

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

[DRAC 5 概要](#)

[DRAC 5 のインストールと設定](#)

[DRAC 5 コマンドラインコンソールの設定と使用](#)

[DRAC 5 ウェブユーザーインターフェースを使用した DRAC 5 の設定](#)

[管理下システムの回復とトラブルシューティング](#)

[DRAC 5 と Microsoft Active Directory との併用](#)

[GUI コンソールリダイレクトの使用](#)

[仮想メディアの設定と使用](#)

[RACADM コマンドラインインターフェースの使用](#)

[WM-CUI を使用したオペレーティングシステムの導入](#)

[DRAC 5 SM-CLP コマンドラインインターフェースの使用](#)

[トラブルシューティング](#)

[RACADM サブコマンドの概要](#)

[DRAC 5 プロパティデータベースグループおよびオブジェクト定義](#)

[対応 RACADM インタフェース](#)

[ブラウザのブレイクアウト](#)

[用語集](#)

メモ、注意、警告

 **メモ:** コンピュータを使いやすい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損失の可能性と、その危険を回避するための方法が記載されています。

 **警告:** 物的損傷、負傷および死亡の危険性があることを示しています。

このマニュアルの情報は予告なしに変更されることがあります。
© 2006 すべての著作権は、Dell Inc. にあります。

Dell Inc. からの書面による許可なしには、いかなる方法においても、このマニュアルの複写、転写を禁じます。

このテキストで使用されている商標: Dell, DELL のロゴ, Dell OpenManage、および PowerEdge は Dell Inc. の商標です。Microsoft と Windows は Microsoft Corporation の登録商標、Windows Server は同社の登録商標です。Red Hat は Red Hat, Inc. の登録商標です。Intel は Intel Corporation の登録商標です。UNIX は米国および他国における The Open Group の登録商標です。

Copyright 1998-2006 The OpenLDAP Foundation. All rights reserved. 変更の有無にかかわらず、ソースおよびバイナリ形式の再配布および使用は、OpenLDAP パブリックライセンスによって認証されている場合に限り許可されます。このライセンスのコピーは、配布の最上位ディレクトリにある「ライセンス」ファイルまたは <http://www.OpenLDAP.org/license.html> から入手できます。OpenLDAP は OpenLDAP Foundation の登録商標です。個々のファイルと提供されたパッケージの著作権は、他の著作権者が権利を有し、追加規制の対象となる場合があります。本著作物はミシガン大学の LDAP v3.3 配布によるものです。本著作物には公的ソースから入手した資料も含まれています。OpenLDAP に関する情報は <http://www.openldap.org/> から入手できます。Portions Copyright 1998-2004 Kurt D. Zeilenga. Portions Copyright 1998-2004 Net Boolean Incorporated. Portions Copyright 2001-2004 IBM Corporation. All rights reserved. 変更の有無にかかわらず、ソースおよびバイナリ形式の再配布および使用は、OpenLDAP パブリックライセンスによって認証されている場合に限り許可されます。Portions Copyright 1999-2003 Howard Y. H. Chu. Portions Copyright 1999-2003 Symas Corporation. Portions Copyright 1998-2003 Hallvard B. Furuseth. All rights reserved. 変更の有無にかかわらず、ソースおよびバイナリ形式の再配布および使用は、この通知が保護されるという条件の下で許可されます。著作権所有者名は、事前の書名による特定の許可なく、本ソフトウェアから派生する製品を是認または促進する目的で使用してはなりません。本ソフトウェアは「現状のまま」で提供され、明示または暗示を問わず何らの保証も行わないものとします。Portions Copyright (c) 1992-1996 Regents of the University of Michigan. All rights reserved. 変更の有無にかかわらず、ソースおよびバイナリ形式の再配布および使用は、この通知が保護され、適切な著作権表示がミシガン大学アーカイブにあるという条件の下で許可されます。大学名は、事前の書名による特定の許可なく、本ソフトウェアから派生する製品を是認または促進する目的で使用してはなりません。本ソフトウェアは「現状のまま」で提供され、明示または暗示を問わず何らの保証も行わないものとします。商標または製品の権利を主張する事業体を表すためにその他の商標および社名が使用されていることがあります。これらの商標や会社名は、一切 Dell Inc. に所属するものではありません。

商標または製品の権利を主張する事業体を表すためにその他の商標および社名が使用されていることがあります。これらの商標や会社名は、一切 Dell Inc. に所属するものではありません。

2006 年 6 月 Rev. A02

[目次ページに戻る](#)

RACADM サブコマンドの概要

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

- [help](#)
- [arp](#)
- [clearasrscreen](#)
- [config](#)
- [getconfig](#)
- [coredump](#)
- [coredumpdelete](#)
- [fwupdate](#)
- [getssninfo](#)
- [getsysinfo](#)
- [getrctime](#)
- [ifconfig](#)
- [netstat](#)
- [ping](#)
- [setniccfq](#)
- [getniccfq](#)
- [getsvctag](#)
- [racdump](#)
- [racreset](#)
- [racresetcfq](#)
- [serveraction](#)
- [getrctlog](#)
- [clrrctlog](#)
- [getsel](#)
- [clrsel](#)
- [getrctellog](#)
- [sslcsrqen](#)
- [sslcertupload](#)
- [sslcertdownload](#)
- [sslcertview](#)
- [testemail](#)
- [testtrap](#)
- [vmdisconnect](#)
- [vmkey](#)

この項では、RACADM コマンドラインインタフェースで使用可能なサブコマンドについて説明します。

help

 **メモ:** このコマンドを使用するには、DRAC 5 への **ログイン** 権限が必要です。

[表 A-1](#) で **help** コマンドについて説明します。

表 A-1. Help コマンド

コマンド	定義
help	racadm と一緒に使用できるすべてのサブコマンドと、各サブコマンドの短い説明を一覧にします。

概要

racadm help

racadm help <サブコマンド>

説明

help サブコマンドは、**racadm** コマンドを使用するときに使えるサブコマンドすべてに1行の簡単な説明を添えてリストにします。 **help** の後ろにサブコマンドを入力して、特定のサブコマンドの構文を表示することもできます。

出力

racadm help コマンドはサブコマンドのリストを表示します。

racadm help<サブコマンド>コマンドは、指定したサブコマンドの情報のみを表示します。

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

arp

 **メモ:** このコマンドを使用するには、**診断コマンドの実行** 権限が必要です。

[表 A-2](#) で **arp** コマンドについて説明します。

表 A-2. arp コマンド

コマンド	定義
arp	ARP テーブルの内容を表示します。 ARP テーブルのエントリは追加や削除ができません。

概要

racadm arp

対応インタフェース

- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

clearasrscreen

 **メモ:** このコマンドを使用するには、**ログのクリア** 権限が必要です。

[表 A-3](#) で **clearasrscreen** サブコマンドについて説明します。

表 A-3. clearasrscreen

サブコマンド	定義
clearasrscreen	メモリの中にある前回クラッシュ画面をクリアします。

概要

racadm clearasrscreen

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

config

 **メモ:** getconfig コマンドを使用するには、DRAC 5 へのログイン 権限が必要です。

表 A-4 で config および getconfig サブコマンドについて説明します。

表 A-4. config/getconfig

サブコマンド	定義
config	DRAC 5 を設定します。
getconfig	DRAC 5 設定データを取得します。

概要

```
racadm config [-c|-p] -f <ファイル名>
```

```
racadm config -g <グループ名> -o <オブジェクト名> [-i <インデックス>] <値>
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

説明

config サブコマンドを使用すると、DRAC 5 設定パラメータを個別に設定するか、設定ファイルの一部として一括設定できます。データが異なる場合は、その DRAC 5 オブジェクトは新しい値で書き込まれます。

入力

表 A-5 で config サブコマンドのオプションについて説明します。

 **メモ:** -f および -p オプションは serial/telnet/ssh コンソールではサポートされていません。

表 A-5. config サブコマンドオプションと説明

オプション	説明
-f	-f <ファイル名> オプションを使用すると、config は <ファイル名> で指定したファイルの内容を読み取り、DRAC 5 を設定します。ファイルには「 解析規則 」で指定した形式のデータが含まれている必要があります。
-p	-p (パスワード) オプションは、設定完了後に設定ファイル -f <ファイル名> に含まれているパスワードエントリを削除するように config に指定します。
-g	-g <グループ名> (グループ) オプションは -o オプションと一緒に使用する必要があります。<グループ名> は、設定するオブジェクトが含まれたグループを指定します。
-o	-o <オブジェクト名> <値> (オブジェクト) オプションは -g オプションと一緒に使用する必要があります。このオプションは、文字列 <値> と一緒に書き込まれたオブジェクト名を指定します。
-i	-i <インデックス> (インデックス) オプションは、インデックス付きのグループのみに有効で、固有のグループを指定するために使用できます。<インデックス> は 1 ~ 16 の 10 進数です。インデックスは名前付きの値ではなく、インデックス値で指定されます。
-c	-c (チェック) オプションは、config サブコマンドと一緒に使用され、ユーザーは .cfg ファイルを解析して構文エラーを見つけることができます。エラーが見つかったら、エラーのあった行番号と短い説明が表示されます。書き込みは DRAC 5 には行われません。このオプションは確認専用で使用します。

出力

このサブコマンドは、次の場合にエラー出力を生成します。

- 1 無効な構文、グループ名、オブジェクト名、インデックスまたはその他の無効なデータベースメンバー
- 1 racadm CLI failures

このサブコマンドは、.cfg ファイル内の合計オブジェクト数のうち、書き込まれた設定オブジェクト数を示す値を返します。

例

```
1 racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.100
```

cfgNicIpAddress 設定パラメータ (オブジェクト) を 10.35.10.110 の値に設定します。この IP アドレスオブジェクトは **cfgLanNetworking** グループにあります。

```
1 racadm config -f myrac.cfg
```

DRAC 5 を設定または再設定します。 **getconfig** から **myrac.cfg** ファイルを作成することもできます。解析規則に従っていれば、**myrac.cfg** ファイルを手動で編集することもできます。

 **メモ:** **myrac.cfg** にパスワード情報は含まれていません。この情報をファイルに含めるには、手動で入力する必要があります。設定中にパスワード情報を **myrac.cfg** ファイルから削除する場合は、**-p** オプションを使用します。

getconfig

getconfig サブコマンドの説明

getconfig サブコマンドを使用すると、DRAC 5 設定パラメータを個別に取得するか、すべての RAC 設定グループを取得してファイルに保存できます。

入力

[表 A-6](#) で **getconfig** サブコマンドのオプションについて説明します。

 **メモ:** **ファイルを指定せずに** **-i** オプションを使用すると、ファイルの内容がターミナルスクリーンに表示されます。

表 A-6. **getconfig** サブコマンドオプション

オプション	説明
-f	-f <ファイル名> オプションを getconfig につけると、RAC 設定のすべてを設定ファイルに書き込みます。このファイルは config サブコマンドを使用した一括設定操作に使用できます。 メモ: -i オプションで cfgIpmiPet および cfgIpmiPef グループにエントリを作成することはできません。 cfgIpmiPet グループをファイルに取り込むためのトラップの送信先を少なくとも 1 つ設定する必要があります。
-g	-g <グループ名> (グループオプション) は、単一グループの設定を表示する場合に使用できます。 グループ名 は、 racadm.cfg ファイルで使用されているグループの名前です。 グループ がインデックスグループの場合は、 -i オプションを使用してください。
-h	-h (ヘルプ) オプションには、使用できるすべての設定グループが一覧表示されます。このオプションは、正確なグループ名を覚えていない場合に便利です。
-i	-i <インデックス> (インデックスオプション) は、インデックス付きのグループのみに有効で、固有のグループを指定するために使用できます。 <インデックス> は 1 ~ 16 の 10 進数です。 -i <インデックス> を指定しないと、グループには 1 の値が想定されます。これは複数のエントリがあるテーブルです。 インデックス は、「名前付き」値ではなく、インデックス値で指定されます。
-o	-o <オブジェクト名> (オブジェクトオプション) は、クエリで使用されるオブジェクト名を指定します。このオプションは省略可能で、 -g オプションと一緒に使用できます。
-u	-u <ユーザー名> (ユーザー名オプション) は、指定したユーザーの設定を表示するために使用できます。 <ユーザー名> オプションは、そのユーザーのログイン名です。
-v	-v オプションはその他の詳細とプロパティを表示し、 -g オプションと一緒に使用します。

出力

このサブコマンドは、次の場合にエラー出力を生成します。

- 1 無効な構文、グループ名、オブジェクト名、インデックスまたはその他の無効なデータベースメンバー
- 1 Racadm CLI ユーティリティトランスポートエラー

エラーが見つからなかった場合、このサブコマンドは指定の設定の内容を表示します。

例

- 1 `racadm getconfig -g cfgLanNetworking`
cfgLanNetworking グループに含まれている設定プロパティ（オブジェクト）をすべて表示します。
- 1 `racadm getconfig -f myrac.cfg`
RAC のグループ設定オブジェクトすべてを **myrac.cfg** に保存します。
- 1 `racadm getconfig -h`
DRAC 5 で使用可能な設定グループのリストを表示します。
- 1 `racadm getconfig -u root`
ルートというユーザーの設定プロパティを表示します。
- 1 `racadm getconfig -g cfgUserAdmin -i 2 -v`
インデックス 2 のユーザーグループインスタンスと、プロパティ値の詳細情報を表示します。

概要

```
racadm getconfig -f <ファイル名>
racadm getconfig -g <グループ名> [-i <インデックス>]
racadm getconfig -u <ユーザー名>
racadm getconfig -h
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

coredump

 **メモ:** このコマンドを使用するには、**デバッグコマンドの実行**権限が必要です。

[表 A-7](#) で **coredump** サブコマンドについて説明します。

表 A-7. **coredump**

サブコマンド	定義
coredump	前回の DRAC 5 コアダンプを表示します。

概要

```
racadm coredump
```

説明

coredump サブコマンドは、RAC で最近発生した重要な問題に関する詳細情報を表示します。 **coredump** 情報は、こうした重要な問題の診断に使用できます。

coredump 情報がある場合は、RAC パワーサイクル中持続し、次のどちらかの状態が発生するまで使用できます。

- 1 `coredumpdelete` サブコマンドによって `coredump` 情報がクリアされる。
- 1 RAC で別の重大な状況が発生する。この場合、`coredump` 情報は最後に発生した重大エラーに関連するものです。

`coredump` のクリアについては、`coredumpdelete` サブコマンドを参照してください。

対応インターフェース

- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

coredumpdelete

 **メモ:** このコマンドを使用するには、**ログのクリア**権限または**デバッグコマンドの実行**権限が必要です。

[表 A-8](#) で `coredumpdelete` サブコマンドについて説明します。

表 A-8. `coredumpdelete`

サブコマンド	定義
<code>coredumpdelete</code>	DRAC 5 に保存されているコアダンプを削除します。

概要

racadm coredumpdelete

説明

`coredumpdelete` サブコマンドは、RAC に保存されている既存の `coredump` データをクリアするために使用できます。

 **メモ:** `coredump` が現在 RAC に保存されていない場合に `coredumpdelete` コマンドを発行すると、コマンド成功のメッセージが表示されます。これは想定内の動作です。

`coredump` 表示の詳細については、`coredump` サブコマンドを参照してください。

対応インターフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

fwupdate

 **メモ:** このコマンドを使用するには、**DRAC 5 の設定**権限が必要です。

 **メモ:** ファームウェアアップデートを始める前に、「[DRAC 5 ファームウェアのアップデート](#)」で手順の詳細を参照してください。

[表 A-9](#) で `fwupdate` サブコマンドについて説明します。

表 A-9. `fwupdate`

サブコマンド	定義
<code>fwupdate</code>	DRAC 5 のファームウェアをアップデートします。

概要

```
racadm fwupdate -s  
racadm fwupdate -g -u -a <TFTP_サーバー_IP_アドレス> -d <パス>  
racadm fwupdate -p -u -d <パス>
```

説明

fwupdate サブコマンドを使用すると、DRAC 5 のファームウェアをアップデートできます。ユーザーは次のような操作ができます。

- 1 ファームウェアアップデートプロセスのステータスを確認する
- 1 IP アドレスとオプションでパスを入力して TFTP サーバーから DRAC 5 のファームウェアをアップデートする
- 1 ローカル RACADM を使用してローカルファイルシステムから DRAC 5 のファームウェアをアップデートする

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

入力

表 A-10 で **fwupdate** サブコマンドのオプションについて説明します。

 **メモ:** **-p** オプションはローカル RACADM でのみサポートされ、serial/telnet/ssh コンソールではサポートされていません。

表 A-10. fwupdate サブコマンドオプション

オプション	説明
-u	アップデート オプションは、ファームウェアアップデートファイルのチェックサムを実行し、実際のアップデート処理を開始します。このオプションは、 -g または -p オプションと一緒に使用できます。アップデートの最後に DRAC 5 はソフトリセットを実行します。
-s	ステータス オプションは、アップデート処理の現在の状態を返します。このオプションは常に単独で使用されます。
-g	get オプションは、TFTP サーバーからファームウェアのアップデートファイルを取得するようにファームウェアに指示します。このほか -a オプションと -d オプションも指定する必要があります。 -a オプションがないと、 cfgRhostsFwUpdateIpAddr プロパティと cfgRhostsFwUpdatePath プロパティを使用して、グループ cfgRemoteHosts に含まれているプロパティからデフォルトが読み取られます。
-a	IP アドレス オプションは TFTP サーバの IP アドレスを指定します。
-d	-d (ディレクトリ) オプションは、ファームウェアアップデートファイルのある TFTP サーバーまたは DRAC 5 のホストサーバー上のディレクトリを指定します。
-p	-p (put) オプションは、管理下システムのファームウェアファイルを DRAC 5 にアップデートするために使用します。 -u オプションは -p オプションと一緒に使用する必要があります。

出力

実行されている操作を示すメッセージを表示します。

例

```
1 racadm fwupdate -g -u -a 143.166.154.143 -d <パス>
```

この例では、**-g** オプションを使用して、特定の IP アドレス (**-a** オプションで指定) の TFTP サーバー上にある場所 (**-d** オプションで指定) からファームウェアのアップデートファイルをダウンロードするようにファームウェアに指示します。TFTP サーバーからイメージファイルがダウンロードされた後、アップデートプロセスが開始します。完了すると、DRAC 5 がリセットされます。

ダウンロードに 15 分以上かかりタイムアウトしてしまう場合は、ファームウェアのフラッシュイメージをサーバーのローカルドライブに転送してください。そして、コンソールリダイレクトを使用して、リモートシステムに接続して、ローカル **racadm** を使用してファームウェアをローカルにインストールします。

```
1 racadm fwupdate -s
```

このオプションはファームウェアアップデートの現在の状態を読み取ります。

```
1 racadm fwupdate -p -u -d c:¥ <イメージ>
```

この例では、アップデートするファームウェアイメージがホストのファイルシステムによって提供されます。

```
1 racadm -r 192.168.0.120 -u root -p racpassword fwupdate -g -u -a 192.168.0.120 -d <イメージ>
```

この例では、提供された DRAC ユーザー名とパスワードを使って、指定した DRAC のファームウェアをリモートでアップデートするために RACADM を使用します。イメージは TFTP サーバから取り込まれます。

 **メモ:** fwupdate サブコマンドの -p オプションは、リモート RACADM インタフェースではサポートされていません。

getssninfo

 **メモ:** このコマンドを使用するには、DRAC 5 へのログイン権限が必要です。

表 A-11 で getssninfo サブコマンドについて説明します。

表 A-11. getssninfo サブコマンド

サブコマンド	定義
getssninfo	Session Manager のセッション表から 1 つまたは複数の現在アクティブなセッションか、保留のセッション情報を取得します。

概要

```
racadm getssninfo [-A] [-u <ユーザー名> | *]
```

説明

getssninfo コマンドは、DRAC に接続しているユーザーのリストを返します。サマリ情報では次の情報が提供されます。

- 1 ユーザー名
- 1 IP アドレス（該当する場合）
- 1 セッションの種類（例：シリアル、telnet）
- 1 使用中のコンソール（例：仮想メディア、仮想 KVM）

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

入力

表 A-12 で getssninfo サブコマンドのオプションについて説明します。

表 A-12. getssninfo サブコマンドのオプション

オプション	説明
-A	-A オプションはデータヘッダの表示を削除します。
-u	-u <ユーザー名> ユーザー名オプションは、指定したユーザー名の詳細セッション記録に出力を限定します。ユーザー名に「*」を付けると、すべてのユーザーが一覧になります。このオプションを指定すると、サマリ情報は表示されません。

例

```
1 racadm getssninfo
```

表 A-13 に `racadm getssninfo` コマンドからの出力例を示します。

表 A-13. `getssninfo` サブコマンド出力例

ユーザー	IP アドレス	種類	コンソール
root	192.168.0.10	Telnet	Virtual KVM

```
1 racadm getssninfo -A
"root" 143.166.174.19 "Telnet" "NONE"
1 racadm getssninfo -A -u *
"root" "143.166.174.19" "Telnet" "NONE"
"bob" "143.166.174.19" "GUI" "NONE"
```

getsysinfo

 **メモ:** このコマンドを使用するには、DRAC 5 へのログイン権限が必要です。

表 A-14 で `racadm getsysinfo` サブコマンドについて説明します。

表 A-14. `getsysinfo`

コマンド	定義
<code>getsysinfo</code>	DRAC 5 情報、システム情報、ウォッチドッグ状態情報を表示します。

概要

```
racadm getsysinfo [-d] [-s] [-w] [-A]
```

説明

`getsysinfo` サブコマンドは、RAC、管理下システム、およびウォッチドッグの設定に関連する情報を表示します。

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

入力

表 A-15 で `getsysinfo` サブコマンドのオプションについて説明します。

表 A-15. `getsysinfo` サブコマンドオプション

オプション	説明
<code>-d</code>	DRAC 5 に関する情報を表示します。
<code>-s</code>	システム情報を表示します。
<code>-w</code>	ウォッチドッグ情報を表示します。
<code>-A</code>	ヘッダ / ラベルの印刷を削除します。

-w オプションが指定されていない場合は、その他のオプションがデフォルトとして使われます。

出力

`getsysinfo` サブコマンドは、RAC、管理下システム、およびウォッチドッグの設定に関連する情報を表示します。

出力例

```
RAC Information:
RAC Date/Time      = Thu Dec 8 20:01:33 2005
Firmware Version   = 1.0
Firmware Build     = 05.12.08
Last Firmware Update = Thu Dec 8 08:09:36 2005

Hardware Version   = A00
Current IP Address = 192.168.0.120
Current IP Gateway = 192.168.0.1
Current IP Netmask = 255.255.255.0
DHCP Enabled       = 0
MAC Address        = 00:14:22:18:cd:f9
Current DNS Server 1 = 0.0.0.0
Current DNS Server 2 = 0.0.0.0
DNS Servers from DHCP = 0
Register DNS RAC Name = 0
DNS RAC Name       = rac-48192
Current DNS Domain =

System Information:
System Model       = PowerEdge 2900
System BIOS Version = 0.2.3
BMC Firmware Version = 0.17
Service Tag       = 48192
Host Name         = racdev103
OS Name           = Microsoft Windows Server 2003
Power Status      = OFF

Watchdog Information:
Recovery Action    = None
Present countdown value = 0 seconds
Initial countdown value = 0 seconds
```

例

```
| racadm getsysinfo -A -s

"System Information:" "PowerEdge 2900" "A08" "1.0" "EF23VQ-0023" "Hostname"

"Microsoft Windows 2000 version 5.0, Build Number 2195, Service Pack 2" "ON"

| racadm getsysinfo -w -s

System Information:
System Model       = PowerEdge 2900
System BIOS Version = 0.2.3
BMC Firmware Version = 0.17
Service Tag       = 48192
Host Name         = racdev103
OS Name           = Microsoft Windows Server 2003
Power Status      = OFF

Watchdog Information:
Recovery Action    = None
Present countdown value = 0 seconds
Initial countdown value = 0 seconds
```

制限

`getsysinfo` の出力のホスト名フィールドと OS 名フィールドには、管理下システムに Dell OpenManage がインストールされている場合にのみ正確な情報が表示されます。管理下システムに OpenManage がインストールされていない場合は、これらのフィールドは空白か不正確になります。

getractive

 **メモ:** このコマンドを使用するには、**DRAC 5 へのログイン** 権限が必要です。

表 A-16 で `getractime` サブコマンドについて説明します。

表 A-16. `getractime`

サブコマンド	定義
<code>getractime</code>	Remote Access Controller の現在の時刻を表示します。

概要

```
racadm getractime [-d]
```

説明

オプションをつけない場合、`getractime` サブコマンドは、時間を通常の可読可能なフォーマットで表示します。

`-d` オプションをつけた場合、`getractime` は、時間を `yyyymmddhhmmss.mmmmmms` のフォーマットで表示します。これは、UNIX の `date` コマンドで得られる結果と同じフォーマットです。

出力

`getractime` サブコマンドでは、1つのライン上に出力を表示します。

出力例

```
racadm getractime
Thu Dec 8 20:15:26 2005

racadm getractime -d
20051208201542.000000
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

ifconfig

 **メモ:** このコマンドを使用するには、**診断コマンドの実行権限**または**DRAC 5 の設定権限**が必要です。

表 A-17 で `ifconfig` サブコマンドについて説明します。

表 A-17. `fconfig`

サブコマンド	定義
<code>ifconfig</code>	ネットワークインタフェーステーブルの内容を表示します。

概要

```
racadm ifconfig
```

netstat

 **メモ:** このコマンドを使用するには、**診断コマンドの実行権限**が必要です。

表 A-18 で netstat サブコマンドについて説明します。

表 A-18. netstat

サブコマンド	定義
netstat	経路指定表と現在の接続を表示します。

概要

```
racadm netstat
```

対応インタフェース

- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

ping

 **メモ:** このコマンドを使用するには、**診断コマンドの実行権限**または**DRAC 5 の設定権限**が必要です。

表 A-19 で ping サブコマンドについて説明します。

表 A-19. ping

サブコマンド	定義
ping	宛先 IP アドレスが、現在のルーティングテーブルの内容が含まれた DRAC 5 から到達可能であることを確認します。宛先 IP アドレスが必要です。ICMP エコーパケットは、現在のルーティングテーブル内容を元にして、宛先 IP アドレスに送信されます。

概要

```
racadm ping <IP アドレス>
```

対応インタフェース

- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

setniccfg

 **メモ:** setniccfg コマンドを使用するには、**DRAC 5 の設定権限**が必要です。

表 A-20 で setniccfg サブコマンドについて説明します。

表 A-20. setniccfg

サブコマンド	定義
setniccfg	コントローラの IP 環境設定を行います。

 **メモ:** NIC と Ethernet 管理ポートは同じ意味で使われる場合があります。

概要

```
racadm setniccfg -d  
racadm setniccfg -s [<IP アドレス> <ネットマスク> <ゲートウェイ>]  
racadm setniccfg -o [<IP アドレス> <ネットマスク> <ゲートウェイ>]
```

説明

setniccfg サブコマンドは、コントローラの IPアドレスを設定します。

- 1 **-d** オプションは Ethernet 管理ポートの DHCP を有効にします。(デフォルトは DHCP 有効)
- 1 **-s** オプションは静的 IP 設定を有効にします。 IPアドレス、ネットマスク、およびゲートウェイを指定できます。 指定しなければ、既存の静的設定が使用されます。 <IP アドレス>、<ネットマスク>、および<ゲートウェイ>は、ドットで区切られた文字列で入力します。

```
racadm setniccfg -s 192.168.0.120 255.255.255.0 192.168.0.1
```

- 1 **-o** オプションは Ethernet 管理ポートを完全に無効にします。 <IP アドレス>、<ネットマスク>、および<ゲートウェイ>は、ドットで区切られた文字列で入力します。

```
racadm setniccfg -o 192.168.0.120 255.255.255.0 192.168.0.1
```

出力

setniccfg サブコマンドは、処理に失敗した場合に該当するエラーメッセージを表示します。 成功した場合は、メッセージが表示されます。

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

getniccfg

 **メモ:** **getniccfg** コマンドを使用するには、**DRAC 5 へのログイン**権限が必要です。

[表 A-21](#) で **setniccfg** および**getniccfg** サブコマンドについて説明します。

表 A-21. setniccfg/getniccfg

サブコマンド	定義
getniccfg	コントローラの現在の IP 環境設定を表示します。

概要

```
racadm getniccfg
```

説明

getniccfg サブコマンドは、現在の Ethernet 管理ポートの設定を表示します。

出力例

getniccfg サブコマンドは、処理に失敗した場合に該当するエラーメッセージを表示します。 成功した場合は、出力が次の形式で表示されます。

```
NIC Enabled      = 1
```

```
DHCP Enabled    = 1
IP Address      = 192.168.0.1
Subnet Mask     = 255.255.255.0
Gateway        = 192.168.0.1
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

getsvctag

 **メモ:** このコマンドを使用するには、**DRAC 5 へのログイン**権限が必要です。

表 A-22 で `getsvctag` サブコマンドについて説明します。

表 A-22. `getsvctag`

サブコマンド	定義
<code>getsvctag</code>	サービスタグを表示します。

概要

```
racadm getsvctag
```

説明

`getsvctag` サブコマンドは、ホストシステムのサービスタグを表示します。

例

コマンドプロンプトで `getsvctag` とタイプします。出力が以下のように表示されます。

```
Y76TP0G
```

どちらのコマンドも成功すると 0 を、エラーの場合はゼロ以外を返します。

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

racdump

 **メモ:** このコマンドを使用するには、**デバッグ**権限が必要です。

表 A-23 で `racdump` サブコマンドについて説明します。

表 A-23. `racdump`

サブコマンド	定義
racdump	状態と一般の DRAC 5 情報を表示します。

概要

```
racadm racdump
```

説明

racdump サブコマンドは、ダンプ、状態および一般 DRAC 5 基板情報を取得する単一のコマンドを提供します。

以下の情報は、**racdump** サブコマンドが処理されるときに表示されます。

- 1 システム /RAC に関する一般情報
- 1 Coredump
- 1 セッション情報
- 1 プロセス情報
- 1 ファームウェアのビルド情報

対応インタフェース

- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

racreset

 **メモ:** このコマンドを使用するには、**DRAC 5 の設定権限**が必要です。

[表 A-24](#) で **racreset** サブコマンドについて説明します。

表 A-24. **racreset**

サブコマンド	定義
racreset	DRAC 5 をリセットします。

 **注意:** **racreset** サブコマンドを発行すると、DRAC が使用可能な状態に戻るまでに 1 分ほどかかる可能性があります。

概要

```
racadm racreset [hard | soft]
```

説明

racreset サブコマンドは DRAC 5 にリセットを発行します。リセットイベントは DRAC 5 ログに書き込まれます。

ハードリセットは RAC に強度のリセットを実行します。したがって、RAC を回復するための最後の手段としてのみ使用してください。

 **注意:** DRAC 5 のハードリセットを実行した後、[表 A-25](#) の説明に従ってシステムを再起動する必要があります。

[表 A-25](#) で **racreset** サブコマンドのオプションについて説明します。

表 A-25. **racreset** サブコマンドオプション

オプション	説明

オプション	説明
hard	ハードリセットはリモートのアクセスコントローラに強度のリセットを実行します。したがって、RAC コントローラを回復するための最後の手段としてのみ使用してください。
soft	ソフトリセットは RAC の正常な再起動を実行します。

例

```
1 racadm racreset
```

DRAC 5 のソフトリセットの手順を開始します。

```
1 racadm racreset hard
```

DRAC 5 のハードリセットの手順を開始します。

対応インターフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

racresetcfg

 **メモ:** このコマンドを使用するには、**DRAC 5 の設定**権限が必要です。

[表 A-26](#) で **racresetcfg** サブコマンドについて説明します。

表 A-26. racresetcfg

サブコマンド	定義
racresetcfg	RAC の設定全体を出荷時のデフォルト値にリセットします。

概要

```
racadm racresetcfg
```

対応インターフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

説明

racresetcfg コマンドはユーザーが設定したデータベースプロパティのエントリをすべて削除します。 データベースには、カードを元のデフォルト設定に戻すデフォルトのプロパティがすべてのエントリにあります。 データベースプロパティのリセット後、DRAC 5 は自動的にリセットされます。

 **注意:** このコマンドは現在の RAC の設定を削除し、RAC とシリアル設定を元のデフォルト設定に戻します。 リセット後のデフォルトの名前とパスワードは、それぞれ **root** と **calvin** で、IP アドレスは 192.168.0.120 です。 ネットワーククライアント（例：対応ウェブブラウザ、telnet/ssh、リモート RACADM）から **racresetcfg** を発行する場合は、デフォルトの IP アドレスを使用する必要があります。

 **メモ:** このサブコマンドも、シリアルインターフェースをデフォルトのボーレート（57600）と COM ポートにリセットします。 シリアルポートを介して RAC にアクセスするには、サーバーの BIOS 設定画面からシリアルのオプションを再設定する必要があります。

serveraction

 **メモ:** このコマンドを使用するには、**サーバー制御コマンドの実行**権限が必要です。

表 A-27 で `serveraction` サブコマンドについて説明します。

表 A-27. `serveraction`

サブコマンド	定義
<code>serveraction</code>	管理下システムのリセットまたはパワーオン / オフ / サイクルを実行します。

概要

```
racadm serveraction <action>
```

説明

`serveraction` サブコマンドを使用すると、ホストシステムに電力の管理操作を実行できます。表 A-28 で `serveraction` 電源制御のオプションについて説明します。

表 A-28. `serveraction` サブコマンドオプション

文字列	定義
<処置> >	処置を指定します。 <処置> の文字列のオプションを次に示します。 <ul style="list-style-type: none">1 <code>powerdown</code> — 管理下システムの電源を切ります。1 <code>powerup</code> — 管理下システムの電源を入れます。1 <code>powercycle</code> — 管理下システムのパワーサイクル処理を発行します。 この処理は、システムの前面パネルにある電源ボタンを押して電源を切ってから電源を入れ直す操作に似ています。1 <code>powerstatus</code> — サーバーの現在の電源状態 ("オン"か "オフ") を表示します。1 <code>hardreset</code> — 管理下システムのリセット (再起動) を実行します。

出力

`serveraction` サブコマンドは、要求した処理を実行できなかった場合はエラーメッセージ、処理が正常に完了した場合は成功メッセージを表示します。

対応インターフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

getraclog

 **メモ:** このコマンドを使用するには、DRAC 5 への **ログイン** 権限が必要です。

表 A-29 に `racadm getraclog` コマンドについて説明します。

表 A-29. `getraclog`

コマンド	定義
<code>getraclog -i</code>	DRAC 5 ログ内のエントリ数を表示します。
<code>getraclog</code>	DRAC 5 ログエントリを表示します。

概要

```
racadm getraclog -i
```

```
racadm getraclog [-A] [-o] [-c カウント] [-s 記録開始] [-m]
```

説明

`getraclog -i` コマンドは、DRAC 5 ログ内のエントリ数を表示します。

以下は、エントリを読み込むための `getraclog` コマンドのオプションです。

- 1 `-A` — ヘッダーやラベルなしで出力を表示します。
- 1 `-c` — リターンされるエントリの最大数を提供します。
- 1 `-m` — 一度に 1 画面で情報を表示して、ユーザーに続行のプロンプトを表示します（UNIX の `more` コマンドに類似）。
- 1 `-o` — 出力を 1 行で表示します。
- 1 `-s` — 表示に使用する開始レコードを指定します。

 **メモ:** オプションを指定しなければ、全部のログが表示されます。

出力

デフォルトの出力表示では、レコード番号、タイムスタンプ、ソース、説明が表示されます。タイムスタンプは、1 月 1 日の午前零時に開始し、システム起動時まで増加します。システム起動後、システムのタイムスタンプが使用されます。

出力例

```
Record:      1
Date/Time:   Dec 8 08:10:11
Source:      login[433]
Description: root login from 143.166.157.103
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

clrraclog

 **メモ:** このコマンドを使用するには、**ログのクリア** 権限が必要です。

概要

```
racadm clrraclog
```

説明

`clrraclog` サブコマンドは、RAC のログから既存のレコードをすべて削除します。新しいレコードが 1 つ作成され、ログがクリアされたときの日時が記録されます。

getsel

 **メモ:** このコマンドを使用するには、**DRAC 5 へのログイン** 権限が必要です。

表 A-30 で `getsel` コマンドについて説明します。

表 A-30. `getsel`

--	--

コマンド	定義
<code>getsel -i</code>	システムイベントログ内のエントリ数を表示します。
<code>getsel</code>	SEL エントリを表示します。

概要

```
racadm getsel -i
```

```
racadm getsel [-E] [-R] [-A] [-o] [-c count] [-s count] [-m]
```

説明

`getsel -i` コマンドは、SEL 内のエントリ数を表示します。

以下の `getsel` オプション (`-i` オプションを除く) はエントリを読み込むために使用されます。

- A — 表示ヘッダーやラベルなしの出力を指定します。
- c — リターンされるエントリの最大数を提供します。
- o — 出力を 1 行で表示します。
- s — 表示に使用する開始レコードを指定します。
- E — 16 バイトの SEL の生データを、16 進数の値のシーケンスとして各行の終わりに付加します。
- R — 生データのみが表示されます。
- m — 一度に 1 画面でを表示して、ユーザーに続行のプロンプトを表示します (UNIX の `more` コマンドに類似)。

 **メモ:** 引数を指定しなければ、全部のログが表示されます。

出力

デフォルトの出力表示では、レコード番号、タイムスタンプ、重大度、説明が表示されます。

例:

```
Record:      1
Date/Time:   11/16/2005 22:40:43
Severity:    2
Description: System Board SEL: event log sensor for System Board, log cleared was asserted
```

対応インタフェース

- ローカル RACADM
- リモート RACADM
- telnet/ssh/serial RACADM

clrsel

 **メモ:** このコマンドを使用するには、**ログのクリア** 権限が必要です。

概要

```
racadm clrsel
```

説明

`clrsel` コマンドは、システムイベントログ (SEL) から既存のレコードをすべて削除します。

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

gettracelog

 **メモ:** このコマンドを使用するには、DRAC 5 へのログイン権限が必要です。

表 A-31 で `gettracelog` サブコマンドについて説明します。

表 A-31. `gettracelog`

コマンド	定義
<code>gettracelog -i</code>	DRAC 5 トレースログ内のエントリ数を表示します。
<code>gettracelog</code>	DRAC 5 ログを表示します。

概要

```
racadm gettracelog -i
```

```
racadm gettracelog [-A] [-o] [-c count] [-s startrecord] [-m]
```

説明

`gettracelog` (-i オプションなしの) コマンドを使ってエントリを読み取ります。以下の `gettracelog` エントリはエントリの読み取りに使用されます。

- i — DRAC 5 トレースログ内のエントリ数を表示します。
- m — 一度に 1 画面でを表示して、ユーザーに続行のプロンプトを表示します (UNIX の `more` コマンドに類似)。
- o — 出力を 1 行で表示します。
- c — 表示するレコード数を指定します。
- s — 表示する開始レコードを指定します。
- A — ヘッダーやラベルを表示しません。

出力

デフォルトの出力表示では、レコード番号、タイムスタンプ、ソース、説明が表示されます。タイムスタンプは、午前零時に開始し、システム起動時まで増加します。システム起動後、システムのタイムスタンプが使用されます。

例:

