するには、DSM SA Data Manager サービスを再起動します。

DSM SA Data Manager サービスが再起動されると、Service Control Manager は、The DSM SA Data Manager service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly (「DSM SA Data Manager サービスは対話型サービスとしてマークされましたが、システムは対話型サービスを許可するように設定されていません。このサービスは正しく機能しない可能性があります」)のメッセージをシステムログに記録します。この変更によって、DSM SA Data Manager は警告処置の対話型アプリケーションを正しく実行できるようになります。対話型アプリケーションによって表示されるインタフェース/プロンプトが見えるようにするため、Interactive Services Detection (対話型サービスの検出) サービスが起動していることを確認してください。これらの変更が適用されると、オペレーティングシステムにより、**対話型サービスダイアログの検出** ダイアログボックスが表示され、対話型アプリケーションのインタフェース / プロンプトにアクセスできるようになります。

BMC/iDRAC プラットフォームイベントフィルタ警告メッセージ

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 7-1](#) に示します。

表 7-1. PEF 警告イベント

イベント	説明
ファンブロープエラー	ファンの稼働速度が遅すぎるかまったく動作していません。
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。
シャーンイントルージョンが検出されました	シャーンが開けられました。
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動作しています。
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一杯か空のため、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。
リムーバブルフラッシュ メディアが存在します	リムーバブルフラッシュメディアが存在します。
リムーバブルフラッシュ メディアエラー	リムーバブルフラッシュメディアがエラー状況にあります。
リムーバブルフラッシュ メディア警告	リムーバブルフラッシュメディアが存在します。

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 7-2. 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	セキュアポート サーバー	DSM SA 接続サービス
	実行ファイル名	Omaws[32]64]	dsm_om_connsvc
			dsm_om_connsvc

スケジューリング 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
			dsm_om_shrsvc

[目次に戻る](#)

[目次に戻る](#)

トラブルシューティング

Dell OpenManage Server Administrator バージョン 6.4 ユーザーズガイド

- [接続サービスエラー](#)
- [ログイン失敗のシナリオ](#)
- [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](#)

接続サービスエラー

Red Hat Enterprise Linux で SELinux が 強制 モードに設定されると、Dell Systems Management Server Administrator (DSM SA) の接続サービスの起動に失敗します。以下のいずれかの操作を行って、このサービスを起動してください。

- 1 SELinux を 無効 モードまたは 許可 モードに設定する。
- 1 SELinux `allow_execstack` プロパティを **ON** 状態に変更する。次のコマンドを実行します。

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

```
chcon -t unconfined_execmem_t /opt/dell/srvadmin/sbin/dsm_om_connsvcd
```

ログイン失敗のシナリオ

次のような場合に、管理下システムにログインできないことがあります。

- 1 無効 / 誤った IP アドレス を入力した。
- 1 誤った資格情報 (ユーザー名およびパスワード) を入力した。
- 1 管理下システムがオフ。
- 1 無効な IP アドレスまたは DNS エラーにより、管理下システムに到達できない。
- 1 管理下システムが信頼されていない証明書を持ち、ログインページで **証明書の警告を無視する** が選択されていない。
- 1 VMware ESX/ESXi システム上で Server Administrator サービスが有効になっていない。VMware ESXi/ESX システム上で Server Administrator サービスを有効にする方法については、『Dell OpenManage Server Administrator インストールガイド』を参照してください。
- 1 VMware ESX/ESXi システム上で、SFCBD (small footprint CIM broker daemon) サービスが実行されていない。
- 1 管理下システム上で Web Server Management サービスが実行されていない。
- 1 **Ignore Certificate Warning** (証明書の警告を無視する) チェックボックスを選択されていないにもかかわらず、管理下システムのホスト名ではなく、IP アドレスを入力した。
- 1 管理下システムにおいて、WinRM 認証機能 (リモート有効化) が設定されていない。この機能の詳細については、『Dell OpenManage Server Administrator インストールガイド』を参照してください。
- 1 VMware ESX 4.1/ESXi 4.1 オペレーティングシステムに接続中に認証エラーがありました。以下のような原因が考えられます。
 - サーバーにログイン中または Server Administrator にログインした後に ロックダウン モードが有効になった。ロックダウン モードの詳細については、VMware マニュアルを参照してください。
 - Server Administrator にログインした後にパスワードが変更された。
 - システム管理者権限なしで普通のユーザーとして Server Administrator にログインした。詳細については、VMware マニュアルで役割の割り当てに関する説明を参照してください。

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


再インストールを行い、Server Administrator のアンインストールを実行するとインストールの不具合を修正できます。

再インストールを強制するには:

- 1 インストールされている Server Administrator のバージョンを特定します。
- 2 support.jp.dell.com から、該当するバージョンのインストールパッケージをダウンロードします。
- 3 `srvadmin\windows\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** 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 Server Administrator 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。

表 A-1. OpenManage Server Administrator サービス

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 (このサービスは、Server Administrator ウェブサーバーと共にインストールされます。)	対応ウェブブラウザとネットワーク接続を持つこのシステムからでも Server Administrator にリモート / ローカルアクセスが可能です。	ユーザーは、ウェブユーザーインターフェースを介して、Server Administrator にログインし、操作を行うことはできません。ただし、CLI を利用することは可能です。	再起動サービス	重要
共通サービス				
Windows: DSM SA 共有 Services(サービス) Linux: dsm_om_shrsvc (このサービスは、管理下システム上で実行されます。)	起動時にインベントリコレクタを実行して、Server Administrator の SNMP と CIM プロバイダが Dell System Management Console と Dell IT Assistant (ITA) を使ってリモートソフトウェアアップデートを行うために消費する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 Server Administrator 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、サードパーティ製のツール (たとえば、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
メモ: 64 ビット Linux システムに 32 ビット互換性ライブラリがインストールされていない場合、共有サービスはインベントリコレクタの起動に失敗し、libstdc++.so.5 is required to run the Inventory Collector. (「インベントリコレクタを実行するには libstdc++.so.5 が必要です」) のエラーメッセージが表示されます。srvadmin-cm.rpm はインベントリコレクタ用のパッチを提供します。srvadmin-cm が依存する RPM のリストについては、『Dell OpenManage Server Administrator インストールガイド』を参照してください。				
計装サービス				
Windows: DSM SA データマネージャ Linux: dsm_sa_datamgrd (dataeng サービス下でホスト) (このサービスは、管理下システム上で実行されます。)	システムの監視、詳細なエラーとパフォーマンス情報への迅速なアクセスの提供、シャットダウン、起動、セキュリティを含む監視下システムのリモート管理の許可。	ユーザーはこれらのサービスを実行することなく GUI/CLI 上でハードウェアレベルの詳細を設定、表示することはできません。	再起動サービス	重要
DSM SA イベントマネージャ (Windows) Linux: dsm_sa_eventmgrd (dataeng サービス下でホスト) (このサービスは、管理下システム上で実行されます。)	オペレーティングシステムとシステム管理用のファイルイベントログサービスを提供し、イベントログアナライザによっても使用されます。	このサービスが停止されると、イベントログ機能は正しく動作しなくなります。	再起動サービス	警告
Linux: dsm_sa_snmpd (dataeng サービス下でホスト) (このサービスは、管理下システム上で実行されます。)	データエンジン Linux SNMP インタフェース	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 (このサービスは管理下システム上で実行されず。)	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できるわけではありません。	再起動サービス	重要


[目次に戻る](#)

[目次に戻る](#)

よくあるお問い合わせ(FAQ)

Dell OpenManage Server Administrator バージョン 6.4 ユーザーズガイド

本項には、Dell 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. OpenManage Server Administrator から ESXi 4.0.x(4.0 U1/U2)ホスト再起動機能が障害を起こすのは何故ですか？

この問題は VMware スタンドアロンライセンス(SAL)キーが理由で発生します。詳細に関しては、kb.vmware.com/kb/1026060 でナレッジベース文書を参照してください。

2. VMware ESX 4.1 オペレーティングシステムを Active Directory ドメインに追加した後に実行する必要があるタスクはどれですか？

VMware ESX 4.1 オペレーティングシステムを Active Directory ドメインに追加した後、Active Directory ユーザーは以下を行う必要があります。

- 1 VMware ESX 4.1 オペレーティングシステムを使ってサーバー管理者として Server Administrator にログインし、DSM SA 接続サービスを再起動します。
- 1 VMware ESX 4.1 オペレーティングシステムを使ってリモート有効化エージェントとしてリモートノードにログインします。sfcbd プロセスが新しいユーザーに権限を加えるまで約 5 分待ちます。

3. Server Administrator 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？

Server Administrator 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 Server Administrator をインストールする権限を持ちません。

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

Server Administrator 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 6.x (x はアップグレードしたい Server Administrator 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。