```
Record: 1
```

```
Date/Time: Dec 8 08:21:30
```

```
Source: ssnmgrd[175]
```

```
Description: root from 143.166.157.103: session timeout sid 0be0aef4
```

対応インタフェース

- 1 ローカル RACADM
 - 1 リモート RACADM
 - 1 telnet/ssh/serial RACADM
-

sslcsrcgen

 **メモ:** このコマンドを使用するには、DRAC 5 の設定権限が必要です。

表 A-32 で `sslcsrcgen` サブコマンドについて説明します。

表 A-32. `sslcsrcgen`

サブコマンド	説明
<code>sslcsrcgen</code>	SSL 証明書署名要求 (CSR) を生成して RAC からダウンロードします。

概要

```
racadm sslcsrcgen [-g] [-f <ファイル名>]
```

```
racadm sslcsrcgen -s
```

説明

`sslcsrcgen` サブコマンドは、CSR を生成してローカルファイルシステムにファイルをダウンロードするために使用できます。CSR は、RAC の SSL トランザクションに使用されるカスタム SSL 証明書を作成するために使用できます。

オプション

 **メモ:** `-f` オプションは serial/telnet/ssh コンソールではサポートされていません。

表 A-33 で `sslcsrcgen` サブコマンドのオプションについて説明します。

表 A-33. `sslcsrcgen` サブコマンドオプション

オプション	説明
<code>-g</code>	新しい CSR を生成します。
<code>-s</code>	CSR 生成処理の状態を返します (生成中、アクティブ、なし)。
<code>-f</code>	<ファイル名> の場所を指定します。ここに CSR がダウンロードされます。

 **メモ:** `-f` オプションを指定しないと、ファイル名はデフォルトで現在のディレクトリ内の `sslcsr` になります。

オプションを指定しなければ、CSR が生成され、デフォルトでローカルファイルシステムに `sslcsr` としてダウンロードされます。`-g` オプション は `-s` オプションと一緒に使用できず、`-f` オプションは `-g` オプションとのみ使用できます。

`sslcsrcgen -s` サブコマンドは、次のステータスコードの 1 つを返します。

- 1 CSR が正常に生成されました。
- 1 CSR は存在しません。
- 1 CSR の生成が進行中です。

制限

`sslcsrcgen` サブコマンドは、ローカルまたはリモートの RACADM クライアントからのみ実行が可能で、シリアル、telnet、SSH インタフェースでは使用できません。

 **メモ:** CSR を生成するには、まず RACADM の `cfgRacSecurity` グループで CSR フィールドを設定する必要があります。例: `racadm config -g cfgRacSecurity -o cfgRacSecCsrCommonName MyCompany`

例

```
racadm sslcsrcgen -s
```

または

```
racadm sslcsrgen -g -f c:\Ycsr\Ycsrtest.txt
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

sslcertupload

 **メモ:** このコマンドを使用するには、**DRAC 5 の設定権限**が必要です。

[表 A-34](#) で `sslcertupload` サブコマンドについて説明します。

表 A-34. `sslcertupload`

サブコマンド	説明
<code>sslcertupload</code>	カスタム SSL サーバー証明書または CA 証明書をクライアントから RAC にアップロードします。

概要

```
racadm sslcertupload -t <タイプ> [-f <ファイル名>]
```

オプション

[表 A-35](#) で `sslcertupload` サブコマンドのオプションについて説明します。

表 A-35. `sslcertupload` サブコマンドオプション

オプション	説明
<code>-t</code>	CA 証明書かサーバー証明書か、アップロードする証明書のタイプを指定します。 1 = サーバー証明書 2 = CA 証明書
<code>-f</code>	アップロードする証明書のファイル名を指定します。 ファイルを指定しないと、現在のディレクトリ内の <code>sslcert</code> ファイルが選択されます。

`sslcertupload` コマンドは成功すると 0 を返し、成功しないと非ゼロの数字を返します。

制限

`sslcertupload` サブコマンドは、ローカルまたはリモートの RACADM クライアントからのみ実行できます。 `sslcsrgen` サブコマンドはシリアル、telnet、SSH インタフェースでは使用できません。

例

```
racadm sslcertupload -t 1 -f c:\Ycert\Ycert.txt
```

対応インタフェース

- 1 ローカル RACADM
 - 1 リモート RACADM
-

sslcertdownload

 **メモ:** このコマンドを使用するには、DRAC 5 の設定権限が必要です。

表 A-36 で `sslcertdownload` サブコマンドについて説明します。

表 A-36. `sslcertdownload`

サブコマンド	説明
<code>sslcertupload</code>	SSL 証明書を RAC からクライアントのファイルシステムにダウンロードします。

概要

```
racadm sslcertdownload -t <タイプ> [-f <ファイル名>]
```

オプション

表 A-37 で `sslcertdownload` サブコマンドのオプションについて説明します。

表 A-37. `sslcertdownload` サブコマンドオプション

オプション	説明
<code>-t</code>	Microsoft® Active Directory® 証明書かサーバー証明書か、ダウンロードする証明書の種類を指定します。 1 = サーバー証明書 2 = Microsoft Active Directory 証明書
<code>-f</code>	アップロードする証明書のファイル名を指定します。 <code>-i</code> オプションまたはファイル名を指定しないと、現在のディレクトリ内の <code>sslcert</code> ファイルが選択されます。

`sslcertdownload` コマンドは成功すると 0 を返し、成功しないと非ゼロの数字を返します。

制限

`sslcertdownload` サブコマンドは、ローカルまたはリモートの RACADM クライアントからのみ実行できます。 `sslcsrcgen` サブコマンドはシリアル、telnet、SSH インタフェースでは使用できません。

例

```
racadm sslcertdownload -t 1 -f c:\%cert%\cert.txt
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM

sslcertview

 **メモ:** このコマンドを使用するには、DRAC 5 の設定権限が必要です。

表 A-38 で `sslcertview` サブコマンドについて説明します。

表 A-38. `sslcertview`

|--|--|

サブコマンド	説明
sslcrtview	RAC に存在する SSL サーバー証明書または CA 証明書を表示します。

概要

```
racadm sslcrtview -t <タイプ> [-A]
```

オプション

[表 A-39](#) で `sslcrtview` サブコマンドのオプションについて説明します。

表 A-39. sslcrtview サブコマンドオプション

オプション	説明
-t	Microsoft Active Directory 証明書かサーバー証明書か、表示する証明書の種類を指定します。 1 = サーバー証明書 2 = Microsoft Active Directory 証明書
-A	ヘッダ / ラベル表示を防止します。

出力例

```
racadm sslcrtview -t 1

Serial Number          : 00

Subject Information:
Country Code (CC)     : US
State (S)              : Texas
Locality (L)          : Round Rock
Organization (O)      : Dell Inc.
Organizational Unit (OU) : Remote Access Group
Common Name (CN)      : DRAC5 default certificate

Issuer Information:
Country Code (CC)     : US
State (S)              : Texas
Locality (L)          : Round Rock
Organization (O)      : Dell Inc.
Organizational Unit (OU) : Remote Access Group
Common Name (CN)      : DRAC5 default certificate

Valid From             : Jul 8 16:21:56 2005 GMT
Valid To               : Jul 7 16:21:56 2010 GMT
```

```
racadm sslcrtview -t 1 A

00
US
Texas
Round Rock
Round Rock
Dell Inc.
Remote Access Group
DRAC5 default certificate
US
Texas
Round Rock
Round Rock
Dell Inc.
Remote Access Group
DRAC5 default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

testemail

表 A-40 で testemail サブコマンドについて説明します。

表 A-40. testemail の設定

サブコマンド	説明
testemail	RAC の電子メール警告機能をテストします。

概要

```
racadm testemail -i <インデックス>
```

説明

RAC から指定の宛先へテスト電子メールを送信します。

testemail コマンドを実行する前に、RACADM [cfgEmailAlert](#) グループ内の指定したインデックスが有効になり、正しく設定されていることを確認します。表 [表 A-41](#) に [cfgEmailAlert](#) グループのリストと関連コマンドを示します。

表 A-41. testemail の設定

処置	コマンド
警告を有効にする	racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
宛先の電子メールアドレスを指定する	racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 user1@mycompany.com
宛先の電子メールアドレスに送信するカスタムメッセージを設定する	racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "This is a test!"
SNMP IP アドレスが正しく設定されていることを確認する	racadm config -g cfgRemoteHosts -o cfgRhostsSmptServerIpAddr -i 192.168.0.152
現在の電子メール警告設定を表示する	racadm getconfig -g cfgEmailAlert -i <インデックス> <インデックス> は 1~4 の数字

オプション

表 A-42 で testemail サブコマンドのオプションについて説明します。

表 A-42. testemail サブコマンド

オプション	説明
-i	テストする電子メール警告のインデックスを指定します。

出力

なし。

対応インタフェース

- 1 ローカル RACADM
 - 1 リモート RACADM
 - 1 telnet/ssh/serial RACADM
-

testtrap

 **メモ:** このコマンドを使用するには、**テスト警告** 権限が必要です。

表 A-43 で testtrap サブコマンドについて説明します。

表 A-43. testtrap

サブコマンド	説明
testtrap	RAC の SNMP トラップ警告機能をテストします。

概要

```
racadm testtrap -i <インデックス>
```

説明

testtrap サブコマンドは、RAC からネットワーク上の指定した宛先トラップリスナにテストトラップを送信して、RAC の SNMP トラップ警告機能をテストします。

testtrap サブコマンドを実行する前に、RACADM [cfglpmiPet](#) グループ内の指定したインデックスが正しく設定されていることを確認してください。

表 [A-41](#) に [cfglpmiPet](#) グループのリストと関連コマンドを示します。

表 A-44. cfgEmailAlert コマンド

処置	コマンド
警告を有効にする	racadm config -g cfglpmiPet -o cfglpmiPetAlertEnable -i 1 1
宛先の電子メール IP アドレスを設定する	racadm config -g cfglpmiPet -o cfglpmiPetAlertDestIpAddr -i 1 192.168.0.110
現在のテストトラップ設定を表示する	racadm getconfig -g cfglpmiPet -i <インデックス> <インデックス> は 1~4 の数字

入力

表 A-45 で testtrap サブコマンドのオプションについて説明します。

表 A-45. testtrap サブコマンドオプション

オプション	説明
-i	テストに使用するトラップ設定のインデックスを指定します。有効な値は 1~4 です。

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

vmdisconnect

 **メモ:** このコマンドを使用するには、**仮想メディアへのアクセス**権限が必要です。

表 A-46 で vmdisconnect サブコマンドについて説明します。

表 A-46. vmdisconnect

サブコマンド	説明
vmdisconnect	開いている RAC 仮想メディア接続すべてをリモートクライアントから終了します。

概要

racadm vmdisconnect

説明

vmdisconnect サブコマンドを使用すると、ユーザーは別のユーザーの仮想メディアセッションを強制的に切断できます。一度切断すると、ウェブベースインタフェースに正しい接続状態が反映されます。これはローカルまたはリモートの racadm からのみ使用できます。

vmdisconnect サブコマンドを使用すると、RAC ユーザーはアクティブな仮想メディアセッションをすべて切断できます。アクティブな仮想メディアセッションは RAC のウェブベースインタフェースか racadm [getsysinfo](#) サブコマンドを使用して表示できます。

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

vmkey

 **メモ:** このコマンドを使用するには、**仮想メディアへのアクセス**権限が必要です。

[表 A-47](#) で **vmkey** サブコマンドについて説明します。

表 A-47. vmkey

サブコマンド	説明
vmkey	仮想メディアキー関連の処理を実行します。

概要

racadm vmkey <処置>

<処置> を reset として設定した場合は、仮想フラッシュメモリがデフォルトサイズの 16 MB にリセットされます。

説明

カスタム仮想メディアキーのイメージが RAC にアップロードされると、キーサイズがイメージサイズになります。vmkey サブコマンドは、キーをその最初のデフォルトサイズ（DRAC 5 の場合は 16 MB）にリセットするために使用します。

対応インタフェース

- 1 ローカル RACADM
- 1 リモート RACADM
- 1 telnet/ssh/serial RACADM

[目次ページに戻る](#)

[目次ページに戻る](#)

DRAC 5 プロパティのデータベースグループとオブジェクトの定義

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

- [表示可能な文字](#)
- [idRacInfo](#)
- [cfgLanNetworking](#)
- [cfgRemoteHosts](#)
- [cfgUserAdmin](#)
- [cfgEmailAlert](#)
- [cfgSessionManagement](#)
- [cfgSerial](#)
- [cfgNetTuning](#)
- [cfgOobSnmpp](#)
- [cfgRacTuning](#)
- [ifcRacManagedNodeOs](#)
- [cfgRacSecurity](#)
- [cfgRacVirtual](#)
- [cfgActiveDirectory](#)
- [cfgIpmiSerial](#)
- [cfgIpmiSol](#)
- [cfgIpmiLan](#)
- [cfgIpmiPef](#)
- [cfgIpmiPet](#)

DRAC 5 プロパティデータベースには DRAC 5 の設定情報が含まれています。データは関連オブジェクト別に整理され、オブジェクトはオブジェクトグループ別に整理されます。この項では、プロパティデータベースがサポートしているグループとオブジェクトの ID をリストにします。

racadm ユーティリティでグループとオブジェクト ID を使って DRAC 5 を設定します。次項では各オブジェクトについて説明し、オブジェクトが読み取り可能、書き込み可能、またはその両方が可能であることを示します。

文字列の値は、特に記載のない限り、表示可能な ASCII 文字のみとします。

表示可能な文字

表示可能な文字には以下のセットがあります。

abcdefghijklmnopqrstuvwxyz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

0123456789~`!@#\$%^&*()_+={}|~:~;'<>, .?/

idRacInfo

このグループには問い合わせられる DRAC 5 の特定の情報を提供するための表示パラメータがあります。

このグループでは 1 つのインスタンスが使用可能です。次の副項ではこのグループのオブジェクトについて説明します。

idRacProductInfo (読み取り専用)

正当値

最大 63 バイトの ASCII 文字列。

デフォルト

"Dell Remote Access Controller 5"

説明

テキスト文字列を使って製品を識別します。

idRacDescriptionInfo（読み取り専用）

正当値

最大 255 バイトの ASCII 文字列。

デフォルト

"このシステムコンポーネントは Dell PowerEdge サーバーのリモート管理機能一式を提供しています。"

説明

RAC の種類を説明するテキスト。

idRacVersionInfo（読み取り専用）

正当値

最大 63 バイトの ASCII 文字列。

デフォルト

"1.0"

説明

現在の製品ファームウェアバージョンを含む文字列。

idRacBuildInfo（読み取り専用）

正当値

最大 16 バイトの ASCII 文字列。

デフォルト

現在の RAC ファームウェアビルドバージョン。 例: "05.12.06"

説明

現在の製品ビルドバージョンを含む文字列。

idRacName（読み取り専用）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

最大 15 バイトの ASCII 文字列。

デフォルト

DRAC 5

説明

このコントローラを識別するためにユーザーが割り当てた名前。

idRacType（読み取り専用）

デフォルト

6

説明

Remote Access Controller タイプを DRAC 5 と識別します。

cfgLanNetworking

このグループには DRAC 5 NIC を設定するためのパラメータが含まれています。

このグループでは 1 つのインスタンスが使用可能です。このグループのすべてのオブジェクトで DRAC 5 NIC がリセットされる必要があり、このため接続が一時的に途絶える場合があります。DRAC 5 NIC IP アドレス設定を変更するオブジェクトによって、すべてのアクティブなユーザーセッションが閉じられ、ユーザーはアップデートされた IP アドレス設定を使って再接続する必要があります。

cfgDNSDomainNameFromDHCP（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

RAC DNS ドメイン名をネットワークの DHCP サーバーから割り当てる必要があることを指定します。

cfgDNSDomainName（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

最大 254 バイトの ASCII 文字列。少なくとも 1 文字が英字でなければなりません。文字は英数字、「-」と「.」に制限されています。

 **メモ:** Microsoft® Active Directory® は 64 バイト以内の完全修飾ドメイン名 (FQDN) のみをサポートしています。

デフォルト

""

説明

DNS ドメイン名。このパラメータは、`cfgDNSDomainNameFromDHCP` が 0 (FALSE) に設定されている場合にのみ有効です。

cfgDNSRacName (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

最大 63 バイトの ASCII 文字列。英字を少なくとも 1 文字含める必要があります。

 **メモ:** 31 文字以内の名前しか登録できない DNS サーバーもあります。

デフォルト

RAC - サービスタグ

説明

RAC 名、つまり RAC - サービスタグ (デフォルト) を表示します。このパラメータは `cfgDNSRegisterRac` が 1 (TRUE) に設定されている場合にのみ有効です。

cfgDNSRegisterRac (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

DNS サーバー上の DRAC 5 名を登録します。

cfgDNSServersFromDHCP (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

DNS サーバーの IP アドレスをネットワーク上の DHCP サーバーから割り当てる必要があることを指定します。

cfgDNSServer1 (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

有効な IP アドレスを表す文字列。 例: "192.168.0.20"

説明

DNS サーバー 1 の IP アドレスを指定します。 このプロパティは、**cfgDNSServersFromDHCP** が 0 (FALSE) に設定されている場合にのみ有効です。

 **メモ:** **cfgDNSServer1** と **cfgDNSServer2** は、アドレスの置き換え時に同じ値に設定することもできます。

cfgDNSServer2 (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

有効な IP アドレスを表す文字列。 例: "192.168.0.20"

デフォルト

0.0.0.0

説明

DNS サーバー 2 で使用する IP アドレスを検索します。 このパラメータは **cfgDNSServersFromDHCP** が、0 (FALSE) に設定されている場合のみ有効です。

 **メモ:** **cfgDNSServer1** と **cfgDNSServer2** は、アドレスの置き換え時に同じ値に設定することもできます。

cfgNicEnable (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC ネットワークインタフェースコントローラを有効または無効にします。 NIC を無効にすると、RAC へのリモートネットワークインタフェースにアクセスできず、シリアルインタフェースかローカル RACADM インタフェースでしか RAC を使用できなくなります。

cfgNicIpAddress（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。 このパラメータは **cfgNicUseDhcp** パラメータが 0（FALSE）に設定されている場合にのみ設定可能です。

正当値

有効な IP アドレスを表す文字列。 例: "192.168.0.20"

デフォルト

192.168.0.120

説明

RAC に割り当てる静的 IP アドレスを指定します。 このプロパティは、**cfgNicUseDhcp** が 0（FALSE）に設定されている場合にのみ有効です。

cfgNicNetmask（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。 このパラメータは **cfgNicUseDhcp** パラメータが 0（FALSE）に設定されている場合にのみ設定可能です。

正当値

有効なサブネットマスクを表す文字列。 例: "255.255.255.0"

デフォルト

255.255.255.0

説明

RAC の IP アドレスの静的割り当てに使用されるサブネットマスク。 このプロパティは、**cfgNicUseDhcp** が 0（FALSE）に設定されている場合にのみ有効です。

cfgNicGateway（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。 このパラメータは **cfgNicUseDhcp** パラメータが 0（FALSE）に設定されている場合にのみ設定可能です。

正当値

ゲートウェイの有効な IP アドレスを表す文字列。 例: "192.168.0.1"

デフォルト

192.168.0.1

説明

RAC の IP アドレスの静的割り当てに使用されるゲートウェイの IP アドレス。 このプロパティは、**cfgNicUseDhcp** が 0（FALSE）に設定されている場合にのみ有効です。

cfgNicUseDhcp（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC の IP アドレスの割り当てに DHCP を使用するかどうかを指定します。このプロパティを 1 (TRUE) に設定すると、RAC の IP アドレス、サブネットマスク、ゲートウェイがネットワーク上の DHCP サーバーから割り当てられます。このプロパティを 0 (FALSE) に設定すると、静的 IP アドレス、サブネットマスク、ゲートウェイが `cfgNicIpAddress`、`cfgNicNetmask`、および `cfgNicGateway` プロパティから割り当てられます。

 **メモ:** システムをリモートでアップデートする場合は、[setniccfg](#) コマンドを使用してください。

cfgNicSelection（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

0 (共有)

1 (フェールオーバー装備の共有)

2 (専用)

デフォルト

2

説明

RAC ネットワークインタフェースコントローラ (NIC) の現在の処理モードを指定します。[表 B-1](#) で、サポートしているモードについて説明します。

表 B-1. cfgNicSelection サポートしているモード

モード	説明
共有	ホストサーバー内蔵 NIC がホストサーバーの RAC と共有される場合に使用します。このモードを使用すると、ホストサーバーと RAC で同じ IP アドレスを使用して、ネットワーク上の共通アクセスが可能になります。
フェールオーバー装備の共有	ホストサーバーのオンボード NIC 間のチーム機能を可能にします。
専用	リモートアクセス用に RAC NIC を専用 NIC として使用するよう指定します。

cfgNicMacAddress（読み取り専用）

正当値

RAC NIC の MAC アドレスを表す文字列。

デフォルト

現在の RAC NIC の MAC アドレス。 例: "00:12:67:52:51:A3"

説明

RAC NIC の MAC アドレス。

cfgNicVlanEnable (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC/BMC の VLAN 機能を有効または無効にします。

cfgNicVlanId (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

0 ~ 4094

デフォルト

0

説明

ネットワーク VLAN 設定の VLAN ID を指定します。 このプロパティは、cfgNicVlanEnable が 1 (有効) に設定されている場合にのみ有効です。

cfgNicVlanPriority (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

0 ~ 7

デフォルト

0

説明

ネットワーク VLAN 設定の VLAN 優先順位を指定します。このプロパティは、cfgNicVlanEnable が 1（有効）に設定されている場合にのみ有効です。

cfgRemoteHosts

このグループは、電子メール警告用 SMTP サーバー、ファームウェアアップグレード用 TFTP サーバーの IP アドレスなど、各種リモートコンポーネントの設定に必要なプロパティを提供します。

cfgRhostsSmtpServerIpAddr（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

有効な SMTP サーバーの有効な IP アドレスを表す文字列。例: "192.168.0.55"

デフォルト

0.0.0.0

説明

ネットワーク SMTP サーバーの IP アドレス。警告が設定されて有効になっている場合は、SMTP サーバーが RAC から電子メール警告を送信します。

cfgRhostsFwUpdateTftpEnable（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

ネットワーク TFTP サーバーからの RAC ファームウェアアップデートを有効または無効にします。

cfgRhostsFwUpdateIpAddr（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

TFTP サーバーの有効な IP アドレスを表す文字列。例: "192.168.0.61"

デフォルト

0.0.0.0

説明

TFTP RAC ファームウェアのアップデート処理に使用されるネットワーク TFTP サーバーの IP アドレスを指定します。

cfgRhostsFwUpdatePath（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

文字列。 最大長 = 255。

デフォルト

""

説明

TFTP サーバーに RAC ファームウェアのイメージファイルが存在する場所を示す TFTP パスを指定します。 TFTP パスは TFTP サーバーの TFTP ルートのパスに相当します。

 **メモ:** 場合によっては、サーバーでドライブを指定する必要があります（たとえば C）。

cfgUserAdmin

このグループは、使用可能なリモートインタフェースから RAC へのアクセスが許可されているユーザーに関する設定情報を提供します。

ユーザーグループの最大 16 のインスタンスが許可されています。 各インスタンスが個々のユーザーの設定を表します。

cfgUserAdminIpmiLanPrivilege（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**ユーザーの設定** 権限が必要です。

正当値

2（ユーザー）

3（オペレーター）

4（システム管理者）

15（アクセスなし）

デフォルト

4（ユーザー 2）

15（その他すべて）

説明

IPMI LAN チャネル上の最大特権。

cfgUserAdminIpmiLanPrivilege（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**ユーザーの設定** 権限が必要です。

正当値

- 2（ユーザー）
- 3（オペレータ）
- 4（システム管理者）
- 15（アクセスなし）

デフォルト

- 4（ユーザー 2）
- 15（その他すべて）

説明

IPMI シリアルチャネル上の最大特権。

cfgUserAdminPrivilege（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**ユーザーの設定** 権限が必要です。

正当値

0x00000000 ~ 0x00001fff、および 0x0

デフォルト

0x00000000

説明

このプロパティは、ユーザーに許可される役割ベースの権限を指定します。値は、特権の値を自由に組み合わせることのできるビットマスクとして表します。[表 B-2](#) に、許可されているユーザー特権のビットマスクを示します。

表 B-2. ユーザー特権に応じたビットマスク

ユーザー特権	特権ビットマスク
DRAC 5 にログイン	0x00000001
DRAC 5 の設定	0x00000002
ユーザーの設定	0x00000004
ログのクリア	0x00000008
サーバーコントロールコマンドの実行	0x00000010
コンソールリダイレクトへのアクセス	0x00000020
仮想メディアへのアクセス	0x00000040
警告のテスト	0x00000080
デバッグコマンドの実行	0x00000100

例

表 B-3 に、1 つまたは複数の特権を持つユーザーの特権ビットマスクの例を示します。

表 B-3. ユーザー特権のビットマスクの例

ユーザー特権	特権ビットマスク
ユーザーは RAC にアクセスできません。	0x00000000
ユーザーは RAC にアクセスして RAC とサーバーの設定情報を見ることができます。	0x00000001
ユーザーは RAC にログインして設定を変更できます。	0x00000001 + 0x00000002 = 0x00000003
ユーザーは RAC にログインして、仮想メディアとコンソールリダイレクトにアクセスできます。	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**ユーザーの設定** 権限が必要です。

正当値

文字列。 最大長 = 16。

デフォルト

""

説明

このインデックスに対するユーザーの名前。 インデックスに何も入っていない場合、文字列をこの名前のフィールドに書き込むことでユーザーインデックスが作成されます。 二重引用符 ("") の文字列を書き込むと、そのインデックスでユーザーが削除されます。 この名前は変更できません。 名前を削除して再度作成する必要があります。 文字列に " / " (フォワードスラッシュ)、" \ " (バックスラッシュ)、" . " (ピリオド)、" @ " (アット記号)、引用符を含めることはできません。

 **メモ:** このプロパティの値は他のユーザーインスタンスと重複してはなりません。

cfgUserAdminPassword (書き込み専用)

 **メモ:** このプロパティを変更するには、**ユーザーの設定** 権限が必要です。

正当値

最大 20 バイトの ASCII 文字列。

デフォルト

""

説明

このユーザーに対するパスワード。 このユーザーパスワードは暗号化され、プロパティに書き込んだ後は参照や表示ができなくなります。

cfgUserAdminEnable

 **メモ:** このプロパティを変更するには、**ユーザーの設定** 権限が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

個々のユーザーを有効または無効にします。

cfgUserAdminSolEnable

 **メモ:** このプロパティを変更するには、**ユーザーの設定**権限が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

シリアルオーバー (SOL) のユーザーアクセスを有効または無効にします。

cfgEmailAlert

このグループには、RAC の電子メール警告機能を設定するパラメータが含まれています。

次の副項ではこのグループのオブジェクトについて説明します。 このグループの最大 4 のインスタンスが許可されています。

cfgEmailAlertIndex (読み取り専用)

正当値

1~4

デフォルト

このパラメータは既存のインスタンスを基に自動入力されます。

説明

警告インスタンスの固有のインデックス。

cfgEmailAlertEnable (読み取り / 書き込み)

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

電子メール警告の送信先電子メールアドレスを指定します。 例: user1@company.com

cfgEmailAlertAddress (読み取り専用)

正当値

最大 64 の長さの ASCII 文字を使用した電子メールアドレス形式。

デフォルト

""

説明

警告ソースの電子メールアドレス。

cfgEmailAlertCustomMsg (読み取り専用)

正当値

文字列。 最大長 = 32。

デフォルト

""

説明

警告と一緒に送信されるカスタムメッセージを指定します。

cfgSessionManagement

このグループには、DRAC 5 に接続できるセッション数を設定するパラメータが含まれます。

このグループでは 1 つのインスタンスが使用可能です。 次の副項ではこのグループのオブジェクトについて説明します。

cfgSsnMgtConsRedirMaxSessions (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

1 ~ 2

デフォルト

2

説明

RAC で許可されるコンソールリダイレクトセッションの最大数を指定します。

cfgSsnMgtRacadmTimeout（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

10 ~ 1920

デフォルト

30

説明

リモート RACADM インタフェースのアイドルタイムアウトを秒で定義します。リモート RACADM セッションのアイドル時間がこの値を超えると、セッションが終了します。

cfgSsnMgtWebserverTimeout（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

60 ~ 1920

デフォルト

300

説明

Web サーバーのタイムアウトを定義します。このプロパティは、接続がアイドル状態を維持できる時間を秒で設定します（ユーザー入力はありません）。このプロパティで設定した時間に達すると、セッションはキャンセルされます。この設定を変更しても現行のセッションには影響はありません（新しい設定を有効にするには、ログアウトしてからログインし直す必要があります）。

時間切れになった Web サーバーセッションは現在のセッションからログアウトします。

cfgSsnMgtSshIdleTimeout（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

0（タイムアウトなし）

60 ~ 1920

デフォルト

説明

Secure Shell のアイドルタイムアウトを定義します。このプロパティは、接続がアイドル状態を維持できる時間を秒で設定します（ユーザー入力はありません）。このプロパティで設定した時間に達すると、セッションはキャンセルされます。この設定を変更しても現行のセッションには影響はありません（新しい設定を有効にするには、ログアウトしてからログインし直す必要があります）。

時間切れになったセキュアシェルセッションでは、<Enter> を入力した後で次のエラーメッセージが表示されます。

```
Warning: Session no longer valid, may have timed out
```

（警告：セッションが無効になりました。タイムアウトの可能性あります。）

メッセージが表示された後、セキュアシェルセッションを生成したシェルに戻ります。

cfgSsnMgtTelnetTimeout（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

0（タイムアウトなし）

60 ~ 1920

デフォルト

0

説明

Telnet のアイドルタイムアウトを定義します。このプロパティは、接続がアイドル状態を維持できる時間を秒で設定します（ユーザー入力はありません）。このプロパティで設定した時間に達すると、セッションはキャンセルされます。この設定を変更しても現行のセッションには影響はありません（新しい設定を有効にするには、ログアウトしてからログインし直す必要があります）。

時間切れになった Telnet セッションでは、<Enter> を入力した後で次のエラーメッセージが表示されます。

```
Warning: Session no longer valid, may have timed out
```

（警告：セッションが無効になりました。タイムアウトの可能性あります。）

メッセージが表示された後、Telnet セッションを生成したシェルに戻ります。

cfgSerial

このグループには、DRAC 5 の設定パラメーターが含まれています。

このグループでは 1 つのインスタンスが使用可能です。次の副項ではこのグループのオブジェクトについて説明します。

cfgSerialBaudRate（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

9600, 28800, 57600, 115200

デフォルト

57600

説明

DRAC 5 シリアルポートのボーレートを設定します。

cfgSerialConsoleEnable (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC シリアルコンソールインタフェースを有効または無効にします。

cfgSerialConsoleQuitKey (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

STRING

MaxLen = 4

デフォルト

^¥ (<Ctrl><¥>)

 **メモ:** 「^」は <Ctrl> キーです。

説明

このキーまたはキーの組合せは、**connect com2** コマンドの使用時にテキストコンソールリダイレクトを終了します。 **cfgSerialConsoleQuitKey** の値は次のいずれかで表します。

1 10 進数値 — 例: "95"

1 16 進数値 — 例: "0x12"

1 8 進数値 — 例: "007"

1 ASCII 値 — 例: "a"

ASCII 値は、次の Esc キーコードを使用して表示される場合があります。

(a) ^ の後にアルファベットが続く (a-z, A-Z)

(b) ^ の後にリストに記載されている特殊文字: []¥^_が続く

cfgSerialConsoleIdleTimeout (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

0 = タイムアウトなし

60 ~ 1920

デフォルト

300

説明

アイドル状態のシリアルセッションが切断されるまでの最大秒数。

cfgSerialConsoleNoAuth（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

0（シリアルログイン認証を有効にする）

1（シリアルログイン認証を無効にする）

デフォルト

0

説明

RAC シリアルコンソールのログイン認証を有効または無効にします。

cfgSerialConsoleCommand（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

説明

ユーザーがシリアルコンソールインタフェースにログインした後で実行されるシリアルコマンドを指定します。

デフォルト

""

例

"connect com2"

cfgSerialHistorySize（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

0 ~ 8192

デフォルト

8192

説明

シリアル履歴バッファの最大サイズを指定します。

cfgSerialSshEnable (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

DRAC 5 のセキュアシェル (SSH) インタフェースを有効または無効にします。

cfgSerialTelnetEnable (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC の telnet コンソールインタフェースを有効または無効にします。

cfgSerialCom2RedirEnable (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

デフォルト

1

正当値

1 (TRUE)

0 (FALSE)

説明

コンソールの COM 2 ポートリダイレクトを有効または無効にします。

cfgNetTuning

このグループは、ユーザーに RAC NIC のネットワークインタフェースパラメータの詳細設定を許可します。これを設定すると、設定のアップデートが有効になるまで 1 分ほどかかる場合があります。

 **注意:** このグループのプロパティを変更するときは注意が必要です。このグループのプロパティを誤って変更すると、RAC NIC が動作不能になる可能性があります。

cfgNetTuningNicAutoneg (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

1 (有効)

0 (無効)

デフォルト

1

説明

物理リンク速度と二重通信モードのオートネゴシエーションを有効にします。有効である場合は、オートネゴシエーション値が **cfgNetTuningNic100MB** および **cfgNetTuningNicFullDuplex** オブジェクトで設定した値を優先します。

cfgNetTuningNic100MB (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

0 (10 MBit)

1 (100 MBit)

デフォルト

1

説明

RAC NIC を使用する速度を指定します。このプロパティは、**cfgNetTuningNicAutoNeg** を 1 (有効) に設定している場合は使用されません。

cfgNetTuningNicFullDuplex (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

0 (半二重)

1 (全二重)

デフォルト

1

説明

RAC NIC の二重設定を指定します。このプロパティは、**cfgNetTuningNicAutoNeg** を 1 (有効) に設定している場合は使用されません。

cfgNetTuningNicMtu (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

576 ~ 1500

デフォルト

1500

説明

DRAC 5 ネットワークアダプタで使用する最大転送ユニットのバイトサイズ。

cfgNetTuningTcpSrttDflt (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

6 ~ 384

デフォルト

6

説明

1/2 秒単位で示した TCP 再伝送往復時間の平滑往復タイムアウトベースデフォルト値。(値は16 進で入力します。)

cfgOobSnmp

グループは、DRAC 5 の SNMP エージェントとトラップ機能を設定するパラメータを持っています。

このグループでは 1 つのインスタンスが使用可能です。次の副項ではこのグループのオブジェクトについて説明します。

cfgOobSnmpAgentCommunity（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

文字列。最大長 = 31。

デフォルト

パブリック

説明

SNMPトラップに使用される SNMP コミュニティ名を指定します。

cfgOobSnmpAgentEnable（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC の SNMP エージェントを有効または無効にします。

cfgRacTuning

このグループは、有効なポートやセキュリティポート制限など、RAC のさまざまなプロパティを設定するために使用します。

cfgRacTuneHttpPort（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

10 ~ 65535

デフォルト

80

説明

RAC との HTTP ネットワーク通信に使用するポート番号を指定します。

cfgRacTuneHttpsPort（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

10 ~ 65535

デフォルト

443

説明

RAC との HTTPS ネットワーク通信に使用するポート番号を指定します。

cfgRacTuneIpRangeEnable

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC の IP アドレス範囲の検証機能を有効または無効にします。

cfgRacTuneIpRangeAddr

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

フォーマットされた文字列、IP アドレス。 例: "192.168.0.44"

デフォルト

192.168.1.1

説明

範囲マスクプロパティの 1 で決定される IP アドレスビットパターンの可能な位置を指定します (cfgRacTuneIpRangeMask)。

cfgRacTuneIpRangeMask

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

左寄せビットを使用した標準的な IP マスク値

デフォルト

255.255.255.0

説明

フォーマットされた文字列、IP アドレス。 例: "255.255.255.0"

cfgRacTunIpBlkEnable

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC の IP アドレスブロック機能を有効または無効にします。

cfgRacTunIpBlkFailcount

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

2 ~ 16

デフォルト

5

説明

この IP アドレスからのログイン試行が拒否される前に、時間枠内で発生するログイン失敗の最大回数。

cfgRacTunIpBlkFailWindow

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

2 ~ 65535

デフォルト

60

説明

ログイン失敗を数える時間枠を秒で定義します。 ログイン試行がこの制限時間に達すると、失敗はカウントからドロップされます。

cfgRacTuneIpBlkPenaltyTime

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

2 ~ 65535

デフォルト

300

説明

失敗が制限を越えた IP アドレスからのセッション要求を拒否する時間枠を秒で定義します。

cfgRacTuneSshPort (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

1 ~ 65535

デフォルト

22

説明

RAC の SSH インタフェースに使用するポート番号を指定します。

cfgRacTuneTelnetPort (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

1 ~ 65535

デフォルト

23

説明

RAC の telnet インタフェースに使用するポート番号を指定します。

cfgRacTuneRemoteRacadmEnable (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

1

説明

RAC のリモート RACADM インタフェースを有効または無効にします。

cfgRacTuneConRedirEncryptEnable (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

コンソールリダイレクトのセッションでビデオを暗号化します。

cfgRacTuneConRedirPort (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

1 ~ 65535

デフォルト

5901

説明

RAC のコンソールリダイレクト活動中、キーボードとマウスのトラフィックに使用するポートを指定します。

 **メモ:** このオブジェクトは、アクティブになる前に DRAC 5 をリセットする必要があります。

cfgRacTuneConRedirVideoPort (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

1 ~ 65535

デフォルト

5901

説明

RAC のコンソールリダイレクト活動中、ビデオのトラフィックに使用するポートを指定します。

 **メモ:** このオブジェクトは、アクティブになる前に DRAC 5 をリセットする必要があります。

cfgRacTuneAsrEnable (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

0 (FALSE)

1 (TRUE)

デフォルト

1

説明

RAC のクラッシュ画面キャプチャ機能を有効または無効にします。

 **メモ:** このオブジェクトは、アクティブになる前に DRAC 5 をリセットする必要があります。

cfgRacTuneDaylightOffset (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

0 ~ 60

デフォルト

0

説明

RAC の時間に使用する夏時間のオフセットを分単位で指定します。

cfgRacTuneTimezoneOffset（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

-720 ~ 780

デフォルト

0

説明

RAC の時間に使用するタイムゾーンのオフセットを GMT/UTC から分単位で指定します。アメリカ合衆国のタイムゾーンで一般に使用されるタイムゾーンオフセットを以下に示します。