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

support.jp.dell.com → Enterprise IT → マニュアル → ソフトウェア → Systems Management → Dell OpenManage Server Administrator にログインします。

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。


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

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。

7. 1311 以外にユーザーが使用できるポートはありますか？

はい、任意の https ポートを設定できます。**プリファレンス** → **一般設定** → **Web サーバー** → **HTTPS ポート** の順で選択します。

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。

 **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。

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

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

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

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

10. PowerEdge 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、その処置を設定または要求するときにその提示を求められます。検出範囲からの資格情報は引き継がれません。

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が稼動するシステム)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には Server Administrator はインストールされていないため、ターゲットで OpenManage クライアントの計装を実行するときには CIM 検出が使用されます。

ネットワークプリンタやその他の多くのデバイスでは、デバイスとの通信(主として検出)にはいまだに 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。

11. SNMP v3 をサポートする予定はありますか?

いいえ、SNMP v3 をサポートする予定はありません。

12. ドメイン名に下線を含めると 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、大小文字は区別されます。

13. Server Administrator のログインページ上で「Active Directory」を選択または選択解除することで、特権レベルにどのような影響がありますか?

Active Directory チェックボックスを選択しない場合、Microsoft Active Directory で設定されたアクセス権限しか付与されません。Microsoft Active Directory の Dell 拡張スキーマソリューションを使用してログインすることはできなくなります。このソリューションは、Server Administrator へのアクセスを提供し、Active Directory ソフトウェアの既存ユーザーに Server Administrator ユーザーおよび特権の追加/管理を可能にします。詳細については、『Dell OpenManage Server Administrator インストールガイド』の「Microsoft Active Directory の使用」を参照してください。

14. Kerberos 認証を行って Web Server からログインするときに必要な操作は何ですか?

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

32 ビットの場合

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

64 ビットの場合

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

[目次に戻る](#)

[目次に戻る](#)

Server Administrator サービス

Dell OpenManage Server Administrator バージョン 6.4 ユーザーズガイド

- [概要](#)
- [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

Dell OpenManage Server Administrator Instrumentation Service は、システムの正常性をモニタし、業界標準のシステム管理エージェントによって収集される障害および性能に関する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 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(エラー最大値と最小値は、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エラー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エラー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 が稼動する管理下システムおよびネットワーク管理ステーションのどちらでも、SNMP パケットを受信できるようにシンプルネットワーク管理プロトコル(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特権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。**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情報が掲載された、個別の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、システム管理者またはパワーユーザー特権が必要です。さらに、システム管理者特権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す。

Storage Management Service コンポーネントの詳細については、support.jp.dell.com/manuals の『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


OpenManage Server Administrator で未サポートの機能

VMware ESXi バージョン 4.X オペレーティングシステムの制限のため、初期バージョンの OpenManage Server Administrator で利用可能であったいくつかの機能は、本リリースでは利用できません。それらの機能は次のとおりです。


ESXi 4.X でサポートされていない機能

- 1 警告管理 - 警告処置
- 1 ネットワークインタフェース - 管理ステータス
- 1 ネットワークインタフェース - DMA
- 1 ネットワークインタフェース - IP (インターネットプロトコル) アドレス
- 1 ネットワークインタフェース - MTU (最大転送単位)
- 1 ネットワークインタフェース - 操作ステータス
- 1 プリファレンス - SNMP 設定
- 1 リモートシャットダウン - 先にオペレーティングシステムをシャットダウンしてからシステムをパワーサイクル
- 1 詳細情報 - 詳細タブに表示されない Server Administrator コンポーネントの詳細
- 1 ロールマップ

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

 **メモ:** 設定可能なシステムツリーオブジェクト、システムコンポーネント、アクションタブ、およびデータ領域機能を表示するには、システム管理者またはパワーユーザー特権が必要です。さらに、システム管理者特権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。

モジュラエンクロージャ

 **メモ:** Server Administrator では、モジュラエンクロージャとはシステムツリーで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。

モジュラシステムのシャーンの情報と 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 監視下のモジュラシステムのシャーン情報を表示する。
- 1 監視下のモジュラシステムの Chassis Management Controller (CMC) に関する詳細情報を表示する。

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

Server Administrator ホームページから Chassis Management Controller **ログイン** ウィンドウにリンクするには:

1. **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。
2. **CMC 情報** タブをクリックし、**CMC ウェブインタフェースの起動** をクリックします。CMC **ログイン** ウィンドウが表示されます。

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

システム / サーバーモジュール


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。


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 (オペレーティングシステムのウォッチドッグタイマー) 処置の表示と設定を行います。

 **メモ:** 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ため、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ため、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、手動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 のシャットダウン

シャットダウン タブでは、以下のことができます。

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

-  **メモ:** サーマルシャットダウンは、センサー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。

- 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。


- 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。

- 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。

- 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。

- 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。
- 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。

- 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。

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


-  **メモ:** 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 [バッテリー](#)
- 1 [BIOS](#)
- 1 [ファン](#)
- 1 [ファームウェア](#)
- 1 [ハードウェアパフォーマンス](#)
- 1 [インテリジェン](#)
- 1 [メモリ](#)
- 1 [ネットワーク](#)
- 1 [ポート](#)
- 1 [Power Management](#)
- 1 [電源ユニット](#)
- 1 [プロセッサ](#)
- 1 [リモートアクセス](#)
- 1 [リムーバブルフラッシュメディア](#)
- 1 [スロット](#)
- 1 [温度](#)
- 1 [電圧](#)





 **メモ:** ハードウェアパフォーマンス は Dell xx0x 以降のシステムでのみサポートされています。電源装置 は Dell PowerEdge 1900 システムでは使用できません。電源管理 は限られた Dell xx0x 以降の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。

- 1 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。 コンポーネントが健全(正常)であることを示します。 コンポーネントは危険(重要ではない)状態で、早急な対応が必要なことを示します。 コンポーネントがエラー(重要)状態にあり、即座な対応が必要なことを示します。 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。
 - [バッテリー](#)
 - [ファン](#)
 - [ハードウェアログ](#)
 - [インテリジェン](#)
 - [メモリ](#)
 - [ネットワーク](#)
 - [Power Management](#)
 - [電源ユニット](#)
 - [プロセッサ](#)
 - [温度](#)
 - [電圧](#)

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

- 1 ホスト名、iDRAC バージョン、Lifecycle Controller バージョン、シャーシモデル、シャーシロック、シャーシサービスタグ、エクスプレスサービスコード、シャーシ Asset Tag などの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。エクスプレスサービスコード(ESC)の属性は、Dell システム用のサービスタグを11桁の数字に変換したものです。自動電話転送を目的としてデルテクニカルサポートに電話する際に、この属性を電話で入力することができます。ストレージ(DAS)には、エクスプレスサービスコードの属性がありません。
- 1 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)。
- 1 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(非マスク割り込み)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。また、管理下システムの LCD セキュリティアクセスレベルも選択します。管理下システムの LCD 情報は、ドロップダウンメニューから選択できます。**フロントパネル** サブタブから リモート KVM セッションの表示を有効にすることもできます。

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特権に従って、**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、マイクロ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特権に従って、**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。

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、ハードディスクドライブの順序、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 ハイバースレディンク、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 フェールセーフ 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、光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。信頼済みプラットフォームモジュール(TPM)と信頼済み暗号モジュール(TCM)の設定を表示できます。

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。ファンプローブは rpm を Server Administrator Instrumentation Service に報告します。デバイスツリーから **ファン** を選択すると、Server Administrator ホームページの右側ペインのデータ領域に詳細が表示されます。**ファン** オブジェクト処置ウィンドウには、ユーザーのグループ特権に従って、**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: ファンプローブ

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で起動して実行できます。各コントローラには、コントローラの機能提供を円滑にする 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特権によっては、**プロパティ** タブが表示されることがあります。

プロパティ

サブタブ: 情報

プロパティタブでは、システムのファームウェア情報を表示できます。

ハードウェアパフォーマンス

ハードウェアのパフォーマンス オブジェクトをクリックすると、システムパフォーマンスの劣化の状態と原因を表示されます。ハードウェアのパフォーマンス オブジェクト処置ウィンドウには、ユーザーのグループ特権によっては、プロパティタブが表示されることがあります。