-480（PST — 太平洋標準時）

-420（MST — 山岳部標準時）

-360（CST — 中央標準時）

-300（EST — 東部標準時）

cfgRacTuneWebserverEnable（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

0（FALSE）

1（TRUE）

デフォルト

1

説明

RAC の Web サーバーを有効または無効にします。このプロパティを無効にすると、クライアントの Web ブラウザやリモート RACADM を使用して RAC にアクセスできなくなります。このプロパティは telnet/ssh/ シリアルまたはローカル RACADM インタフェースには影響を与えません。

ifcRacManagedNodeOs

このグループには、Managed Server オペレーティングシステムについて説明するプロパティが含まれています。

このグループでは 1 つのインスタンスが使用可能です。次の副項ではこのグループのオブジェクトについて説明します。

ifcRacMnOsHostname（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

文字列。 最大長 = 255。

デフォルト

""

説明

管理システムのホスト名。

ifcRacMnOsOsName（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

文字列。 最大長 = 255。

デフォルト

""

説明

管理システムのオペレーティングシステム名。

cfgRacSecurity

このグループは、RAC SSL 証明書署名要求（CSR）機能に関連するオプションを設定するために使用されます。このグループのプロパティは、RAC から CSR を生成する前に設定する必要があります。

証明書署名要求の詳細については、RACADM [sslcsrqlen](#) サブコマンドを参照してください。

cfgSecCsrCommonName（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

文字列。 最大長 = 254。

デフォルト

""

説明

CSR 共通名（CN）を指定します。

cfgSecCsrOrganizationName（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

文字列。 最大長 = 254。

デフォルト

""

説明

CSR 組織名 (O) を指定します。

cfgSecCsrOrganizationUnit (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

文字列。 最大長 = 254。

デフォルト

""

説明

CSR 部門名 (OU) を指定します。

cfgSecCsrLocalityName (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

文字列。 最大長 = 254。

デフォルト

""

説明

CSR 地域 (L) を指定します。

cfgSecCsrStateName (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

文字列。 最大長 = 254。

デフォルト

""

説明

CSR 州名 (S) を指定します。

cfgSecCsrCountryCode (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

文字列。 最大長 = 2。

デフォルト

""

説明

CSR 国番号 (CC) を指定します。

cfgSecCsrEmailAddr (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

文字列。 最大長 = 254。

デフォルト

""

説明

CSR の電子メールアドレスを指定します。

cfgSecCsrKeySize (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

512

1024

2048

デフォルト

説明

CSR の非対称キーサイズを指定します。

cfgRacVirtual

このグループには DRAC 5 仮想メディア機能を設定するためのパラメータが含まれています。このグループでは 1 つのインスタンスが使用可能です。次の副項ではこのグループのオブジェクトについて説明します。

cfgVirMediaAttached（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

このオブジェクトは、USB バスを介して仮想デバイスをシステムに接続するために使用されます。デバイスを接続すると、サーバーはシステムに接続している有効な USB 大量ストレージデバイスを認識するようになります。これは、ローカルの USB CDROM/フロッピードライブをシステムの USB ポートに接続する場合と同じです。デバイスが接続されると、DRAC5 の ウェブベースインタフェースまたは CLI を使用して仮想デバイスにリモートで接続できるようになります。このオブジェクトを 0 に設定すると、デバイスが USB バスから切断されます。

 **メモ:** 変更をすべて有効にするには、システムを再起動する必要があります。

cfgVirAtapiSrvPort（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**仮想メディアへのアクセス**権限が必要です。

正当値

1 ~ 65535

デフォルト

3669

説明

暗号化された仮想メディアと RAC との接続に使用されるポート番号を指定します。

cfgVirAtapiSrvPortSsl（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

0 ~ 65535 までの 10 進数で未使用のポート番号。

デフォルト

3669

説明

SSL 仮想メディアの接続に使用されるポートを設定します。

cfgVirMediaKeyEnable (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC の仮想メディアキー機能を有効または無効にします。

cfgVirMediaBootOnce (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

1 (有効)

0 (無効)

デフォルト

0

説明

RAC の仮想メディアの起動 1 度機能を有効または無効にします。 ホストサーバーの再起動時にこのプロパティが有効であれば、デバイスに適切なメディアが取り付けられている場合に、仮想メディアデバイスから再起動が試行されます。

cfgActiveDirectory

このグループには DRAC 5 Active Directory 機能を設定するためのパラメータが含まれています。

cfgADracDomain (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

余白のない印刷可能なテキスト文字列。 最大長は 254 文字です。

デフォルト

""

説明

DRAC が存在する Active Directory ドメイン。

cfgADRacName (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

余白のない印刷可能なテキスト文字列。 最大長は 254 文字です。

デフォルト

""

説明

Active Directory フォレストに記録された DRAC 名。

cfgADEnable (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

1 (TRUE)

0 (FALSE)

デフォルト

0

説明

RAC で Active Directory によるユーザー認証を有効または無効にします。 このプロパティを無効にすると、ユーザーログインにローカルの RAC 認証が使用されます。

cfgADAuthTimeout (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

デフォルト

120

説明

Active Directory 認証要求の完了がタイムアウトになるまでの時間を秒で指定します。

cfgADRootDomain（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

余白のない印刷可能なテキスト文字列。 最大長は 254 文字です。

デフォルト

""

説明

ドメインフォレストのルートドメイン。

cfgIpmiSerial

このグループは、BMC の IPMI シリアルインタフェースの設定に使用されるプロパティを指定します。

cfgIpmiSerialConnectionMode（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

0（ターミナル）

1（基本）

デフォルト

1

説明

DRAC 5 `cfgSerialConsoleEnable` プロパティを 0（無効）に設定すると、DRAC 5 のシリアルポートが IPMI のシリアルポートになります。 このプロパティによって、IPMI 定義のシリアルポートのモードが決まります。

基本モードの場合、ポートはシリアルクライアントのアプリケーションプログラムと通信するためにバイナリデータを使用します。 ターミナルモードでは、ポートは非プログラム式 ASCII 端末が接続していると想定し、ごく単純なコマンドの入力を許可します。

cfgIpmiSerialBaudRate（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

9600、19200、57600、115200

デフォルト

57600

説明

IPMI を介したシリアル接続のボーレートを指定します。

cfgIpmiSerialChanPrivLimit (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

- 2 (ユーザー)
- 3 (オペレータ)
- 4 (システム管理者)

デフォルト

4

説明

IPMI シリアルチャンネルで許可される最大特権レベルを指定します。

cfgIpmiSerialFlowControl (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

- 0 (なし)
- 1 (CTS/RTS)
- 2 (XON/XOFF)

デフォルト

1

説明

IPMI シリアルポートのフロー制御の設定を指定します。

cfgIpmiSerialHandshakeControl (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

0 (FALSE)

1 (TRUE)

デフォルト

1

説明

IPMI ターミナルモードのハンドシェイク制御を有効または無効にします。

cfgIpmiSerialLineEdit (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

0 (FALSE)

1 (TRUE)

デフォルト

1

説明

IPMI シリアルインタフェースのライン編集を有効または無効にします。

cfgIpmiSerialEchoControl (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

0 (FALSE)

1 (TRUE)

デフォルト

1

説明

IPMI シリアルインタフェースのエコー制御を有効または無効にします。

cfgIpmiSerialDeleteControl (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

0 (FALSE)

1 (TRUE)

デフォルト

0

説明

IPMI シリアルインタフェースの削除制御を有効または無効にします。

cfgIpmiSerialNewLineSequence (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

0 (なし)

1 (CR-LF)

2 (NULL)

3 (<CR>)

4 (<CR>)

5 (<CR>)

デフォルト

1

説明

IPMI シリアルインタフェースのニューラインシーケンスの仕様を指定します。

cfgIpmiSerialInputNewLineSequence (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

0 (<ENTERCR>)

1 (NULL)

デフォルト

1

説明

IPMI シリアルインタフェースの入力ニューラインシーケンスの仕様を指定します。

cfgIpmiSol

このグループは、システムのシリアルオーバー LAN 機能の設定に使用されます。

cfgIpmiSolEnable (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

0 (FALSE)

1 (TRUE)

デフォルト

1

説明

シリアルオーバー (SOL) を有効または無効にします。

cfgIpmiSolBaudRate (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

9600、19200、57600、115200

デフォルト

57600

説明

シリアルオーバー LAN 通信のボーレート。

cfgIpmiSolMinPrivilege (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

2 (ユーザー)

3 (オペレータ)

4 (システム管理者)

デフォルト

説明

シリアルオーバー LAN アクセスに必要な最小限の特権レベルを指定します。

cfgIpmiSolAccumulateInterval（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

1 ~ 255

デフォルト

10

説明

SOL 文字データパケットの一部を送信する前に通常 BMC が待機する時間を指定します。この値は 1 を基準に 5 ms 間隔で増分されます。

cfgIpmiSolSendThreshold（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

1 ~ 255

デフォルト

255

説明

SOL しきい値の限界値。

cfgIpmiLan

このグループは、システムの IPMIオーバー LAN 機能の設定に使用されます。

cfgIpmiLanEnable（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

0 (FALSE)

1 (TRUE)

デフォルト

1

説明

IPMI オーバー LAN を有効または無効にします。

cfgIpmiLanPrivLimit (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

- 2 (ユーザー)
- 3 (オペレータ)
- 4 (システム管理者)

デフォルト

0

説明

IPMI オーバー LAN アクセスに要許可される最小限の特権レベルを指定します。

cfgIpmiLanAlertEnable (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、DRAC 5 の設定権限が必要です。

正当値

- 0 (FALSE)
- 1 (TRUE)

デフォルト

1

説明

グローバル電子メール警告を有効または無効にします。 このプロパティは個々の電子メール警告の有効 / 無効プロパティすべてに優先されます。

cfgIpmiEncryptionKey (読み取り / 書き込み)

 **メモ:** このプロパティを表示または変更するには、DRAC 5 の設定権限とシステム管理者特権が必要です。

正当値

スペースのない 0～20 文字の16 進数文字列。

デフォルト

"00000000000000000000"

説明

IPMI 暗号化キー。

cfgIpmiPetCommunityName (読み取り / 書き込み)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

最大 18 文字の文字列。

デフォルト

"public"

説明

トラップの SNMP コミュニティ名。

cfgIpmiPef

このグループは、管理下サーバーで使用可能なプラットフォームの設定に使用されます。

イベントフィルタは、管理下システムで重大なイベントが発生したときにトリガされる処置に関するポリシーを制御するために使用できます。

cfgIpmiPefName (読み取り専用)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

文字列。 最大長 = 255。

デフォルト

インデックスフィルタの名前。

説明

プラットフォームイベントフィルタの名前を指定します。

cfgIpmiPefIndex (読み取り専用)

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定**権限が必要です。

正当値

1 ~ 17

デフォルト

プラットフォームイベントフィルタオブジェクトのインデックス値。

説明

特定のプラットフォームイベントフィルタのインデックスを指定します。

cfglpmiPefAction（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

- 0（なし）
- 1（電源を切る）
- 2（リセット）
- 3（パワーサイクル）

デフォルト

0

説明

警告がトリガされたときに管理下システムで実行される処置を指定します。

cfglpmiPefEnable（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

- 0（FALSE）
- 1（TRUE）

デフォルト

1

説明

特定のプラットフォームイベントフィルタを有効または無効にします。

cfglpmiPet

このグループは、管理下システムのプラットフォームイベントトラップの設定に使用されます。

cfglpmiPetIndex（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

1 ~ 4

デフォルト

適切なインデックス値。

説明

トラップに対応するインデックスの固有の識別子。

cfgIpmiPetAlertDestIpAddr（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

有効な IP アドレスを表す文字列。 例: 192.168.0.67

デフォルト

0.0.0.0

説明

ネットワーク上でトラップシーバの送信先 IP アドレスを指定します。 トラップシーバは、管理下システムでイベントがトリガされたときに SNMP トラップを受信します。

cfgIpmiPetAlertEnable（読み取り / 書き込み）

 **メモ:** このプロパティを変更するには、**DRAC 5 の設定権限**が必要です。

正当値

0 (FALSE)

1 (TRUE)

デフォルト

1

説明

特定のトラップを有効または無効にします。

[目次ページに戻る](#)

[目次ページに戻る](#)

サポートされている RACADM インタフェース

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

以下の表は、RACADM サブコマンドとそれに対応するインタフェースのサポートについて概要を提供しています。

表 C-1. RACADM サブコマンドのインタフェースサポート

サブコマンド	Telnet/SSH/シリアル	ローカル RACADM	リモート RACADM
arp	✓	✗	✓
clearascreen	✓	✓	✓
clrraclog	✓	✓	✓
clrsel	✓	✓	✓
coredump	✓	✗	✓
coredumpdelete	✓	✓	✓
fwupdate	✓	✓	✓
getconfig	✓	✓	✓
getniccfg	✓	✓	✓
getraclog	✓	✓	✓
getractime	✓	✓	✓
getsel	✓	✓	✓
getssninfo	✓	✓	✓
getsvctag	✓	✓	✓
getsysinfo	✓	✓	✓
gettracelog	✓	✓	✓
help	✓	✓	✓
ifconfig	✓	✗	✓
netstat	✓	✗	✓
ping	✓	✗	✓
racdump	✓	✗	✓
racreset	✓	✓	✓
racresetcfg	✓	✓	✓
serveraction	✓	✓	✓
setniccfg	✓	✓	✓
sslcertdownload	✗	✓	✓
sslcertupload	✗	✓	✓
sslcertview	✓	✓	✓
sslcsrgen	✗	✓	✓
testemail	✓	✓	✓
testtrap	✓	✓	✓
vmdisconnect	✓	✓	✓
vmkey	✓	✓	✓

✓ = サポートされている、✗ = サポートされていない

[目次ページに戻る](#)

[目次ページに戻る](#)

ブラウザのプレインストール

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

- [プラグインインストールパッケージの入手](#)
- [プラグインインストール](#)

Linux を利用し、管理ステーションが読み取り専用システムである場合、DRAC 5 に接続せずに、ブラウザをクライアントシステムにインストールすることができます。ネイティブプラグインインストールパッケージを使用して、クライアントの設定の段階でブラウザを手動でインストールすることができます。

- **注意:** 読み取り専用のクライアント環境で、DRAC 5 ファームウェアをプラグインの新しいバージョンにアップデートする場合、インストールされている VM プラグインは動作不能になります。これはファームウェアに新しいプラグインのバージョンが含まれている場合、以前のプラグイン機能は動作できなくなるからです。この場合、クライアントはプラグインのインストールを要求されます。ファイルシステムが読み取り専用なので、インストールは失敗し、プラグイン機能は使用不能となります。

プラグインインストールパッケージの入手

プラグインインストールパッケージを入手するには、以下の手順を実行します。

1. 既存の DRAC5 にログインします。

2. ブラウザのアドレスバーの URL を

```
https://<RAC_IP>/cgi-bin/webcgi/main
```

から:

```
https://<RAC_IP>/plugins/  
に変更します。# Be sure to include the trailing slash. (最後のスラッシュを忘れないようにしてください。)
```

3. vm と vkm の 2 つのサブディレクトリに注意してください。適切なサブディレクトリに進み、rac5XXX.xpi ファイルを右クリックして、**リンクターゲットに名前をつけて保存** を選択します。
4. プラグインインストールパッケージファイルを保存する場所を選択します。

プラグインのインストール

以下の手順で、プラグインインストールパッケージをインストールします。

1. インストールパッケージを、クライアントがアクセスできるクライアントのネイティブファイルシステム共有にコピーします。
2. クライアントシステム上のブラウザのインスタンスを開きます。
3. ブラウザのアドレスバーのプラグインインストールパッケージにファイルパスを入力します。例:

```
file:///tmp/rac5vm.xpi
```

4. ブラウザの指示に従ってプラグインインストールを行います。

一度インストールすると、DRAC5 ファームウェアにプラグインの新しいバージョンが含まれていない限り、ブラウザがプラグインのインストールを要求することはありません。

[目次ページに戻る](#)

[目次ページに戻る](#)

DRAC 5 概要

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

- [このリリースの DRAC 5 の新機能](#)
- [DRAC 5 ハードウェア機能](#)
- [ハードウェア仕様](#)
- [対応リモートアクセス接続](#)
- [DRAC 5 セキュリティ機能](#)
- [対応プラットフォーム](#)
- [対応オペレーティングシステム](#)
- [対応 Web ブラウザ](#)
- [機能](#)
- [その他の必要マニュアル](#)

Dell™ Remote Access Controller 5 (DRAC 5) はシステム管理ハードウェアおよびソフトウェアのソリューションで、Dell PowerEdge™ システムのリモート管理、クラッシュしたシステムの回復、電源制御などの機能を提供するように設計されています。

DRAC 5 をインストールすると、システムのベースボード管理コントローラ (BMC) と通信して、電圧、温度、インテリジョン、ファン速度などに関する警告やエラーを電子メールで通知するように設定できます。DRAC 5 はイベントデータと最新のクラッシュ画面 (Microsoft® Windows® オペレーティングシステムを実行中のシステムのみ) もログに記録するので、システムクラッシュの原因解明に役立ちます。

DRAC 5 は独自のマイクロプロセッサとメモリを搭載し、インストール先のシステムで作動します。DRAC 5 はシステムに既にインストールされている場合と、キットで別途配布される場合があります。

DRAC 5 を起動するには、「[DRAC 5 のインストールと設定](#)」を参照してください。

このリリースの DRAC 5 の新機能

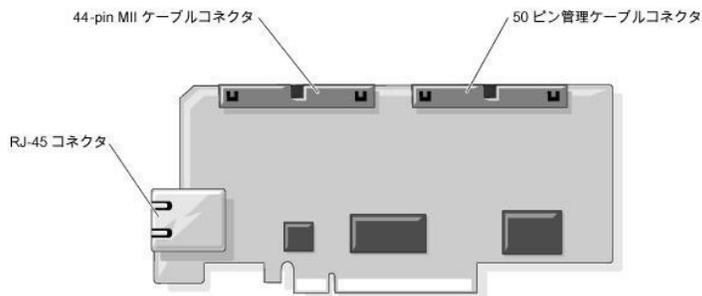
このリリースの DRAC 5 ファームウェアバージョン 1.0 は次の機能をサポートしています。

- 1 IP アドレスのブロックとフィルタ。「[DRAC 5 の追加セキュリティオプションを有効にする](#)」を参照してください。
- 1 Server Management Workgroup (SMWG) Server Management Command Line Protocol (SM-CLP) インタフェース。「[5 SM-CLP コマンドラインインタフェースの使用](#)」を参照してください。
- 1 プラットフォームのイベントトリガとフィルタの設定。「[プラットフォームイベントの設定](#)」を参照してください。
- 1 センサー情報の設定と表示
- 1 IPMI 2.0 のサポート
- 1 USB メディアのサポート

DRAC 5 ハードウェア機能

[図 1-1](#) に DRAC 5 のハードウェアを示します。

図 1-1. DRAC 5 ハードウェア機能



ハードウェア仕様

電源要件

表 1-1 に DRAC 5 の電源要件をリストにします。

表 1-1. DRAC 5 の電源要件

システム電源
+3.3 V AUX (最大) で 1.2 A
+3.3 V Main (最大) で 550 mA
+5 V Main (最大) で 0 mA

コネクタ

 **メモ:** DRAC 5 ハードウェアのインストール手順については、システムに付属の『リモートアクセスカードのインストール』マニュアルまたは『インストールおよびトラブルシューティングガイド』を参照してください。

DRAC 5 にはオンボード 10/100 Mbps RJ-45 NIC が 1 台、50 ピン管理ケーブル、および 44 ピン MII ケーブルが含まれています。DRAC 5 のケーブルコネクタについては、[図 1-1](#) を参照してください。

50 ピンケーブルは DRAC へのメインインタフェースとなり、USB、シリアル、ビデオ、および内蔵回路 (12C) バスへの接続性を提供しています。44 ピン MII ケーブルは DRAC NIC をシステムのマザーボードに接続します。RJ-45 コネクタは、DRAC が**専用 NIC** モードに設定されている場合に、帯域外の接続に DRAC NIC を接続します。

管理ケーブルと MII ケーブルを使用すると、ニーズに応じて DRAC を 3 通りのモードで設定できます。詳細については、[「RACADM コマンドラインインタフェースの使用」の「DRAC のモード」](#)を参照してください。

DRAC 5 ポート

表 1-2 に、サーバーの接続を受信する DRAC 5 が使用するポートを示します。表 1-3 に、DRAC 5 がクライアントとして使用するポートを示します。これらの情報は、ファイアウォールを開いて DRAC 5 にリモートからアクセスする場合に必要です。

表 1-2. DRAC 5 サーバー受信ポート

ポート番号	機能
22*	Secure Shell (SSH)
23*	Telnet
80*	HTTP
161	SNMP エージェント
443*	HTTPS
623	RMCP/RMCP+
3668*	仮想メディアサーバー
3669*	仮想メディアセキュアサービス
5900*	コンソールリダイレクトキーボード / マウス
5901*	コンソールリダイレクトビデオ
*設定可能なポート	

表 1-3. DRAC 5 クライアントのポート

ポート番号	機能
25	SMTP
53	DNS
68	DHCP で割り当てた IP アドレス
69	TFTP
162	SNMP トラップ
636	LDAPS
3269	グローバルカタログ (GC) 用 LDAPS

対応リモートアクセス接続

表 1-4 に接続の機能をリストにします。

表 1-4. 対応リモートアクセス接続

接続	機能
DRAC 5 NIC	<ul style="list-style-type: none">1 10/100 Mbps イーサネット1 DHCP 対応1 SNMP トラップと電子メールイベント通知1 DRAC 5 ウェブインタフェース専用ネットワークインタフェース1 システム起動、リセット、電源投入、シャットダウンコマンドなどの telnet/ssh コンソールおよび RACADM CLI コマンドに対応
シリアルポート	<ul style="list-style-type: none">1 システムブート、リセット、電源投入、およびシャットダウンコマンドなどのシリアルコンソールおよび racadm CLI コマンドに対応1 VT-100 ターミナルまたはターミナルエミュレータへのテキスト専用コンソールリダイレクトに対応

DRAC 5 セキュリティ機能

DRAC 5 は次のセキュリティ機能を備えています。

- 1 Microsoft® Active Directory® (オプション) またはハードウェアに保存されたユーザー ID とパスワードによるユーザー認証
- 1 システム管理者が各ユーザーに特定の特権を設定できる役割ベースの権限
- 1 ウェブインタフェースまたは racadm CLI を使用したユーザー ID とパスワードの設定
- 1 RACADM CLI とウェブインタフェース操作で、128 ビットの SSL 暗号化と 40 ビットの SSL 暗号化をサポート (128 ビットが許可されていない国)
 **メモ:** Telnet は SSL 暗号化に対応していません。
- 1 ウェブベースインターフェースまたは RACADM CLI を使用したセッションタイムアウトの設定 (秒単位)
- 1 設定可能な IP ポート (該当する場合)
- 1 暗号化トランスポート層を使用してセキュリティを強化する Secure Shell (SSH)
- 1 IP アドレスごとのログイン失敗制限により制限を越えた IP アドレスのログインを阻止
- 1 DRAC 5 に接続するクライアントの IP アドレス範囲を限定

対応プラットフォーム

DRAC 5 では現在、次の PowerEdge システムをサポートしています。

- 1 1900
- 1 1950
- 1 2900
- 1 2950

対応プラットフォームの最新情報は、デルのサポートウェブサイト support.dell.com で『Dell PowerEdge 互換性ガイド』を確認してください。

対応オペレーティングシステム

表 1-5 に、DRAC 5 をサポートしているオペレーティングシステムをリストにします。

最新情報は、デルのサポートウェブサイト support.dell.com で『Dell OpenManage™ Server Administrator 互換性ガイド』を確認してください。

表 1-5. 対応オペレーティングシステム

オペレーティングシステムファミリ	オペレーティングシステム
Microsoft Windows®	Windows2000 Server Service Pack 4 (SP4) Windows Server™ 2003 Standard Editions および Enterprise Editions Service Pack 1 (SP1) Windows Server 2003 Standard Edition と Enterprise Editions R2 Windows Server 2003 Standard Editions と Enterprise x64 Editions

	Windows Storage Server 2003 R2 x64 Editions
Red Hat® Linux	Intel x86 および Intel Extended Memory 64 Technology (Intel EM64T) 用 Enterprise Linux AS、ES、WS (バージョン 3) Intel x86 および Intel Extended Memory 64 Technology (Intel EM64T) 用 Enterprise Linux AS、ES、WS (バージョン 4)
SUSE® Linux	Enterprise Server (バージョン 9) (アップデート 2、Intel EM64T 用) Enterprise Server (バージョン 10) (Intel EM64T 用) (管理下システムのみ)

対応 Web ブラウザ

注意: コンソールリダイレクトおよび仮想メディアは、32 ビットウェブブラウザのみをサポートしています。64 ビットウェブブラウザの使用は、予期しない結果や故障の原因となる可能性があります。

表 1-6 に、DRAC 5 をサポートしているウェブブラウザをリストにします。

最新情報は、デルのサポートウェブサイト support.dell.com で『Dell OpenManage™ Server Administrator 互換性ガイド』を確認してください。

表 1-6. 対応 Web ブラウザ

オペレーティングシステム	対応ウェブブラウザ
Microsoft Windows	Internet Explorer 6.0 (32 ビット) Service Pack 1 (SP1) 以降 DRAC 5 ウェブインタフェースの日本語版を表示するには、次の手順に従ってください。 <ol style="list-style-type: none"> Windows の コントロールパネル を開きます。 地域のオプション アイコンをダブルクリックします。 ロケール(国または地域) ドロップダウンメニューから、目的のロケールを選択します。 <p>注意: 仮想メディアセンターを実行している場合は、Internet Explorer 6.0 と Service Pack 1 以降を使用する必要があります。</p>
Linux	Mozilla 1.7.8 以降 (32 ビット) Mozilla Firefox 1.0.7 のみ (32 ビット)

Mozilla Firefox のホワイトリスト機能を無効にする

Firefox には、追加的なセキュリティを提供する "ホワイトリスト" 機能が含まれています。ホワイトリスト機能が有効になっている場合、ブラウザはプラグインを持つ各サイトごとにプラグインのインストールの許可を要求します。このプロセスでは、プラグインのバージョンが識別されている場合でも、それぞれの RAC IP/DNSname のプラグインのインストールを要求されます。

ホワイトリスト機能を無効にし不要なプラグインインストールの繰り返しを回避するには、次の手順を実行します。

- Firefox ウェブブラウザのウィンドウを開きます。
- アドレス フィールドに次のように入力し、<Enter> を押します。

```
about:config
```

- プリファランス名** 行の、`xpinstall.whitelist.required` を検索しダブルクリックします。

プリファランス名、**状態**、**種類**、**値**の値が太字に変更されます。**状態**の値が**ユーザー設定**に変わり、**値**が **false** に変わります。

- プリファランス名** 行の中で、`xpinstall.enabled` を検索します。

値が **true** になっているか確認します。true になっていない場合は、`xpinstall.enabled` をダブルクリックし、**値**を **true** に設定します。

機能

DRAC 5 は次の機能を提供しています。

- ダイナミックドメイン名システム (DNS) の登録
- ウェブインタフェース、シリアル接続、リモート RACADM、または telnet 接続を使用したリモートシステムの管理および監視
- Active Directory 認証のサポート — Dell スキーマエクステンションおよびスナップインツールを使用してすべての DRAC 5 ユーザー ID およびパスワードを Active Directory へ集約します。
- コンソールリダイレクト — リモートシステムのキーボード、ビデオ、マウスの機能を提供
- 仮想メディア — 管理下システムから管理ステーションのメディアドライブへのアクセスが可能

- 1 システムイベントログへのアクセス — システムイベントログ (SEL)、DRAC 5 のログ、およびオペレーティングシステムの状態とは関係なくクラッシュしたシステムや応答しないシステムの前回クラッシュ画面にアクセスを提供
- 1 Dell OpenManage™ ソフトウェアの統合 — DRAC5 のウェブインタフェースを Dell OpenManage Server Administrator または IT Assistant から起動可能
- 1 RAC 警告 — **専用**、**フェールオーバーと共有**、または **共有** NIC 設定を使用して電子メールメッセージまたは SNMP トラップで管理下ノードの問題を通知
- 1 ローカル設定とリモート設定 — RACADM コマンドラインユーティリティを使用するローカルとリモートの設定を提供
- 1 リモート電源管理 — シャットダウンやリセットなどのリモート電源管理の機能を管理コンソールから提供
- 1 IPMI のサポート
- 1 Secure Sockets Layer (SSL) 暗号化 — ウェブインタフェースからセキュアリモートシステム管理を提供
- 1 パスワードレベルのセキュリティ管理 — リモートシステムへの不正アクセスを防止
- 1 役割ベースの権限 — さまざまなシステム管理タスク別に割り当て可能な権限

その他の必要マニュアル

このユーザーズガイド以外にも、次のマニュアルにはシステムにある DRAC 5 のセットアップと操作に関する追加情報が含まれています。

- 1 DRAC 5 オンラインヘルプでは、ウェブベースのインタフェースの使用法について説明しています。
- 1 『Dell OpenManage™ IT Assistant ユーザーズガイド』と『Dell OpenManage IT Assistant リファレンスガイド』には、IT Assistant に関する情報が含まれています。
- 1 『Dell OpenManage Server Administrator ユーザーズガイド』では、Server Administrator のインストールと使用法について説明しています。
- 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』では、ベースボード管理コントローラ (BMC) の設定、BMC 管理ユーティリティを使用した管理下システムの設定、その他の BMC 情報を提供しています。
- 1 『Dell Update Packages ユーザーズガイド』では、システムアップデート対策の一環として Dell Update Packages を入手して使用する方法を説明しています。

また、以下のシステムマニュアルには、DRAC 5 のインストール先のシステムに関する詳細が含まれています。

 『製品情報ガイド』には、安全および法的に重要な情報が記載されています。保証に関する情報は、本マニュアル内に記述されているか、または別のマニュアルとして構成されている場合があります。

- 1 ラックソリューションに付属の『ラックインストールガイド』と『ラックインストール手順』では、システムにラックをインストールする方法を説明しています。
- 1 『Getting Started Guide』では、システムの機能、システムの設定、および技術仕様の概要を提供しています。
- 1 『ハードウェアオーナーズマニュアル』では、システムの機能とトラブルシューティング方法、およびシステムコンポーネントのインストールまたは交換方法について説明しています。
- 1 システム管理ソフトウェアマニュアルでは、ソフトウェアの機能、要件、インストール、および基本操作を説明しています。
- 1 オペレーティングシステムのマニュアルでは、オペレーティングシステムソフトウェアのインストール、設定、および使用法を説明しています。
- 1 単体で購入したコンポーネントには、それぞれのオプションの設定とインストールに関する情報を提供するマニュアルが付属しています。
- 1 アップデートはシステムに含まれていることがあり、システム、ソフトウェア、およびマニュアルの変更が説明されています。

 **メモ:** アップデートは他の文書より新しい情報が含まれている場合が多いので、必ず先にお読みください。

- 1 リリースノートと readme ファイルには、システムやマニュアルに加えられた最新のアップデートや、経験豊富なユーザーや技術者向けの高度な技術参考資料が含まれている場合があります。

[目次ページに戻る](#)

[目次ページに戻る](#)

VM-CLI を使用したオペレーティングシステムの導入

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

- [はじめに](#)
- [ブータブルイメージファイルの作成](#)
- [導入の準備](#)
- [オペレーティングシステムの導入](#)

仮想メディアコマンドラインインタフェース (VM-CLI) ユーティリティは、管理ステーションからリモートシステムの DRAC 5 に仮想メディアの機能を提供するコマンドラインインタフェースです。VM-CLI とスクリプト方式を使用すると、ネットワーク内の複数のリモートシステムにオペレーティングシステムを導入できます。

この項では、企業のネットワークに VM-CLI ユーティリティを統合する方法について説明します。

はじめに

VM-CLI ユーティリティを使用する前に、リモートのターゲットシステムと企業のネットワークが以下の項で述べる要件を満たしていることを確認してください。

リモートシステムの要件

- 1 各リモートシステムに DRAC 5 カードが搭載されている
- 1 各リモートシステムの仮想デバイスが BIOS 起動順序の最初のデバイスである

Dell カスタムファクトリーインテグレーション

Dell カスタムファクトリーインテグレーション (CFI) オプションを選択して Dell システムを注文すると、DDNS 名が含まれた DRAC 5 カードと、仮想メディアに対応する事前設定されたシステム BIOS を使用してデルでシステムを事前に設定できます。この設定を使用すると、企業のネットワークにインストールしたときに、すぐにその仮想メディアデバイスからシステムを起動できます。

詳細については、デルのウェブサイト www.dell.com を参照してください。

ネットワークの要件

ネットワーク共有に以下のコンポーネントが含まれている必要があります。

- 1 オペレーティングシステムファイル
- 1 必要なドライバ
- 1 オペレーティングシステムのブートイメージファイル

イメージファイルは、業界標準のブータブル形式のフロッピーイメージか CD/DVD ISO イメージであることが必要です。

ブータブルイメージファイルの作成

イメージファイルのリモートシステムに展開する前に、対応システムがファイルから起動可能であることを確認してください。イメージファイルをテストするには、DRAC 5 ウェブユーザーインタフェースを使用してイメージファイルをテストシステムに転送してから、システムを再起動します。

以下の項では、Linux および Windows システム用にイメージファイルを作成する方法について説明します。

Linux システム用イメージファイルの作成

Linux システム用にブータブルイメージファイルを作成するには、データ複製ユーティリティを使用します。

ユーティリティを実行するには、コマンドプロンプトを開き、次のコマンドを入力します。

```
dd if=<入力-デバイス> of=<出力-ファイル>
```

例:

```
dd if=/dev/fd0 of=myfloppy.img
```

Windows システム用イメージファイルの作成

Windows イメージファイル用データ複製ユーティリティを選択する場合は、イメージファイルと CD/DVD ブートセクターをコピーするユーティリティを選択します。

導入の準備

リモートシステムの設定

1. 管理ステーションでアクセスできるネットワーク共有を作成します。
 2. オペレーティングシステムファイルをネットワーク共有にコピーします。
 3. リモートシステムにオペレーティングシステムを導入するために、事前に設定済みのブータブルな導入イメージファイルがある場合は、このステップを飛ばします。
設定済みのブータブルな導入イメージファイルがない場合は、ファイルを作成します。オペレーティングシステムの導入手順に使用されるプログラムやスクリプトをすべて含めます。
たとえば、Microsoft® Windows® を導入するには、Microsoft Systems Management Server (SMS) が使用する導入方式に似たプログラムをイメージファイルに含めます。
イメージファイルを作成するときは、以下の操作を行ってください。
 - 1 ネットワークベースのインストール手順に従う
 - 1 ターゲットシステムのそれぞれが同じ導入手順を起動して実行するように導入イメージを「読み取り専用」とマークする
 4. 次のいずれかの処理を実行してください。
 - 1 RACADM と仮想メディアコマンドラインインタフェース (VM-CLI) を既存のオペレーティングシステム導入アプリケーションに統合します。DRAC 5 のユーティリティを既存のオペレーティングシステム導入アプリケーションに統合するときは、サンプル導入スクリプトをガイドとして使用してください。
 - 1 既存の `vmdeploy` スクリプトを使用して、オペレーティングシステムを導入します。
-

オペレーティングシステムの導入

ユーティリティに含まれている VM-CLI と `vmdeploy` スクリプトを使用して、リモートシステムにオペレーティングシステムを導入します。

始める前に、VM-CLI ユーティリティに含まれている `vmdeploy` サンプルスクリプトを確認してください。このスクリプトは、ネットワーク内のリモートシステムにオペレーティングシステムを導入するための詳しい要件を提供しています。

以下の手順は、ターゲットのリモートシステムにオペレーティングシステムを導入するための概要です。

1. 導入するリモートシステムを特定します。
 2. DRAC 5 の名前とターゲットリモートシステムの IP アドレスを記録します。
 3. ターゲットの各リモートシステムに以下の手順を実行します。
 - a. ターゲットシステムの以下のパラメータを含む VM-CLI プロセスを設定します。
 - DRAC 5 の IP アドレスまたは DDNS 名
 - ブータブル導入イメージファイルの名前
 - DRAC 5 のユーザー名
 - DRAC 5 のユーザーパスワード
 - b. RACADM を使用して、ターゲット DRAC 5 の `boot once (起動 1 度)` オプションを設定します。
 - c. RACADM を使用して、DRAC 5 システムを再起動します。
-

[目次ページに戻る](#)

[目次ページに戻る](#)

DRAC 5 SM-CLP コマンドラインインタフェースの使用

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

- [DRAC 5 SM-CLP のサポート](#)
- [SM-CLP の機能](#)

この項では、DRAC 5 に組み込まれている Workgroup (SMWG) Server Management Command Line Protocol (SM-CLP) について説明します。

 **メモ:** ここでは、ユーザーが Systems Management Architecture for Server Hardware (SMASH) イニシアチブおよび SMWG SM-CLP 仕様熟知していることを前提としています。これらの仕様の詳細は、ウェブサイト www.dmtf.org Distributed Management Task Force (DMTF) を参照してください。

DRAC 5 SM-CLP は DMTF と SMWG が提唱するプロトコルで、システム管理 CLI の実装標準となっています。システム管理コンポーネントの標準化の基盤となることを目標とする SMASH アーキテクチャの定義がその原動力となっています。SMWG SM-CLP は DMTF が提唱する全体的な SMASH 作業のサブコンポーネントです。

DRAC 5 SM-CLP のサポート

DRAC 5 は SM-CLP 標準に基づくコマンドラインプロトコルのサポートを最初に提供した RAC 製品です。SM-CLP は DRAC 5 コントローラのファームウェアからホストされ、telnet、SSH、およびシリアルベースのインタフェースをサポートしています。DRAC 5 SM-CLP インタフェースは DMTF 組織が提供する SM-CLP 仕様バージョン 1.0 に基づいています。

以下の項では、DRAC 5 からホストされる SM-CLP 機能の概要を提供します。

SM-CLP の機能

SM-CLP 仕様は、CLI による単純なシステム管理に使用できる標準的な SM-CLP の共通セットを提供しています。

[表 11-1](#) に、サポートしている CLI のバープをリストにします。

表 11-1. サポートしている CLI のバープ

バープ	定義
CD	シェルを使用して MAP を移動します。
delete	オブジェクトのインスタンスを削除します。
help	特定のターゲットのヘルプを表示します。
reset	ターゲットをリセットします。
show	ターゲットのプロパティ、バープ、およびサブターゲットを表示します。
start	ターゲットをオンにします。
stop	ターゲットをシャットダウンします。
exit	SM-CLP シェルのセッションを終了します。
version	ターゲットのバージョン属性を表示します。

SM-CLP の管理操作とターゲット

SM-CLP はバープとターゲットの概念を奨励して、CLI を通じたシステム管理を提供します。バープは実行する処理を指し、ターゲットはその処理を実行するエンティティ(またはオブジェクト)を決定します。

次は SM-CLP コマンドライン構文の例です。

<バープ> [<オプション>] [<ターゲット>] [<プロパティ>]

通常の SM-CLP セッション中、ユーザーは [表 11-1](#) にあるバープを使って操作を実行できます。

管理操作

DRAC 5 の SM-CLP 使用すると、以下のような管理ができます。

- 1 サーバーの電源管理 — システムのオン、シャットダウン、再起動
- 1 システムイベントログ (SEL) 管理 — SEL レコードの表示やクリア

ターゲット

表 11-2 に、これらの操作をサポートするために SM-CLP から提供されるターゲットをリストにします。

表 11-2. SM-CLP のターゲット

ターゲット	定義
/system1	管理下システムターゲット
/system1/logs1	ログ収集ターゲット
/system1/logs1/log1	管理下システムのシステムイベントログ (SEL) ターゲット
/system1/logs1/log1/record1	管理下システムの SEL レコードの個々のインスタンス

オプション

表 11-3 に、サポートしている SM-CLP オプションを示します。

表 11-3. サポートしている SM-CLP オプション

SM-CLP オプション	説明
-all	可能な機能のすべてを実行するようにバープに指示します。
-display	ユーザー定義のデータを表示します。
-examine	コマンドを実行せずにコマンド構文を確認するようにコマンドプロセッサに指示します。
-help	コマンドバープのヘルプを表示します。
-version	コマンドバープのバージョンを表示します。

SM-CLP 出力形式

DRAC 5 は現在、SM-CLP 仕様に記載されているようにテキストベースの出力をサポートしています。

DRAC 5 SM-CLP の例

以下のサブセクションでは、SM-CLP を使用して以下の処理を実行するためのサンプルシナリオを提供します。

- 1 サーバーの電源管理
- 1 SEL の管理
- 1 MAP ターゲットのナビゲーション
- 1 システムのプロパティの表示

サーバーの電源管理

表 11-4 に、SM-CLP を使用して管理下システムの電源管理操作を実行する例を示します。

表 11-4. サーバーの電源管理操作

操作	構文
telnet/SSH インタフェースを使用して RAC にログインする	>ssh 192.168.0.120 >login: root >password:
SM-CLP 管理シェルを開始する	- >smclp DRAC5 SM-CLP System Management Shell, version 1.0 Copyright (c) 2004-2006 Dell, Inc. All Rights Reserved ->
サーバーの電源を切る	- ->stop /system1 system1 has been stopped successfully
電源オフの状態からサーバーの電源を入れる	-

	->start /system1 system1 has been started successfully
サーバーを再起動する	->reset /system1 system1 has been reset successfully

SEL の管理

表 11-5 に、SM-CLP を使用して管理下システムに SEL 関連の操作を実行する例を示します。

表 11-5. SEL の管理操作

操作	構文
SEL を表示する	<pre>->show /system1/logsl/log1 /system1/logsl/log1 Targets: Record1 Record2 Record3 Record4 Record5 Properties: InstanceID = IPMI:BMCL SEL Log MaxNumberOfRecords = 512 CurrentNumberOfRecords = 5 Name = IPMI SEL EnabledState = 2 OperationalState = 2 HealthState = 2 Caption = IPMI SEL Description = IPMI SEL ElementName = IPMI SEL Commands: cd show help exit version</pre>
SEL のレコードを表示する	<pre>->show /system1/logsl/log1/record4 /system1/logsl/log1/record4 Properties: LogCreationClassName = CIM_RecordLog CreationClassName = CIM_LogRecord LogName = IPMI SEL RecordID = 1 MessageTimeStamp = 20050620100512.000000-000 Description = FAN 7 RPM: fan sensor, detected a failure ElementName = IPMI SEL Record Commands: cd show help exit version</pre>
SEL をクリアする	<pre>->delete /system1/logsl/log1/record* All records deleted successfully</pre>

MAP ターゲットのナビゲーション

表 11-6 に、cd パープを使用して MAP をナビゲートする例を示します。すべての例で、最初のデフォルトターゲットは / であると想定されます。

表 11-6. Map ターゲットのナビゲーション操作

操作	構文
システムターゲットまでナビゲートして再起動する	<pre>->cd system1 ->reset</pre> <p>メモ: 現在のデフォルトターゲットは / です。</p>
SEL ターゲットまでナビゲートしてログレコードを表示する	<pre>->cd system1 ->cd logsl/log1</pre>

	->show
	->cd system1/logsl/log1
	->show
現在のターゲットを表示する	->cd .
1つ上のレベルへ移動する	->cd ..
シェルを終了する	->exit

システムのプロパティ

表 11-7 に、ユーザーが次のように入力したときに表示されるシステムプロパティを示します。

```
show /system1
```

これらのプロパティは、標準的な本文によって提供され、CIM スキーマで定義されている **CIM_ComputerSystem** クラスに基づくベースシステムプロファイルから導出されるプロパティです。

詳細については、DMTF CIM スキーマ定義を参照してください。

表 11-7. システムのプロパティ

オブジェクト	プロパティ	説明
CIM_ComputerSystem	Name	企業の環境に存在するシステムのインスタンスを固有に識別する ID。 MaxLen = 256
	ElementName	システムのユーザーフレンドリな名前。 MaxLen = 64
	NameFormat	Name が生成される方法を示します。 値: Other, IP, Dial, HID, NWA, HWA, X25, ISDN, IPX, DCC, ICD, E.164, SNA, OID/OSI, WWN, NAA
	Dedicated	システムが特殊な目的のシステムか汎用システムかを示す列挙。 値: 0=専用ではない 1=不明 2=その他 3=ストレージ 4=ルーター 5=スイッチ 6=レイヤ 3 スイッチ 7=本社スイッチ 8=ハブ 9=アクセスサーバー 10=ファイアウォール 11=印刷 12=I/O 13=ウェブキャッシュ 14=管理 15=ブロックサーバー 16=ファイルサーバー 17=モバイルユーザーデバイス、 18=リピーター 19=ブリッジ / 拡張装置

		<p>20=ゲートウェイ</p> <p>21=ストレージバーチャライザ</p> <p>22=メディアライブラリ</p> <p>23=拡張ノード</p> <p>24=NAS ヘッド</p> <p>25=内蔵型 NAS</p> <p>26=UPS</p> <p>27=IP フォン</p> <p>28=管理コントローラ</p> <p>29=シャーシマネージャ</p>
	ResetCapability	<p>システムで使用可能なリセット方法を定義します。</p> <p>値:</p> <p>1=その他</p> <p>2=不明</p> <p>3=無効</p> <p>4=有効</p> <p>5=実装されていない</p>
	CreationClassName	このインスタンスの導出元スーパークラス
	EnabledState	<p>システムの有効 / 無効の状態を示します。</p> <p>値:</p> <p>0=不明</p> <p>1=その他</p> <p>2=有効</p> <p>3=無効</p> <p>4=シャットダウン</p> <p>5=該当なし</p> <p>6=有効であるがオフライン</p> <p>7=テスト中</p> <p>8=保留</p> <p>9=無活動</p> <p>10=起動中</p>
	EnabledDefault	<p>システムの有効状態のデフォルトの起動設定を示します。デフォルトではシステムは「有効」(値=2)です。</p> <p>値:</p> <p>2=有効</p> <p>3=無効</p> <p>4=該当なし</p> <p>5=有効であるがオフライン</p> <p>6=デフォルトなし</p>
	RequestedState	<p>システムに最後に要求された状態を示します。</p> <p>値:</p> <p>2=有効</p> <p>3=無効</p> <p>4=シャットダウン</p>

		<p>5=変更なし</p> <p>6=オフライン</p> <p>7=テスト</p> <p>8=保留</p> <p>9=無活動</p> <p>10=再起動</p> <p>11=リセット</p> <p>12=該当なし</p>
	HealthState	<p>システムの現在の正常性を示します。</p> <p>値:</p> <p>0=不明</p> <p>5=正常</p> <p>10=低下 / 警告</p> <p>15=小さいエラー</p> <p>20=大きいエラー</p> <p>30=重大なエラー</p> <p>35=回復不能なエラー</p>
	OperationalStatus	<p>システムの現在の状態を示します。</p> <p>値:</p> <p>0=不明</p> <p>1=その他</p> <p>2=正常</p> <p>3=低下</p> <p>4=過負荷</p> <p>5=予測エラー</p> <p>6=エラー</p> <p>7=回復不能なエラー</p> <p>8=起動中</p> <p>9=停止中</p> <p>10=停止</p> <p>11=サービス提供中</p> <p>12=接続なし</p> <p>13=通信切断</p> <p>14=中止</p> <p>15=休止中</p> <p>16=補助エンティティのエラー</p> <p>17=完了</p> <p>18=電源モード</p>
	説明	<p>システムの状態を説明するテキスト。</p>

[目次ページに戻る](#)

トラブルシューティング

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

- [DRAC 5 のトラブルシューティング](#)

DRAC 5 のトラブルシューティング

DRAC 5 と RACADM のトラブルシューティングに関するヘルプは、次の表を参照してください。

[表 6-8、「DRAC 5 と Active Directory の使用:よくあるお問い合わせ \(FAQ\)」](#)

[表 7-7、「コンソールリダイレクトの使用:よくあるお問い合わせ \(FAQ\)」](#)

[表 8-2、「仮想メディアの使用:よくあるお問い合わせ \(FAQ\)」](#)

[表 9-4、「シリアルおよび racadm コマンドの使用:よくあるお問い合わせ \(FAQ\)」](#)

[目次ページに戻る](#)

[目次ページに戻る](#)

DRAC 5 のインストールと設定

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

- [はじめに](#)
- [DRAC 5 ハードウェアのインストール](#)
- [システムで DRAC 5 を使用するための設定](#)
- [ソフトウェアのインストールと設定概要](#)
- [管理下システムのソフトウェアのインストール](#)
- [管理ステーションのソフトウェアのインストール](#)
- [対応Web ブラウザの設定](#)
- [DRAC 5 プロパティの設定](#)
- [DRAC 5 ネットワークの設定](#)
- [DRAC 5 ユーザーの追加と設定](#)
- [DRAC 5 ファームウェアのアップデート](#)
- [ネットワーク経由による DRAC 5 へのアクセス](#)
- [IPMI の設定](#)
- [プラットフォームイベントの設定](#)

本項では、DRAC 5 のハードウェアとソフトウェアをインストールして設定する方法を説明します。

はじめに

システムに含まれている以下のアイテムを用意してから、DRAC 5 のインストールと設定を開始してください。

- 1 DRAC 5 のハードウェア(現在インストール中、またはオプションキットに同梱)
- 1 DRAC 5 のインストール手順(本章)
- 1 Dell™ PowerEdge™ Installation and Server Management CD
- 1 Dell Systems Management Consoles CD
- 1 Dell PowerEdge Service and Diagnostic Utilities CD
- 1 Dell PowerEdge Documentation CD

DRAC 5 ハードウェアのインストール

 **メモ:** DRAC 5 接続が USB キーボード接続をエミュレートします。その結果、システムの再起動時に、キーボードが取り付けられていない場合でもユーザーに通知されません。

DRAC 5 はシステムにインストール済みか、別途キットが用意されています。システムにインストール済みの DRAC 5 を使用して開始するには、「[ソフトウェアのインストールと設定概要](#)」を参照してください。

システムに DRAC 5 がインストールされていない場合は、先へ進む前に、DRAC 5 キットに付属の『リモートアクセスカードのインストールマニュアル』を参照するか、使用しているプラットフォームの『インストールおよびトラブルシューティングガイド』のハードウェア取り付け手順に従ってください。

 **メモ:** DRAC 5 の削除については、システムに付属の『インストールおよびトラブルシューティングガイド』を参照してください。さらに、セキュリティを確保するため、削除した DRAC 5 に関連付けられている Microsoft® Active Directory® の RAC プロパティを確認してください。

システムで DRAC 5 を使用するための設定

システムに DRAC 5 を設定するには、Dell リモートアクセス設定ユーティリティ(旧称 BMC セットアップモジュール)を使用します。

リモートアクセス設定ユーティリティを実行するには、以下の手順に従います。

1. システムをオンにするか、再起動します。
2. POST 中にプロンプトが表示されたら <Ctrl><E> を押します。

<Ctrl><E> を押す前にオペレーティングシステムがロードを開始した場合は、起動が完了するのを待ってからシステムを再起動して、もう一度実行します。
3. NIC を設定します。
 - a. 下矢印キーを使用して **NIC の選択** をハイライトします。
 - b. 左矢印キーと右矢印キーを使用して、以下の NIC 選択から 1 つを選択します。

- **専用** — リモートアクセスデバイスを有効にして、Remote Access Controller (RAC) で使用可能な専用ネットワークインタフェースを利用するには、このオプションを選択します。このインタフェースはホストオペレーティングシステムと共有されず、管理トラフィックを別の物理ネットワークに転送するため、アプリケーションのトラフィックから分離できません。このオプションは、システムに DRAC カードが搭載されている場合にのみ使用可能です。
- **共有** — ネットワークインタフェースをホストオペレーティングシステムと共有するには、このオプションを選択します。リモートアクセスデバイスのネットワークインタフェースは、ホストオペレーティングシステムに NIC チームが設定されている場合に完全に機能します。リモートアクセスデバイスは NIC 1 と NIC 2 でデータを受信しますが、NIC 1 からのみデータを送信します。NIC 1 でエラーが発生すると、リモートアクセスデバイスにアクセスできなくなります。
- **フェールオーバー** — ネットワークインタフェースをホストオペレーティングシステムと共有するには、このオプションを選択します。リモートアクセスデバイスのネットワークインタフェースは、ホストオペレーティングシステムに NIC チームが設定されている場合に完全に機能します。リモートアクセスデバイスは NIC 1 と NIC 2 でデータを受信しますが、NIC 1 からのみデータを送信します。NIC 1 でエラーが発生すると、リモートアクセスデバイスはすべてのデータ送信を NIC 2 にフェールオーバーします。リモートアクセスデバイスはデータ送信に NIC 2 を使い続けます。NIC 2 でエラーが発生した場合、リモートアクセスデバイスはすべてのデータ送信を再び NIC 1 にフェールオーバーします。

4. DHCP または静的 IP アドレスソースを使用するようにネットワークコントローラの LAN パラメータを設定します。

- a. 下矢印キーを使用して、**LAN パラメータ** を選択して <Enter> を押します。
- b. 上矢印キーと下矢印キーを使用して、**IP アドレスソース** を選択します。
- c. 右矢印キーと左矢印キーを使用して、**DHCP** または **静的** を選択します。
- d. **静的** を選択した場合は、**Ethernet IP アドレス**、**サブネットマスク**、および **デフォルトゲートウェイ** の設定を指定します。
- e. <Esc> を押します。

5. <Esc> を押します。

6. **変更を保存して終了** を選択します。

システムが自動的に再起動します。

 **メモ:** NIC 1 枚で構成されている Dell PowerEdge 1900 システム上で、ウェブユーザーインタフェースを表示する場合、NIC 設定ページでは NIC を 2 枚 (NIC1 および NIC2) 表示します。これは通常の動作です。PowerEdge 1900 システム (およびその他の 単一のマザーボード上の LAN で構成されている) は、NIC チューニングで構成することができます。これらのシステムでは、共有およびチームモードは別個に動作します。

Dell リモートアクセス設定ユーティリティの詳細に関しては、『Dell OpenManage™ ベースボード管理コントローラユーティリティユーザーズガイド』を参照してください。

ソフトウェアのインストールと設定概要

ここでは、DRAC 5 ソフトウェアのインストールと設定のプロセスについて概説します。ウェブインタフェースの RACADM CLI またはシリアル / Telnet / SSH コンソールを使用して、DRAC 5 を設定します。

DRAC 5 ソフトウェアコンポーネントの詳細に関しては、「[管理下システムのソフトウェアのインストール](#)」を参照してください。

DRAC 5 ソフトウェアのインストール

DRAC 5 ソフトウェアをインストールするには、次の手順を実行してください。

1. 管理下システムでソフトウェアをインストールします。「[管理下システムのソフトウェアのインストール](#)」を参照してください。
2. 管理ステーションでソフトウェアをインストールします。「[管理ステーションのソフトウェアのインストール](#)」を参照してください。

DRAC 5 の設定

DRAC 5 を設定するには、次の手順を実行してください。

1. 次のいずれかの設定ツールを選択します。
 - I Web インタフェース
 - I RACADM CLI
 - I シリアル/Telnet/SSH コンソール

 **注意:** 複数の DRAC 5 設定ツールを同時に使用すると、不測の結果が生じることがあります。

2. DRAC 5 ネットワーク設定を設定します。「[DRAC 5 ネットワークの設定](#)」を参照してください。
3. DRAC 5 ユーザーを追加および設定します。「[DRAC 5 ユーザーの追加と設定](#)」を参照してください。

4. ウェブインタフェースにアクセスするウェブブラウザを設定します。「[対応 Web ブラウザの設定](#)」を参照してください。
5. Windows 自動再起動オプションを無効にします。「[Windows 自動再起動オプションを無効にする](#)」を参照してください。
6. DRAC 5 ファームウェアをアップデートします。「[DRAC 5 ファームウェアのアップデート](#)」を参照します。
7. ネットワーク経由で DRAC 5 にアクセスします。「[ネットワーク経由による DRAC 5 へのアクセス](#)」を参照してください。

管理下システムのソフトウェアのインストール

管理下システムのソフトウェアのインストールはオプションです。Managed System Software がないと、RACADM をローカルで使用したり、RAC が前回クラッシュ画面をキャプチャできません。

Managed System Software をインストールするには、『Dell PowerEdge Installation and Server Management CD』を使って管理下システムにソフトウェアをインストールします。このソフトウェアのインストール手順については、『[クイックインストールガイド](#)』を参照してください。

Managed System Software は Server Administrator の適切なバージョンで行った選択を管理下システムにインストールします。

 **メモ:** DRAC 5 Management Station Software と DRAC 5 Mmanaged System Software を同じシステムにインストールしないでください。

管理下システムに Server Administrator がインストールされていない場合は、システムの前回クラッシュ画面を見たり、**自動回復**機能を使用したりできません。

前回クラッシュ画面の詳細に関しては、『[システムの前回クラッシュ画面の表示](#)』を参照してください。

管理下システムが前回クラッシュ画面をキャプチャするように設定する

DRAC 5 が前回クラッシュ画面をキャプチャする前に、次の前提条件を使って管理下システムを設定する必要があります。

1. Managed System Software をインストールします。Managed System Software のインストールの詳細に関しては、『Server Administrator ユーザーズガイド』を参照してください。

2. Windows の「自動再起動」機能を **Windows スタートアップおよびリカバリ設定** でオフにして、Microsoft Windows の対応オペレーティングシステムを実行します。

3. 前回クラッシュ画面を有効にします(デフォルトは無効)。

ローカル RACADM の使用を有効にするには、コマンドプロンプトを開いて次のコマンドを入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1
```

4. 自動回復タイマーを有効にし、**自動回復** 処置を **リセット**、**電源オフ**、または **パワーサイクル** に設定します。**自動回復**タイマーを設定するには、Server Administrator または IT Assistant を使用する必要があります。

自動回復タイマーの設定方法については、『Server Administrator ユーザーズガイド』を参照してください。前回クラッシュ画面を確実にキャプチャするには、**自動回復**タイマーを 60 秒以上に設定する必要があります。デフォルト設定は 480 秒です。

管理下システムの電源がオフの場合、**自動回復**処置が **シャットダウン** または **パワーサイクル** に設定されていると、前回クラッシュ画面を使用できません。

Windows 自動再起動オプションを無効にする

DRAC 5 の Web インタフェースの前回クラッシュ画面機能を正しく動作させるには、Microsoft Windows Server 2003 および Windows 2000 Server オペレーティングシステムを実行している管理下システムで、**自動再起動** オプションを無効にしてください。

Windows Server 2003 の自動再起動オプションを無効にする

1. Windows の **コントロールパネル** を開いて、**システム** アイコンをダブルクリックします。
2. **詳細** タブをクリックします。
3. **起動 / 回復** で、**設定** をクリックします。
4. **自動再起動** チェックボックスを選択解除します。
5. **OK** を 2 度クリックします。

Windows 2000 Server の自動再起動オプションを無効にする

1. Windows の **コントロールパネル** を開いて、**システム** アイコンをダブルクリックします。
2. **詳細** タブをクリックします。
3. **起動 / 回復** ボタンをクリックします。
4. **自動再起動** チェックボックスを選択解除します。

管理ステーションのソフトウェアのインストール

システムには Dell OpenManage System Management Software Kit が含まれています。このキットには以下のようなコンポーネントが含まれています。

1. Dell PowerEdge Installation and Server Management CD — システムの設定とオペレーティングシステムのインストールに必要なツールを提供するブータブル CD。この CD には、Dell OpenManage Server Administrator Diagnostics、Storage Management、Remote Access Service などの最新のシステム管理ソフトウェア製品が含まれています。
1. Dell Systems Management Consoles CD — Dell OpenManage IT Assistant などの最新の Dell システム管理コンソール製品がすべて含まれています。
1. Dell PowerEdge Service and Diagnostic Utilities CD — システムの設定に必要なツールを提供し、システムの最新の BIOS、ファームウェア、診断、Dell 用に最適化したドライバを配布します。
1. Dell PowerEdge Documentation CD — システム、システム管理ソフトウェア製品、周辺機器、RAID コントローラなどの最新マニュアルを提供します。

Server Administrator ソフトウェアのインストール方法については、『Server Administrator ユーザーズガイド』を参照してください。

Red Hat Enterprise Linux (バージョン 4) 管理ステーションの設定

Dell デジタル KVM ビューアを Red Hat Enterprise Linux (バージョン 4) の管理ステーションで実行するには、追加の設定作業が必要です。Red Hat Enterprise Linux (バージョン 4) オペレーティングシステムを管理ステーションにインストールするときに、次の手順を実行してください。

1. パッケージの追加または削除のプロンプトが表示されたら、オプションの **Legacy Software Development** ソフトウェアをインストールします。このソフトウェアパッケージには、管理ステーションで Dell デジタル KVM ビューアを実行するのに必要なソフトウェアコンポーネントが含まれています。
1. Dell デジタル KVM ビューアが正しく機能するように、ファイアウォールの次のポートを開きます。
 - キーボードとマウスのポート (デフォルトはポート 5900)
 - ビデオポート (デフォルトはポート 5901)

Linux 管理ステーションでの RACADM のインストールと削除

リモート RACADM 機能を使用するには、Linux を実行している管理ステーションに RACADM をインストールします。

 **メモ:** 『Systems Management Consoles CD』で **セットアップ** を実行すると、すべての対応オペレーティングシステムの RACADM ユーティリティが管理ステーションにインストールされます。

RACADM のインストール

1. 管理ステーションコンポーネントをインストールするシステムにルートとしてログインします。
2. 必要に応じて、次のようなコマンドを使用して『Dell Systems Management Consoles CD』をマウントします。

```
mount /media/cdrom
```

3. **/linux/rac** ディレクトリに移動し、次のコマンドを実行します。

```
rpm -ivh *.rpm
```

RACADM コマンドのヘルプを表示するには、前のコマンドを発行した後、**racadm help** と入力します。RACADM の詳細に関しては、『[RACADM コマンドラインインタフェースの使用](#)』を参照してください。

RACADM のアンインストール

RACADM をアンインストールするには、コマンドプロンプトを開いて次のように入力します。

```
rpm -e <racadm_パッケージ_名>
```

<racadm_パッケージ_名> は、RAC ソフトウェアのインストールに使用した rpm パッケージです。

たとえば、rpm パッケージ名が `srvadmin-racadm5` であれば、次のように入力します。

```
rpm -e srvadmin-racadm5
```

対応 Web ブラウザの設定

次項には、対応する Web ブラウザの設定手順を説明しています。対応する Web ブラウザについては、「[対応 Web ブラウザ](#)」のリストを参照してください。

ウェブインタフェースに接続する Web ブラウザの設定

プロキシサーバーを介してインターネットに接続している管理ステーションから DRAC 5 のウェブインタフェースに接続する場合は、このサーバーからインターネットにアクセスするように Web ブラウザを設定する必要があります。

Internet Explorer Web ブラウザがプロキシサーバーにアクセスするように設定するには、次の手順を実行してください。

1. Web ブラウザのウィンドウを開きます。
2. ツール をクリックし、インターネットオプション をクリックします。
3. インターネットオプション ウィンドウで、接続 タブをクリックします。
4. ローカルエリアネットワーク(LAN)の設定 で LAN の設定 をクリックします。
5. プロキシサーバーを使用 ボックスが選択されている場合は、ローカルアドレスにはプロキシサーバーを使用しない ボックスを選択します。
6. OK を 2 度クリックします。

信頼できるドメインのリスト

ウェブブラウザを使って、DRAC 5 ウェブインタフェースにアクセスする場合は、IP アドレスがリストにない場合は、DRAC 5 IP アドレスをリストに加えるよう要求されます。追加が完了すると、更新をクリックするか、またはウェブブラウザを再起動し、DRAC 5 ウェブインタフェースへの接続を再確立します。

32 ビット および 64 ビットのウェブブラウザ

DRAC 5 ウェブインタフェースは、64ビットウェブブラウザでサポートされていません。64 ビットブラウザを開いた場合、コンソールリダイレクトのページにアクセスし、プラグインをインストールしようとしても、インストールの手続きは失敗します。このエラーに回答せず手順を繰り返した場合、コンソールリダイレクトページは、最初の試行でプラグインのインストールに失敗したにもかかわらず、読み込みを行います。この不具合は、プラグインインストール手続きに失敗しても、ウェブブラウザがプラグイン情報をプロファイルディレクトリに保存しているためです。この不具合を修正するには、32ビット対応のウェブブラウザをインストールして起動し、DRAC 5 にログインします。

ローカライズされた Web インタフェースバージョンの表示

Windows

DRAC 5 ウェブインタフェースは次の Windows オペレーティングシステム言語でサポートされています。

- 1 英語
- 1 フランス語
- 1 ドイツ語
- 1 スペイン語
- 1 日本語
- 1 簡体中国語

Internet Explorer で DRAC 5 ウェブインタフェースのローカライズバージョンを表示するには、次の手順を実行してください。

1. ツール メニューをクリックし、インターネットオプション を選択します。
2. インターネットオプション ウィンドウで 言語 をクリックします。

3. **言語の設定 ウィンドウ**で **追加** をクリックします。
4. **言語の追加** ウィンドウで、サポートされている言語から 1 つを選択します。
複数の言語を選択するには、<Ctrl> を押します。
5. 使用する言語を選択し、**上へ移動** をクリックしてその言語をリストの一番上に移動します。
6. **OK** をクリックします。
7. **言語の設定** ウィンドウで **OK** をクリックします。

Linux

Red Hat Enterprise Linux (バージョン 4) クライアント上で、簡体字中国語の GUI でコンソールリダイレクトを起動している場合、表示メニューおよびタイトルがランダム文字で表示される可能性があります。この不具合は、Red Hat Enterprise Linux (version 4) での不適切な簡体字中国語のエンコーディングが原因です。この不具合を修正するには、次の手順を実行し、現在のエンコーディングの設定にアクセス、修正をします。

1. コマンドターミナルを開きます。
2. "locale" を入力し、<Enter> キーを押します。次の出力が表示されます。

```
LANG=zh_CN.UTF-8
LC_CTYPE="zh_CN.UTF-8"
LC_NUMERIC="zh_CN.UTF-8"
LC_TIME="zh_CN.UTF-8"
LC_COLLATE="zh_CN.UTF-8"
LC_MONETARY="zh_CN.UTF-8"
LC_MESSAGES="zh_CN.UTF-8"
LC_PAPER="zh_CN.UTF-8"
LC_NAME="zh_CN.UTF-8"
LC_ADDRESS="zh_CN.UTF-8"
LC_TELEPHONE="zh_CN.UTF-8"
LC_MEASUREMENT="zh_CN.UTF-8"
LC_IDENTIFICATION="zh_CN.UTF-8"
LC_ALL=
```

3. 値に「zh_CN.UTF-8」が含まれる場合は、変更の必要はありません。値に「zh_CN.UTF-8」が含まれない場合は、ステップ 4 に進みます。
4. /etc/sysconfig/i18n ファイルを検索します。
5. ファイルに、次の変更を適用します。

現在のエントリ

```
LANG="zh_CN.GB18030"
SUPPORTED="zh_CN.GB18030:zh_CN.GB2312:zh_CN:zh"
```

アップデートされたエントリ

```
LANG="zh_CN.UTF-8"
SUPPORTED="zh_CN.GB18030:zh_CN.GB2312:zh_CN:zh"
```

6. ログアウトし、そしてオペレーティングシステムにログインします。
7. DRAC 5 を再起動します。

簡体字中国語以外の言語から簡体字中国語に移行する場合は、この修正が有効になっているか確認してください。有効でない場合は、この手順を繰り返します。

DRAC 5 プロパティの設定

ウェブインタフェースまたは RACADM を使用して、DRAC 5 のプロパティ(ネットワーク、ユーザー、警告など)を設定します。

ウェブインタフェースの使い方の詳細に関しては、「[ウェブインタフェースへのアクセス](#)」を参照してください。RACADM をシリアルまたは telnet 接続で使用する方法的詳細に関しては、「[RACADM コマンドラインインタフェースの使用](#)」を参照してください。

DRAC 5 ネットワークの設定

 **注意:** DRAC 5 のネットワーク設定を変更すると、現在のネットワーク接続が切断される可能性があります。

DRAC 5 のネットワーク設定には、次のいずれかのツールを使用します。

- 1 Web インタフェース — 「[DRAC 5 NIC の設定](#)」を参照してください。
- 1 RACADM CLI — 「[cfgLanNetworking](#)」を参照してください。
- 1 Dell リモートアクセス設定ユーティリティ — 「[システムへの DRAC 5 の使用の設定](#)」を参照してください。

 **メモ:** DRAC 5 を Linux 環境に導入する場合は、「[RACADM のインストール](#)」を参照してください。

DRAC 5 ユーザーの追加と設定

DRAC 5 のユーザーを追加して設定するには、次のいずれかのツールを使用します。

- 1 Web インタフェース — 「[DRAC 5 ユーザーの追加と設定](#)」を参照してください。
 - 1 racadm CLI — 「[cfgUserAdmin](#)」を参照してください。
-

DRAC 5 ファームウェアのアップデート

DRAC 5 ファームウェアをアップデートするには、次のいずれかの方法を使用します。

- 1 ウェブインタフェース — 「[ウェブインタフェースを使用した DRAC 5 ファームウェアのアップデート](#)」を参照してください。
- 1 RACADM CLI — 「[fwupdate](#)」を参照してください。
- 1 Dell Update Packages — システムアップデート対策の一環として Dell Update Packages を入手して使用する方法については、『Dell Update Packages ユーザーズガイド』を参照してください。

はじめに

ローカル RACADM または Dell Update Packages を使って DRAC 5 ファームウェアをアップデートする前に、次の手順を実行します。実行しない場合は、ファームウェアのアップデートが失敗する可能性があります。

- 1 適切な IPMI および管理下ノードドライバをインストールおよび有効化します。
- 2 Windows オペレーティングシステムを実行している場合、**Windows Management Instrumentation (WMI)** サービスを有効にして起動します。
- 3 Intel EM64T 用 SUSE Linux Enterprise サーバー (バージョン 10) を起動している場合、**Raw** サービスを開始します。
- 4 RAC 仮想フラッシュが、アンマウントされているか、または他のオペレーティングシステム、アプリケーションまたはユーザーが使用していないか確認します。
- 5 仮想メディアを切断およびアンマウントします。
- 6 USB が有効であることを確認します。

DRAC 5 ファームウェアのダウンロード

DRAC 5 ファームウェアをアップデートするには、デルのサポートウェブサイト [support.dell.com](#) から最新ファームウェアをダウンロードして、ファイルをローカルシステムに保存します。

DRAC 5 ファームウェアパッケージには、次のソフトウェアコンポーネントが含まれています。

- 1 コンパイル済み DRAC 5 のファームウェアコードとデータ
- 1 拡大 ROM イメージ
- 1 Web インタフェース、JPEG、および他のユーザーインタフェースデータファイル
- 1 デフォルト設定ファイル

DRAC 5 ファームウェアを最新バージョンにアップデートするには、**ファームウェアのアップデート** ページを使用します。ファームウェアアップデートを実行すると、現在の DRAC 5 の設定が維持されます。

ウェブインタフェースを使用した DRAC 5 ファームウェアのアップデート

- 1 ウェブインタフェースを開き、リモートシステムにログインします。

「[ウェブインタフェースへのアクセス](#)」を参照してください。

2. **システム** ツリーで、**リモートアクセス** をクリックし、**アップデート** タブをクリックします。
3. **ファームウェアアップデート** ページの **ファームウェアイメージ** フィールドに、[support.dell.com](#) からダウンロードしたファームウェアイメージのパスを入力するか、**参照** をクリックしてイメージまで移動します。

 **メモ:** Firefox を実行している場合は、**ファームウェアイメージ** フィールドにテキストカーソルが表示されません。

例:

C:\Updates\%V1.0%<イメージ名>

デフォルトのファームウェアイメージ名は **firmimg.d5** です。

4. **アップデート** をクリックします。
アップデートの完了に数分かかる場合があります。完了すると、ダイアログボックスが表示されます。
5. **OK** をクリックすると、セッションが閉じて自動的にログアウトします。
6. DRAC 5 がリセットした後、**ログイン** をクリックして DRAC 5 にログインします。

ブラウザのキャッシュのクリア

ファームウェアのアップデート後、ウェブブラウザのキャッシュをクリアします。

詳細に関しては、ウェブブラウザのオンラインヘルプを参照してください。

ネットワーク経路による DRAC 5 へのアクセス

DRAC 5 の設定後、次のいずれかのインタフェースを使用して管理下システムにリモートからアクセスできます。

- 1 Web インタフェース
- 1 RACADM
- 1 telnet コンソール
- 1 SSH
- 1 IPMI

[表 2-1](#) で DRAC 5 の各インタフェースについて説明します。

表 2-1. DRAC 5 インタフェース

インタフェース	説明
Web インタフェース	グラフィカルユーザーインタフェースを使用して DRAC 5 へのリモートアクセスを提供します。ウェブインタフェースは DRAC 5 のファームウェアに組み込まれ、管理ステーションで対応 Web ブラウザから NIC インタフェースを介してアクセスします。 対応する Web ブラウザについては、「 対応 Web ブラウザ 」のリストを参照してください。
RACADM	コマンドラインインタフェースを使用して DRAC 5 へのリモートアクセスを提供します。RACADM は管理下システムの IP アドレスを使用して RACADM コマンド (RACADM リモート機能オプション [-r]) を実行します。 メモ: RACADM のリモート機能は、Windows 2000 Server、Windows XP Professional、Windows 2000 Professional、Windows Server 2003、Windows Server 2003 R2、Red Hat Enterprise Linux (バージョン 3 とバージョン 4)、SUSE Linux の各オペレーティングシステムを実行している管理ステーションでのみサポートされています。
telnet コンソール	DRAC 5 を介したサーバー RAC ポートと DRAC 5 NIC を介したハードウェア管理インタフェースへのアクセスを提供し、 powerdown 、 powerup 、 powercycle 、 hardreset コマンドなどのシリアルおよび RACADM コマンドのサポートを提供します。 メモ: Telnet は、パスワードを含むすべてのデータをプレーンテキストで送信するセキュアでないプロトコルです。機密情報を送信する場合は、SSH インタフェースを使用してください。
SSH インタフェース	高度なセキュリティを実現するために暗号トランスポート層を使用して、telnet コンソールと同じ機能を提供します。
IPMI インタフェース	DRAC 5 を介してリモートシステムの基本的な管理機能へのアクセスを提供します。このインタフェースには IPMI オーバー LAN、IPMI オーバーシリアル、およびシリアルオーバー

ース LANが含まれます。詳細に関しては、『Dell OpenManage ベースボード管理コントローラユーザーズガイド』を参照してください。

 **メモ:** DRAC 5 mpデフォルトのユーザー名は root、デフォルトのパスワードは calvin です。

DRAC 5 NIC を介して DRAC 5 のウェブインタフェースにアクセスするには、対応 Web ブラウザか、Server Administrator または IT Assistant を使用します。

サポートされている Web ブラウザについては、「[対応 Web ブラウザ](#)」のリストを参照してください。

対応 Web ブラウザを使用して DRAC 5 にアクセスするには、「[ウェブインタフェースへのアクセス](#)」を参照してください。

Server Administrator を使って DRAC 5 リモートアクセスインタフェースにアクセスするには、Server Administrator を起動します。Server Administrator ホームページの左ペインのシステムツリーから、**システム**→**メインシステムシャーシ**→**Remote Access Controller** の順にクリックします。詳細に関しては、『Server Administrator ユーザーズガイド』を参照してください。

RACADM コマンドラインインタフェースを使用して DRAC 5 にアクセスする方法については、「[RACADM コマンドラインインタフェースの使用](#)」を参照してください。

IPMI の設定

本項では、DRAC 5 IPMI インタフェースの設定と使用について説明します。このインタフェースには以下が含まれています。

- 1 IPMI オーバー LAN
- 1 IPMI オーバーシリアル
- 1 シリアルオーバー LAN

DRAC5 は IPMI 2.0 に完全準拠しています。DRAC IPMI はブラウザを使用するか、ipmitool のようなオープンソースユーティリティを使用するか、Dell OpenManage IPMI シェル ipmish を使用するか、RACADM を使用して設定できます。

IPMI シェル ipmish の使い方の詳細については、デルのサポートウェブサイト support.dell.com にある『Dell OpenManage™ BMC ユーザーズガイド』を参照してください。

RACADM の使い方の詳細に関しては、「[RACADM の使用](#)」を参照してください。

ウェブインタフェースを使用した IPMI の設定

1. 対応 Web ブラウザを使用してリモートシステムにログインします。「[ウェブインタフェースへのアクセス](#)」を参照してください。
2. IPMI オーバー LAN を設定します。

- a. **システム** ツリーで **リモートアクセス** をクリックします。
- b. **設定** タブをクリックして、**ネットワーク** をクリックします。
- c. **ネットワーク設定** ページの **IPMI LAN 設定** で、**IPMI オーバー LAN を有効にする** を選択して **変更の適用** をクリックします。
- d. 必要に応じて、IPMI LAN チャンネルの特権を更新します。

 **メモ:** この設定によって、IPMI オーバー LAN インタフェースから実行できる IPMI コマンドが決まります。詳細に関しては、IPMI 2.0 の仕様を参照してください。

IPMI LAN 設定 で **チャンネル特権レベルの制限** ドロップダウンメニューをクリックし、**システム管理者、オペレータ、ユーザー** のいずれかを選択して **変更の適用** をクリックします。

- e. 必要に応じて、IPMI LAN チャンネルの暗号化キーを設定します。

 **メモ:** DRAC 5 IPMI は RMCP+ プロトコルをサポートしています。

IPMI LAN 設定 の **暗号化キー** フィールドに暗号化キーを入力して、**変更の適用** をクリックします。

 **メモ:** 暗号化キーは、最大 40 文字の偶数の 16 進数文字で構成する必要があります。

3. IPMI シリアルオーバー LAN (SOL) を設定します。

- a. **システム** ツリーで **リモートアクセス** をクリックします。
- b. **設定** タブで **シリアルオーバー LAN** をクリックします。
- c. **シリアルオーバー LAN 設定** ページで **シリアルオーバー LAN を有効にする** を選択します。
- d. IPMI SOL のポーレートを更新します。

 **メモ:** シリアルコンソールを LAN 経由でリダイレクトするには、SOL のポーレートが管理下システムのポーレートと同じであることを確認してください。

- e. **ポーレート** ドロップダウンメニューをクリックし、適切なポーレートを選択して **変更の適用** をクリックします。
- f. **必要な最小特権** を更新します。このプロパティは、**シリアルオーバー LAN** 機能を使用するのに必要な最小限のユーザー特権を定義します。

チャンネル特権レベルの制限 ドロップダウンメニューをクリックし、**ユーザー、オペレータ、システム管理者** のいずれかを選択します。

g. **変更の適用** をクリックします。

4. IPMI シリアルを設定します。

a. **設定** タブで **シリアル** をクリックします。

b. **シリアル設定** メニューで、IPMI シリアル接続モードを適切な設定に変更します。

IPMI シリアル で **接続モード設定** ドロップダウンメニューをクリックして、適切なモードを選択します。

c. IPMI シリアルのボーレートを設定します。

ボーレート ドロップダウンメニューをクリックし、適切なボーレートを選択して **変更の適用** をクリックします。

d. チャンネル特権レベルの制限を設定します。

チャンネル特権レベルの制限 ドロップダウンメニューをクリックし、**ユーザー、オペレータ、システム管理者** のいずれかを選択します。

e. **変更の適用** をクリックします。

f. 管理下システムの BIOS 設定プログラムでシリアル MUX が正しく設定されていることを確認します。

- システムを再起動します。
- POST 中、<F2> を押して BIOS 設定プログラムを入力します。
- **シリアル通信** に移動します。
- **シリアル通信** メニューで、**外部シリアルコネクタ** が **リモートアクセスデバイス** に設定されていることを確認します。
- 保存して BIOS 設定プログラムを終了します。
- システムを再起動します。

IPMI シリアルがターミナルモードの場合は、次の追加設定ができます。

- 1 削除制御
- 1 エコー制御
- 1 ライン編集
- 1 新しいラインシーケンス
- 1 新しいラインシーケンスの入力

これらのプロパティの詳細に関しては、IPMI 2.0 の仕様を参照してください。

RACADM CLI を使用した IPMI の設定

1. RACADM インタフェースのいずれかを使用してリモートシステムにログインします。「[RACADM の使用](#)」を参照してください。
2. IPMI オーバー LAN を設定します。

コマンドプロンプトを開き、次のコマンドを入力して <Enter> を押します。