表 4-1 には、ステータスの一覧とブロープの原因が表示されます。

表 4-1. ステータスとブロープの原因

状態値	原因値
劣化	ユーザー設定
	不十分な電源容量
	原因不明
正常	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、システムのシャールが開かれている、あるいは開かれたことを示します。イントルージョン オブジェクト処置ウィンドウには、ユーザーのグループ特権によっては、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エラーセンサーは、ECC メモリ修正数のカウントによってメモリモジュールをモニタします。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特権によっては、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:** スペアバンクメモリが有効になっているシステムが「冗長性喪失」状態に入った場合、どのメモリモジュールが原因か明らかでない場合があります。交換する DIMM を特定できない場合は、ESM システムログの検出されたス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、リモート接続が維持されていることを確認します。システムで NIC チューニングがすでに設定されている場合、Dell OpenManage Server Administrator はその詳細を表示します。システム管理者は、複数の物理 NIC を単一の論理 NIC のチームにまとめて、1 つの IP アドレスを割り当てることができます。チューニングは NIC ベンダーツールを使って設定できます。例: Broadcom - BACS 物理 NIC の 1 台が故障しても、IP アドレスはその 1 台の物理 NIC ではなく論理 NIC に関連付けられているため、その IP アドレスに引き続きアクセスできます。チームインタフェースを設定すると、チームプロパティの詳細が表示されます。チームインタフェースとそのメンバーである物理 NIC 間の関係も表示されます。**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特権によっては、**プロパティ** タブが表示されることがあります。

プロパティ

サブタブ: 情報

プロパティ タブでは、物理 NIC インタフェースとシステムに取り付けられている 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特権によっては、**プロパティ** タブが表示されることがあります。

プロパティ

サブタブ: 情報

プロパティ タブでは、システムの内部および外部ポート情報を表示できます。

Power Management

 **メモ:** 電力の管理機能はホットスワップ対応の電源ユニットを搭載した PowerEdge システムのみで使用することができ、固定非冗長電源ユニット搭載のシステムでは使用できません。

監視

サブタブ: 消費量 | 統計

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

$BTU/hr = Watt \times 3.413$ (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、システム電源ブロープ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特権によっては、**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。


- ・ 電源装置の冗長性属性についての情報を表示します。
- ・ 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 `xx1x` 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。

- 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。
- 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。
- 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特権によっては、**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

警告管理 タブでは、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。

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特権によっては、**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。

設定


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。


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

DRAC 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 の有効または無効は、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。

リムーバブルフラッシュメディア

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

プロパティ

サブタブ: 情報

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

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、リムーバブルフラッシュメディアプローブが警告値またはエラー値を返したときに実行する警告処置を設定できます。
- 1 現在の SNMP トラップ警告しきい値を表示し、リムーバブルフラッシュメディアプローブの警告しきい値のレベルを設定できます。選択した重大度レベルのイベントをシステム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。

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

スロット

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

プロパティ

サブタブ: 情報

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

温度

温度 オブジェクトをクリックすると、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特権に応じて、**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: 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。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特権に応じて、**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せん。

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特権によっては、**プロパティ** タブが表示されることがあります。

プロパティ

サブタブ: 概要

プロパティ タブでは、モニタされているシステムのシステムのオペレーティングシステムと System Management Software 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特権によっては、**プロパティ** タブが表示されることがあります。

プロパティ

サブタブ: 情報

プロパティ タブでは、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ストレージデバイス、システムディスクなどの状態および設定が表示されます。

Storage Management Service の場合、**ストレージ** オブジェクト処置ウィンドウには、ユーザーのグループ特権によっては、**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、アレイサブシステム、オペレーティングシステムディスクなど、接続しているストレージコンポーネントやセンサーの正常性や状態を表示できます。

プリファランス: 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は次の通りです。

- 1 一般設定
- 1 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特権によっては、**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 タブ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 IPv4 または IPv6 アドレス指定モードでの SMTP サーバーアドレスとバインド IP アドレスの設定。
- 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、ユーザーまたはパワーユーザー特権を持つユーザーのアクセスを有効または無効にして、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特権によっては、**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 ユーザーまたはパワーユーザー特権を持つユーザーのアクセスを有効または無効にします。
- 1 SNMP ルートパスワードを設定します。

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

- 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が稼動するシステムでは、Windows SNMP サービスを再起動する必要があります。対応 Red Hat Enterprise Linux および SUSE Linux Enterprise Server オペレーティングシステムが稼動するシステムでは、`srvadmin-services.sh 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。

[目次に戻る](#)

[目次に戻る](#)

はじめに

Dell OpenManage Server Administrator バージョン 6.4 ユーザーズガイド

- [概要](#)
- [バージョン 6.4 の新機能](#)
- [利用可能なシステム管理標準](#)
- [Server Administrator ホームページ](#)
- [その他の必要マニュアル](#)
- [テクニカルサポートの利用法](#)

概要

Dell OpenManage Server Administrator では、統合されたウェブ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)、またはオペレーティングシステムから使用するコマンドラインインターフェイス(CLI)の2つの方法で、包括的な1対1のシステム管理を行うことができます。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。

Server Administrator との関連では、システムとは、スタンダードアロン、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システムを指します。

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

Server Administrator は、包括的な統合管理サービスを利用した使いやす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。リモートに監視され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せん。Server Administrator は、役割 ベースのアクセス制御(RBAC)、認証、セキュアソケットレイヤ(SSL)を使用して管理接続をセキュリティ保護します。

インストール

『Dell Systems Management Tools and Documentation DVD(OM DVD)』を使用して、Server Administrator をインストールします。この DVD は、Server Administrator、管理下システム、および管理ステーションの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、そしてアンインストールするためのセットアッププログラムを提供します。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。

Dell OpenManage インストーラは、管理下システムに Dell OpenManage Server Administrator やその他の管理下システムソフトウェアコンポーネントをインストール / アンインストールするためのインストールスクリプトと RPM パッケージを提供しています。詳細については、『Dell OpenManage Server Administrator インストールガイド』および『Dell OpenManage Management Station Software インストールガイド』を参照してください。これらの文書は、support.jp.dell.com/manuals から入手できます。

 **メモ:** OM DVD からオープンソースのパッケージをインストールする場合、該当するライセンス ファイルは自動的にシステムにコピーされます。これらのパッケージを削除する際、該当するファイルは削除されます。

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

個々のシステムコンポーネントのアップデート

個々のシステムコンポーネントをアップデートするには、コンポーネント専用の 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、アップデートを検出し、システムに適用する 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.jp.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、リポジトリ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

ストレージ管理サービスは、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。

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

計装サービス

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

Remote Access Controller

Remote Access Controller は、Dell Remote Access Controller (DRAC) またはベースボード管理コントローラ (BMC) / Integrated Dell Remote Access Controller (iDRAC) ソリューションを装備したシステム向けの完全なリモートシステム管理ソリューションを提供します。Remote Access Controller は、動作不能のシステムへのリモートアクセスを提供するため、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、システムに / から発行されたコマンド、監視されているハードウェアイベントおよびシステム警告など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。

バージョン 6.4 の新機能

OpenManage Server Administrator 6.4 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 Dell OpenManage Server Administrator ユーザーインターフェースの再設計により、以下を含むカスタマエクスペリエンスが総合的に向上しました。
 - ログインページでユーザー名やパスワードが無効などのエラーがある場合、エラーメッセージが 30 秒表示され、その後ログインプロンプトが表示されます。30 秒が経過する前にログインプロンプトを表示するには、**再試行** をクリックします。
 - **Server Administrator に戻る** ボタンの名前は **ホーム** に変更されました。
 - **OK** ボタンの名前はログインページで **送信** に変更されました。
 - **電子メール、エキスポート、更新** のボタンはアイコンとして表示されるようになりました。
 - **電子メール、エキスポート、更新** のアイコンに加え、画面の右角で **ヘルプ** のアイコンが使えるようになりました。
 - **名前を付けて保存、ログのクリア、再起動、デフォルトにリセット** のようなボタンは **オプション** のセクションでグループ化されています。
 - **ユーザー権限** と **ホスト名** のボタンは画面の右角でなく左角で使えるようになりました。
 - **リモートノードの管理、バージョン情報、サポート** のリンクはログインページ下に表示されるようになりました。
 - **印刷** や **エキスポート** などのボタンはすべて、OMSA の全ページに表示されます。特定のページに該当するボタンのみが有効となり、残りのボタンはグレー表示されます。
 - データ領域のボタンとリンクのツールヒント機能が有効です。
 - **システム概要** と **資産情報の概要** ページでは、**移動** と **トップへ戻る** のリンクは使えません。その代わりに、ページの各セクションを展開したり折りたたむことができます。
 - **バージョン情報** ページの **詳細** ボタンがなくなりました。詳細はすべて同じページに表示されます。
- 1 エクスプレスサービスコード (ESC) の属性が追加されました。
- 1 以下のオペレーティングシステムに対するサポートが追加されました。
 - Microsoft Windows 2008 HPC Edition Server R2
 - Red Hat Enterprise Linux 5
 - VMware ESX 4.0 U2
 - VMware ESXi 4.0 U2
- 1 以下のオペレーティングシステムのサポートを終了しました。
 - Red Hat Enterprise Linux 4.8
 - VMware ESX 4.0 U1
 - VMware ESXi 4.0 U1
- 1 スキンの設定機能は廃止されました。
- 1 ページレベルでの状態ステータスアイコン機能は廃止されました。