```
racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
```

 **メモ:** この設定によって、IPMI オーバー LAN インタフェースから実行できる IPMI コマンドが決まります。詳細に関しては、IPMI 2.0 の仕様を参照してください。

a. IPMI チャンネルの特権を更新します。

コマンドプロンプトで次のコマンドを入力し、<Enter> を押します。

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <レベル>
```

<レベル> は次のいずれかになります。

- 2(ユーザー)
- 3(オペレータ)
- 4(システム管理者)

たとえば、IPMI LAN チャンネルの特権を 2(ユーザー)に設定する場合は、次のコマンドを入力します。

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit 2
```

b. 必要に応じて、IPMI LAN チャンネルの暗号化キーを設定します。

 **メモ:** DRAC 5 IPMI は RMCP+ プロトコルをサポートしています。詳細に関しては、IPMI 2.0 の仕様を参照してください。

コマンドプロンプトで次のコマンドを入力し、<Enter> を押します。

```
racadm config -g cfgIpmlan -o cfgIpmlanEncryptionKey <キー>
```

<キー> は有効な 16 進フォーマットの 20 文字の暗号化キーです。

3. IPMI シリアルオーバー LAN(SOL)を設定します。

コマンドプロンプトで次のコマンドを入力し、<Enter> を押します。

```
racadm config -g cfgIpmlan -o cfgIpmlanSolEnable 1
```

a. IPMI SOL の最小特権レベルを更新します。

IPMI SOL の最小限の特権レベルによって、IPMI SOL をアクティブにするのに必要とされる最小特権が決まります。詳細に関しては、IPMI 2.0 の仕様を参照してください。

コマンドプロンプトで次のコマンドを入力し、<Enter> を押します。

```
racadm config -g cfgIpmlan -o cfgIpmlanSolMinPrivilege <レベル>
```

<レベル> は次のいずれかになります。

- 2(ユーザー)
- 3(オペレータ)
- 4(システム管理者)

たとえば、IPMI の特権を 2(ユーザー)に設定する場合は、次のコマンドを入力します。

```
racadm config -g cfgIpmlan -o cfgIpmlanSolMinPrivilege 2
```

b. IPMI SOL のボーレートを更新します。

 **メモ:** シリアルコンソールを LAN 経由でリダイレクトするには、SOL のボーレートが管理下システムのボーレートと同じであることを確認してください。

コマンドプロンプトで次のコマンドを入力し、<Enter> を押します。

```
racadm config -g cfgIpmlan -o cfgIpmlanSolBaudRate <ボーレート>
```

<ボーレート> は 9600、19200、57600、115200 bps のいずれかになります。

例:

```
racadm config -g cfgIpmlan -o cfgIpmlanSolBaudRate 57600
```

c. SOL を有効にします。

 **メモ:** SOL はユーザーごとに有効または無効にできます。

コマンドプロンプトで次のコマンドを入力し、<Enter> を押します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <id> 2
```

<id> はユーザーの固有の ID です。

4. IPMI シリアルを設定します。

a. IPMI シリアル接続モードを適切な設定に変更します。

コマンドプロンプトで次のコマンドを入力し、<Enter> を押します。

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

b. IPMI シリアルのボーレートを設定します。

コマンドプロンプトを開き、次のコマンドを入力して <Enter> を押します。

```
racadm config -g cfgIpmlan -o cfgIpmlanSerialBaudRate <ボーレート>
```

<ボーレート> は 9600、19200、57600、115200 bps のいずれかになります。

例:

```
racadm config -g cfgIpmlan -o cfgIpmlanSerialBaudRate 57600
```

c. IPMI シリアルのハードウェアフロー制御を有効にします。

コマンドプロンプトで次のコマンドを入力し、<Enter> を押します。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1
```

- d. IPMI シリアルノットの最小特権レベルを設定します。

コマンドプロンプトで次のコマンドを入力し、<Enter> を押します。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <レベル>
```

<レベル> は次のいずれかになります。

- o 2(ユーザー)
- o 3(オペレーター)
- o 4(システム管理者)

たとえば、IPMI シリアルチャンネルの特権を 2(ユーザー)に設定する場合は、次のコマンドを入力します。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit 2
```

- e. BIOS 設定プログラムでシリアル MUX が正しく設定されていることを確認します。

- o システムを再起動します。
- o POST 中、<F2> を押して BIOS 設定プログラムを入力します。
- o **シリアル選定** に移動します。
- o **シリアル選定** メニューで、**外部シリアルコネクタ** が **リモートアクセスデバイス** に設定されていることを確認します。
- o 保存して BIOS 設定プログラムを終了します。
- o システムを再起動します。

これで IPMI の設定が完了しました。

IPMI シリアルがターミナルモードの場合は、`racadm config cfgIpmiSerial` コマンドを使用して次の追加設定ができます。

- o 削除制御
- o エコー制御
- o ライン編集
- o 新しいラインシーケンス
- o 新しいラインシーケンスの入力

これらのプロパティの詳細に関しては、IPMI 2.0 の仕様を参照してください。

プラットフォームイベントの設定

プラットフォームイベントの設定は、リモートアクセスデバイスが特定のイベントメッセージについて、選択した処置を実行するように設定するためのメカニズムを提供します。これらの処置には、再起動、パワーサイクル、電源オフ、警告のトリガ (Platform Events Trap [PET] や電子メール) があります。

フィルタ可能なプラットフォームイベントには次のものがあります。

- 1 ファンブロープエラー
- 1 バッテリブロープ警告
- 1 バッテリブロープエラー
- 1 離散的電圧ブロープエラー
- 1 温度ブロープ警告
- 1 温度ブロープエラー
- 1 シャーシントルージョン検出
- 1 冗長性低下
- 1 冗長性喪失
- 1 プロセッサ警告
- 1 プロセッサエラー
- 1 プロセッサの不在
- 1 PS/VRM/D2D 警告
- 1 PS/VRM/D2D エラー

- 1 電源装置の不在
- 1 ハードウェアログ警告
- 1 自動システム回復

プラットフォームイベント(たとえばファンブローブエラー)が発生すると、システムイベントが生成され、システムイベントログ(SEL)に記録されます。このイベントがウェブインタフェースのプラットフォームイベントフィルタ(PEF)リストと一致し、このフィルタが警告(PET や電子メール)を生成するように設定してある場合は、PET または電子メールの警告が 1 つまたは複数の設定済みの宛先に送信されます。

同じプラットフォームフィルタが処置(システムの再起動など)も実行するように設定してある場合は、その処置が実行されます。

プラットフォームイベントフィルタ(PEF)の設定

プラットフォームイベントトラップや電子メール警告設定を指定する前に、プラットフォームイベントフィルタを設定します。

ウェブユーザーインタフェースを使用した PEF の設定

1. 対応 Web ブラウザを使用してリモートシステムにログインします。「[ウェブインタフェースへのアクセス](#)」を参照してください。
2. **警告管理** タブをクリックし、**プラットフォームイベント** をクリックします。
3. グローバル警告を有効にします。
 - a. **警告管理** をクリックし、**プラットフォームイベント** をクリックします。
 - b. **プラットフォームイベントフィルタ警告を有効にする** チェックボックスをオンにします。
4. **プラットフォームのイベントフィルタ設定** で、**プラットフォームイベントフィルタ警告を有効にする** チェックボックスをオンにして **変更の適用** をクリックします。
5. **プラットフォームのイベントフィルタリスト** で、設定するフィルタをダブルクリックします。
6. **プラットフォームイベントの設定** ページで、適切な選択を行って **変更の適用** をクリックします。

 **メモ:** 設定済みの有効な宛先 (PET または e-mail) に警告が送信されるためには、**警告の生成** を有効にする必要があります。

RACADM CLI を使用した PEF の設定

1. PEF を有効にします。

コマンドプロンプトを開き、次のコマンドを入力して <Enter> を押します。

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 1 1
```

1 と 1 は PEF のインデックスで、それぞれ選択を有効 / 無効にします。

PEF のインデックスは 1 ~ 17 の値になります。有効 / 無効の選択は 1(有効)または 0(無効)に設定できます。

たとえば、インデックス 5 の PEF を有効にするには、次のコマンドを入力します。

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 5 1
```

2. PEF の処置を設定します。

コマンドプロンプトで次のコマンドを入力し、<Enter> を押します。

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 <処置>
```

<処置> の値ビットは次のようになります。

- 1 <処置> 値ビット 0-1 = 警告を有効にする、0 = 警告を無効にする
- 1 <処置> 値ビット 1-1 = 電源オフ、0 = 電源オフにしない
- 1 <処置> 値ビット 2-1 = 再起動、0 = 再起動しない
- 1 <処置> 値ビット 3-1 = パワーサイクル、0 = パワーサイクルなし

たとえば、PEF を有効にしてシステムを再起動するには、次のコマンドを入力します。

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 1 2
```

1 は PEF のインデックスで、2 は PEF の処置で再起動を示します。

PET の設定

ウェブユーザーインターフェースを使用した PET の設定

1. 対応 Web ブラウザを使用してリモートシステムにログインします。「[ウェブインタフェースへのアクセス](#)」を参照してください。
2. 必ず「[ウェブインタフェースを使用した PEF の設定](#)」の手順に従ってください。
3. PET のポリシーを設定します。
 - a. **警告管理** タブで **トラップ設定** をクリックします。
 - b. **送信先の設定** で、**コミュニティ文字列** フィールドに適切な情報を入力して **変更の適用** をクリックします。
4. PET の送信先 IP アドレスを設定します。
 - a. **送信先番号** 列で、送信先の番号をクリックします。
 - b. **送信先を有効にする** チェックボックスがオンになっていることを確認します。
 - c. **送信先の IP アドレス** フィールドに、PET の有効な IP アドレスを入力します。
 - d. **変更の適用** をクリックします。
 - e. 必要に応じて **テストトラップの送信** をクリックして、設定した警告をテストします。

 **メモ:** この手順を実行するための **テスト警告権限** がユーザーアカウントに必要です。 [表 4-8](#) を参照してください。

- f. 残りの送信先番号にも a ~ e の手順を繰り返します。

RACADM CLI を使用した PET の設定

1. グローバル警告を有効にします。

コマンドプロンプトを開き、次のコマンドを入力して <Enter> を押します。

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```
2. PET を有効にします。

コマンドプロンプトで次のコマンドを入力し、各コマンドの後で <Enter> を押します。

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
```

1 と 1 は PET の送信先 インデックスで、それぞれ選択を有効 / 無効にします。

PEF の送信先 インデックスは 1 ~ 4 の値になります。有効 / 無効の選択は 1 (有効) または 0 (無効) に設定できます。

たとえば、インデックス 4 の PET を有効にするには、次のコマンドを入力します。

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 0
```
3. PET のポリシーを設定します。

コマンドプロンプトで次のコマンドを入力し、<Enter> を押します。

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i 1 <IP アドレス>
```

1 は PET の送信先インデックスで、<IP アドレス> は、プラットフォームイベント警告を受け取るシステムの宛先 IP アドレスです。
4. コミュニティ文字列を設定します。

コマンドプロンプトで次のように入力します。

```
racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName <名前>
```

電子メール警告の設定

ウェブインタフェースを使用した電子メール警告の設定

1. 対応 Web ブラウザを使用してリモートシステムにログインします。「[ウェブインタフェースへのアクセス](#)」を参照してください。
2. 必ず「[ウェブインタフェースを使用した PEF の設定](#)」の手順に従ってください。
3. 電子メール警告設定を指定します。
 - a. **警告管理** タブで、**電子メール警告設定** をクリックします。
 - b. **SMTP(電子メール) サーバーアドレス** 設定で、**SMTP(電子メール) サーバー IP アドレス** フィールドに適切な情報を入力し、**変更の適用** をクリックします。
4. 電子メール警告の送信先を指定します。
 - a. **電子メール警告番号** 列で、電子メール警告番号をクリックします。
 - b. **電子メール警告を有効にする** チェックボックスがオンになっていることを確認します。
 - c. **送信先電子メールアドレス** フィールドに有効な電子メールアドレスを入力します。
 - d. 必要に応じて、**電子メールの説明** フィールドに説明を入力します。
 - e. **変更の適用** をクリックします。
 - f. 必要に応じて **テスト電子メールの送信** をクリックして、設定した電子メール警告をテストします。

 **メモ:** この手順を実行するための**テスト警告権限**がユーザーアカウントに必要です。[表 4-8](#)を参照してください。

 - g. 残りの電子メール警告設定にも [a](#) ~ [e](#) の手順を繰り返します。
5. グローバル警告を有効にします。
 - a. **警告管理** をクリックし、**プラットフォームイベント** をクリックします。
 - b. **プラットフォームイベントフィルタ警告を有効にする** チェックボックスをオンにします。

RACADM CLI を使用した電子メール警告の設定

1. グローバル警告を有効にします。

コマンドプロンプトを開き、次のコマンドを入力して <Enter> を押します。

```
racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1
```
2. 電子メール警告を有効にする

コマンドプロンプトで次のコマンドを入力し、各コマンドの後で <Enter> を押します。

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
```

1 と 1 は電子メール送信先インデックスで、それぞれ選択を有効 / 無効にします。

電子メール送信先インデックスは 1 ~ 4 の値になります。有効 / 無効の選択は 1(有効)または 0(無効)に設定できます。

たとえば、インデックス 4 の電子メールを有効にするには、次のコマンドを入力します。

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
```
3. 電子メール設定を指定します。

コマンドプロンプトで次のコマンドを入力し、<Enter> を押します。

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <電子メールアドレス>
```

1 は電子メール送信先のインデックスで、<電子メールアドレス> は、プラットフォームイベント警告を受け取る宛先電子メールアドレスです。

カスタムメッセージを設定するには、コマンドプロンプトで次のコマンドを入力して <Enter> を押します。

```
racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 <カスタム_メッセージ>
```

1 は電子メール送信先インデックスで、<カスタム_メッセージ> はカスタムメッセージです。

[目次ページに戻る](#)

[目次ページに戻る](#)

DRAC 5 コマンドラインコンソールの設定と使用

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

- [コマンドラインコンソールの機能](#)
- [管理下システムでシリアルまたは telnet コンソールを使用するための管理下システムの有効化と設定](#)
- [Secure Shell \(SSH\) の使い方](#)
- [DRAC 5 の追加セキュリティオプションを有効にする](#)
- [ローカルシリアルポートまたは Telnet 管理ステーション\(クライアントシステム\)を使った管理下システムへの接続](#)
- [シリアルコンソールの DB-9 ケーブルの接続](#)
- [管理ステーションのターミナルエミュレーションソフトウェアの設定](#)
- [シリアルまたは telnet コンソールの使い方](#)

この項では、DRAC 5 コマンドラインコンソール(またはシリアル /telnet/ssh コンソール)の機能について情報を提供し、コンソールから管理操作を実行できるようにシステムを設定する方法を説明します。

コマンドラインコンソールの機能

DRAC 5 は、次のシリアルおよび telnet コンソール機能をサポートしています。

- 1 単一のシリアルクライアント接続と同時に最大 4 つの telnet クライアント接続が可能
 - 1 同時に最大 4 つの SSH クライアント接続
 - 1 システムシリアルポートと DRAC 5 NIC を使った管理下システムコンソールへのアクセス
 - 1 DRAC 5 の電源導入、電源切断、パワーサイクル、リセット、ログ表示、設定などができるコンソールコマンド
 - 1 スクリプト記述に便利な RACADM コマンドのサポート
 - 1 コマンドラインの編集と履歴
 - 1 シリアルポート経由で出力される管理下システムテキストコンソールを使って接続、表示、対話するための **connect com2** シリアルコマンド (BIOS とオペレーティングシステムを含む)
-  **メモ:** 管理下システムで Linux を実行している場合は、**connect com2** シリアルコマンドが真の Linux コンソールストリームインタフェースを提供します。
- 1 すべてのコンソールインタフェースでタイムアウト制御

管理下システムでシリアルまたは telnet コンソールを使用するための管理下システムの有効化と設定

以下の項では、管理下システムでシリアル/telnet/ssh コンソールを有効にして設定する方法を説明します。

connect com2 シリアルコマンドの使用

connect com2 シリアルコマンドを使用する場合は、次の項目を正しく設定する必要があります。

- 1 BIOS 設定プログラムの **Serial Communication** → **シリアルポート** の設定。
- 1 DRAC の設定。

これらの設定が間違っていると、DRAC 5 に telnet セッションを確立したとき、**connect com2** に空白画面が表示される可能性があります。

管理下システムで BIOS 設定プログラムにシリアル接続を設定する方法

出力をシリアルポートにリダイレクトするように **BIOS 設定** プログラムを設定するには、次の手順を実行してください。

 **メモ:** **セットアップユーティリティ**を**connect com2**コマンドと一緒に設定する必要があります。

- 1 システムをオンにするか、再起動します。
- 2 次のメッセージが表示されたら、ただちに <F2> を押します。

<F2> = System Setup
(<F2>=セットアップユーティリティ)

3. 下にスクロールし、<Enter> を押して **シリアル通信** を選択します。

4. **シリアル通信** 画面を次のように設定します。

外部シリアルコネクタ — リモートアクセスデバイス

起動後のリダイレクト — 無効

5. <Esc> を押して**セットアップ**ユーティリティを終了すると、**セットアップ**ユーティリティの設定が完了します。

リモートサクセスシリアルインタフェースの使用

RAC デバイスへのシリアル接続を確立する場合は、次のインタフェースを使用できます。

- 1 IPMI シリアルインタフェース
- 1 RAC シリアルインタフェース

IPMI シリアルインタフェース

IPMI シリアルインタフェースには次のモードがあります。

- 1 **IPMI ターミナルモード** — シリアルターミナルから送信される ASCII コマンドをサポートしています。コマンドセットは数に限りがあり(電源制御を含む)、16 進数の ASCII 文字で入力する未加工の IPMI コマンドをサポートしています。
- 1 **IPMI 基本モード** — プログラムアクセス用には、ベースボード管理ユーティリティ(BMU)に含まれている IPMI シェル(IPMISH)などのバイナリインタフェースをサポートしています。

RACADM を使用して IPMI モードを設定するには、次の手順を実行してください。

1. RAC シリアルインタフェースを無効にします。

コマンドプロンプトで次のように入力します。

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

2. 適切な IPMI モードを有効にします。

たとえば、コマンドプロンプトで次のように入力します。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode <0 または 1>
```

詳細に関しては、「[DRAC 5 プロパティグループとオブジェクト定義](#)」を参照してください。

RAC シリアルインタフェース

RAC は、RAC の CLI を提供するシリアルコンソールインタフェース(または RAC シリアルコンソール)もサポートしています。これは IPMI では定義されません。システムに **シリアルコンソール** を有効にした RAC カードが含まれている場合は、RAC カードが IPMI シリアル設定を上書きして、RAC CLI シリアルインタフェースが表示されます。

RAC シリアルターミナルインタフェースを有効にするには、**cfgSerialConsoleEnable** プロパティを 1(TRUE)に設定します。

例:

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
```

詳細に関しては、「[cfgSerialConsoleEnable\(読み取り / 書き込み\)](#)」を参照してください。

[表 3-1](#) に、シリアルインタフェースの設定を示します。

表 3-1. シリアルインタフェースの設定

IPMI モード	RAC シリアルコンソール	インタフェース
基本	無効	基本モード
基本	有効	RAC CLI
ターミナル	無効	IPMI ターミナルモード
ターミナル	有効	RAC CLI

Linux に起動中のシリアルコンソールリダイレクトを設定する方法

次の手順は Linux GRand Unified Bootloader (GRUB) にのみ適用します。別のブートローダーを使用する場合も、同様の変更が必要です。

メモ: クライアント VT100 エミュレーションウィンドウを設定する場合は、テキストが正しく表示されるように、リダイレクトされたコンソールを表示するウィンドウまたはアプリケーションを 25 行 x 80 列に設定してください。このように設定しないと、画面の文字化けが発生することがあります。

`/etc/grub.conf` ファイルを次のように編集します。

1. ファイルの一般設定セクションを見つけ、次の 2 行を新たに追加します。

```
serial --unit=1 --speed=57600
terminal --timeout=10 serial
```

2. カーネル行に 2 つのオプションを付け加えます。

```
kernel ..... console=ttyS1,57600
```

3. `/etc/grub.conf` に `splashimage` ディレクティブが含まれている場合は、それをコメントアウトします。

表 3-2 は、この手順で説明した変更を示したサンプル `/etc/grub.conf` ファイルです。

表 3-2. サンプルファイル: `/etc/grub.conf`

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes
# to this file
# (このファイルに変更を加えた後、grub を再実行する必要はありません。)
# NOTICE: You do not have a /boot partition. This means that
#           all kernel and initrd paths are relative to /, e.g.
#           root (hd0,0)
# (注意: /boot パーティションがありません。これは
#         すべての kernel および initrd パスは / に相対しています。例:)
#           kernel /boot/vmlinuz-version ro root=/dev/sdal
#           initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
  root (hd0,0)
  kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sdal hda=ide-scsi console=ttyS0 console=ttyS1,57600
  initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
  root (hd0,0)
  kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sdal s
  initrd /boot/initrd-2.4.9-e.3.im
```

`/etc/grub.conf` ファイルを編集するときは、次のガイドラインに従ってください。

1. GRUB のグラフィカルインタフェースを無効にし、テキストインタフェースを使用します。そうしないと、RAC コンソールリダイレクトで GRUB 画面が表示されません。グラフィカルインタフェースを無効にするには、`splashimage` で始まる行をコメントアウトします。
2. 複数の GRUB オプションを開始して RAC シリアル接続でコンソールセッションを起動するには、すべてのオプションに次の行を追加します。

```
console=ttyS1,57600
```

表 3-2 は、最初のオプションだけに `console=ttyS1,57600` を追加したところを示しています。

起動後のコンソールへのログイン有効化

`/etc/inittab` ファイルを次のように編集します。

次の新しい行を追加して、COM2 シリアルポートで `agetty` を設定します。

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

表 3-3 に、新しい行を追加したサンプルファイルを示します。

表 3-3. サンプルファイル: `/etc/inittab`

```
#
# inittab This file describes how the INIT process should set up
```

```

# the system in a certain run-level. (このファイルでは、INIT
# プロセスの特定したレベルでどのようにシステムを設定するか説明しています。)
#
# Author: Miquel van Smoorenburg
# Modified for RHS Linux by Marc Ewing and Donnie Barnes
# (作者: Miquel van Smoorenburg <miquels@drinkel.nl.mugnet.org
# RHS Linux の編集: Marc Ewing および Donnie Barnes)
#
# Default runlevel. The runlevels used by RHS are:
# (デフォルト runlevel RHS で使われている runlevels:)
# 0 - halt (Do NOT set initdefault to this)
# (中止 [これに initdefault を設定しないでください])
# 1 - Single user mode (シングルユーザーモード)
# 2 - Multiuser, without NFS (The same as 3, if you do not have
# networking)
# (マルチユーザー [NFS なし][ネットワークがない場合は3と同じ])
# 3 - Full multiuser mode (完全マルチユーザーモード)
# 4 - unused (未使用)
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
# (再起動 [これに initdefault を設定しないでください])
#
id:3:initdefault:

# System initialization. (システムの初期化。)
si:sysinit:/etc/rc.d/rc.sysinit

10:0:wait:/etc/rc.d/rc 0
11:1:wait:/etc/rc.d/rc 1
12:2:wait:/etc/rc.d/rc 2
13:3:wait:/etc/rc.d/rc 3
14:4:wait:/etc/rc.d/rc 4
15:5:wait:/etc/rc.d/rc 5
16:6:wait:/etc/rc.d/rc 6

# Things to run in every runlevel. (すべての runlevel で実行する項目。)
ud:once:/sbin/update

# Trap CTRL-ALT-DELETE (トラップ CTRL-ALT-DELETE)
ca:ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few
# minutes of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your
# UPS is connected and working correctly. (UPS が電源喪失を報告した場合、
# それから数分の電源しか残っていないと推測されます。2 分後にシャットダウンを
# スケジュールします。これは 電源が取り付けられていて、UPS がせつぞくされて正常に機能
# していることを前提としています。)
pf:powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
# (シャットダウンする前に電源を回復した場合はキャンセルします。)
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

# Run gettys in standard runlevels (標準 runlevels で gettys を実行します)
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5 (runlevel 5 で xdm を実行)
# xdm is now a separate service (xdm は別のサービスになります)
x:5:respawn:/etc/X11/prefdm -nodaemon

```

/etc/securitytty ファイルを次のように編集します。

COM2 のシリアル tty の名前を使用して次の新しい行を追加します。

```
ttyS1
```

[表 3-4](#) に、新しい行を追加したサンプルファイルを示します。

表 3-4. サンプルファイル: /etc/securitytty

```

vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4

```

```
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

DRAC 5 のシリアル /Telnet/SSH コンソールを有効にする

シリアル /telnet/ssh コンソールはローカルまたはリモートで有効にできます。

シリアル /Telnet/SSH コンソールをローカルで有効にする

 **メモ:** この項の手順を実行するには、システム管理者 (現在のユーザー) に DRAC 5 の設定権限が必要です。

管理下システムからシリアル /telnet/ssh コンソールを有効にするには、コマンドプロンプトで次のローカル RACADM コマンドを入力します。

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

RACADM、シリアル /telnet/ssh、および RACADM コマンドの使い方の詳細については、「[RACADM コマンドラインインタフェースの使用](#)」を参照してください。

シリアル /Telnet/SSH コンソールをリモートで有効にする

シリアル /telnet/ssh コンソールをリモートで有効にするには、コマンドプロンプトから次のリモート RACADM コマンドを入力します。

```
racadm -u <ユーザー名> -p <パスワード> -r <DRAC 5 IP アドレス> config -g cfgSerial cfgSerialConsoleEnable 1
racadm -u <ユーザー名> -p <パスワード> -r <DRAC 5 IP アドレス> config -g cfgSerial cfgSerialTelnetEnable 1
racadm -u <ユーザー名> -p <パスワード> -r <DRAC 5 の IP アドレス> config -g cfgSerial cfgSerialSshEnable 1
```

Racadm コマンドを使用してシリアルおよび telnet コンソールを設定する

このサブセクションでは、シリアル /telnet/ssh コンソールリダイレクトのデフォルトの設定手順について説明します。

設定するには、適切なグループ、プロパティ、プロパティの値を使用して RACADM config コマンドを入力します。

RACADM コマンドはローカルおよびリモートで入力できます。RACADM コマンドをリモートで使用する場合は、ユーザー名、パスワード、および管理下システムの DRAC 5 の IP アドレスを入力する必要があります。

使用可能なシリアル /telnet/ssh および RACADM CLI コマンドについては、「[RACADM コマンドラインインタフェースの使用](#)」を参照してください。

racadm のローカルでの使い方

RACADM コマンドをローカルで使用する場合は、管理下システムのコマンドプロンプトから次のコマンドを入力します。

```
racadm config -g <グループ> -o <プロパティ> <値>
```

プロパティのリストを表示するには、管理下システムのコマンドプロンプトから次のコマンドを入力します。

```
racadm getconfig -g <グループ>
```

Racadm をリモートで使用する

RACADM コマンドをリモートで使用するには、管理ステーションのコマンドプロンプトから次のコマンドを入力します。

```
racadm -u <ユーザー名> -p <パスワード> -r <DRAC 5 の IP アドレス> config -g <グループ> -o <プロパティ> <値>
```

RACADM をリモートで使用する前に、Web サーバーに DRAC 5 が設定されていることを確認してください。そうでないと、RACADM がタイムアウトになり、次のようなメッセージが表示されます。

```
Unable to connect to RAC at specified IP address.
(指定された IP アドレスの RAC に接続できません。)
```

Secure Shell (SSH)、telnet、またはローカル RACADM を使用して Web サーバーを有効にするには、管理ステーションでコマンドプロンプトから次のコマンドを入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneWebServerEnable 1
```

設定の表示

[表 3-5](#) に、設定を表示するための処置と関連コマンドを示します。コマンドを実行するには、管理下システムでコマンドプロンプトを開き、コマンドを入力して <Enter> を押します。

表 3-5. 設定の表示

処置	コマンド
使用可能なグループをリストにします。	racadm getconfig -h
特定のグループの現在の設定を表示します。	racadm getconfig -g <グループ> たとえば、 cfgSerial グループの設定をすべて表示するには、次のコマンドを入力します。 racadm getconfig -g cfgSerial
特定のグループの現在の設定をリモートで表示します。	racadm -u <ユーザー> -p <パスワード> -r <DRAC 5 IP アドレス> getconfig -g cfgSerial たとえば、リモートで cfgSerial グループの設定をすべて表示するには、次のコマンドを入力します。 racadm -u root -p calvin -r 192.168.0.1 getconfig -g cfgSerial

Telnet ポート番号の設定

DRAC 5 の telnet ポート番号を変更するには、次のコマンドを入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort <新しいポート番号>
```

Secure Shell (SSH) の使用

システムのデバイスとデバイス管理が安全であることが重要です。接続している組み込みデバイスは多くのビジネスプロセスで中心的な役割を果たしています。これらのデバイスに不正侵入が発生すると、顧客のビジネスにリスクが生じるため、コマンドラインインタフェース (CLI) のデバイス管理ソフトウェアに新たなセキュリティ対策が必要になります。

Secure Shell (SSH) は、telnet セッションと同じ機能を備えていますが、さらにセキュリティが強化されたコマンドラインセッションです。DRAC 5 は、パスワード認証付きの SSH バージョン 2 をサポートしています。DRAC 5 ファームウェアをインストールまたはアップデートすると、DRAC 5 上の SSH が有効になります。

管理ステーションの PuTTY または OpenSSH を使って、管理下システムの DRAC 5 に接続します。ログイン手続中にエラーが発生すると、セキュアシェルクライアントからエラーメッセージが発行されます。メッセージのテキストはクライアントによって異なり、DRAC 5 ではコントロールできません。

 **メモ:** OpenSSH は Windows の VT100 または ANSI ターミナルエミュレータから実行する必要があります。Windows のコマンドプロンプトで OpenSSH を実行すると、完全には機能しません (一部のキーが応答せず、グラフィックが表示されません)。

1 度にサポートされる SSH セッションは 4 つだけです。セッションのタイムアウトは `cfgSsnMgtSshIdleTimeout` プロパティによって制御されます ([「DRAC 5 プロパティのデータベースグループとオブジェクトの定義」](#)を参照)。

次のコマンドで DRAC 5 の SSH を有効にできます。

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

次のコマンドで SSH ポートを変更できます。

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort <ポート番号>
```

`cfgSerialSshEnable` および `cfgRacTuneSshPort` プロパティの詳細については、「[DRAC 5 プロパティのデータベースグループとオブジェクトの定義](#)」を参照してください。

DRAC 5 の SSH の実装では、[表 3-6](#) に示すように複数の暗号化スキームがサポートされています。

表 3-6. 暗号化スキーム

スキームの種類	スキーム
非対称暗号	Diffie-Hellman DSA/DSS 512-1024 (ランダム) ビット (NIST 仕様当り)
対称暗号	1 AES256-CBC 1 RIJNDAEL256-CBC 1 AES192-CBC 1 RIJNDAEL192-CBC 1 AES128-CBC 1 RIJNDAEL128-CBC 1 BLOWFISH-128-CBC

	<ul style="list-style-type: none"> 1 3DES-192-CBC 1 ARCFOUR-128
メッセージの整合性	<ul style="list-style-type: none"> 1 HMAC-SHA1-160 1 HMAC-SHA1-96 1 HMAC-MD5-128 1 HMAC-MD5-96
認証	<ul style="list-style-type: none"> 1 パスワード

 **メモ:** SSHv1 はサポートされていません。

DRAC 5 の追加セキュリティオプションを有効にする

リモートシステムへの不正アクセスを防ぐため、DRAC 5 では次の機能を提供しています。

- 1 IP アドレスのフィルタ (IPRange) — DRAC 5 にアクセスできる特定の IP アドレス範囲を定義します。
- 1 IP アドレスのブロック — 特定の IP アドレスからのログイン試行の失敗回数を制限します。

これらの機能は DRAC 5 のデフォルト設定では無効になっています。次のサブコマンドまたはウェブインタフェースを使用して、これらの機能を有効にしてください。

```
racadm config -g cfgRacTuning -o <オブジェクト名> <値>
```

さらに、これらの機能をセッションのアイドルタイムアウト値や、ネットワークに定義済みのセキュリティプランと一緒に使用してください。

以下のサブセクションでは、これらの機能について詳しく説明します。

IP フィルタ (IpRange)

IP アドレスフィルタ (または IP 範囲チェック) を使用すると、ユーザーが特定した範囲内にある IP アドレスのクライアントワークステーションや管理ワークステーションからのみ DRAC 5 へのアクセスを許可できます。その他のログインはすべて拒否されます。

IP フィルタは着信ログインの IP アドレスを、次の `cfgRacTuning` プロパティで指定する IP アドレス範囲と比べます。

- 1 `cfgRacTuneIpRangeAddr`
- 1 `cfgRacTuneIpRangeMask`

`cfgRacTuneIpRangeMask` プロパティは着信 IP アドレスと `cfgRacTuneIpRangeAddr` プロパティの両方に適用されます。両方のプロパティの結果が同じであれば、着信ログイン要求が DRAC 5 へのアクセスを許可されます。この範囲外の IP アドレスからのログインはエラーを受け取ります。

次の式がゼロと等しい場合に、ログインが続行します。

```
cfgRacTuneIpRangeMask & (<着信 IP アドレス> ^ cfgRacTuneIpRangeAddr)
```

& は数量のビットワイズの AND で、^ はビットワイズの exclusive-OR です。

`cfgRacTune` の全リストは「[DRAC 5 プロパティのデータベースグループとオブジェクトの定義](#)」に掲載されています。

表 3-7. IP アドレスフィルタ (IpRange) のプロパティ

プロパティ	説明
<code>cfgRacTuneIpRangeEnable</code>	IP アドレスのチェック機能を有効にします。
<code>cfgRacTuneIpRangeAddr</code>	サブネットマスクの 1 によって、受け入れる IP アドレスビットパターンを決定します。 このプロパティはビットワイズの AND'd と <code>cfgRacTuneIpRangeMask</code> で、許可する IP アドレスの上位部分を決定します。上位ビットにこのビットパターンを含んでいる IP アドレスは、DRAC 5 とのセッションを確立できます。この範囲外の IP アドレスからのログインは失敗します。DRAC 5 セッションを確立するには、各プロパティのデフォルト値に 192.168.1.0 ~ 192.168.1.255 を使用できます。
<code>cfgRacTuneIpRangeMask</code>	IP アドレスの重要なビット位置を定義します。サブネットマスクはネットマスクの形態で、より重要なビットがすべて 1 となり、下位のビットでは 1 回の遷移ですべてゼロになります。

IP フィルタを有効にする

以下は、IP フィルタ設定のコマンド例です。

RACADM と RACADM コマンドの詳細に関しては、「[RACADM の使用](#)」を参照してください。

 **メモ:** 次の RACADM コマンドは 192.168.0.57 以外のすべての IP アドレスをブロックします。

ログインを1つのIPアドレスに限定するには(たとえば192.168.0.57)、次のように完全マスクを使用してください。

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.57
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.255
```

ログインを4つの連続するIPアドレスに限定するには(192.168.0.212 ~ 192.168.0.215)、次のようにマスクの最下位の2ビットを除くすべてを選択します。

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.252
```

IPフィルタのガイドライン

IPフィルタを有効にする場合は、次のガイドラインに従ってください。

- 1 `cfgRacTunelpRangeMask` がネットマスクの形態で設定されるようにします。最重要ビットがすべて1で(これがマスクのサブネットを定義)、下位のビットではすべてゼロに遷移します。
- 1 必要な範囲の基底アドレスを `cfgRacTunelpRangeAddr` の値として使用します。このアドレスの32ビットのバイナリ値は、マスクにゼロがある下位ビットのすべてでゼロになる必要があります。

IPブロック

IPブロックは、事前に選択した時間内に特定のIPアドレスからのログイン失敗回数が過剰になる時を動的に決定し、そのアドレスがDRAC 5にログインするのをブロック(防止)します。

IPブロックのパラメータは、次のような `cfgRacTuning` グループ機能を使用します。

- 1 許可するログイン失敗回数 (`cfgRacTunelpBlkFailcount`)
- 1 これらの失敗を数える時間枠(秒) (`cfgRacTunelpBlkFailWindow`)
- 1 失敗の合計許可回数を超えた後、「有罪」のIPアドレスのセッション確立が防止される時間(秒) (`cfgRacTunelpBlkPenaltyTime`)