対応オペレーティングシステムについては、support.jp.dell.com/manuals にある『Dell システムソフトウェアサポートマトリックス』を参照してください。

本リリースで追加された新機能の詳細については、Server Administrator オンラインヘルプを参照してください。

利用可能なシステム管理標準

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

- 1 HTTPS
- 1 CIM (共通情報モデル)
- 1 SNMP

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

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

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

利用可能な対応オペレーティングシステム

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

Server Administrator は、これらのシステム管理標準に対して、かなりのセキュリティ機能を追加しています。いかなる属性設定の操作 (例: 管理タグの値の変更など) を行うにも、Dell OpenManage IT Assistant を使用する必要があり、必要な権限でログインしていなければなりません。

[表 1-1](#) は、対応オペレーティングシステムごとに利用できるシステム管理標準を記載しています。

表 1-1. 利用可能なシステム管理標準

オペレーティングシステム	SNMP	CIM
Windows Server 2008 シリーズおよび Windows Server 2003 シリーズ	オペレーティングシステムのインストールメディアから使用可能	常にインストール
Red Hat Enterprise Linux	オペレーティングシステムのインストールメディアの <code>net-snmp</code> パッケージから使用可能	使用不可
SUSE Linux Enterprise Server	オペレーティングシステムのインストールメディアの <code>net-snmp</code> パッケージから使用可能	使用不可
VMware ESX	オペレーティングシステムによってインストールされる <code>net-snmp</code> パッケージから使用可能	使用可能
VMware ESXi	SNMP トラップのサポート メモ: While ESXi は SNMP トラップをサポートしていますが、SNMP を介したハードウェアのインベントリをサポートしていません。	使用可能
Citrix XenServer 5.6	オペレーティングシステムのインストールメディアの <code>net-snmp</code> パッケージから使用可能	使用不可

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持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キストヘルプを提供します。

その他の必要マニュアル

このガイド以外にも、デルサポートサイト [support.jp.dell.com/manuals](#) から次のガイドを入手できます。**マニュアル** ページで、**ソフトウェア** → **Systems Management** をクリックします。右側の製品リンクをクリックして、ドキュメントにアクセスします。

- 『Dell システムソフトウェアサポートマトリックス』は、各種 Dell システム、これらのシステムでサポートされているオペレーティングシステム、これらのシステムにインストールできる Dell OpenManage コンポーネントについての情報を提供しています。
- 『Dell OpenManage Server Administrator インストールガイド』では、Dell OpenManage Server Administrator のインストール手順が説明されています。
- 『Dell OpenManage Management Station Software インストールガイド』では、Dell OpenManage Management Station Software (ベースボード管理ユーティリティ、DRAC ツール、Active Directory スナップインを含む) のインストール手順が説明されています。
- 『Dell OpenManage Server Administrator SNMP リファレンスガイド』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。
- 『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。
- 『Dell OpenManage Server Administrator メッセージリファレンスガイド』には、Server Administrator ホームページの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が掲載されています。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。
- 『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。
- 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。
- 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。
- 『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せん。
- 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 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 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 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 Server Update Utility ユーザーズガイド』では、Dell システムをアップデートしたり、リポジトリに登録されているシステムに適用可能なアップデートを表示できるサーバーアップデートユーティリティ(SUU)の入手方法と使用方法に関する情報を掲載しています。
- 1 Dell 管理コンソールのインストール、設定、使用については、『Dell Management Console ユーザーズガイド』で説明しています。Dell 管理コンソールは、ネットワーク上のデバイスを検出し、インベントリ化を可能にするウェブベースのシステム管理ソフトウェアです。ネットワークデバイスの正常性と性能の監視や Dell システム用のパッチ管理機能などの高度な機能も提供します。
- 1 『Dell Life Cycle Controller ユーザーズガイド』は、システムのライフサイクルにわたって、システムおよびストレージ管理タスクを行うための、Unified Server Configurator の設定および使用に関する情報を提供しています。また、オペレーティングシステムを導入したり、RAID(個別ディスクの冗長アレイ)を設定したり、診断を実行して、システムとそれに接続しているハードウェアを検証するために、Unified Server Configurator を使用することもできます。Remote Service の機能は、管理コンソールによるシステムプラットフォームの自動検出を可能にし、リモートのオペレーティングシステムの展開機能を強化します。これらの機能は、Lifecycle Controller ファームウェアが提供するハードウェア管理インタフェースベースのウェブサービスにより実現されます。
- 1 **用語集**では、本書で使用される用語について説明されています。

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資格認定もご利用いただけます。詳細については、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。

[目次に戻る](#)

[目次に戻る](#)

Server Administrator ログ

Dell OpenManage Server Administrator バージョン 6.4 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、**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利用できます。

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を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 xx7x 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、早急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、即座の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 メッセージ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。


[目次に戻る](#)

[目次に戻る](#)

Remote Access Controller の操作

Dell OpenManage Server Administrator バージョン 6.4 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、一定の閾値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 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が稼動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、前回のクラッシュ画面を保存します。

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

Remote Access Controller を使用する場合、**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 の詳細については、『Dell OpenManage ベースボード管理コントローラユーザーリテリユーザーズガイド』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 5-1](#) には、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 5-1. 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
モジュラエンクロージャ	モジュラシステム
サーバーモジュール	モジュラシステム
メインシステム	モジュラシステム
システム	非モジュラシステム
メインシステムシャーシ	非モジュラシステム

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 を Server Administrator グラフィカルユーザーインターフェースから管理するには、**メインシステムシャーシ / メインシステム** グループのサブコンポーネントである **リモートアクセス オブジェクト** をクリックします。

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、`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、リモートアクセスコントローラの設定をデフォルト値に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。

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 を順にクリックします。

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

リモートアクセスデバイス


- 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

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。


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. **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。

4. 次の NIC 設定詳細を設定します。


1 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。

1 NIC の選択

 **メモ:** NIC の選択は、モジュラシステムでは設定できません。

1 IPMI オーバー LAN を有効にする

1 IP アドレスソース

1 IP アドレス

1 サブネットマスク

1 ゲートウェイアドレス

1 チャンネル権限レベルの制限

1 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。)

5. 次の VLAN 設定詳細を設定します。

 **メモ:** VLAN 設定は iDRAC のシステムには該当しません。

VLAN ID 有効

VLAN ID

優先度

6. 次の IPv4 プロパティを設定します。

IP アドレスソース

IP アドレス

サブネットマスク

ゲートウェイアドレス

7. 次の IPv6 プロパティを設定します。

IP アドレスソース

IP アドレス


プレフィックス長

デフォルトゲートウェイ

DNS アドレスソース

優先 DNS サーバー

代替 DNS サーバー

 **メモ:** 追加設定 で IPv4 と IPv6 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。

8. 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** を順にクリックします。
2. **設定** タブをクリックします。
3. **シリアルポート** をクリックします。

シリアルポート設定 ウィンドウが表示されます。

4. 次の詳細を設定します。
 - 接続モード設定
 - ボーレート
 - フロー制御
 - チャン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、限られたいくつかのテキストコマンドにも対応して、テキストベースのレガシー環境をサポートしています。この環境は、単純なターミナルやターミナルエミュレータを使用できるように設計されています。

7. 既存のターミナルとの互換性を強化するには、次のカスタマイズを指定します。

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

8. **変更の適用** をクリックします。

9. **シリアルポート設定ウィンドウに戻る** をクリックすると、**シリアルポート設定** ウィンドウに戻ります。

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** を順にクリックします。
2. **設定** タブをクリックします。
3. **シリアルオーバー LAN** をクリックします。

シリアルオーバー LAN 設定 ウィンドウが表示されます。

4. 次の詳細を設定します。
 - シリアルオーバー LAN を有効にする
 - ボーレート
 - 必要とされる最小特権

5. **変更の適用** をクリックします。

6. **詳細設定** をクリックすると、BMC をさらに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。

- 文字累積間隔
 - 文字送信しきい値
8. **変更の適用** をクリックします。
 9. **シリアルオーバー LAN 設定に戻る** をクリックすると、**シリアルオーバー LAN 設定** ウィンドウに戻ります。

iDRAC の追加設定

追加設定 タブを使って IPv4 と IPv6 プロパティを設定できます。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。
 - **ユーザーを有効にする** を選択すると、ユーザーが有効になります。
 - **ユーザー名** フィールドにユーザーの名前を入力します。
 - **パスワードの変更** チェックボックスを選択します。
 - **新しいパスワード** フィールドに新しいパスワードを入力します。
 - **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。
 - **最大 LAN ユーザー特権レベル制限** を選択します。
 - **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。
 - 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 を有効にします。
6. DRAC/iDRAC ユーザー特権のユーザーグループを指定します。
7. **変更の適用** をクリックして変更を保存します。
8. **リモートアクセスユーザーウィンドウ** に戻る をクリックすると、**リモートアクセスユーザー** ウィンドウに戻ります。


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


プラットフォームのイベントフィルタ警告の設定


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. **アラート管理** 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 PEF 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、PEF 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 **電力の低減**
CPU をスロットルします。

 **メモ:** すべてのシステムで電力低減がサポートされているわけではありません。

 **注意:** なし または **電力の低減** 以外のプラットフォームイベントシャットダウン処置を選択した場合には、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。
-

[目次に戻る](#)

[目次に戻る](#)

設定と管理

Dell OpenManage Server Administrator バージョン 6.4 ユーザーズガイド

- [セキュリティ管理](#)
- [ユーザー権限の割り当て](#)
- [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 が稼動す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

Dell OpenManage 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決定して、セキュリティを管理します。各ユーザーには 1 つ、または複数の役割が割り当てられており、各役割にはその役割内のユーザーが使用できるユーザー特権が 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場合のアラート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応答しない場合の自動回復処置の設定、ハードウェアログ、イベントログ、およびコマンドログのクリアなどを実行できます。[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 2-1](#) を参照してください。

表 2-1. ユーザー特権

ユーザー特権	アクセスタイプ	
	表示	管理
ユーザー	はい	いいえ
パワーユーザー	はい	はい
管理者	はい	はい
昇格システム管理者 (Linux のみ)	はい	はい

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

[表 2-2](#) は、Server Administrator サービスにアクセスして管理できるユーザーをまとめたものです。

表 2-2. 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	
	表示	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	U、P、A、EA	A、EA

表 2-3 は、表 2-2 で使用されるユーザー特権レベルの略語の意味を説明しています。

表 2-3. 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	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、Server Administrator ホームページまたは CLI からアクセスしたかを問わず、Server Administrator のすべての機能が正しく認証されるようにします。

Microsoft Windows 認証

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


Red Hat Enterprise Linux および SUSE Linux Enterprise Server 認証

対応の 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。

VMware ESX Server 4.X


ESX Server は、ユーザーが ESX Server ホストにアクセスする際、認証に PAM (Pluggable Authentication Modules) の仕組みを使用します。VMware サービスの PAM 設定は、認証モジュールへのパスを格納する `/etc/pam.d/vmware-authd` にあります。

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

-  **メモ:** VMware ESX Server 4.1 オペレーティングシステムが稼働しているシステムから Server Administrator にログインするためにはどのユーザーもシステム管理者特権が必要です。役割の割り当てについては、VMware のマニュアルを参照してください。

VMware ESXi Server 4.X

ESXi Server は、vSphere/VI Client または Software Development Kit (SDK) を使って ESXi ホストにアクセスするユーザーを認証します。ESXi のデフォルトインストールでは、認証にローカルパスワードデータベースを使用します。Server Administrator での ESXi 認証トランザクションは、`vmware-host` プロセスとの直接的なインタラクションでもあります。サイト上で認証が効率的に動作するようにするには、ユーザー、グループ、権限、および役割のセットアップ、ユーザー属性の設定、独自の証明書の追加、SSL の使用有無の決定などの基本的なタスクを行ってください。

-  **メモ:** VMware ESXi Server 4.1 オペレーティングシステムが稼働しているシステムから Server Administrator にログインするためにはどのユーザーもシステム管理者特権が必要です。役割の割り当てについては、VMware のマニュアルを参照してください。


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。


ユーザー権限の割り当て

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、Dell OpenManage ソフトウェアのユーザー全員に正しくユーザー特権を割り当てます。新しいユーザーは、オペレーティングシステムのユーザー特権で 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 が稼働するシステムでは、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の手順は、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 の使用の詳細については、[Active Directory の使用](#) 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

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ます。

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


パワーユーザー特権を持つユーザーの作成

1. コマンドラインから次のコマンドを実行します。

```
useradd -d <ホームディレクトリ> -g root <ユーザー名>
```


 **メモ:** rootをプライマリグループとして設定します。

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ます。

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

Linux オペレーティングシステムで 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します。

1. /opt/dell/srvadmin/etc/omarolemap にある omarolemap ファイルを開きます。
2. 以下を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 2-4](#) に、役割の定義を omarolemap に追加する凡例を示します。

表 2-4. OpenManage Server Administrator に役割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	管理者
(+)グループ名	ドメイン	ユーザー
ワイルドカード (*)	ワイルドカード (*)	ユーザー

[Tab] = \t (タブ文字)

[表 2-5](#) に、役割の定義を omarolemap に追加する凡例を示します。

表 2-5. OpenManage Server Administrator に役割の定義を追加する例

<ユーザー名>	<ホスト名>	<権限>
Bob	Ahost	パワーユーザー
+ルート	Bhost	管理者
+ルート	Chost	管理者
Bob	*.aus.amer.com	パワーユーザー
Mike	192.168.2.3	パワーユーザー

3. ファイルを保存して閉じます。

omarolemap ファイル使用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	*	管理者
1	+ルート	*	パワーユーザー
1	*	*	ユーザー


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 **omarolemap** ファイルの変更が反映されない場合は、コマンドログでエラーを調べてください。
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 <ホスト名> に重複したユーザー名またはユーザーグループのエントリがあると、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。

VMware ESX 4.X および ESXi 4.X 用の Server Administrator の作成

ユーザーテーブルにユーザーを追加するには:

1. vSphere クライアントを使用してホストにログインします。
2. **ユーザーおよびグループ** タブをクリックし、**ユーザー** をクリックします。
3. ユーザー テーブルを右クリックし、**追加** をクリックして、**新規ユーザーの追加** ダイアログボックスを開きます。
4. ログイン、ユーザー名、ユーザー ID (UID)、パスワードを入力します。ユーザー名と UID の指定はオプションです。UID を指定しない場合、vSphere クライアントは UID を割り当てます。
5. コマンドシェルを通じてユーザーが ESX/ESXi ホストにアクセスできるようにするには、**このユーザーにシェルアクセスを許可する** を選択します。vSphere クライアントのみからホストにアクセスするユーザーは、シェルアクセスを必要としません。
6. ユーザーをグループに追加するには、**グループ** ドロップダウンメニューからグループ名を選択し、**追加** をクリックします。
7. **OK** をクリックします。

対応する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している必要があります。


1. **コンピュータの管理** ウィンドウを開きます。
2. コンソールツリーで、**ローカルユーザーとグループ** を展開し、**ユーザー** をクリックします。
3. 対象ユーザーのプロパティを表示するには、**ゲスト** または **IUSR_システム名** ユーザーアカウントをダブルクリック、または **ゲスト** または **IUSR_システム名** ユーザーアカウントを右クリックし、**プロパティ** を選択します。
4. **アカウントを無効にする** 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、利用している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ことが必要です。

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連携するように SNMP エージェントを設定するには、次項で説明する手順に従ってください。

 **メモ:** 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。

 **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 が稼動するシステムでの SNMP エージェントの設定](#)」
- 1 「[VMware MIB をプロキシするために対応 VMware ESX 4.0 オペレーティングシステムが稼動するシステムにおいて SNMP エージェントを設定する](#)」
- 1 「[対応 VMware ESXi 4.X オペレーティングシステムが稼動するシステムにおける SNMP エージェントの設定](#)」

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連携するように SNMP エージェントを設定するには、次項で説明する手順に従ってください。

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

リモートホストによる 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 パケットを受け付けません。Windows Server 2003 が稼動す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が稼動するシステムでリモートホストから SNMP パケットを受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、同ウィンドウの **コンピュータの管理** アイコンを展開します。
3. **サービスとアプリケーション** アイコンを展開して、**サービス** をクリックします。
4. リストを下にスクロールして SNMP サービス を見つけ、SNMP サービス を右クリックして、**プロパティ** をクリックします。
SNMP サービスプロパティ ウィンドウが表示されます。
5. **セキュリティ** タブをクリックします。
6. **任意のホストから SNMP パケットを受け入れる** を選択するか、**リモートホストをこれらのホストの SNMP パケットを受け入れる** リストに追加します。

SNMP コミュニティ名の変更

SNMP コミュニティ名を設定すると、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** ウィンドウを開きます。
2. 必要に応じて、同ウィンドウの **コンピュータの管理** アイコンを展開します。
3. **サービスとアプリケーション** アイコンを展開して、**サービス** をクリックします。
4. サービスのリストを下にスクロールして **SNMP サービス** を見つけ、**SNMP サービス** を右クリックしてから、**プロパティ** をクリックします。
SNMP サービスプロパティ ウィンドウが表示されます。
5. **セキュリティ** タブをクリックして、コミュニティ名を追加または編集します。
 - a. コミュニティ名を追加するには、**受理されたコミュニティ名** 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、**受理されたコミュニティ名** リストでコミュニティ名を選択して、**編集** をクリックします。
SNMP サービス設定 ウィンドウが表示されます。