特定のIPアドレスからのログイン失敗が累積すると、それらは内部カウンタによって「経年」されます。ユーザーがログインに成功すると、失敗履歴はクリアされ、内部カウンタがリセットされます。



メモ: クライアントIPアドレスからのログイン試行が拒否されると、SSHに「ssh exchange identification: Connection closed by remote host」のようなメッセージが表示される場合があります。

`cfgRacTune` の全リストは「[DRAC 5 プロパティのデータベースグループとオブジェクトの定義](#)」に掲載されています。

[表 3-8](#) にユーザー定義のパラメータをリストにします。

表 3-8. ログイン試行制限のプロパティ

プロパティ	定義
<code>cfgRacTunelpBlkEnable</code>	IPブロック機能を有効にします。 一定時間内に(<code>cfgRacTunelpBlkFailWindow</code>)1つのIPアドレスからの失敗が連続すると(<code>cfgRacTunelpBlkFailCount</code>)、以降そのアドレスからのセッション確立試行がすべて一定の時間(<code>cfgRacTunelpBlkPenaltyTime</code>)拒否されます。
<code>cfgRacTunelpBlkFailCount</code>	ログイン試行を拒否するまでのIPアドレスのログイン失敗回数を設定します。
<code>cfgRacTunelpBlkFailWindow</code>	失敗回数を数える時間枠を秒で指定します。失敗がこの制限を越えると、カウンタからドロップされます。
<code>cfgRacTunelpBlkPenaltyTime</code>	失敗が制限を越えたIPアドレスからのセッションをすべて拒否する時間枠を秒で定義します。

IPブロックを有効にする

次の例では、クライアントが1分間に5回ログイン試行に失敗した場合に、5分間このクライアントIPアドレスのセッション確立を防止します。

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

次の例は、1分以内に失敗が3回を超えた場合に、1時間ログイン試行を防止します。

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkEnable 1
```

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 3600
```

ローカルシリアルポートまたは Telnet 管理ステーション(クライアントシステム)を使った管理下システムへの接続

管理下システムでは、システム上の DRAC 5 とシリアルポート間をアクセスでき、管理下システムの電源オン、電源オフ、リセット、およびログへのアクセスが可能になります。

シリアルコンソールは、管理下システムの外付けのシリアルコネクタを使って DRAC 5 で使用できます。アクティブなシリアルクライアントシステム(管理ステーション)は 1 つだけです。DRAC 5 では DRAC モードで telnet および SSH コンソールを使用できます(「[DRAC のモード](#)」を参照)。一度に最大 4 台の telnet クライアントシステムと 4 台の SSH クライアントを接続できます。管理ステーションから管理下システムのシリアルまたは telnet コンソールへの接続には、管理ステーションのターミナルエミュレーションソフトウェアが必要です。詳細に関しては、「[管理ステーションターミナルエミュレーションソフトウェアの設定](#)」を参照してください。

以下のサブセクションでは、次の方法を使用して管理ステーションを管理下システムに接続する方法を説明します。

- 1 ターミナルソフトウェアとヌルモデムケーブルを使用する管理下システムの外部シリアルポート
- 1 管理下システムの DRAC 5 NIC または共有のチーム NIC からターミナルソフトウェアを使用する telnet 接続

シリアルコンソールの DB-9 ケーブルの接続

シリアルテキストコンソールを使って管理下システムにアクセスするには、DB-9 ヌルモデムケーブルを管理下システムの COM ポートに接続します。DB-9 ケーブルのすべてが、この接続に必要なピン配置 / 信号を備えているわけではありません。この接続用の DB-9 ケーブルは、[表 3-9](#) で示した仕様に一致している必要があります。

 **メモ:** DB-9 ケーブルは、BIOS テキストコンソールリダイレクトにも使用できます。

表 3-9. DB-9 ヌルモデムケーブルに必要なピンアウト

信号名	DB-9 ピン(サーバーピン)	DB-9 ピン(ワークステーションピン)
FG (Frame Ground)	–	–
TD (Transmit Data)	3	2
RD (Receive Data)	2	3
RTS (Request To Send)	7	8
CTS (Clear To Send)	8	7
SG (Signal Ground)	5	5
DSR (Data Set Ready)	6	4
CD (Carrier Detect)	1	4
DTR (Data Terminal Ready)	4	1 および 6

管理ステーションのターミナルエミュレーションソフトウェアの設定

DRAC 5 は、次のいずれかのタイプのターミナルエミュレーションソフトウェアを実行中の管理ステーションからのシリアルまたは telnet テキストコンソールをサポートしています。

- 1 Linux Minicom in an Xterm
- 1 Hilgraeve's HyperTerminal Private Edition (バージョン 6.3)
- 1 Linux Telnet in an Xterm
- 1 Microsoft® Telnet

使用するタイプのターミナルソフトウェアを設定するには、以下の項の手順に従ってください。Microsoft Telnet を使用している場合は、設定は不要です。

Linux Minicom でのシリアルコンソールエミュレーションの設定

Minicom は Linux 用のシリアルポートアクセスユーティリティです。以下の手順は、Minicom のバージョン 2.0 に使用できます。他のバージョンでは若干異なる場合がありますが、基本的な設定方法は同じです。他のバージョンの Minicom を設定するには、「[シリアルコンソールエミュレーションに必要な Minicom の設定](#)」を参照してください。

Minicom バージョン 2.0 でのシリアルコンソールエミュレーションの設定

 **メモ:** テキストが正しく表示されるように、Linux のインストールで提供されるデフォルトウィンドウでなく、Xterm のウィンドウを使って telnet コンソールを表示することをお勧めします。

1. 新しい Xterm セッションを開始するには、コマンドプロンプトで `xterm &` と入力します。
2. Xterm ウィンドウで、マウス矢印をウィンドウの右下端に移動し、ウィンドウを 80 x 25 にサイズ変更します。
3. Minicom の設定ファイルがない場合は、次のステップに進みます。
Minicom 設定ファイルがある場合は、`minicom <Minicom config ファイル名>` と入力して、[手順 17](#)に進みます。
4. Xterm コマンドプロンプトで `minicom-s` と入力します。
5. **シリアルポートセットアップ** を選択して、<Enter>を押します。
6. <a>を押して、該当するシリアルデバイスを選択します(例 `/dev/ttyS0`)。
7. <e>を押して、**Bps/Par/Bits** オプションを **57600 8N1** に設定します。
8. <f>を押して、**ハードウェアフロー制御** を **はい** に設定し、**ソフトウェアフロー制御** を **いいえ** に設定します。
9. **シリアルポートセットアップ** を終了するには、<Enter>を押します。
10. **モデムとダイヤル** を選択して、<Enter>を押します。
11. **モデムダイヤルとパラメーターのセットアップ** メニューで、<Backspace>を押して **初期化、リセット、接続、および切断** 設定をクリアすると、設定が空白になります。
12. <Enter>を押して空白の値をそれぞれ保存します。
13. 指定のフィールドをすべてクリアする場合は、<Enter >を押して **モデムダイヤルとパラメータのセットアップ** メニューを終了します。
14. **セットアップを config_name として保存** を選択し、<Enter>を押します。
15. **Minicom から終了** を選択し、<Enter>を押します。
16. コマンドシェルプロンプトで、`minicom <Minicom config ファイル名>` と入力します。
17. Minicom ウィンドウを 80 x 25 に拡大するには、ウィンドウの隅をドラッグします。
18. <Ctrl+a>、<Z>、<X>を押して Minicom を終了します。

 **メモ:** シリアルテキストコンソールダイレクトに Minicom を使用して、管理下システムの BIOS を設定する場合は、Minicom で色をオンにすることをお勧めします。色をオンにするには、コマンドプロンプトで次のコマンドを入力します。 `minicom -c on`

Minicom ウィンドウに `[DRAC 5√root]#` などのコマンドプロンプトが表示されるのを確認します。コマンドプロンプトが表示されたら、正常に接続したことになり、**connect** シリアルコマンドを使って管理下システムコンソールに接続できます。

Minicom でのシリアルコンソールエミュレーションの設定

Minicom を設定するには、[表 3-10](#) を使用します。

表 3-10. Minicom でのシリアルコンソールエミュレーションの設定

設定の説明	必要な設定
Bps/Par/Bits	57600 8N1
ハードウェアフロー制御	必要
ソフトウェアフロー制御	不要
ターミナルエミュレーション	ANSI
モデムダイヤルとパラメーターの設定	初期化、リセット、接続、および切断 設定をクリアして空白にします。
ウィンドウのサイズ	80 x 25 (サイズ変更するには、ウィンドウの隅をドラッグする)

ハイパーターミナルでのシリアルコンソールリダイレクトの設定

HyperTerminal は Microsoft Windows のシリアルポートアクセスユーティリティです。コンソール画面のサイズを正しく設定するには、Hilgraeve の HyperTerminal Private Edition バージョン 6.3 を使用します。

シリアルコンソールリダイレクト用に HyperTerminal を設定するには、次の手順に従ってください。

1. HyperTerminal プログラムを起動します。
2. 新しい接続名を入力して、**OK** をクリックします。
3. **使用する接続方法**：の横から、DB-9 スルモデムケーブルを接続した管理ステーション上の COM ポート(たとえば、COM2)を選択し、**OK** をクリックします。
4. [表 3-11](#) のように COM ポートを設定します。
5. **OK** をクリックします。
6. **ファイル**→**プロパティ**の順にクリックし、**設定** タブをクリックします。
7. **Telnet ターミナル ID**：を **ANSI** に設定します。
8. **ターミナル設定** をクリックして、**画面の列** を **26** に設定します。
9. **列** を **80** に設定して、**OK** をクリックします。

表 3-11. 管理ステーションの COM ポート設定

設定の説明	必要な設定
ビット/秒	57600
データビット	8
パリティ	なし
ストップビット	1
フロー制御	ハードウェア

HyperTerminal ウィンドウに、[DRAC 5\root]# などのコマンドプロンプトが表示されます。コマンドプロンプトが表示されたら、接続が確立し、**connect com2** シリアルコマンドを使って管理下システムコンソールに接続する準備ができています。

Linux XTerm での Telnet コンソールリダイレクトの設定

この項のステップを実行するときは、次のガイドラインに従ってください。

1. telnet コンソール経由で **connect com2** コマンドを使ってシステム設定画面を表示する場合は、システム設定と telnet セッションで、ターミナルタイプを **ANSI** に設定します。
1. テキストが正しく表示されるように、Linux のインストールで提供されるデフォルトウィンドウでなく、Xterm のウィンドウを使って telnet コンソールを表示することをお勧めします。

Linux で telnet を実行するには、次の手順を実行してください。

1. Xterm の新しいセッションを開始します。
コマンドプロンプトで `xterm &` と入力します。
2. マウスの矢印を使って、XTerm ウィンドウの右下隅をクリックしてウィンドウのサイズを 80 x 25 に変更します。
3. 管理下システムの DRAC 5 に接続します。
Xterm プロンプトで、`telnet <DRAC 5 の IP アドレス>` と入力します。

telnet コンソールリダイレクト用に Microsoft Telnet を有効にする

 **メモ**：Microsoft オペレーティングシステム環境の telnet クライアントの中には、BIOS コンソールリダイレクトが VT100 のエミュレーションに設定されていると、BIOS 設定画面が正しく表示されない場合があります。この不具合は、BIOS コンソールリダイレクトを ANSI モードに変えてディスプレイを更新すると解決します。BIOS 設定メニューでこの手順を実行するには、**コンソールリダイレクト** → **リモートターミナルタイプ** → **ANSI** の順に選択します。

1. **Windows Component Services** で **Telnet** を有効にします。

2. 管理ステーションの DRAC 5 に接続します。

コマンドプロンプトを開き、次のコマンドを入力して <Enter> を押します。

```
telnet <IP アドレス>:<ポート番号>
```

IP アドレス は DRAC 5 の IP アドレスで、ポート番号 は telnet のポート番号です(新しいポートを使用している場合)。

Telnet セッションのバックスペースキーの設定

クライアントによっては、<Backspace> キーを使用すると、不測の結果が生じることがあります。たとえば、セッションが ^h をエコーする場合があります。ただし、ほとんどの Microsoft および Linux telnet クライアントでは <Backspace> キーを使えるように設定できます。

Microsoft telnet クライアントで <Backspace> キーを使えるように設定するには、次の手順を実行してください。

1. コマンドプロンプトウィンドウを開きます(必要な場合)。
2. telnet セッションを実行していない場合は、次のように入力します。

```
Telnet
```

telnet セッションを実行している場合は、<Ctrl><|> を押します。

3. プロンプトで次のように入力します。

```
set bsasdel
```

次のメッセージが表示されます。

```
Backspace will be sent as delete.
```

(Backspace が削除として送信されます。)

Linux の telnet セッションで <Backspace> キーを使えるように設定するには、次の手順を実行してください。

1. コマンドプロンプトを開き、次のように入力します。

```
stty erase ^h
```

2. プロンプトで次のように入力します。

```
Telnet
```

シリアルまたは telnet コンソールの使い方

Serial および telnet コマンドと RACADM CLI はシリアルまたは telnet コンソールで入力し、ローカルまたはリモートからサーバーで実行できます。ローカルの RACADM CLI はルートユーザー専用でインストールされます。

シリアル /telnet/ssh コマンド、および RACADM CLI の詳細については、「[RACADM コマンドラインインタフェースの使用](#)」を参照してください。

Windows XP または Windows 2003 を使用した Telnet の実行

管理ステーションで Windows XP または Windows 2003 を実行している場合は、DRAC 5 の telnet セッションで文字の不具合が発生する可能性があります。リターンキーが応答しなかったり、パスワードプロンプトが表示されないなど、ログインの停止が発生することがあります。

この不具合を修正するには、Microsoft のサポートウェブサイト support.microsoft.com から修正プログラム 824810 をダウンロードしてください。詳細に関しては、Microsoft Knowledge Base の記事 824810 を参照してください。

Windows 2000 を使用した Telnet の実行

管理ステーションで Windows 2000 を実行している場合は、<F2> キーを押して BIOS 設定にアクセスすることができません。この不具合は、Microsoft から無料でダウンロードできる Windows Services for UNIX@ 3.5 に同梱されている telnet クライアントを使用すると解決します。Windows Services for UNIX 3.5 は、www.microsoft.com/windows/sfu/downloads/default.asp からダウンロードできます。

[目次ページに戻る](#)

[目次ページに戻る](#)

ウェブインタフェースを使用した DRAC 5 の設定

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

- [Web インタフェースへのアクセス](#)
- [DRAC 5 NIC の設定](#)
- [DRAC 5 ユーザーの追加と設定](#)
- [Active Directory 証明書の設定と管理](#)
- [SSL とデジタル証明書を使用した DRAC 5 通信のセキュリティ](#)
- [シリアルおよびターミナルモードの設定](#)
- [シリアルオーバー LAN の設定](#)
- [設定サービス](#)
- [よくあるお問い合わせ \(FAQ\)](#)

DRAC 5 のウェブインタフェースと Racadm CLI (コマンドラインインタフェース) を使用すると、DRAC 5 のプロパティやユーザーの設定、リモート管理タスクの実行、リモート管理システムの問題のトラブルシューティングなどができます。日常のシステム管理では、DRAC 5 のウェブインタフェースを使用します。この章では、DRAC 5 のウェブインタフェースを使って一般的なシステム管理タスクを実行する方法について説明し、関連情報へのリンクも掲載します。

ウェブインタフェースの設定タスクは RACADM から実行することもできます。テキストベースの各タスクの実行に使用する Racadm CLI およびシリアル/ telnet コンソールの全コマンドについては、「[RACADM コマンドラインインタフェースの使用](#)」のリストを参照してください。

各ウェブインタフェースページのコンテキスト別の情報については、DRAC 5 オンラインヘルプを参照してください。

ウェブインタフェースへのアクセス

DRAC 5 ウェブインタフェースにアクセスするには、次の手順を実行してください。

1. 対応 Web ブラウザのウィンドウを開きます。

詳細については、「[対応 Web ブラウザ](#)」を参照してください。

2. **アドレス** フィールドに次のように入力し、<Enter> を押します。

https://<IP アドレス>

デフォルトの HTTPS ポート番号 (ポート 443) が変更されていたら、次のように入力します。

https://<IPアドレス>:<ポート番号>

「IPアドレス」はDRAC 5用のIPアドレスで、「ポート番号」はHTTPSポート番号です。

DRAC 5 **ログイン** ウィンドウが表示されます。

ログイン

DRAC 5 ユーザーまたは Microsoft® Active Directory® ユーザーとしてログインできます。デフォルトのユーザー名は **root**、デフォルトのパスワードは **calvin** です。

DRAC 5 にログインする前に、**DRAC 5 へのログイン**権限があることを確認してください。

ログインするには、次の手順を実行してください。

1. **ユーザー名** フィールドで、次の 1 つを入力します。

- 1 DRAC 5 のユーザー名

たとえば、<ユーザー名>

ローカルユーザーの DRAC 5 ユーザー名は大文字と小文字が区別されます。

- 1 Active Directory ユーザー名。

たとえば、<ドメイン>*<ユーザー名>、<ドメイン>/<ユーザー名>、<ユーザー>@<ドメイン> などです。

Active Directory ユーザー名の例: **dell.com*john_doe** または **john_doe@dell.com** です。

Active Directory ユーザー名は大文字と小文字が区別されません。

2. **パスワード** フィールドに、DRAC 5 ユーザーパスワードまたは Active Directory ユーザーパスワードを入力します。

このフィールドは大文字と小文字が区別されます。

3. **OK** をクリックするか、<Enter> を押します。

ログアウト

1. セッションを終了するには、DRAC 5 ウェブインタフェースウィンドウの右上隅の **ログアウト** をクリックします。
2. ブラウザのウィンドウを閉じます。

 **メモ:** ログインするまで **ログアウト** ボタンは表示されません。

 **メモ:** 正常にログアウトせずにブラウザを閉じると、セッションはタイムアウトになるまで開いたままになります。ログアウトボタンをクリックしてセッションを終了することをお勧めします。ログアウトしなければ、タイムアウトになるまでセッションが開いたままになります。

 **メモ:** Microsoft Internet Explorer で、ウィンドウの右上端の閉じるボタン("X")を使用して DRAC 5 ウェブベースインタフェースを閉じると、アプリケーションエラーが発生する可能性があります。この不具合を修正するには、Microsoft Support ウェブサイト(support.microsoft.com)から Internet Explorer 用の最新の Cumulative Security Update をダウンロードします。

DRAC 5 NIC の設定

ネットワークと IPMI LAN の設定

 **メモ:** 次の手順を実行するには、**DRAC 5 の設定権限**が必要です。

 **メモ:** ほとんどの DHCP サーバーでは、クライアント識別トークンをその予約テーブルに保存する必要があります。このトークンはクライアント(例、DRAC 5)が DHCP ネゴシエーション中に提供します。RAC の場合、DRAC 5 は 6 バイトの MAC アドレスに続いて 1 バイトのインタフェース番号(0)を使用してクライアント識別オプションを提供します。

 **メモ:** 管理下システムの DRAC が **共有**または**フェールオーバー付き共有** モードに設定され、スパニングツリープロトコル(STP)が有効のスイッチに接続している場合は、STP 変換中に管理ステーションの LOM リンク状態が変わると、ネットワーククライアントの接続に 20 ~ 30 秒の遅延が生じます。

1. システム ツリーで **リモートアクセス** をクリックします。
2. **設定** タブをクリックして、**ネットワーク** をクリックします。
3. **ネットワーク設定** ページで、DRAC 5 NIC を設定します。

[表 4-1](#) と [表 4-2](#) で、**ネットワーク設定** ページの **ネットワーク設定** と **IPMI 設定** について説明します。

4. 設定が完了すると、**変更の適用** をクリックします。
5. **ネットワーク設定** ページの適切なボタンをクリックして続行します。[表 4-3](#) を参照してください。

表 4-1. ネットワーク設定

設定	説明
NIC の選択	選択した NIC モード(専用 、 フェールオーバー と 共有 または 共有する)が表示されます。 デフォルト設定は 専用 です。
MAC アドレス	DRAC 5 の MAC アドレスを表示します。
NIC 有効	DRAC 5 NIC を有効にし、このグループの残りのコントロールをアクティブにします。 デフォルト設定は 有効 です。
DHCP を使用 (NIC IP アドレス用)	Dell OpenManage™ Server Administrator が動的ホスト構成プロトコル(DHCP)サーバーから DRAC 5 NIC IP アドレスを取得できるようにします。チェックボックスをオンにすると、 静的 IP アドレス 、 静的ゲートウェイ 、および 静的サブネットマスク のコントロールが無効になります。 デフォルト設定は 無効 です。
静的 IP アドレス	DRAC 5 NIC の静的 IP アドレスを指定または編集します。この設定を変更するには、 DHCP を使用 (NIC IP アドレス用) チェックボックスをオフにします。
静的ゲートウェイ	DRAC 5 NIC の静的ゲートウェイを指定または編集します。この設定を変更するには、 DHCP を使用 (NIC IP アドレス用) チェックボックスをオフにします。
静的サブネットマスク	DRAC 5 NIC の静的サブネットマスクを指定または編集します。この設定を変更するには、 DHCP を使用 (NIC IP アドレス用) チェックボックスをオフにします。
DHCP を使用して DNS サーバーアドレスを取得する	静的な設定ではなく DHCP サーバーから、一次および二次の DNS サーバー アドレスを取得します。 デフォルト設定は 無効 です。
静的優先 DNS サーバー	DHCP を使用して DNS サーバーアドレスを取得する が 選択されていない 場合のみ、一次 DNS サーバーの IP アドレスを使用します。
静的代替 DNS サーバー	DHCP を使用して DNS サーバーアドレスを取得する が 選択されていない 場合は、二次 DNS サーバーの IP アドレスを使用します。代替 DNS サーバーがない場合は、IP アドレスに「0.0.0.0」と入力します。

DNS に DRAC を登録	DNS サーバーに DRAC 5 の名前を登録します。 デフォルト設定は 無効 です。
DNS DRAC の名前	DNS に DRAC 5 を登録 が選択されている場合にのみ、DRAC 5 の名前が表示されます。RAC 5 のデフォルト名は RAC-service tag です。service tag は Dell サーバーのサービスタグ番号です(例: RAC-EK00002)。
DNS ドメイン名の DHCP を使用	デフォルトの DNS ドメイン名を使用します。このチェックボックスがオフで、DNS に DRAC 5 を登録 オプションがオンの場合は、DNS ドメイン名 フィールドで DNS ドメイン名を変更できます。 デフォルト設定は 無効 です。
DNS ドメイン名	デフォルトの DNS ドメイン名は MYDOMAIN です。DNS ドメイン名に DHCP を使用 チェックボックスがオンになっていると、このオプションはグレー表示になり、変更できません。
オートネゴシエーション	DRAC が最も近いルーターまたはハブと通信して自動的に 二重モード と ネットワーク速度 を設定するか(オン)、 二重モード と ネットワーク速度 を手動で設定するか(オフ)を決定します。
ネットワーク速度	ネットワーク環境に合わせてネットワーク速度を 100Mb または 10 Mb に設定します。 オートネゴシエーション が オン の場合、このオプションは使用できません。
二重モード	ネットワーク環境に合わせて、通信モードを全二重または半二重に設定します。 オートネゴシエーション が オン の場合、このオプションは使用できません。

表 4-2. IPMI LAN の設定

設定	説明
IPMI オーバー LAN を有効にする	IPMI LAN チャネルを有効にします。
チャネル特権レベルの制限	LAN チャネルで受け入れられるユーザーの最大特権レベルを設定します。管理者、オペレータ、ユーザーのオプションから 1 つを選択します。
暗号化キー	暗号化キーの文字形式の設定では、0 から 20 の 16進法の文字を使用します(空白は使用できません)。 デフォルト設定は 00000000000000000000 です。
VLAN ID を有効にする	VLAN ID を有効にします。有効にすると、一致する VLAN ID トラフィックのみが受け入れられます。
VLAN ID	802.1g の VLAN ID フィールド。
優先順位	802.1g フィールドの優先順位フィールド。

表 4-3. ネットワーク設定ページのボタン

ボタン	説明
印刷	ネットワーク設定 ページを印刷します。
更新	ネットワーク設定 ページを再ロードします。
詳細設定	ネットワークセキュリティ ページを表示します。
変更の適用	ネットワーク設定の変更を保存します。 メモ: NIC IP アドレスの設定を変更すると、すべてのユーザーセッションが閉じます。ユーザーはアップデート後の IP アドレス設定を使用して DRAC 5 ウェブインタフェースに再接続する必要があります。その他を変更するには、NIC をリセットする必要があります。その場合、接続が短時間中断することがあります。

ネットワークセキュリティの設定

 **メモ:** 次の手順を実行するには、DRAC 5 の設定権限が必要です。

1. システム ツリーで **リモートアクセス** をクリックします。
2. **設定** タブをクリックして、**ネットワーク** をクリックします。
3. **ネットワーク設定** ページで、**詳細設定** をクリックします。
4. **ネットワークセキュリティ** ページで、属性値を設定して **変更の適用** をクリックします。
[表 4-4](#) で、**ネットワークセキュリティ** ページの設定について説明します。
5. **ネットワークセキュリティ** ページの適切なボタンをクリックして続行します。[表 4-5](#) を参照してください。

表 4-4. ネットワークセキュリティページの設定

設定	説明

IP 範囲有効	DRAC 5 にアクセスできる IP アドレスの範囲を定義する IP 範囲チェック機能を有効にします。
IP 範囲のアドレス	受け入れる IP サブネットアドレスを決定します。
IP 範囲のサブネットマスク	IP アドレスの重要なビット位置を定義します。サブネットマスクは、下位ビットのすべての「1」が 1 度の移行ですべて「0」になるネットマスクの形式にします。 例: 255.255.255.0
IP ブロック有効	事前に選択した時間帯で、特定の IP アドレスからのログイン失敗回数を制限する IP アドレスブロック機能を有効にします。
IP ブロックのエラーカウント	IP アドレスからのログイン失敗回数を設定して、それを越えた場合にそのアドレスからのログインを拒否します。
IP ブロックのエラーウィンドウ	IP ブロックのペナルティ時間をトリガするために、IP ブロックのログイン失敗回数を数える時間帯を秒で指定します。
IP ブロックのペナルティ時間	ログイン失敗回数が制限を越えた IP アドレスからのログインを拒否する時間を秒で指定します。

表 4-5. ネットワークセキュリティページのボタン

ボタン	説明
印刷	ネットワークセキュリティ ページを印刷します。
更新	ネットワークセキュリティ ページを再ロードします。
変更の適用	ネットワークセキュリティ に加えた変更を保存します。
ネットワーク設定 ページに戻る	ネットワーク設定 ページに戻ります。

DRAC 5 ユーザーの追加と設定

DRAC 5 を使用してシステムを管理し、システムのセキュリティを確保するには、特定の管理者権限 (役割ベースの権限) を持つ固有のユーザーを作成します。また、セキュリティを強化するため、特定のイベントが発生したときに特定のユーザーに警告の電子メールを送信するように設定することもできます。

DRAC 5 のユーザーを追加して設定するには、次の手順を実行してください。

 **メモ:** 次の手順を実行するには、DRAC 5 の設定権限が必要です。

1. システム ツリーを展開して **リモートアクセス** をクリックします。
2. **設定** タブをクリックして、**ユーザー** をクリックします。
ユーザー ページには、各ユーザーの **状況**、**RAC 特権**、**IPMI LAN 特権**、および **IPMI シリアル特権** が表示されます。
3. **ユーザー ID** 列のユーザー ID 番号をクリックします。
4. **ユーザー設定** ページで、ユーザーのプロパティと特権を設定します。
[表 4-6](#) では、新規または既存の DRAC ユーザー名とパスワードを設定するための **一般** 設定について説明します。
[表 4-7](#) では、ユーザーの LAN 特権を設定するための **IPMI ユーザー特権** について説明します。
[表 4-8](#) では、**IPMI ユーザー特権** および **DRAC ユーザー特権** の **ユーザーグループ 特権** について説明します。
[表 4-9](#) で **DRAC グループ** 権限について説明しています。DRAC ユーザー特権をシステム管理者、パワーユーザー、またはゲストユーザーに追加すると、**DRAC グループ** が **カスタム** グループに変わります。
5. 設定が完了すると、**変更の適用** をクリックします。
6. 適切な **ネットワーク設定** ページのボタンをクリックして続行します。[表 4-10](#) を参照してください。

表 4-6. 一般プロパティ

プロパティ	説明
ユーザー ID	16 プリセットユーザー ID 番号の 1 つを指定します。 ユーザールートの情報を編集する場合、このフィールドは静的です。ルートのユーザー名は編集できません。
ユーザーの有効	ユーザーが DRAC 5 にアクセスできるようにします。このチェックボックスをオフにした場合は、ユーザー名を変更できません。
ユーザー名	DRAC 5 ユーザー名は最大 16 文字で指定します。各ユーザーに固有のユーザー名が必要です。 メモ: ローカル DRAC 5 のユーザー名に /(フォワードスラッシュ) または ..(ピリオド) を含めることはできません。

	メモ: ユーザー名を変更した場合は、ユーザーが次回ログインするまで新しい名前は表示されません。
パスワードの変更	新しいパスワード および 新しいパスワードの確認 フィールドを有効にします。このチェックボックスをオフにした場合は、ユーザーの パスワード を変更できません。
新しいパスワード	DRAC 5 ユーザーのパスワードを指定または編集します。
新しいパスワードの確認	DRAC 5 ユーザーのパスワードを確認のために再入力します。

表 4-7. IPMI ユーザーの特権

プロパティ	説明
LAN ユーザー最大特権認可	IPMI LAN チャネルでのユーザーの最大特権を システム管理者、オペレータ、ユーザー、なし の中から指定します。
シリアルポートユーザー最大特権認可	IPMI シリアルチャネルでのユーザーの最大特権を 管理者、オペレータ、ユーザー、なし の中から指定します。
シリアルオーバー LAN の有効	ユーザーが IPMI シリアルオーバー LAN を使用できるようにします。このチェックボックスをオンにすると、この特権が有効になります。

表 4-8. DRAC ユーザーの特権

プロパティ	説明
DRAC グループ	ユーザーの最大の DRAC 特権を システム管理者、パワーユーザー、ゲストユーザー、なし、カスタム の中から指定します。 表 4-9 で DRAC グループ 権限を参照してください。
DRAC ヘログイン	DRAC 5 にログインできます。
DRAC の設定	DRAC 5 を設定できます。
ユーザーの設定	特定のユーザーにシステムへのアクセスを許可できます。
ログのクリア	DRAC のログをクリアできます。
サーバーコントロールコマンドの実行	racadm コマンドを実行できます。
コンソールリダイレクトへのアクセス	コンソールリダイレクトを実行できます。
仮想メディアへのアクセス	仮想メディアを実行して使用できます。
テスト警告	テスト警告(電子メールと PET)を特定のユーザーに送信できます。
診断コマンドの実行	診断コマンドを実行できます。

表 4-9. DRAC グループの権限

ユーザーグループ	与える権限
システム管理者	DRAC 5 へのログイン、DRAC 5 の設定、ユーザー設定、ログのクリア、サーバー制御コマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行
パワーユーザー	DRAC 5 へのログイン、ログのクリア、サーバー制御コマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告
ゲストユーザー	DRAC 5 へのログイン
カスタム	次の権限を組み合わせて選択します。DRAC 5 へのログイン、DRAC 5 の設定、ユーザーの設定、ログのクリア、サーバー処置コマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行
なし	権限の割り当てなし

表 4-10. ユーザー設定ページのボタン

ボタン	処置
印刷	ユーザー設定 ページを印刷します。
更新	ユーザー設定 ページを再ロードします。
ユーザーページに戻る	ユーザーページに戻ります。
変更の適用	ネットワーク設定の変更を保存します。

Active Directory 証明書の設定と管理

メモ: Active Directory を設定して Active Directory 証明書をアップロード、ダウンロード、表示するには、**DRAC 5 の設定**権限が必要です。

Microsoft® Active Directory® サービスを使用して、DRAC 5 にアクセスできるようにソフトウェアを設定します。このサービスを使用すると、既存のユーザーの DRAC 5 ユーザー特権を追加したり制御したりできます。

詳細については、「[DRAC 5 と Microsoft Active Directory との併用](#)」を参照してください。

Active Directory メインメニューにアクセスするには、次の手順を実行してください。

1. システム ツリーを展開して、リモートアクセス をクリックします。
2. 設定 タブをクリックして、Active Directory を選択します。

表 4-11 に、Active Directory メインメニュー ページのオプションを一覧にします。表 4-12 のボタンは、Active Directory メインメニュー ページで使用できます。

表 4-11. Active Directory メインメニューページのオプション

フィールド	説明
Active Directory の設定	Active Directory の DRAC 名、ルートドメイン名、DRAC ドメイン名および Active Directory 認証タイムアウトを設定します。
Active Directory CA 証明書のアップロード	DRAC に Active Directory 証明書をアップロードします。
DRAC サーバー証明書のダウンロード	Windows ダウンロードマネージャは、システムに DRAC サーバー証明書をダウンロードできます。
Active Directory CA 証明書の表示	DRAC にアップロードされた Active Directory 証明書を表示します。

表 4-12. Active Directory メインメニューページのボタン

ボタン	定義
印刷	開いているウィンドウの内容をデフォルトのプリンタに印刷します。
次へ	次に選択する オプション ページへ移動します。

Active Directory の設定

1. Active Directory メインメニュー ページで、Active Directory の設定 を選択して 次へ をクリックします。
2. Active Directory の設定 ページで、Active Directory の設定を入力します。
表 4-13 で、Active Directory の設定 ページの設定について説明します。
3. 適用 をクリックして設定を保存します。
4. Active Directory の設定 ページの適切なボタンをクリックして続行します。表 4-14 を参照してください。

表 4-13. Active Directory 設定ページの設定

設定	説明
Active Directory の有効	Active Directory を有効にする オン=有効、オフ=無効。
DRAC 名	Active Directory で DRAC 5 カードを識別する固有の名前。この値は デフォルトでは NULL です。 名前には 1 ~ 256 文字の ASCII 文字列を使用し、空白スペースは使用できません。
ルートドメイン名	Active Directory のルートドメイン名。この値は デフォルトでは NULL です。 名前は xy から成る有効なドメイン名にします。x は文字間に空白スペースのない 1 ~ 256 の ASCII 文字列で、y は com, edu, gov, int, mil, net, org などの有効なドメインタイプです。
DRAC ドメイン名	Active Directory DRAC 5 オブジェクトがあるドメインの DNS 名 (文字列)。この値は デフォルトでは NULL です。 名前は xy から成る有効なドメイン名にします。x は文字間に空白スペースのない 1 ~ 256 の ASCII 文字列で、y は com, edu, gov, int, mil, net, org などの有効なドメインタイプです。
タイムアウト	Active Directory クエリが完了するまでの時間 (秒)。最小は 15 秒より大きい値です。デフォルト値は 120 秒です。

表 4-14. Active Directory 設定ページのボタン

ボタン	説明
印刷	Active Directory 設定 ページを印刷します。
適用	Active Directory 設定 ページの変更を保存します。
Active Directory メインメニューに戻る	Active Directory メインメニュー ページに戻ります。

Active Directory CA 証明書のアップロード

1. Active Directory メインメニュー ページで、Active Directory CA 証明書をアップロードする を選択して 次へ をクリックします。
2. 証明書のアップロード ページで、ファイルパス フィールドに証明書のファイルパスを入力するか、参照 をクリックして証明書ファイルまで移動します。

 **メモ:** アップロードする証明書の相対パスが **ファイルパス** の値に表示されます。完全なファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

3. 適用 をクリックします。
4. 証明書のアップロード ページの適切なボタンをクリックして続行します。表 4-15 を参照してください。

表 4-15. 証明書管理ページのボタン

ボタン	説明
印刷	証明書のアップロード ページを印刷します。
Active Directory メインメニューに戻る	Active Directory メインメニュー ページに戻ります。
適用	DRAC 5 ファームウェアに証明書を適用します。

DRAC サーバー証明書のダウンロード

1. Active Directory メインメニュー ページで、Active Directory CA 証明書をダウンロードする を選択して 次へ をクリックします。
2. ファイルのダウンロード ウィンドウで、保存 をクリックしてシステムのディレクトリにファイルを保存します。
3. ダウンロードの完了 ウィンドウで、閉じる をクリックします。

Active Directory CA 証明書の表示

Active Directory メインメニュー ページを使用して、DRAC 5 の CA サーバー証明書を表示します。

1. Active Directory メインメニュー ページで、Active Directory CA 証明書をアップロードする を選択して 次へ をクリックします。
[表 4-16](#) に、証明書 ウィンドウに表示されるフィールドとその説明を示します。
[表 4-17](#) には、Active Directory の CA 証明書を表示する ページで使用可能なボタンを示します。
2. Active Directory の CA 証明書を表示する ページの該当するボタンをクリックして続行します。[表 4-17](#) を参照してください。

表 4-16. Active Directory CA 証明書の情報

フィールド	説明
シリアルナンバー	証明書のシリアル番号
対象者情報	対象者が入力した証明書の属性
発行者情報	発行者から返された証明書の属性
発効日	証明書の発行日
失効日	証明書の有効期日

表 4-17. Active Directory の CA 証明書の表示ページのボタン

ボタン	説明
印刷	Active Directory の CA 証明書を印刷します。
Active Directory メインメニューに戻る	Active Directory メインメニュー ページに戻ります。

SSL とデジタル証明書を使用した DRAC 5 通信のセキュリティ

この項では、DRAC 5 に組み込まれているデータセキュリティの機能について説明します。

- 1 セキュアソケットレイヤー(SSL)
- 1 証明書署名要求(CSR)
- 1 SSL メインメニューへのアクセス
- 1 新しい CSR の生成
- 1 サーバー証明書のアップロード
- 1 サーバー証明書の表示

セキュアソケットレイヤー(SSL)

DRAC には、暗号化されたデータをインターネットで転送する業界標準 SSL セキュリティプロトコルの使用が設定された Web Server が含まれています。公開キーと秘密キーの暗号化技術を基盤とする SSL は、ネットワークでの盗聴を防ぐためにクライアントとサーバー間に認証された暗号化通信を提供する技術として広く普及しています。

SSL は、SSL を有効にしたシステムで次のタスクを実行します。

- 1 SSL が有効のクライアントへの認証
- 1 クライアントのサーバーへの認証の許可
- 1 両システムの暗号化接続の確立許可

この暗号化プロセスは高度なデータ保護を提供します。DRAC では、北米のインターネットブラウザで使用できる暗号化の最も安全な方式である 128 ビットの SSL 暗号化標準を導入しています。

DRAC Web Server は、Dell の署名入り SSL デジタル証明書(Server ID)を提供します。インターネットで高度なセキュリティを確保するには、新しい証明書署名要求(CSR)を生成する要求を DRAC に送信して、Web Server SSL 証明書を置き換えてください。

証明書署名要求(CSR)

CSR とは、認証局(CA)に安全なサーバー証明書のデジタル要求を送ることです。安全なサーバー証明書があれば、リモートシステムの身元を確実に識別でき、そのシステムとやり取りする情報を他のユーザーが表示したり変更したりするを防ぐことができます。DRAC のセキュリティを保護するには、CSR を生成して CA に送信し、CA から返された証明書をアップロードすることをお勧めします。

認証局は、IT 業界で認められたビジネス組織で、高水準で信頼できる審査、身元確認、その他の重要なセキュリティ要件を満たしています。CA には、Thawte や VeriSign があります。CA は CSR を受信したら、CSR にある情報を調べて確認します。申請者が CA のセキュリティ基準を満たした場合には、CA は申請者に証明書を発行します。この証明書によって、ネットワークまたはインターネット上で行ったトランザクションに対して、申請者を一意に識別できます。

CA が CSR を承認し、証明書を送信したら、証明書を DRAC ファームウェアにアップロードする必要があります。DRAC ファームウェアに保存した CSR 情報は、証明書に含まれている情報と一致していなければなりません。

SSL メインメニューへのアクセス

- 1 システム ツリーを展開して **リモートアクセス** をクリックします。
- 2 **設定** タブをクリックして、**SSL** をクリックします。

SSL メインメニュー ページのオプション(表 4-18 参照)を使って、CA に送る CSR を生成します。CSR 情報は DRAC 5 ファームウェアに保存されています。表 4-19 のボタンは、SSL メインメニュー ページで使用できます。

表 4-18. SSL メインメニューのオプション

フィールド	説明
新しい証明書署名要求(CSR)の生成	次へ をクリックして、 証明書署名要求の生成 ページを開くと、CSR を生成して CA に送信し、安全な Web 証明書を要求できます。 注意: 新しい CSR はファームウェアの以前の CSR を上書きします。CA が CSR を受け入れるには、CA から返される証明書とファームウェアの CSR が一致する必要があります。
サーバー証明書のアップロード	次へ をクリックし、ユーザーの会社が権利を有し、DRAC 5 へのアクセス制御に使用する既存の証明書をアップロードします。 注意: DRAC 5 が受け入れるのは、X509 の Base 64 エンコード証明書のみです。DER エンコード証明書は受け入れられません。新しい証明書をアップロードすると、DRAC 5 を使って受信したデフォルトの証明書が置き換えられます。
サーバー証明書の表示	次へ をクリックして、既存のサーバー証明書を表示します。

表 4-19. SSL メインメニューのボタン

ボタン	説明
印刷	SSL メインメニュー ページを印刷します。
次へ	次のページへ進みます。

新しい証明書署名要求の生成

 **メモ:** 新しい CSR はファームウェアの以前の CSR を上書きします。CA が CSR を受け入れるには、CA から返される証明書とファームウェアの CSR が一致する必要があります。一致しない場合は、証明書がアップロードされません。

1. SSL メインメニュー ページで、**新しい証明書署名要求 (CSR) の生成** を選択して、**次へ** をクリックします。
2. **証明書署名要求 (CSR) の生成** ページで、各 CSR 属性値の値を入力します。
[表 4-20](#) で、**証明書署名要求 (CSR) の生成** ページのオプションについて説明します。
3. CSR を保存または表示するには、**生成** をクリックします。
4. **証明書署名要求 (CSR) の生成** ページの適切なボタンをクリックして続行します。[表 4-21](#) を参照してください。

表 4-20. 証明書署名要求 (CSR) の生成

フィールド	説明
共通名	認証する名前 (通常は <code>www.xyzcompany.com</code> のような Web サーバーのドメイン名)。使用できるのは、英数字、ハイフン、下線、ピリオドのみです。スペースは使用できません。
組織名	この組織に付ける名前 (たとえば、XYZ Corporation)。使用できるのは、英数字、ハイフン、下線、ピリオド、スペースのみです。
部門名	部門など組織単位に関連付ける名前 (たとえば Enterprise Group)。使用できるのは、英数字、ハイフン、下線、ピリオド、スペースのみです。
地域	認証する組織の都市その他の場所 (たとえば、Round Rock)。使用できるのは、英数字とスペースのみです。下線や他の文字で単語を区切らないでください。
地域 2	証明書を申請している組織のある都道府県 (たとえば、Texas)。使用できるのは、英数字とスペースのみです。略語は使用しないでください。
国番号	証明書を申請している組織がある国の名前。国を選択するには、ドロップダウンメニューを使用します。
電子メール	CSR に関連付ける電子メールアドレス。ユーザーの会社の電子メールアドレスなど、CSR に関連付ける電子メールアドレスを入力できます。このフィールドはオプションです。

表 4-21. 証明書署名要求 (CSR) の生成ページのボタン

ボタン	説明
印刷	証明書署名要求 (CSR) の生成ページを印刷します。
セキュリティのメインメニューに戻る	SSL メインメニュー ページに戻ります。
生成	CSR を生成します。

サーバー証明書のアップロード

1. SSL メインメニュー ページで、**サーバー証明書のアップロード** を選択して **次へ** をクリックします。

証明書のアップロード ページが表示されます。

2. **ファイルパス** フィールドで、**値** フィールドに、証明書のファイルパスを入力するか、**参照** をクリックして証明書ファイルまで移動します。

 **メモ:** アップロードする証明書の相対パスが **ファイルパス** の値に表示されます。完全なファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

3. **適用** をクリックします。
4. ページの適切なボタンをクリックして続行します。[表 4-22](#) を参照してください。

表 4-22. 証明書管理ページのボタン

ボタン	説明

ボタン	説明
印刷	証明書のアップロード ページを印刷します。
SSL メインメニューに戻る	SSL メインメニュー ページに戻ります。
適用	DRAC 5 ファームウェアに証明書を適用します。

サーバー証明書の表示

1. SSL メインメニュー ページで、**サーバー証明書の表示** を選択して **次へ** をクリックします。

[表 4-23](#) に、**証明書** ウィンドウに表示されるフィールドとその説明を示します。

2. **サーバー証明書の表示** ページの適切なボタンをクリックして続行します。[表 4-24](#) を参照してください。

表 4-23. 証明書情報

フィールド	説明
シリアルナンバー	証明書のシリアル番号
対象者情報	対象者が入力した証明書の属性
発行者情報	発行者から返された証明書の属性
発効日	証明書の発効日
失効日	証明書の有効期日

表 4-24. サーバー証明書の表示ページのボタン

ボタン	説明
印刷	サーバー証明書の表示 ページを印刷します。
SSL メインメニューに戻る	SSL メインメニュー ページに戻ります。

シリアルおよびターミナルモードの設定

IPMI および RAC シリアルの設定

1. システム ツリーを展開して **リモートアクセス** をクリックします。

2. **設定** タブをクリックして、**シリアル** をクリックします。

3. IPMI シリアルを設定します。

[表 4-25](#) で、IPMI シリアル設定について説明します。

4. RAC シリアルを設定します。

[表 4-26](#)では、IPMI シリアル設定について説明します。

5. **変更の適用** をクリックします。

6. **シリアル設定** ページの適切なボタンをクリックして続行します。[表 4-27](#) を参照してください。

表 4-25. IPMI シリアル設定

設定	説明
接続モード設定	<ul style="list-style-type: none"> 1 ダイレクト接続基本モード - IPMI シリアル基本モード 1 ダイレクト接続ターミナルモード - IPMI シリアルターミナルモード
ボーレート	データ速度を設定します。 9600 bps、19.2 kbps、57.6 kbps、115.2 kbps から選択します。
フロー制御	<ul style="list-style-type: none"> 1 なし — ハードウェアフロー制御オフ

	1 RTS/CTS — ハードウェアフロー制御オン
チャンネル特権レベルの制限	1 システム管理者 1 オペレータ 1 ユーザー

表 4-26. RAC シリアル設定

設定	説明
有効	RAC シリアルコンソールを有効または無効にします。オン=有効、オフ=無効。
最大セッション	システムで許可される同時セッションの最大数。
タイムアウト	回線が切断される前の回線アイドル最大時間を秒で指定します。範囲は 60 ~ 1920 秒です。デフォルトは 300 秒です。タイムアウト機能を無効にするには 0 秒にします。
リダイレクト有効	コンソールリダイレクトを有効または無効にします。オン=有効、オフ=無効。
ボーレート	外部シリアルポート上のデータ速度。値は 9600 bps、28.8 kbps、57.6 kbps、115.2 kbps です。デフォルトは 57.6 kbps です。
Esc キー	<Esc> キーを指定します。デフォルトは ^M 文字です。
履歴バッファサイズ	コンソールに書き込まれた最後の文字を保持するシリアル履歴バッファのサイズ。最大とデフォルトは 8192 文字です。
ログインコマンド	有効なログイン時に実行される DRAC コマンドライン。

表 4-27. シリアルページの設定

ボタン	説明
印刷	シリアル設定 ページを印刷します。
更新	シリアル設定 ページを更新します。
変更の適用	IPMI および RAC シリアルの変更を適用します。
ターミナルモード設定	ターミナルモード設定 ページを開きます。

設定ターミナルモード

1. システム ツリーを展開して **リモートアクセス** をクリックします。
2. **設定** タブをクリックして、**シリアル** をクリックします。
3. **シリアル 設定** ページで、**ターミナルモード設定** をクリックします。
4. ターミナルモードを設定します。

[表 4-28](#) で、ターミナルモードの設定について説明します。

5. **変更の適用** をクリックします。
6. **ターミナル設定** ページの適切なボタンをクリックして続行します。[表 4-29](#) を参照してください。

表 4-28. ターミナルモード設定

設定	説明
ライン編集	ライン編集を有効または無効にします。
削除制御	次のいずれかを選択します。 <ul style="list-style-type: none"> 1 BMC は、<code>bksp</code> または <code></code> を受信したとき、<code><bksp><sp><bksp></code> 文字を出力 1 BMC は、<code>bksp</code> または <code></code> を受信したとき <code></code> 文字を出力
エコー制御	エコーを有効または無効にします。
ハンドシェイク制御	ハンドシェイクを有効または無効にします。
新しいラインシーケンス	なし、 <code><CR-LF></code> 、 <code><NULL></code> 、 <code><CR></code> 、 <code><LF-CR></code> または <code><LF></code> を選択します。
新しいラインシーケンスの入力	<code><CR></code> または <code><NULL></code> を選択します。

表 4-29. ターミナルモード設定ページのボタン

--	--

ボタン	説明
印刷	ターミナルモード設定 ページを印刷します。
更新	ターミナルモード設定 ページを更新します。
シリアルポート設定に戻る	シリアルポート設定 ページに戻ります。
変更の適用	ターミナルモード設定の変更を適用します。

シリアルオーバー LAN の設定

 **メモ:** シリアルオーバー LAN の詳細については、『Dell OpenManage ベースボード管理コントローラ ユーザーズガイド』を参照してください。

1. システム ツリーを展開して **リモートアクセス** をクリックします。
2. **設定** タブをクリックして、**シリアルオーバー LAN** をクリックします。
3. シリアルオーバー LAN を設定します。

[表 4-30](#) で、**シリアルオーバー LAN 設定** ページの設定について説明します。

4. **変更の適用** をクリックします。
5. 必要に応じて詳細設定を指定します。詳細を指定しない場合は、**シリアルオーバー LAN 設定** ページの適切なボタンをクリックして続行します ([表 4-31](#) を参照)。

詳細設定を指定するには、次の手順を実行してください。

- a. **詳細設定** をクリックします。
- b. **シリアルオーバー LAN 詳細設定** ページで、必要に応じて詳細を指定します。 [表 4-32](#) を参照してください。
- c. **変更の適用** をクリックします。
- d. **シリアルオーバー LAN 詳細設定** ページの適切なボタンをクリックして続行します。 [表 4-33](#) を参照してください。

表 4-30. シリアルオーバー LAN 設定ページの設定

設定	説明
シリアルオーバー LAN の有効	シリアルオーバー LAN の有効 オン=有効、オフ=無効。
ポーレート	IPMI のデータ速度。9600 bps、19.2 kbps、57.6 kbps、115.2 kbps から選択します。
チャネル特権レベルの制限	IPMI シリアルオーバー LAN の最小ユーザー特権(システム管理者、オペレータ、ユーザー)を設定します。

表 4-31. シリアルオーバー LAN 設定ページのボタン

ボタン	説明
印刷	シリアルオーバー LAN 設定 ページを印刷します。
更新	シリアルオーバー LAN 設定 ページを更新します。
詳細設定	シリアルオーバー LAN 詳細設定 ページを開きます。
変更の適用	シリアルオーバー LAN 詳細設定 ページの設定を適用します。

表 4-32. シリアルオーバー LAN 詳細設定 ページの設定

設定	説明
文字累積間隔	BMC が SOL 文字データパッケージの一部を転送するまで待機する時間です。1 ベースで 5ms ずつ増加。
文字送信しきい値	この文字数がそれ以上が受け入れられ次第に、BMC は文字を含んだ SOL 文字データパッケージを送信します。1 ベース単位。

表 4-33. シリアルオーバー LAN 詳細設定ページのボタン

ボタン	説明
印刷	シリアルオーバー LAN 詳細設定 ページを印刷します。
更新	シリアルオーバー LAN 詳細設定 ページを更新します。

シリアルオーバー LAN 設定ページに戻る	シリアルオーバー LAN 設定 ページに戻ります。
変更の適用	シリアルオーバー LAN 詳細設定 ページの設定を適用します。

サービスの設定

 **メモ:** これらの設定を変更するには、DRAC 5 の設定権限が必要です。また、リモート RACADM コマンドラインユーティリティは、root でログインしたときのみ有効にできます。

1. システム ツリーを展開して **リモートアクセス** をクリックします。
2. **設定** タブをクリックして、**サービス** をクリックします。
3. 必要に応じて、次のサービスを設定します。
 - 1 Web サーバー(表 4-34)
 - 1 SSH(表 4-35)
 - 1 Telnet(表 4-36)
 - 1 リモート RACADM(表 4-37)
 - 1 SNMP エージェント(表 4-38)
 - 1 自動システムリカバリエージェント(表 4-39)

自動システムリカバリエージェントを使用して、DRAC 5 の **前回クラッシュ画面** 機能を有効にします。

 **メモ:** Server Administrator は、DRAC 5 で **前回クラッシュ画面** が機能するには、**処置** を **システムの再起動**、**システムの電源を切る**、または **システムの電源を入れなおす** に設定して、**自動回復** 機能がアクティブな状態でインストールする必要があります。

4. **変更の適用** をクリックします。
5. **サービス** ページの適切なボタンをクリックして続行します。表 4-40 を参照してください。

表 4-34. Web Server の設定

設定	説明
有効	Web Server を有効または無効にします。オン=有効、オフ=無効。
最大セッション数	システムで許可される同時セッションの最大数。
アクティブセッション	システムの現在のセッション数(最大セッション数 かそれ以下)。
タイムアウト	接続がアイドル状態でいられる秒数。タイムアウトになると、セッションはキャンセルされます。タイムアウト設定の変更は、現在のセッションには影響しません。タイムアウト設定を変更した場合、新しい設定を有効にするには、いったんログアウトしてからログインし直す必要があります。タイムアウト範囲は 60 ~ 1920 秒です。
HTTP ポート番号	DRAC がサーバー接続の受信に使用するポート。デフォルト設定は 80 です。
HTTPS ポート番号	DRAC がサーバー接続の受信に使用するポート。デフォルト設定は 443 です。

表 4-35. SSH の設定

設定	説明
有効	SSH を有効または無効にします。オン=有効、オフ=無効。
最大セッション数	システムで許可される同時セッションの最大数。4 セッションまでサポートされます。
アクティブセッション	システムの現在のセッション数(最大セッション数 かそれ以下)。
タイムアウト	Secure Shell のアイドルタイムアウト(秒)。範囲 = 60 ~ 1920 秒。タイムアウト機能を無効にするには、0 秒を入力します。デフォルト設定は 300 です。
ポート番号	DRAC がサーバー接続の受信に使用するポート。デフォルト設定は 22 です。

表 4-36. Telnet の設定

設定	説明
有効	Telnet を有効または無効にします。オン=有効、オフ=無効。
最大セッション数	システムで許可される同時セッションの最大数。4 セッションまでサポートされます。

アクティブセッション	システムの現在のセッション数(最大セッション数 かそれ以下)。
タイムアウト	Secure Shell のアイドルタイムアウト(秒)。範囲 = 60 ~ 1920 秒。タイムアウト機能を無効にするには、0 秒を入力します。デフォルト設定は 0 です。
ポート番号	DRAC がサーバー接続の受信に使用するポート。デフォルト設定は 23 です。

表 4-37. リモート RACADM の設定

設定	説明
有効	リモート RACADM を有効または無効にします。オン=有効、オフ=無効。
最大セッション数	システムで許可される同時セッションの最大数。4 セッションまでサポートされます。
アクティブセッション	システムの現在のセッション数(最大セッション数 かそれ以下)。

表 4-38. SNMPエージェントの設定

設定	説明
有効	SNMPエージェントを有効または無効にします。オン=有効、オフ=無効。
コミュニティ名	SNMP 警告の送信先 IP アドレスを含むコミュニティ名。コミュニティ名は、空白文字を含まずに最大 31 文字まで使用できます。デフォルト設定は public です。

表 4-39. 自動システムリカバリエージェントの設定

設定	説明
有効	自動システムリカバリエージェントを有効にします。

表 4-40. サービスページのボタン

ボタン	説明
印刷	サービス ページを印刷します。
更新	サービス ページを更新します。
変更の適用	サービス ページの設定を適用します。

よくあるお問い合わせ(FAQ)

表 4-41 に、よくあるお問い合わせ(FAQ)とその回答を示します。

表 4-41. リモートシステムの管理と回復:よくあるお問い合わせ

質問	回答
DRAC 5 ウェブインタフェースにアクセスするとき、SSL 証明書のホスト名と DRAC 5 のホスト名が一致しないというセキュリティ警告が表示されます。	<p>DRAC 5 には、ウェブインタフェースのネットワークセキュリティを保護するため、デフォルトの DRAC 5 サーバー証明書と、リモート racadm の機能が含まれています。この証明書を使用すると、Web ブラウザにセキュリティ警告が表示されます。これは、デフォルトの証明書は、DRAC 5 のホスト名(例:IP アドレス)と一致しない RAC デフォルト証明書 に発行されるためです。</p> <p>このセキュリティの問題に対処するには、DRAC 5 の IP アドレスに発行された DRAC 5 サーバー証明書をアップロードします。証明書の発行に使用する証明書署名要求(CSR)を生成するとき、CSR の共通名(CN)が DRAC 5 の IP アドレス(例:192.168.0.120)と一致することを確認してください。</p> <p>登録した DNS DRAC 名と CSR が同じであることを確認するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. システムツリーで リモートアクセス をクリックします。 2. 設定 タブをクリックして、ネットワーク をクリックします。 3. ネットワーク設定 ページで、次の手順を実行します。 <ol style="list-style-type: none"> a. DNS に DRAC を登録 チェックボックスをオンにします。 b. DNS DRAC 名 フィールドに DRAC 名を入力します。 4. 変更の適用 をクリックします。 <p>CSR と証明書の発行の詳細については、「SSL とデジタル証明書を使用した DRAC 5 通信のセキュリティ」を参照してください。</p>
プロパティを変更すると、リモート racadm とウェブサービスを使用できなくなるのはなぜですか？	<p>DRAC 5 Web Server をリセットすると、リモート racadm サービスとウェブインタフェースに再度アクセスできるようになるまで 1 分ほどかかる場合があります。</p> <p>次のような状況で DRAC 5 Web サーバーはリセットされます。</p> <ol style="list-style-type: none"> 1. DRAC 5 ウェブインタフェースを使用してネットワーク設定やネットワークセキュリティのプロパティを変更する場合 1. cfgRacTuneHttpsPort プロパティが変更されたとき (config -f <設定ファイル> が変更した場合も含む) 1. racresetcfg を使用したとき 1. DRAC 5 がリセットされたとき

	1 新しい SSL サーバー証明書がアップロードされたとき
DNS サーバーで DRAC 5 を登録できない理由は何ですか?	DNS サーバーによっては、31 文字以内の名前しか登録できない場合があります。
DRAC 5 ウェブインタフェースにアクセスすると、「SSL 証明書が信頼されていない認証局 (CA) によって発行されました」というセキュリティ警告が表示されます。	DRAC 5 には、ウェブインタフェースのネットワークセキュリティを保護するため、DRAC 5 サーバー証明書とリモート racadm の機能が含まれています。この証明書は信頼された CA から発行されませんでした。このセキュリティ問題に対処するには、信頼された CA (例: Thawte または Verisign) が発行した DRAC 5 サーバー証明書をアップロードします。詳細については、「 SSL とデジタル証明書を使用した DRAC 5 通信のセキュリティ 」を参照してください。
不明な理由で次のメッセージが表示されました。 Remote Access: SNMP Authentication Failure (リモートアクセス : SNMP 認証エラー) 何が原因ですか?	<p>検出機能の一部として、IT Assistant がデバイスの get および set のコミュニティ名の検証を試みました。IT Assistant では、get コミュニティ名 = パブリックで、set コミュニティ名 = プライベートです。DRAC 5 エージェントのデフォルトのコミュニティ名はパブリックです。IT Assistant が set 要求を送信すると、DRAC 5 エージェントはコミュニティ = パブリックからの要求しか受け入れないため、SNMP 認証エラーが生成されます。</p> <p>RACADM を使用して、DRAC 5 のコミュニティ名を変更できます。</p> <p>DRAC 5 コミュニティ名を表示するには、次のコマンドを使用します。</p> <pre>racadm getconfig -g cfgOobSnmp</pre> <p>DRAC 5 コミュニティ名を設定するには、次のコマンドを使用します。</p> <pre>racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <コミュニティ名></pre> <p>SNMP 認証トラップの生成を防ぐには、エージェントが受け入れるコミュニティ名を入力する必要があります。DRAC 5 は 1 つのコミュニティ名しか許可しないので、IT Assistant の検出設定と同じ get および set コミュニティ名を入力する必要があります。</p>

[目次ページに戻る](#)

[目次ページに戻る](#)

管理下システムの回復とトラブルシューティング

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

- [リモートシステムのトラブルシューティング最初のステップ](#)
- [リモートシステムの電源管理](#)
- [システム情報の表示](#)
- [システムイベントログ \(SEL\) の使用](#)
- [システムの前回クラッシュ画面の表示](#)
- [RAC ログの使用](#)
- [診断コンソールの使用](#)
- [ネットワーク問題のトラブルシューティング](#)
- [警告の不具合のトラブルシューティング](#)

この項では、DRAC 5 ウェブインタフェースを使って、クラッシュしたリモートシステムの回復とトラブルシューティングに関連するタスクの実行方法について説明します。DRAC 5 のトラブルシューティングについては、「[VM-CLI を使用したオペレーティングシステムの起動](#)」を参照してください。

- 1 リモートシステムのトラブルシューティング
- 1 リモートシステムの電源管理
- 1 システムイベントログ (SEL) の使用
- 1 システムの前回クラッシュ画面の表示
- 1 RAC ログの使用
- 1 診断コンソールの使用

リモートシステムのトラブルシューティング最初のステップ

以下は、管理下システムで発生する複雑な問題をトラブルシューティングする際に確認すべき事項です。

1. システムの電源はオンになっていますか、オフになっていますか？
2. 電源がオンの場合は、オペレーティングシステムが正しく機能していますか、それともクラッシュまたはフリーズしていますか？
3. 電源がオフの場合は、電源が突然オフになりましたか？

クラッシュしたシステムは、前回クラッシュ画面（「[前回のシステムクラッシュ画面の表示](#)」を参照）をチェックし、コンソールリダイレクト（「[管理下システムの対応画面解像度およびリフレッシュレート](#)」）およびリモート電源管理（「[リモートシステムの電源管理](#)」を参照）を使用してシステムを再起動し、再起動プロセスを監視してください。

リモートシステムの電源管理

DRAC 5 では、管理下システムでシステムクラッシュその他のシステムイベントが発生した後、リモートで電源管理処置を実行して回復することができます。

電源管理 ページで次の手順を実行してください。

- 1 再起動するとき、オペレーティングシステムから正常なシャットダウンを実行して、システムをオンまたはオフにします。
- 1 システムの現在の **電源状態** が **オン** か **オフ** かを確認します。

システム ツリーから **電源管理** ページにアクセスするには、**システム** をクリックしてそれから **電源管理** タブをクリックします。

 **メモ:** 電源管理処置を実行するには、**サーバー処置コマンドの実行権限**が必要です。

電源制御処置の選択

1. 次のいずれかの **電源制御処置** を選択します。
 - 1 **システムの電源を入れる** — システムの電源を入れます（電源がオフのときに電源ボタンを押す操作と同じ）。
 - 1 **システムの電源を切る** — システムの電源を切ります（電源がオンのときに電源ボタンを押す操作と同じ）。
 - 1 **システムのリセット** — システムをリセットします（リセットボタンを押す操作と同じ）。この機能に使っても電源はオフになりません。
 - 1 **システムの電源を入れなおす** — 電源オフにしてシステムを再起動（コールドブート）します。
2. 電源の管理処置を実行するには、**適用** をクリックします（たとえば、パワーサイクルを実行する場合）。

3. 電力の管理 ページの適切なボタンをクリックして続行します(表 5-1 を参照)。

表 5-1. 電源管理ページのボタン(右上)

ボタン	処置
印刷	電力の管理 ページを印刷します。
更新	電力の管理 ページを再ロードします。

システム情報の表示

システム概要 ページに次のシステムコンポーネントが表示されます。

- 1 メインシステムシャーシ
- 1 Remote Access Controller
- 1 ベースボード管理コントローラ

システム情報にアクセスするには、システム ツリーを展開してプロパティをクリックします。

メインシステムシャーシ

表 5-2 と 表 5-3 で、メインシステムシャーシのプロパティについて説明します。

 **メモ:** ホスト名 と OS 名 の情報を受け取るには、管理下システムに DRAC 5 サービスをインストールしておく必要があります。

表 5-2. システム情報フィールド

フィールド	説明
説明	システムの説明。
BIOS バージョン	システムの BIOS バージョン。
サービスタグ	システムのサービスタグナンバー。
ホスト名	ホストシステム名。
OS 名	システムで実行しているオペレーティングシステム。

表 5-3. 自動回復のフィールド

フィールド	説明
回復処置	「システムハング」が検知されたときに、処置が不要か、ハードリセット、電源を切る、パワースイクルなどの処置を行うかを設定できます。
初期カウントダウン	「システムハング」が検知されてから DRAC が回復処置を実行するまでの秒数。
現在のカウントダウン	カウントダウンタイマーの現在の値(秒)。

Remote Access Controller

表 5-4 では、Remote Access Controller のプロパティについて説明します。

表 5-4. RAC の情報フィールド

フィールド	説明
名前	短い名前。
製品情報	長い名前。
ハードウェアバージョン	Remote Access Controller のカード バージョンまたは「不明」。
ファームウェアバージョン	現在の DRAC 5 ファームウェアのバージョンレベル。
ファームウェアアップデート	ファームウェアを最後にアップデートした日時。
RAC 時間	システムクロックの設定。

ベースボード管理コントローラ

表 5-5 で、ベースボード管理コントローラのプロパティについて説明します。

表 5-5. BMC の情報フィールド

フィールド	説明
名前	ベースボード管理コントローラ。
IPMI バージョン	Intelligent Platform Management Interface (IPMI) のバージョン。
アクティブ可能なセッション数	同時にアクティブにできるセッションの最大数。
現在アクティブなセッション数	現在アクティブなセッションの合計数。
ファームウェアバージョン	BMC ファームウェアのバージョン。
LAN 有効	LAN の有効または無効。

システムイベントログ (SEL) の使用

SEL ログ ページには、管理下システムで発生するシステムの重要イベントが表示されます。

システムイベントログを表示するには、次の手順を実行してください：

1. システムツリーで **システム** をクリックします。
2. **ログ** タブをクリックしてから **システムイベントログ** をクリックします。

システムイベントログ ページにイベントの重大度が表示され、その他 表 5-6 に示すような情報も提供されます。

3. システムイベントログ ページの適切なボタンをクリックして続行します (表 5-7 を参照)。

表 5-6. 状態インジケータのアイコン

アイコン / カテゴリ	説明
	緑のチェックマークは、正常な (平常) 状態を示します。
	感嘆符の入った黄色の三角形は、警告 (非重要) 状態を示します。
	赤い X は、重大な (エラー) 状態を示します。
	疑問符のアイコンは、不明な状態を示します。
日付/時刻	イベントが発生した日時。日付が空白の場合は、システム起動時にイベントが実行されます。24 時間クロックを基本とした mm/dd/yyyy hh:mm:ss の形式です。
説明	イベントの短い説明

表 5-7. SEL ページのボタン

ボタン	処置
印刷	ウィンドウに表示されるソート順で SEL を印刷します。
ログのクリア	SEL をクリアします。 メモ: ログのクリア ボタンは、ログのクリア権限がある場合にのみ表示されます。
名前を付けて保存	ポップアップウィンドウが開き、SEL を選択したディレクトリに保存できます。 メモ: Internet Explorer で保存中に問題が発生した場合、Microsoft Support ウェブサイト (support.microsoft.com) から Internet Explorer 用の Cumulative Security Update をダウンロードします。
更新	SEL ページを再ロードします。

システムの前回クラッシュ画面の表示

 **注意:** 前回クラッシュ画面の機能を使用するには、管理下システムの Server Administrator に **自動回復** 機能が設定されている必要があります。さらに、DRAC を使った **自動システムリカバリ** 機能が有効になっていることを確認します。この機能は、**リモートアクセス** セクションの **設定** タブにある **サービス** ページで有効にします。

前回クラッシュ画面 ページには、システムクラッシュ前に発生したイベントに関する情報を含む一番新しいクラッシュ画面が表示されます。前回システムクラッシュ情報は、DRAC 5 メモリに保存され、リモートからアクセスできます。

前回クラッシュ画面 ページを表示するには、次の手順を実行してください。

1. **システム** ツリーで **システム** をクリックします。
2. **ログ** タブをクリックして、**前回クラッシュ** をクリックします。

前回クラッシュ画面 ページの右上に次のボタンがあります(表 5-8 を参照)。

表 5-8. 前回クラッシュ画面ページのボタン

ボタン	処置
印刷	前回クラッシュ画面 ページを印刷します。
保存	ポップアップウィンドウが開き、選択したディレクトリに前回クラッシュ画面 を保存できます。
削除	前回クラッシュ画面 ページを削除します。
更新	前回クラッシュ画面 ページを再ロードします。

 **メモ:** 自動回復タイマーの変動により、システムリセットタイマーの値が 30 秒未満に設定されている場合は、**前回クラッシュ画面** をキャプチャできない可能性があります。Server Administrator と IT Assistant でシステムリセットタイマーを 30 秒以上に設定して、**前回クラッシュ画面** が正しく機能することを確認します。詳細については、「[管理下システムに前回クラッシュ画面のキャプチャを設定する方法](#)」を参照してください。

RAC ログの使用

DRAC ログ は持続的なログで、DRAC 5 ファームウェアに保管されています。ログにはユーザーの処置(ログイン、ログアウト、セキュリティポリシーの変更など)と DRAC 5 が発行する警告のリストが含まれています。ログが一杯になると、古いエントリから順に上書きされます。

RAC ログにアクセスするには、次の手順を実行してください。

1. **システムツ** ツリーで **リモートアクセス** をクリックします。
2. **ログ** タブをクリックして、**RAC ログ** をクリックします。

DRAC ログ には、表 5-9 に示す情報が含まれています。

表 5-9. RAC ログページの情報

フィールド	説明
日付 / 時刻	日付と時刻(例: Dec 19 16:55:47)。 DRAC 5 の最初の開始時に管理下システムと通信できない場合は、DRAC 5 が起動してからの経過時間が表示されます。DRAC 5 では Thu Jan 1 00:00:00 1970 に起動したと想定されます。
ソース	イベントを引き起こしたインタフェース。
説明	イベントの要約と DRAC 5 にログインしたユーザー名。

DRAC ログページボタンの使い方

DRAC ログ ページには、次のボタンが含まれています(表 5-10 を参照)。

表 5-10. RAC ログボタン

ボタン	処置
印刷	RAC ログ ページを印刷します。
ログのクリア	RAC ログ エントリをクリアします。 メモ: ログのクリアボタンは、ログのクリア権限がある場合にのみ表示されます。
名前を付けて保存	ポップアップウィンドウが開き、 DRAC ログ を選択したディレクトリに保存できます。

	<p>メモ: Internet Explorer を使用していて問題が発生した場合、Cumulative Security Update for Internet Explorer をダウンロードし、support.microsoft.com の Microsoft Support を検索してください。</p>
更新	RAC ログ ページを再ロードします。

診断コンソールの使用

DRAC 5 は、Microsoft® Windows® システムや Linux システムのツールに似た標準的なネットワーク診断ツール(表 5-11 を参照)一式を提供します。DRAC 5 ウェブインタフェースを使用して、ネットワークのデバッグツールにアクセスできます。

診断コンソール ページにアクセスするには、次の手順を実行してください。

1. システム ツリーで **リモートアクセス** をクリックします。
2. **診断** タブをクリックします。

表 5-11 で、診断コンソール ページで使用できるオプションについて説明します。コマンドを入力して、送信 をクリックします。デバッグの結果が 診断コンソール ページに表示されます。

診断コンソール ページを更新するには、更新 をクリックします。別のコマンドを実行するには、診断ページに戻る をクリックします。

表 5-11. 診断コマンド

コマンド	説明
arp	ARP (Address Resolution Protocol) テーブルの内容を表示します。ARP エントリの追加や削除はできません。
ifconfig	ネットワークインタフェーステーブルの内容を表示します。
netstat	ルーティングテーブルの内容を印刷します。NetStat オプションの右のテキストフィールドにオプションのインタフェース番号を入力すると、インタフェース間のトラフィック、バッファの使用などのネットワークインタフェースに関する追加情報が印刷されます。
ping <IP アドレス>	送信先の IP アドレスに、現在のルーティングテーブルの内容が含まれた DRAC 5 からアクセス可能であることを確認します。送信先の IP アドレスは、このオプションの右側のフィールドに入力する必要があります。現在のルーティングテーブルの内容に基づいて、インターネットコントロールメッセージプロトコル (ICMP) のエコーパケットが送信先の IP アドレスに送信されます。
gettracelog	DRAC 5 ログを表示します。詳細については、「 gettracelog 」を参照してください。

ネットワーク問題のトラブルシューティング

DRAC 5 の内部トレースログは、管理者が DRAC 5 から警告またはネットワークをデバッグするときに使用できます。DRAC 5 ウェブベース インタフェースからトレースログにアクセスするには、診断タブをクリックして `gettracelog` コマンドまたは `racadm gettracelog` コマンドを入力します。詳細については、「[gettracelog](#)」を参照してください。

トレースログは次の情報を追跡します。

- 1 DHCP – DHCP サーバーから送受信したパケットをトレースします。
- 1 IP – 送受信した IP パケットをトレースします。

トレースログには、管理下システムのオペレーティングシステムではなく、DRAC 5 の内部ファームウェアに関連する DRAC ファームウェア固有のエラーコードが含まれている場合もあります。

メモ: DRAC 5 は、1500 バイトより大きいパケットサイズの ICMP (Ping) にはエコーしません。

警告の不具合のトラブルシューティング

DRAC 5 の特定タイプの警告をトラブルシューティングするには、ログに記録された SNMP トラップを使用します。SNMP トラップの配信内容はデフォルトでは Trace ログに記録されます。ただし、SNMP ではトラップの配信を確認できないため、ネットワークアナライザや Microsoft の `snmputil` などのツールを使って、管理下システム上のパケットをトレースすることをお勧めします。

[目次ページに戻る](#)

[目次ページに戻る](#)

DRAC 5 と Microsoft Active Directory との併用

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

- [Active Directory スキーマ拡張](#)
- [RAC スキーマ拡張の概要](#)
- [Active Directory オブジェクトの概要](#)
- [DRAC 5 にアクセスするための Active Directory の設定](#)
- [Active Directory スキーマの拡張](#)
- [Active Directory ユーザーとコンピュータスナップインへの Dell 拡張のインストール](#)
- [Active Directory への DRAC 5 ユーザーと特権の追加](#)
- [ドメインコントローラにおける SSL の有効化](#)
- [DRAC 5 の設定](#)
- [Active Directory を使用して DRAC 5 にログインする方法](#)
- [よくあるお問い合わせ \(FAQ\)](#)

ディレクトリサービスは、ネットワーク上のユーザー、コンピュータ、プリンタなどを制御するのに必要な全情報に共通のデータベースを維持します。会社が Microsoft® Active Directory® サービスソフトウェアを使用している場合は、DRAC 5 にアクセスできるように設定して、Active Directory ソフトウェアで DRAC 5 のユーザー特権を既存のユーザーに追加して制御できます。

 **メモ:** Microsoft Windows 2000 および Windows Server 2003 オペレーティングシステムでは Active Directory を使用して DRAC 5 のユーザーを認識できます。

Active Directory スキーマの拡張

Active Directory データは、属性とクラスのデータベースに分散されます。Active Directory スキーマには、データベースに追加または挿入するデータタイプを決定する規則があります。ユーザークラスは、データベースに保存されるクラスの一例です。ユーザークラスの属性の例としては、ユーザーの名、姓、電話番号、などがあります。企業は独自の一意な属性とクラスを環境に特有のニーズを満たすのに追加することで、Active Directory データベースを拡張できます。デルでは、このスキーマにリモート管理の認証と許可をサポートするための変更を加えて、機能を拡張しました。

既存の Active Directory スキーマに追加した各属性やクラスは、固有の ID で定義する必要があります。業界全体で固有の ID を維持するために、Microsoft では Active Directory オブジェクト識別子 (OID) が入ったデータベースを保持しています。その結果、企業がスキーマに拡張を追加する場合、相互の競合や重複がないことが保証されます。Microsoft の Active Directory でスキーマを拡張するため、デルはディレクトリサービスに追加された属性とクラス用の固有の OID、固有の名前の拡張子、および固有のリンク属性 ID を受け取りました。

デルの拡張子: dell

データベースの OID: 1.2.840.113556.1.8000.1280

RAC LinkID の範囲: 12070 ~ 12079

Microsoft が保持する Active Directory OID データベースを <http://msdn.microsoft.com/certification/ADAcctInfo.asp> で表示するには、拡張子 Dell を入力します。

RAC スキーマ拡張の概要

幾多の顧客環境において極めて柔軟な対応を実現するため、デルではユーザーが希望する成果に応じた設定が行えるプロパティグループを提供しています。デルでは、関連、デバイス、および特権のプロパティを加えて、このスキーマを拡張しました。関連プロパティは、特定の特権セットを持つユーザーまたはグループを 1 台以上の RAC デバイスにリンクするために使用します。このモデルでは、ユーザー、RAC 特権、およびネットワーク上の RAC デバイスを自由に組み合わせる柔軟性が備わる一方、複雑になることはありません。