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

SNMP サービスプロパティ ウィンドウが表示されます。

5. **セキュリティ** タブをクリックして、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ためのシステム設定

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

SNMP サービスプロパティ ウィンドウが表示されます。

5. **トラップ** タブをクリックしてトラップのコミュニティを追加するか、トラップコミュニティのトラップ送信先を追加します。
 - a. トラップのコミュニティを追加するには、**コミュニティ名** ボックスにコミュニティ名を入力し、**コミュニティ名** ボックスの横にある **リストに追加** をクリックします。
 - b. トラップコミュニティのトラップ送信先を追加するには、**コミュニティ名** ドロップダウンボックスからコミュニティ名を選択して、**トラップ送信先** ボックスの下の **追加** をクリックします。
 - 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、*net-snmp* 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、ご利用のオペレーティングシステムのマニュアルを参照してください。

SNMP エージェントのアクセスコントロールの設定

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

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

Server Administrator SNMP エージェントのインストールアクション

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、`public` 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ようとします。Server Administrator は、`/etc/snmp/snmpd.conf` SNMP エージェント設定ファイルを 2 通りの方法で変更します。

1 つめの方法では、次の行が存在しない場合に、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
```


2 つめの方法では、デフォルトの「アクセス」行を変更し、`public` コミュニティに対して、MIB ツリー全体への読み取り専用アクセス権を与えます。Server Administrator 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、`public` コミュニティには、MIB ツリー全体への読み取り専用アクセス権が与えられます。

 **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)プロトコルを使用して 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時、自らを SMUX ピアとして識別するため、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 エージェントで設定される必要があるため、Server Administrator はインストール時に、SNMP エージェント設定ファイルの `/etc/snmp/snmpd.conf` に以下の行を追加します。

```
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. 次の行を見つけます。

```
com2sec publicsec default public
```

または

```
com2sec notConfigUser default public
```

2. この行の `public` の部分を SNMP コミュニティ名に置き換えます。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 の属性を変更するには、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. 次の行を見つけます。

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

または

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

2. この行の最初の `none` を `all` に置き換えます。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ためのシステム設定

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_address community_name
```

ここで `IP_address` は、管理ステーションの IP アドレスを表し、`community_name` 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 が稼動するシステムでの SNMP エージェントの設定

Server Administrator は、`net-snmp` エージェントによって提供される 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、Set 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連携するように SNMP エージェントを設定するには、次項で説明する手順に従ってください。

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


Server Administrator SNMP インストールアクション

Server Administrator SNMP は、SMUX プロトコルを使用して 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時、自らを SMUX ピアとして識別するため、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 はインストール時に、SNMP エージェント設定ファイル(`/etc/snmp/snmpd.conf`)に、既に追加されていない場合は、下の行を追加します。

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

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


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

1. 次の行を見つけます。

```
rocommunity public 127.0.0.1
```

2. この行の 127.0.0.1 をリモートホストの IP アドレスに書き換えます。編集後の行は、次のようになります。

```
rocommunity public <IP アドレス>
```

 **メモ:** 各リモートホストに対し rocommunity 指令を追加することにより、複数の特定リモートホストからの SNMP アクセスを有効にできます。

3. SNMP 設定の変更を有効にするには、次のように入力して SNMP エージェントを再起動します。

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

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

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を取得するのに使うデフォルト 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の /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. この行の public を新しい SNMP コミュニティ名に置き換えます。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、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。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の /etc/snmp/snmpd.conf を編集して、次の手順を実行します。

1. 次の行を見つけます。

```
rocommunity public 127.0.0.1
```

2. この行の rocommunity を rwcommunity に置き換えます。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ためのシステム設定

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_address community_name
```

ここで `IP_address` は、管理ステーションの IP アドレスを表し、`community_name` 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
```

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

SNMP プロトコルを使用して、単一のデフォルトポート 161 経由で ESX4.0 Server を管理できます。これには、`snmpd` がデフォルトポートの 161 を使用し、`vmwarehostd` が別の未使用ポート (例:167) を使用するように設定します。VMWare MIB 上の SNMP リクエストは、`snmpd` デモンのプロキシ機能を使用して `vmware-hostd` に転送されます。

VMWare SNMP 設定ファイルは、ESX Server 上で手動で、またはリモートシステム (Windows または Linux) から VMware リモートコマンドラインインタフェース (RCLI) コマンドの `vicfg-snmp` を実行することで変更できます。RCLI ツールは、VMware ウェブサイト (http://www.vmware.com/download/vi/drivers_tools.html) からダウンロードできます。

以下が、設定に必要な手順です。

1. SNMP 設定を変更するには、VMWare SNMP 設定ファイル (`/etc/vmware/snmp.xml`) を手動で、または次の `vicfg-snmp` コマンドを実行することで編集します。これには、SNMP リスニングポート、コミュニティ文字列、トラップターゲットの IP アドレス / ポート番号、およびトラップコミュニティ名の編集と VMWare SNMP サービスを有効にする作業が含まれます。

```
a. vicfg-snmp.pl --server <ESX IP アドレス> --username root --password <パスワード> -c <コミュニティ名> -p X -t <DMC IP アドレス>@162/<コミュニティ名>
```

ここで X は使用されていないポートを表します。未使用のポートを見つけるには、定義されたシステムサービスのポート割り当てが記載されている `/etc/services` ファイルをご覧ください。また、選択したポートが他のアプリケーション/サービスによって使用されていないことを確認するには、ESX Server 上で `netstat -a` コマンドを実行します。

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

- b. VMWare SNMP サービスを有効にするには、次のコマンドを実行します。

```
vicfg-snmp.pl --server <ESX IP アドレス> --username root --password <パスワード>
```

```
-E
```

- c. 設定を表示するには、次のコマンドを実行します。

```
vicfg-snmp.pl --server <ESX IP アドレス> --username root --password <パスワード>
```

```
-s
```

変更後の設定ファイルは、次のようになります。

```
<?xml version="1.0">
<config>
<snmpSettings>
<enable>true</enable>
<communities>public</communities>
<targets>143.166.152.248@162/public</targets>
<port>167</port>
</snmpSettings>
</config>
```

2. システムで SNMP サービスが既に起動している場合は、次のコマンドを入力して停止させます。

```
service snmpd stop
```

3. /etc/snmp/snmpd.conf の最後に次の行を追加します。

```
pro@ -v 1 -c public udp:127.0.0.1:X .1.3.6.1.4.1.6876
```

ここで、X は、上記の SNMP 設定時に指定された未使用ポートを表します。

4. <送信先_IPアドレス> <コミュニティ名> コマンドを使用してトラップの送信先を設定します。

専用 MIB で定義されたトラップを送信するには、trapsink 仕様が必要です。

5. 次のコマンドを実行して、mgmt-vmware サービスを再起動します。

```
service mgmt-vmware restart
```

6. 次のコマンドを実行して、snmpd サービスを再起動します。

```
service snmpd start
```

 **メモ:** このサービスは `snmpd` サービスに依存するため、`srvadmin` がインストールされ、サービスがすでに開始されている場合はサービスを再起動してください。

7. 再起動ごとに `snmpd` デーモンが開始されるようにするため、次のコマンドを実行します。


```
chkconfig snmpd on
```

8. 管理ステーションにトラップを送信する前に、次のコマンドを実行して、SNMP ポートが開かれていることを確認します。

```
esxcfg-firewall -e snmpd
```

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

Server Administrator は、VMware ESXi 4 上の SNMP トラップをサポートしています。必要な SNMP サポートがないため、Server Administrator は VMware ESXi 4.x での SNMP Get および Set 操作をサポートしていません。VMware ESXi 4 が稼働するシステムで、管理ステーションに SNMP トラップを送信させるように設定するには、VMware vSphere コマンドラインインタフェース (CLI) を使用します。

 **メモ:** VMware vSphere CLI の使用の詳細については、VMware サポートサイト www.vmware.com/support を参照してください。

SNMP トラップを管理ステーションに送信するためのシステム設定


Server Administrator は、センサー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。


管理ステーションにトラップを送信できるように、Server Administrator が実行される ESXi システムを設定するには、次の手順に従います。

1. VMware vSphere CLI をインストールします。
2. VMware vSphere CLI をインストールしたシステム上で、コマンドプロンプトを開きます。
3. VMware vSphere CLI のインストール先ディレクトリに移動します。Linux の場合、デフォルトの場所は `/usr/bin` です。Windows の場合、デフォルトの場所は `C:\Program Files\VMware\VMware vSphere CLI\bin` です。
4. 次のコマンドを実行します。

```
vicfg-snmp.pl --server <server> --username <username> --password <password> -c <community> -t <hostname>/<community>
```

ここで、<server> は ESXi システムのホスト名または IP アドレス、<username> は ESXi システム上のユーザー、<password> は ESXi ユーザーのパスワード、<community> は SNMP コミュニティ名、<hostname> は管理システムのホスト名または IP アドレスを指します。

 **メモ:** `.pl` の拡張子は、Linux では必要ありません。

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

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

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

Red Hat Enterprise Linux/SUSE Linux 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。この操作は、Server Administrator の起動前後に行えます。

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

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


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

ツールの選択 メニューが表示されます。

2. 下矢印を使用して **ファイアウォール設定** を選択し、**<Enter>** を押します。

ファイアウォールの設定 画面が表示されます。

3. **<Tab>** を押して **セキュリティレベル** を選択し、スペース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、**ファイアウォールなし** または **無効** を選択して **手順 7** に進みます。
- b. ネットワークインタフェース全体または SNMP ポートを開くには、**高**、**中** または **有効** を選択して **手順 4** に進みます。

4. **<Tab>** を押して **カスタマイズ** へ移動し、**<Enter>** を押します。

ファイアウォールの設定-カスタマイズ 画面が表示されます。

5. ネットワークインタフェース全体を開放するか、すべてのネットワークインタフェースの SNMP ポートだけを開放するかを選択します。

- a. 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ている場合、インタフェース全体が開放されたことを意味します。
- 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 **その他のポート** 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。

ファイアウォールの設定 画面が表示されます。

7. **<Tab>** を押して **OK** を選択し、**<Enter>** を押します。

ツールの選択 メニューが表示されます。

8. **<Tab>** を押して **終了** を選択し、**<Enter>** を押します。

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. コンソールで
 - a. `# yast2 firewall` を実行し、`SUSEfirewall2` を設定します。
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。

[目次に戻る](#)

[目次に戻る](#)

Server Administrator の使用

Dell OpenManage Server Administrator バージョン 6.4 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 ウェブサーバーの処置 タブ](#)
- [Server Administrator の管理](#)
- [Server Administrator コマンドラインインタフェースの使い方](#)

Server Administrator セッションの開始

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

Server Administrator ログイン 画面が表示されます。Dell OpenManage Server Administrator のデフォルトポートは 1311 です。ポート番号は必要に応じて変更できます。システムブリア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。

ログインとログアウト

OpenManage Server Administrator は、以下の 3 種類のログイン方法 それらの機能は次のとおりです。

- 1 Server Administrator ローカルシステムログイン
- 1 Server Administrator 管理下システムログイン
- 1 Central Web Server ログイン


Server Administrator ローカルシステムログイン

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

ローカルシステム上で Server Administrator にログインするには、次のログインウィンドウを使用します。

1. System Management の **ログイン** ウィンドウの適切なフィールドに、あらかじめ割り当てられた **ユーザー名** および **パスワード** を入力します。
定義されたドメインから Server Administrator にアクセスするには、正しい **ドメイン** 名も指定する必要があります。
2. システムで Microsoft Windows オペレーティングシステムが稼動しており、Windows ドメインのメンバーである場合は、ドメインリストからドメインを選択します。
3. 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。[Active Directory ログインの使用](#) を参照してください。
4. **送信** をクリックします。

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

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

Server Administrator 管理下システムログイン

このログインは、Server Administrator ウェブサーバーのコンポーネントをインストールした場合のみ、利用可能です。リモートシステムを管理するために、Server Administrator にログインするには:

方法 1

1. デスクトップ上の DellOpenManageServer Administrator アイコンをクリックします。
2. 管理下システムの IP アドレスまたはシステム名、あるいは完全修飾ドメイン名 (FQDN) を入力します。

 **メモ:** システム名または FQDN を入力すると、Dell OpenManage Server ウェブサーバーホストによって管理下システムの IP アドレスに変換されます。管理下システムのポート番号を入力することもできます。たとえば、ホスト名:ポート番号、または IP アドレス:ポート番号 Citrix XenServer 5.6 管理下ノードに接続する場合は、ホスト名:ポート番号 または IP アドレス:ポート番号の形式でポート 5986 に接続します。

3. イン트라ネット接続を利用している場合は、**証明書**の警告を無視する チェックボックスを選択します。
4. **Active Directory ログイン チェックボックス** を選択します。Microsoft Active Directory 認証を用いてログインする場合は、このオプションを選択します。ネットワークへのアクセスを制御するために Active Directory ソフトウェアを使用していない場合は、このチェックボックスを選択しないでください。[Active Directory ログインの使用](#) を参照してください。
5. **送信** をクリックします。

方法 2

ウェブブラウザを開き、アドレスフィールドに以下のいずれかを入力し、<Enter> キーを押します。


```
https://hostname:1311
```

hostname 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 address:1311
```


IPaddress 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。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:// ではなく) と入力します。

 **メモ:** Server Administrator にログインするには、事前に割り当てられたユーザー権限が必要です。新しいユーザーを設定する手順は、[設定と管理](#)を参照してください。

Central Web Server ログイン


このログインは、Server Administrator ウェブサーバーのコンポーネントをインストールした場合のみ、利用可能です。OpenManage Server Administrator Central Web Server を管理するには、このログインを使用します。

1. デスクトップ上の DellOpenManageServer Administrator アイコンをクリックします。リモートログインページが表示されます。


 **注意:** ログイン画面には **証明書**の警告を無視する チェックボックスがあります。このオプションは慎重にご使用ください。このオプションは、信頼されたイントラネット環境においてのみ、使用することが強く推奨されます。

2. 画面の右角の **ウェブサーバーの管理** リンクをクリックします。
3. **ユーザー名**、**パスワード** および **ドメイン名** (定義されたドメインから Server Administrator にアクセスしている場合)を入力し、**送信** をクリックします。
4. 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。[Active Directory ログインの使用](#) を参照してください。
5. **送信** をクリックします。

Server Administrator セッションを終了するには、「[グローバルナビゲーションバー](#)」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。

 **メモ:** Mozilla Firefox バージョン 3.0 または 3.5、あるいは Microsoft Internet Explorer バージョン 7.0 または 8.0 を使って Server Administrator を起動すると、中度の警告ページが開いてセキュリティ証明書に問題があると表示されることがあります。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。

システムのセキュリティを保つために、認証局(CA)からルート証明書または証明書チェーンをインポートすることを、強くお勧めします。詳細については、VMware のマニュアルを参照してください。

 **メモ:** 管理下システム上の認証局が有効にも関わらず、Server Administrator ウェブサーバーがまだ信頼されていない証明書エラーを報告する場合は、certutil.exe を使用して管理下システムの CA を信頼されたものにできます。この .exe へのアクセスについての詳細は、オペレーティングシステムのマニュアルを参照してください。対応 Windows オペレーティングシステム上では、証明書をインポートする代わりに、証明書スナップインのオプションを利用することもできます。

Active Directory ログインの使用

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

このソリューションは、Server Administrator へのアクセスを提供し、Active Directory ソフトウェアの既存ユーザーに Server Administrator ユーザーおよび特権の追加/管理を可能にします。詳細については、『Dell OpenManage インストールおよびセキュリティ ユーザーズガイド』の「Microsoft Active Directory の使用」を参照してください。

シングルサインオン

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関しては、support.microsoft.com/default.aspx?scid=kb;en-us;Q258063 でナレッジベース記事をご覧ください。

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、またはシステム管理者）のあるアカウントを持っている必要があります。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=[plugin name]
```

plugin name = *omsa, ita* (プラグイン名 は *omsa, ita*) などになります。

たとえば、次のとおりです。

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

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

```
authType=ntlm&application=[plugin name]&locallogin=true
```

plugin name = *omsa, ita* (プラグイン名 は *omsa, ita*) などになります。

たとえば、次のとおりです。


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

また、Server Administrator は他の製品 (Dell OpenManage IT Assistant など) もログインページを介さずに直接 Server Administrator の Web ページにアクセスできるように機能が拡張されています (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 オペレーティングシステムが稼動するシステム上のセキュリティ設定

対応の Microsoft Windows オペレーティングシステムが稼動するリモート管理下システムから 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されます。

Internet Explorer

- 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** を順にクリックします。
- 信頼済みサイト** のアイコンをクリックします。
- サイト** をクリックします。
- 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。
- カスタムレベル** をクリックします。

Windows Server 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。
- アクティブスクリプト** 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ルのスクリプトを許可する** ラジオボタンを選択します。

- 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。


- 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** を順にクリックします。
- 信頼済みサイト** のアイコンをクリックします。
- サイト** をクリックします。
- 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 Firefox

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 のホームページには 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。
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 3-1](#) には、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 3-1. 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
モジュラエンクロージャ	モジュラシステム
サーバーモジュール	モジュラシステム
メインシステム	モジュラシステム
システム	非モジュラシステム
メインシステムシャーシ	非モジュラシステム

[図 3-1](#) は、非モジュラシステムにシステム管理者特権でログインしたユーザー用のサンプル Server Administrator ホームページのレイアウトを示します。

図 3-1. サンプル Server Administrator ホームページ - 非モジュラシステム



図 3-2 は、モジュラシステムにシステム管理者特権でログインしたユーザー用のサンプル Server Administrator ホームページのレイアウトを示します。

図 3-2. サンプル Server Administrator ホームページ - モジュラシステム



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、処置ウィンドウ内を移動します。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、システムプローブゲ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、システム管理者またはパワーユーザー特権が必要です。さらに、システム管理者特権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。

モジュラおよび非モジュラシステムにおける Server Administrator ユーザーインターフェースの違い

表 3-2 は、モジュラおよび非モジュラシステムにおいて利用できる Server Administrator 機能を記載しています。チェックマークは対象の機能が利用可能であること、×印は利用できないことを意味しています。

表 3-2. モジュラおよび非モジュラシステムにおける Server Administrator ユーザーインターフェースの違い

機能	モジュラシステム	非モジュラシステム
バッテリー	✓	✓
電源装置	✗	✓
ファン	✗	✓
ハードウェアパフォーマンス	✗	✓
		(xxOx システム以降)
イントルージョン	✗	✓
メモリ	✓	✓
ネットワーク	✓	✓
ポート	✓	✓
Power Management	✓	✓

		(xxOx システム以降)
プロセッサ	✓	✓
リモートアクセス	✓	✓
リムーバブルフラッシュメディア	✓	✓
スロット	✓	✓
温度	✓	✓
電圧	✓	✓
モジュラエンクロージャ(シャーシ情報および CMC 情報)	✓	✗

グローバルナビゲーションバー

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

- 1 **プリファランス** をクリックして、**プリファランス** ホームページを開きます。「[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** をクリックして、デルのサポートサイトに接続します。
- 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が終了します。

システムツリー

システムツリーは Server Administrator ホームページの左側に表示され、システムの表示可能なコンポーネントをリストにします。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**、および **ストレージ** です。

ツリーを展開するには、オブジェクトの左側にあるプラス記号 (+) をクリックするか、オブジェクトをダブルクリックします。マイナス記号 (-) が付いているものは、展開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。あらかじめ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。

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

システム / サーバーモジュールコンポーネントステータスインジケータ

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

表 3-3. システム / サーバーモジュールコンポーネントステータスインジケータ

✓	コンポーネントが健全(正常)であることを示します。
⚠	コンポーネントが警告(非重要)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。警告状態は早急な対処を必要とします。
✗	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。重要な状態は即座な対処を必要とします。
?	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**、**ヘルプ**、**更新** の 5 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。

- 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生成されます。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分する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。
- 1 **ヘルプ** (❓) をクリックすると、表示中の特定のウィンドウやタスクボタンの詳細が表示されます。

メモ: エクスポート、電子メール、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システム管理者特権でログインしたユーザーにのみ表示されます。

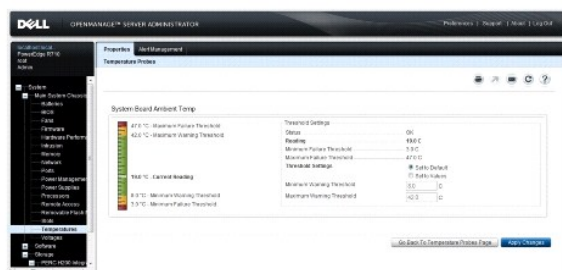
下線付きアイテム

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 3-3](#)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 3-3. 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。**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しい情報が掲載された、個別の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 ホームページの左ペイン(システムツリーが Server Administrator ホームページで表示されている)には、システムツリーウィンドウの使用可能な設定オプションがすべて表示されず。

使用可能なプリファランスホームページオプションは次の通りです。

- 1 一般設定
- 1 Server Administrator

リモートシステムを管理するためにログインすると、**プリファランス** タブが表示されます。このタブは、Server Administrator ウェブサーバーまたはローカルシステムを管理するために、ログインした場合でも、利用可能です。

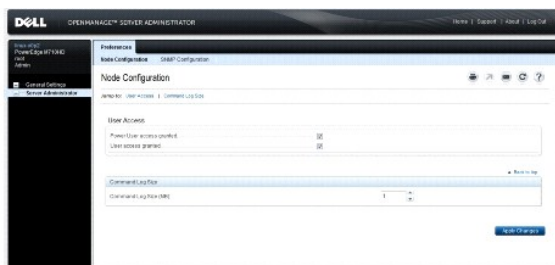
Server Administrator ホームページ同様、**プリファランス** ホームページには 3 つの主な領域があります。

- 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。

- **ホーム** をクリックすると、Server Administrator のホームページに戻ります。
- 1 **プリファランス** ホームページの左ペイン(システムツリーが Server Administrator ホームページで表示されている)には、管理下システムまたは Server Administrator ウェブサーバーのプリファランスカテゴリが表示されます。
- 1 配置ウィンドウには、管理下システムまたは Server Administrator ウェブサーバーで利用可能な設定およびプリファランスが表示されます。

図 3-4 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。

図 3-4. プリファランス ホームページのサンプル - 管理下システム



管理下システムのプリファランス

リモートシステムにログインする際、プリファランスホームページには、**プリファランス** タブ配下の **ノード設定** ウィンドウがデフォルトで表示されます。

ユーザーまたはパワーユーザー特権を持つユーザーのアクセスを有効または無効にするには、Server Administrator オブジェクトをクリックします。ユーザーのグループ特権によっては、Server Administrator オブジェクト配置ウィンドウに、**プリファランス** タブがある場合もあります。

プリファランス タブでは、以下のことができます。

- 1 ユーザーまたはパワーユーザー特権を持つユーザーのアクセスを有効または無効にします。
- 1 コマンドログサイズの設定
- 1 SNMP の設定

Server Administrator ウェブサーバーのプリファランス

Server Administrator ウェブサーバーにログインする際、**プリファランス** ホームページには、プリファランス Server Administrator タブ配下の **ユーザープリファランス** ウィンドウがデフォルトで表示されます。

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


- 1 ウェブサーバーのプリファランス
- 1 X.509 証明書管理

これら機能へのアクセスの詳細については、「[Server Administrator サービス](#)」を参照してください。

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


ユーザーとシステムのプリファランスの設定

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

 **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の受取人を追加するには、指定するサービス連絡先の電子メールアドレスを **宛先**: フィールドに入力し、**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** をクリックし、そのウィンドウの HTML ファイルが添付された電子メールを、指定したアドレスに送信します。

4. ホームページの外觀を変更するには、**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 Server** タブをクリックします。


3. **サーバープリファランス** ウィンドウで、必要に応じてオプションを設定します。

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。

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

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。確立されたすべてのセッションに、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

1. **キー署名アルゴリズム** には、サポートされる署名アルゴリズムが表示されます。ドロップダウンリストからアルゴリズムを選択します。SHA 512 または SHA 256 のいずれかを選択する場合、ご利用のオペレーティングシステム / ブラウザが同アルゴリズムをサポートしていることを確認してください。オペレーティングシステム / ブラウザのサポート要件を満たすことなく、これらのオプションを選択した場合、Server Administrator は、「ウェブページを表示できません」のエラーを表示します。このフィールドは、Server Administrator により自動生成される自己署名証明書のみを利用されます。Server Administrator で新しい証明書をインポートまたは生成した場合、ドロップダウンリストは灰色表示になります。

 **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. **サーバープリファレンス** ウィンドウのオプション設定が完了したら、**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、ウェブ証明書が必要です。システムのセキュリティを確保するために、以下の対策を推奨します。

- 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:** 証明書を管理するには、システム管理者特権でログインする必要があります。

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

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 ウェブサーバーの処置 タブ

Server Administrator ウェブサーバーを管理するためにログインすると、以下の処置タブが表示されます。

- 1 シャットダウン
- 1 ログ
- 1 セッション管理

Server Administrator の管理

Server Administrator は、管理下システム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 を管理するには、システム管理者特権でログインする必要があります (対応 Citrix XenServer、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

対応 Microsoft Windows オペレーティングシステム

Server Administrator を開始するには、対応 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. **開始** をクリックします。

対応 Citrix XenServer、Red Hat Enterprise Linux、SUSE Linux Enterprise Server オペレーティングシステム

対応 Citrix XenServer、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

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. **停止** をクリックします。

対応 Citrix XenServer、Red Hat Enterprise Linux、SUSE Linux Enterprise Server オペレーティングシステム

対応 Citrix XenServer、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 Citrix XenServer、Red Hat Enterprise Linux、SUSE Linux Enterprise Server オペレーティングシステム

対応 Citrix XenServer、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
```

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

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

CLI 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 コマンドを使用すると、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実証したり、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フェースユーザーズガイド』を参照してください。

[目次に戻る](#)