Active Directory オブジェクトの概要

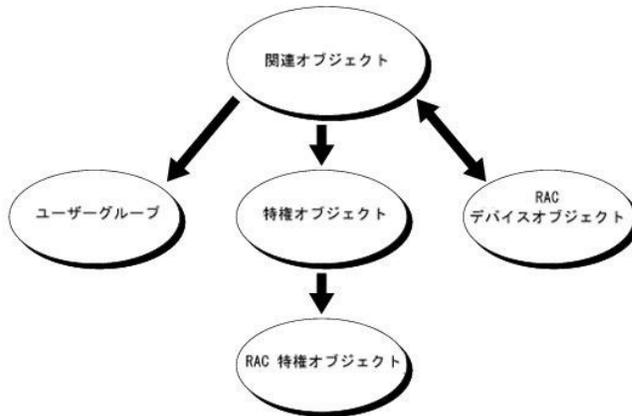
認証と許可のために Active Directory に統合するネットワーク上の物理的な RAC 1 台につき、少なくとも 1 個ずつ関連オブジェクトと RAC デバイスオブジェクトを作成しておきます。関連オブジェクトは複数作成することができ、それぞれにリンクできるユーザー、ユーザーグループ、RAC デバイスオブジェクトの数の制限はありません。ユーザーと RAC デバイスオブジェクトは、企業内のどのドメインのメンバーでもかまいません。

ただし、各関連オブジェクトは 1 つの特権オブジェクトにしかリンクできません。また、ユーザー、ユーザーグループ、RAC デバイスオブジェクトを 1 つの特権オブジェクトにしかリンクできません。この例では、システム管理者が特定の RAC で各ユーザーの特権を制御できます。

RAC デバイスオブジェクトは、Active Directory に認証と認可を照会するための RAC ファームウェアへのリンクです。RAC がネットワークに追加されると、システム管理者は Active Directory 名を使って RAC とそのデバイスオブジェクトを設定する必要があります。その結果、ユーザーは Active Directory を使って認証と承認を実行できます。さらに、システム管理者はユーザーが認証できるように、RAC を少なくとも 1 つの関連オブジェクトに追加する必要があります。

 6-1 は、すべての認証と認可に必要な接続を関連オブジェクトが提供する仕組みを示しています。

図 6-1. Active Directory オブジェクトの標準的な設定



メモ: RAC 特権オブジェクトは DRAC 4 と DRAC 5 の両方に適用されます。

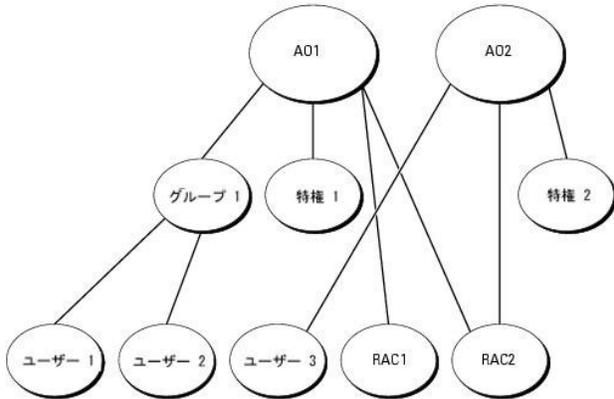
作成する関連オブジェクトの数に制限はありませんが、少なくとも 1 つは作成する必要があります。また、RAC (DRAC 5) を使って認証と承認ができるように Active Directory と統合するネットワーク上の各 RAC (DRAC 5) に RAC デバイスオブジェクトが 1 つ必要です。

関連オブジェクトには、RAC デバイスオブジェクトのほか、含めるユーザとグループの数にも制限がありません。ただし、関連オブジェクトに含まれる特権オブジェクトは、関連オブジェクト 1 つにつき 1 つだけです。関連オブジェクトは RAC (DRAC 5) に「特権」のある「ユーザー」を接続します。

また、Active Directory オブジェクトは、単一ドメインにでも複数ドメインにでも設定できます。たとえば、DRAC 5 カードが 2 枚 (RAC1 と RAC2)、既存の Active Directory ユーザーが 3 台 (user1、user2、user3) あるとします。user1 と user2 に 両方の DRAC 5 カードへの管理者権限を与え、user3 に RAC2 カードへのログイン特権を与えることにします。図 6-2 に、このシナリオで Active Directory オブジェクトを設定する方法を示します。

別のドメインからユニバーサルグループを追加する場合は、ユニバーサルスコープの関連オブジェクトを作成します。Dell Schema Extender ユーティリティを使って作成したデフォルト関連オブジェクトは、ドメインのローカルグループであるため、他のドメインのユニバーサルグループと相互作用できません。

図 6-2. 単一ドメインで Active Directory オブジェクトを設定する方法



単一ドメインでオブジェクトを設定するシナリオでは、次のタスクを実行します。

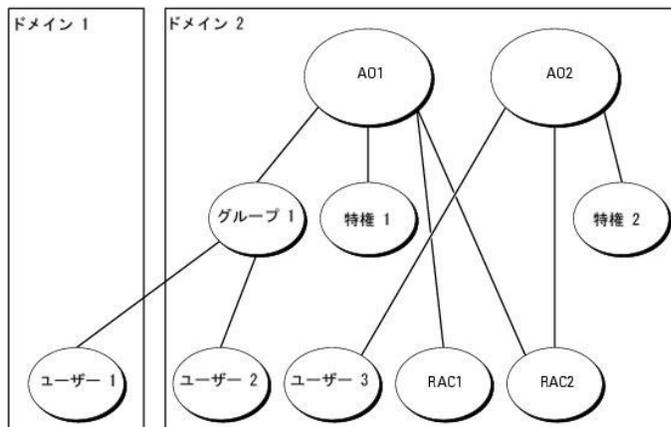
1. 関連オブジェクトを 2 つ作成します。
2. 2 枚の DRAC 5 カードを表す 2 つの RAC デバイスオブジェクト (RAC1 と RAC2) を作成します。
3. 2 つの特権オブジェクト Priv1 と Priv2 を作成し、Priv1 にはすべての特権 (システム管理者)、Priv2 にはログイン特権を与えます。
4. user1 と user2 を Group1 に入れます。
5. Group1 を関連オブジェクト 1 (A01) のメンバに、Priv1 を特権オブジェクトとして A01 に、RAC1、RAC2 を RAC デバイスとして A01 にそれぞれ追加します。
6. User3 をメンバとして関連オブジェクト 2 (A02) に、Priv2 を特権オブジェクトとして A02 に、RAC2 を RAC デバイスとして A02 に追加します。

詳しい手順については、「[Active Directory への DRAC 5 ユーザーと特権の追加](#)」を参照してください。

図 6-3 に、複数ドメインの Active Directory オブジェクトの例を示します。このシナリオでは、DRAC 5 カードが 2 枚 (RAC1 と RAC2)、既存の Active Directory ユーザーが 3 台 (user1、user2、user3) あるとします。user1 はドメイン 1 に、user2 と user3 はドメイン 2 にあります。このシナリオでは、両方の DRAC 5 カードへのシステム管理者特権を持つ user1 と user2 を設定し、RAC2 カ

ードへのログイン特権を持つ user3 を設定します。

図 6-3. 複数のドメインで Active Directory オブジェクトを設定する方法



複数ドメインでオブジェクトを設定するシナリオでは、次のタスクを実行します。

1. ドメインのフォレスト機能がネイティブまたは Windows 2003 モードにあることを確認します。
2. 2つの関連オブジェクトである(ユニバーサルスコープの)AO1とAO2を任意のドメインに作成します。
[図 6-3](#)に、ドメイン 2 のオブジェクトを示します。
3. 2枚の DRAC 5 カードを表す 2つの RAC デバイスオブジェクト(RAC1とRAC2)を作成します。
4. 2つの特権オブジェクト Priv1とPriv2を作成し、Priv1にはすべての特権(システム管理者)、Priv2にはログイン特権を与えます。
5. user1とuser2をGroup1に入れます。Group1のグループスコープはユニバーサルでなければなりません。
6. Group1を関連オブジェクト1(AO1)のメンバに、Priv1を特権オブジェクトとしてAO1に、RAC1、RAC2をRACデバイスとしてAO1にそれぞれ追加します。
7. User3をメンバとして関連オブジェクト2(AO2)に、Priv2を特権オブジェクトとしてAO2に、RAC2をRACデバイスとしてAO2に追加します。

DRAC 5 にアクセスするための Active Directory の設定

Active Directory を使って DRAC 5 にアクセスする前に、次の手順を実行して、Active Directory ソフトウェアと DRAC 5 を設定する必要があります。

1. Active Directory スキーマを拡張します([「Active Directory スキーマの拡張」](#)を参照)。
2. Active Directory ユーザーとコンピュータスナップインを拡張します([「Active Directory ユーザーとコンピュータスナップインへの Dell 拡張のインストール」](#)を参照)。
3. DRAC 5 ユーザーとその特権を Active Directory に追加します([「Active Directory への DRAC 5 ユーザーと特権の追加」](#)を参照)。
4. 各ドメインコントローラの SSL を有効にします([「ドメインコントローラの SSL の有効化」](#)を参照)。
5. DRAC 5 のウェブインタフェースまたは racadm CLI を使用して、DRAC 5 Active Directory のプロパティを設定します([「DRAC 5 の設定」](#)を参照)。

Active Directory スキーマの拡張

Active Directory スキーマを拡張すると、Dell の組織ユニット、スキーマクラスと属性、およびサンプル特権と関連オブジェクトが Active Directory スキーマに追加されます。スキーマを拡張する前に、ドメインフォレストのスキーママスター Flexible Single Master Operation (FSMO) Role Owner にスキーマ管理者特権が必要です。

次の方法を使用してスキーマを拡張できます。

1. Dell Schema Extender ユーティリティ
1. LDIF スクリプトファイル

LDIF スクリプトファイルを使用すると、デルの組織ユニットは追加されません。

LDIF ファイルと Dell のスキーマ拡張は、それぞれ『Dell Systems Management Consoles CD』の次のディレクトリにあります。

- 1 CD ドライブ*support\OMActiveDirectory Tools\RAC4\LDIF Files-5
- 1 CD ドライブ*support\OMActiveDirectory Tools\RAC4\Schema Extender-5

LDIF ファイルを使用するときは、LDIF ファイルディレクトリにある readme の説明を参照してください。Dell Schema Extender を使用して Active Directory スキーマを拡張するには、「[Dell スキーマ拡張の使用](#)」を参照してください。

スキーマ拡張または LDIF ファイルはどの場所からでもコピーと実行ができます。

Dell スキーマ拡張の使用

 **注意:** Dell Schema Extender は `SchemaExtenderOem.ini` ファイルを使用します。Dell のスキーマ拡張ユーティリティ機能が正しく機能するように、このファイルの名前は変更しないでください。

1. ようこそ画面で **次へ** をクリックします。
2. 警告を読んでから、もう一度 **次へ** をクリックします。
3. **現在のログイン認証情報の使用** を選択するか、スキーマ管理者権限を使ってユーザー名とパスワードを入力します。
4. **次へ** をクリックして、Dell スキーマ拡張を実行します。
5. **終了** をクリックします。

スキーマが拡張されます。スキーマ拡張子を確認するには、Microsoft 管理コンソール (MMC) と Active Directory スキーマスナップインを使用して、次のものがあることを確認します。

- 1 クラス ([表 6-1](#) から [表 6-6](#) を参照)
- 1 属性 ([表 6-7](#))

MMC における Active Directory のスキーマスナップインを有効にし使用する方法的詳細については、Microsoft のマニュアルを参照してください。

表 6-1. Active Directory スキーマに追加されたクラスのクラス定義

クラス名	割り当てられるオブジェクト識別番号 (OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

表 6-2. dellRacDevice クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.1
説明	Dell RAC デバイスを表します。RAC デバイスは Active Directory では dellRacDevice として設定する必要があります。この設定を使って、DRAC 5 は Lightweight Directory Access Protocol (LDAP) クエリを Active Directory に送信できます。
クラスタイプ	構造体クラス
スーパークラス	dellProduct
属性	dellSchemaVersion dellRacType

表 6-3. dellAssociationObject クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.2
説明	Dell 関連オブジェクトを表します。関連オブジェクトはユーザーとデバイスを結び付けます。
クラスタイプ	構造体クラス
スーパークラス	グループ

属性	dellProductMembers dellPrivilegeMember
----	---

表 6-4. dellRAC4Privileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.3
説明	DRAC 5 デバイスの特権 (承認権限) を定義します。
クラスタイプ	補助クラス
スーパークラス	なし
属性	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

表 6-5. dellPrivileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.4
説明	Dell の特権 (承認権限) のコンテナクラスとして使用します。
クラスタイプ	構造体クラス
スーパークラス	ユーザー
属性	dellRAC4Privileges

表 6-6. dellProduct クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.5
説明	これはメインのクラスで、このクラスからすべての Dell 製品が派生しています。
クラスタイプ	構造体クラス
スーパークラス	コンピュータ
属性	dellAssociationMembers

表 6-7. Active Directory スキーマに追加される属性のリスト

属性名 / 説明	割り当てられる OID/ 構文オブジェクト識別子	単数値
dellPrivilegeMember この属性に属する dellPrivilege オブジェクトのリスト。	1.2.840.113556.1.8000.1280.1.1.2.1 識別名 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers この役割に属する dellRacDevices オブジェクトのリスト。この属性は dellAssociationMembers 後方リンクへの前方リンクです。 リンク ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 識別名 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser ユーザーがデバイスでログイン権限を持っている場合には TRUE。	1.2.840.113556.1.8000.1280.1.1.2.3 ブーリアン (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin ユーザーがデバイスでカード設定権限を持っている場合には TRUE。	1.2.840.113556.1.8000.1280.1.1.2.4 ブーリアン (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin	1.2.840.113556.1.8000.1280.1.1.2.5	TRUE

ユーザーがデバイスでユーザー設定権限を持っている場合は TRUE。	ブーリアン (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
dellsLogClearAdmin ユーザーがデバイスでログのクリア権限を持っている場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.6 ブーリアン (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellsServerResetUser ユーザーがデバイスでサーバーリセット権限を持っている場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.7 ブーリアン (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellsConsoleRedirectUser ユーザーがデバイスでコンソールリダイレクト権限を持っている場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.8 ブーリアン (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellsVirtualMediaUser ユーザーがデバイスで仮想メディア権限を持っている場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.9 ブーリアン (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellsTestAlertUser ユーザーがデバイスでテスト警告ユーザー権限を持っている場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.10 ブーリアン (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellsDebugCommandAdmin ユーザーがデバイスでデバッグコマンド管理者権限を持っている場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.11 ブーリアン (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion 現在のスキーマバージョンを使って、スキーマをアップデートします。	1.2.840.113556.1.8000.1280.1.1.2.12 ケース無視文字列 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType この属性は、dellRacDevice オブジェクトの現在の Rac の種類で、dellAssociationObjectMembers 前方リンクへの後方リンクです。	1.2.840.113556.1.8000.1280.1.1.2.13 ケース無視文字列 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers この製品に属する dellAssociationObjectMembers のリスト。この属性は dellProductMembers リンク属性への後方リンクです。 リンク ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 識別名 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Active Directory ユーザーとコンピュータのスナップインへの Dell 拡張機能のインストール

Active Directory でスキーマを拡張する場合は、RAC (DRAC 5) デバイス、ユーザーとユーザーグループ、RAC の関連、RAC の特権などを管理できるように、Active Directory ユーザーとコンピュータスナップインも拡張する必要があります。

『Dell Systems Management Consoles CD』を使用して Systems Management Software をインストールする場合は、インストール時に **Active Directory ユーザーおよび コンピュータスナップインへの Dell 拡張子** オプションを選択すると、スナップインを拡張できます。Systems Management Software のインストールの詳細については、『Dell OpenManage ソフトウェアクイックインストールガイド』を参照してください。

Active Directory ユーザーとコンピュータスナップインの詳細については、Microsoft のマニュアルを参照してください。

Administrator Pack のインストール

Active Directory DRAC 5 オブジェクトを管理している各システムに、Administrator Pack をインストールする必要があります。Administrator Pack をインストールしないと、コンテナ内の Dell RAC オブジェクトを表示できません。

詳細については、「[Active Directory ユーザーとコンピュータスナップインを開く](#)」を参照してください。

Active Directory ユーザーとコンピュータスナップインを開く

Active Directory ユーザーとコンピュータスナップインを開くには、次の手順を実行してください。

- ドメインコントローラにいる場合は、**管理ツール** → **Active Directory ユーザー コンピュータ** の順にクリックします。

ドメインコントローラにログインしていない場合は、適切な Microsoft Administrator Pack がローカルシステムにインストールされている必要があります。この Administrator Pack をインストールするには、**スタート** → **ファイル名を指定して実行** をクリックし、MMC と入力してから **Enter** を押します。

Microsoft 管理コンソール (MMC) が表示されます。

2. **コンソール 1** ウィンドウで **ファイル**(Windows 2000 を実行しているシステムでは **コンソール**)をクリックします。
3. **追加 / 削除 スナップイン** をクリックします。
4. **Active Directory ユーザーとコンピュータ** スナップインを選択し、**追加** クリックします。
5. **閉じる** をクリックして、**OK** をクリックします。

Active Directory への DRAC 5 ユーザーと特権の追加

Dell の拡張 Active Directory ユーザーとコンピュータスナップインを使用して、RAC、関連、および特権オブジェクトを作成すると、DRAC 5 ユーザーと特権を追加できます。各オブジェクトタイプを追加するには、次の手順を実行します。

- 1 RAC デバイスオブジェクトを作成する
- 1 特権オブジェクトを作成する
- 1 関連オブジェクトを作成する
- 1 関連オブジェクトにオブジェクトを追加する

RAC デバイスオブジェクトの作成

1. MMC **コンソールルート** ウィンドウで、コンテナを右クリックします。
2. **新規作成** → **Dell RAC オブジェクト** をクリックします。
新しいオブジェクト ウィンドウが表示されます。
3. 新しいオブジェクトの名前を入力します。この名前は、「[DRAC 5 の設定](#)」の [手順 7](#) で入力する DRAC 5 名と一致する必要があります。
4. **RAC デバイスオブジェクト** を選択します。
5. **OK** をクリックします。

特権オブジェクトの作成

 **メモ:** 特権オブジェクトは、関係する関連オブジェクトと同じドメインに作成する必要があります。

1. **コンソールルート**(MMC) ウィンドウで、コンテナを右クリックします。
2. **新規作成** → **Dell RAC オブジェクト** を選択します。
新しいオブジェクト ウィンドウが表示されます。
3. 新しいオブジェクトの名前を入力します。
4. **特権オブジェクト** を選択します。
5. **OK** をクリックします。
6. 作成した特権オブジェクトを右クリックして、**プロパティ** を選択します。
7. **RAC 特権** タブをクリックして、ユーザーに与える DRAC 4 特権を選択します(詳細は [表 4-8](#) を参照)。

関連オブジェクトの作成

関連オブジェクトはグループから派生し、グループタイプが含まれている必要があります。関連スコープで、関連オブジェクトのセキュリティグループタイプを指定します。関連オブジェクトを作成する場合は、追加するオブジェクトの種類に適用される関連のスコープを選択します。

たとえば、**ユニバーサル** を選択すると、関連オブジェクトは Active Directory ドメインがネイティブモード以上で機能するときのみ使用可能になります。

1. **コンソールルート**(MMC)ウィンドウで、コンテナを右クリックします。
2. **新規作成**→ **Dell RAC オブジェクト** を選択します。
新規オブジェクト ウィンドウが開きます。
3. 新しいオブジェクトの名前を入力します。
4. **関連オブジェクト** を選択します。
5. **関連オブジェクト** のスコープを選択します。
6. **OK** をクリックします。

関連オブジェクトへのオブジェクトの追加

関連オブジェクトプロパティ ウィンドウを使用すると、ユーザーやユーザーグループ、特権オブジェクト、RAC デバイスや RAC デバイスグループを関連付けることができます。Windows 2000 モード以上のシステムを使用している場合は、ユニバーサルグループを使ってユーザーまたは RAC オブジェクトでドメインを拡張する必要があります。

ユーザーと RAC デバイスのグループを追加できます。Dell 関連グループと Dell に関連しないグループを作成する手順は同じです。

ユーザーまたはユーザーグループの追加

1. **関連オブジェクト** を右クリックして、**プロパティ** を選択します。
2. **ユーザー** タブを選択して、**追加** をクリックします。
3. ユーザーまたはユーザーグループ名を入力して、**OK** をクリックします。

ユーザーの特権やユーザーグループの特権を定義する特権オブジェクトを関連に追加するには、RAC デバイスに認証するときに **特権オブジェクト** タブをクリックします。関連オブジェクトに追加できる特権オブジェクトは 1 つだけです。

特権の追加

1. **特権オブジェクト** タブを選択し、**追加** をクリックします。
2. 特権オブジェクト名を入力し、**OK** をクリックします。

製品 タブをクリックして、1 つまたは複数の RAC デバイスを関連に追加します。関連デバイスは、ネットワークに接続している RAC デバイスのうち、定義したユーザーまたはユーザーグループが使用できるものを指定します。関連オブジェクトには複数の RAC デバイスを追加できます。

RAC デバイスまたは RAC デバイスグループの追加

RAC デバイスまたは RAC デバイスグループを追加するには、次の操作を実行します。

1. **製品** タブを選択して、**追加** をクリックします。
2. RAC デバイスまたは RAC デバイスグループ名を入力して、**OK** をクリックします。
3. **プロパティ** ウィンドウで、**適用**、**OK** の順にクリックします。

ドメインコントローラの SSL の有効化

Microsoft Enterprise ルート CA を使ってすべてのドメインコントローラを SSL 証明書に自動的に割り当てる場合は、次の手順を実行して各ドメインコントローラで SSL を有効にする必要があります。

1. Microsoft Enterprise ルート CA をドメインコントローラにインストールします。
 - a. **スタート**→**コントロール パネル**→**プログラムの追加と削除** の順に選択します。
 - b. **Windows コンポーネントの追加 / 削除** を選択します。

- c. Windows コンポーネントウィザードで、**証明書サービス** チェックボックスをオンにします。
 - d. CAの種類として **Enterprise ルート CA** を選択し、**次へ** をクリックします。
 - e. この CA の **共通名 (CN)** を入力し、**次へ** をクリックしてから、**終了** をクリックします。
2. 各コントローラに SSL 証明書をインストールして、それぞれのドメインコントローラで SSL を有効にします。
 - a. **スタート**→**管理ツール**→**ドメイン セキュリティ ポリシー** の順にクリックします。
 - b. **公開キーポリシー** フォルダを展開し、**自動証明書要求設定** を右クリックして、**自動証明書要求** をクリックします。
 - c. **自動証明書要求セットアップウィザード** で、**次へ** をクリックし、**ドメインコントローラ** を選択します。
 - d. **次へ** をクリックして、**終了** をクリックします。

ドメインコントローラルート CA 証明書のエクスポート

 **メモ:** Windows 2000 を実行しているシステムでは、次の手順が異なる場合があります。

1. Microsoft Enterprise CA サービスを実行しているドメインコントローラを見つけます。
2. **スタート**→**ファイル名を指定して実行** の順にクリックします。
3. **ファイル名を指定して実行** のフィールドに「mmc」と入力し、**OK** をクリックします。
4. **コンソール 1 (MMC)** ウィンドウで、**ファイル** (Windows 2000 システムでは **コンソール**) をクリックし、**スナップインの追加 / 削除** を選択します。
5. **スナップインの追加 / 削除** ウィンドウで、**追加** をクリックします。
6. **スタンドアロンスナップイン** ウィンドウで、**証明書** を選択し、**追加** をクリックします。
7. **コンピュータ** アカウントを選択し、**次へ** をクリックします。
8. **ローカルコンピュータ** を選択し、**終了** をクリックします。
9. **OK** をクリックします。
10. **コンソール 1** ウィンドウで、**証明書** フォルダを展開し、**個人** フォルダを展開してから、**証明書** フォルダをクリックします。
11. ルート CA 証明書を見つけて右クリックし、**すべてのタスク** を選択して、**エクスポート...** をクリックします。
12. **証明書のエクスポートウィザード** で、**次へ** をクリックし、**プライベートキーをエクスポートしない** を選択します。
13. **次へ** をクリックして、フォーマットとして **Base-64 エンコード X.509 (.cer)** を選択します。
14. **次へ** をクリックしてシステムのディレクトリに証明書を保存します。
15. [ステップ 14](#) で DRAC 5 に保存した証明書をアップロードします。

RACADMを使って証明書をアップロードするには、「[RACADMを使用した DRAC 5 Active Directory の設定](#)」を参照してください。

ウェブインタフェースを使って証明書をアップロードするには、次の手順を実行します。

- a. サポートされている Web ブラウザのウィンドウを開きます。
- b. DRAC 5 ウェブインタフェースにログインします。
- c. **システム** ツリーを展開して **リモートアクセス** をクリックします。
- d. **設定** タブをクリックして、**セキュリティ** をクリックします。
- e. **セキュリティ証明書のメインメニュー** ページの **サーバー証明書のアップロード** を選択して、**適用** をクリックします。
- f. **証明書のアップロード** 画面で、次の手順の 1 つを実行します。
 - o **参照** をクリックして証明書を選択します。
 - o **値** のフィールドに証明書のパスを入力します。
- g. **適用** をクリックします。

DRAC 5 ファームウェア SSL 証明書のインポート

次の手順を使って、すべてのドメインコントローラの信頼された証明書のリストに DRAC 5 ファームウェア SSL 証明書をインポートします。

 **メモ:** Windows 2000 を実行しているシステムでは、次の手順が異なる場合があります。

 **メモ:** DRAC 5 ファームウェア SSL 証明書が既知の CA によって署名されている場合は、この手順を実行する必要はありません。

DRAC 5 の SSL 証明書は、DRAC 5 Web サーバーで使用される証明書と同じです。DRAC 5 のコントローラには、デフォルトの自己署名証明書が同梱されています。

DRAC 5 ウェブインタフェースを使って証明書にアクセスするには、**設定** → **Active Directory** → **DRAC 5 サーバー証明書のダウンロード** の順に選択します。

1. ドメインコントローラで **MMC コンソール** ウィンドウを開き、**証明書** → **信頼されたルート認証局** の順に選択します。
2. **証明書** を右クリックし、**すべてのタスク** を選択して、**インポート** をクリックします。
3. **次へ** をクリックして、SSL 証明書ファイルを参照します。
4. 各ドメインコントローラの **信頼されたルート認証局** に RAC SSL 証明書をインストールします。

ユーザー独自の証明書をインストールしている場合は、証明書に署名をしている CA が **信頼されたルート認証局** リストにあることを確認します。認証局がリストにない場合は、それをすべてのドメインコントローラにインストールする必要があります。

5. **次へ** をクリックし、証明書の種類に基づいて Windows に自動的に証明書ストアを選択させるか、指定するストアまで参照します。
6. **終了** をクリックして、**OK** をクリックします。

DRAC 5 の設定

1. サポートされている Web ブラウザのウィンドウを開きます。
2. DRAC 5 ウェブインタフェースにログインします。
3. **システム** ツリーを展開して **リモートアクセス** をクリックします。
4. **設定** タブをクリックして **Active Directory** を選択します。
5. **Active Directory メインメニュー** ページの **Active Directory を設定する** を選択して、**次へ** をクリックします。
6. **Active Directory を有効にする** チェックボックスをオンにします。
7. **DRAC 名** を入力します。この名前は、先にドメインコントローラで作成した RAC オブジェクトの共通名と同じでなければなりません。(「[RAC デバイスオブジェクトの作成](#)」の [ステップ 3](#) を参照してください)。
8. **ルートドメイン名** を入力します。**ルートドメイン名** はフォレストの完全修飾ルートドメイン名です。
9. **DRAC ドメイン名** を入力します (drac5.com など)。NetBIOS 名は使用しないでください。**DRAC ドメイン名** は RAC デバイスオブジェクトがあるサブドメインの完全修飾ドメイン名です。
10. **タイムアウト** の時間を秒で入力します。
11. **適用** をクリックして、Active Directory の設定を保存します。
12. **Active Directory メインメニューに戻る** をクリックします。
13. ドメインフォレストのルート CA 証明書を DRAC 5 にアップロードします。
 - a. **Active Directory CA 証明書をアップロードする** チェックボックスをオンにして、**次へ** をクリックします。
 - b. **証明書のアップロード** ページで、証明書のファイルパスを入力するか、証明書ファイルまで参照して **適用** をクリックします。

 **メモ:** アップロードする証明書の相対パスが **ファイルパス** の値に表示されます。フルパスと完全なファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

ドメインフォレストのドメインコントローラの SSL 証明書は、このルート CA 証明書に署名をしている必要があります。ルート CA 証明書をローカルシステムで使用できるようにします(「[ドメインコントローラのルート CA 証明書のエクスポート](#)」を参照)

DRAC 5 Web サーバーは、**適用** をクリックすると自動的に再起動します。

- DRAC 5 Active Directory 機能の設定を完了するには、ログアウトしてから DRAC 5 にログインします。
- システム ツリーで **リモートアクセス** をクリックします。
- 設定** タブをクリックして **ネットワーク** をクリックします。
ネットワーク設定 ページを再ロードします。
- ネットワーク設定** で **DHCP を使用 (NIC IP アドレス用)** を選択している場合は、**DNS サーバーアドレスの取得に DHCP を使用** を選択します。
DNS サーバー IP アドレスを手動で入力する場合は、**DNS サーバーアドレスの取得に DHCP を使用** をオフにし、一次および代替 DNS サーバー IP アドレスを入力します。
- 変更の適用** をクリックします。
これで、DRAC 5 Active Directory 機能の設定が完了します。

RACADM を使用した DRAC 5 Active Directory 設定の設定

ウェブインタフェースでなく、RACADM を使用して DRAC 5 Active Directory 機能を設定するには、次のコマンドを使用します。

- コマンドプロンプトを開き、次の RACADM コマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1  
  
racadm config -g cfgActiveDirectory -o cfgADRacDomain <完全修飾 RAC ドメイン名>  
  
racadm config -g cfgActiveDirectory -o cfgADRootDomain <完全修飾ルートドメイン名>  
  
racadm config -g cfgActiveDirectory -o cfgADRacName <RAC 共通名>  
  
racadm sslcertupload -t 0x2 -f <ADS ルート CA 証明書>  
  
racadm sslcertdownload -t 0x1 -f <RAC SSL 証明書>
```

- DRAC 5 で DHCP が有効になり、DHCP サーバーが提供する DNS を使用する場合は、次のように入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
```

- DRAC 5 で DHCP が無効になっている場合、または手動で DNS IP アドレスを入力する場合は、次のように入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0  
  
racadm config -g cfgLanNetworking -o cfgDNSServer1 <一次 DNS IP アドレス>  
  
racadm config -g cfgLanNetworking -o cfgDNSServer2 <二次 DNS IP アドレス>
```

- <Enter>** を押して、DRAC 5 Active Directory 機能の設定を完了します。

Active Directory を使用して DRAC 5 にログインする方法

次のいずれかの方法を使用すると、Active Directory を使って DRAC 5 にログインできます。

- ウェブインタフェース
- リモート RACADM
- シリアルまたは telnet コンソール。

ログイン構文は、この 3 つの方法で共通しています。

<ユーザー名@ドメイン>

または

<ドメイン>\<ユーザー名> または <ドメイン>/<ユーザー名>

「ユーザー名」は、1 ~ 256 バイトの ASCII 文字列です。

ユーザー名とドメイン名に、空白スペースや特殊文字 (¥、/、または @ など) は使用できません。

 **メモ:** "America" などの NetBIOS ドメイン名は名前解決できないため、指定できません。

よくあるお問い合わせ(FAQ)

[表 6-8](#) に、よくあるお問い合わせ(FAQ)とその回答を示します。

表 6-8. Active Directory での DRAC 5 の使い方: よくあるお問い合わせ(FAQ)

質問	回答
複数のフォレストで Active Directory を使って DRAC 5 にログインできますか?	DRAC 5 の Active Directory クエリアルゴリズムでは、1 つのフォレストで 1 つのツリーだけをサポートしていません。
混合モードで Active Directory を使って DRAC 5 にログインできますか(フォレストのドメインコントローラが Microsoft Windows NT® 4.0、Windows 2000、Windows Server 2003 など種類の異なるオペレーティングシステムを実行している場合)?	はい。混合モードでは、DRAC 5 クエリプロセスが使用するすべてのオブジェクト(ユーザー、RAC デバイスオブジェクト、関連オブジェクト)は、同一のドメインになければなりません。 デル拡張 Active Directory ユーザーとコンピュータスナップインはモードをチェックし、混合モードであれば、ドメイン間でオブジェクトを作成するためにユーザーを制限します。
Active Directory と DRAC 5 の使用は複数のドメイン環境をサポートしていますか?	はい。ドメインフォレスト機能のレベルがネイティブまたは Windows 2003 モードでなければなりません。さらに、関連オブジェクト、RAC ユーザーオブジェクト、および RAC デバイスオブジェクト(関連オブジェクトを含む)間のグループがユニバーサルグループでなければなりません。
これらのデル拡張オブジェクト(デル関連オブジェクト、Dell RAC デバイス、およびデル特権オブジェクト)が別のドメインにあってもかまいませんか?	関連オブジェクトと特権オブジェクトは、同じドメインになければなりません。Dell 拡張 Active Directory ユーザーとコンピュータスナップインを使用すると、同じドメインにこれら 2 つのオブジェクトを作成するように強制されます。その他のオブジェクトは別のドメインに作成できます。
ドメインコントローラ SSL 設定に制限はありますか?	はい。フォレストにある Active Directory サーバーの SSL 証明書は、すべて同じルートによって署名される必要があります。これは、DRAC 5 でアップロードできる信頼された CA SSL 証明書は 1 つだけからです。
新しい RAC 証明書を作成してアップロードしましたが、ウェブインタフェースが起動しません。	Microsoft 証明書サービスを使用して RAC 証明書を生成した場合、証明書の作成時に Web 証明書 でなく ユーザー証明書 を誤って選択した可能性があります。この問題を修正するには、Microsoft 証明書サービスから新しい Web 証明書を作成し、管理下システムから RACADM を使ってロードします。次のように入力してください。 <pre>racadm sslcertupload -t 0x1 -f <Web SSL 証明書></pre>
Active Directory 認証を使って DRAC 5 にログインできない場合は、どうすればよいでしょうか? トラブルシューティングの方法を教えてください。	<ol style="list-style-type: none">ログイン中、NetBIOS 名ではなく、正しいユーザードメイン名を使用していることを確認します。ローカル DRAC ユーザーアカウントがある場合は、ローカルの資格情報を使用して DRAC 5 にログインします。 <p>ログインした後、次の手順を実行してください。</p> <ol style="list-style-type: none">DRAC 5 Active Directory 設定ページにある Active Directory を有効にする ボックスがオンになっていることを確認します。DRAC 5 ネットワーク設定ページの DNS 設定が正しいことを確認します。Active Directory ルート CA から DRAC 5 に Active Directory 証明書をアップロードしたことを確認します。ドメインコントローラの SSL 証明書の有効期限が切れていないことを確認します。DRAC 5 名、ルートドメイン名、および DRAC 5 ドメイン名 が Active Directory の環境設定と一致していることを確認します。DRAC 5 のパスワードが 127 文字以下であることを確認します。DRAC 5 が最大 256 文字のパスワードをサポートしている一方、Active Directory がサポートしているパスワードは、最大 127 文字です。

[目次ページに戻る](#)

[目次ページに戻る](#)

コンソールリダイレクトの使用

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

- [概要](#)
- [コンソールリダイレクトの使用](#)
- [Video Viewer の使用](#)
- [よくあるお問い合わせ \(FAQ\)](#)

この項では、DRAC 5 コンソールリダイレクト機能の使用法について説明します。

概要

DRAC 5 コンソールリダイレクト機能を使用すると、グラフィックまたはテキストモードでローカルサーバーコンソールにリモートでアクセスできます。この機能を使用すると、1 つの場所から単一または複数の DRAC 5 システムを制御できます。

今日の高度なネットワークとインターネットを利用すると、各サーバーの前に座って定期メンテナンスのすべてを実行する必要はありません。別の都市、または地球の反対側にいても、デスクトップやラップトップを使ってサーバーを管理できます。また、リモートから瞬時に他のユーザーと情報を共有することもできます。

コンソールリダイレクトの使用

 **メモ:** コンソールリダイレクトのセッションを開くと、管理下システムにはそのコンソールがリダイレクトされていることが表示されません。

コンソールリダイレクト ページで、ローカルの管理ステーションのキーボード、ビデオ、マウスなどを使ってリモートシステムを管理し、リモート管理下システムで対応するデバイスを制御できます。この機能を仮想メディア機能と併用すると、リモートソフトウェアのインストールを実行することもできます。

コンソールリダイレクトセッションには次の規則が適用されます。

- 1 同時コンソールリダイレクトは 2 セッションのみがサポートされています。
- 1 コンソールリダイレクトセッションは 1 台のリモートターゲットシステムのみ接続可能です。
- 1 ローカルシステムでは、コンソールリダイレクトセッションを設定できません。
- 1 1 MB/sec 以上の使用可能ネットワーク帯域幅が必要です。

管理下システムの対応画面解像度およびリフレッシュレート

[表 7-1](#)は、管理下システムで起動しているコンソールリダイレクトセッションの対応画面解像度および対応リフレッシュレートを一覧しています。

表 7-1. 対応画面解像度およびリフレッシュレート

画面解像度	リフレッシュレート(Hz)
720x400	70
640x480	60、72、75、85
800x600	60、70、72、75、85
1024x768	60、70、72、75、85
1280x1024	60

管理ステーションの設定

管理ステーションでコンソールリダイレクトを使用するには、次の手順を実行してください。

1. 対応ウェブブラウザをインストールして設定します。詳細については、以下の項を参照してください。

- [対応 Web ブラウザ](#)

 **注意:** コンソールリダイレクトおよび仮想メディアは、32 ビットウェブブラウザのみをサポートしています。64 ビットウェブブラウザの使用は、予期しない結果や故障の原因となる可能性があります。

- [対応 Web ブラウザの設定](#)

1. モニターの画面解像度を 60 Hz で最小 1280 x 1024 ピクセル、128 色に設定します。このように設定しなければ、コンソールを **全画面表示モード** で表示できない可能性があります。

コンソールリダイレクトの設定

1. 管理ステーションで、対応 Web ブラウザを開いて DRAC 5 にログインします。詳細については、「[ウェブインタフェースへのアクセス](#)」を参照してください。
2. システム ツリーで **システム** をクリックします。
3. **コンソール** タブをクリックして、**ネットワーク** をクリックします。
4. **コンソールリダイレクト設定** ページで、[表 7-2](#) の情報を使用してコンソールリダイレクトセッションを設定し、**変更の適用** をクリックします。

表 7-2. コンソールリダイレクト設定ページの情報

情報	説明
有効	オン=有効、オフ=無効。
最大セッション数	使用できるコンソールリダイレクトセッション数を表示します。
アクティブセッション	アクティブなコンソールリダイレクトセッション数を表示します。
キーボードおよびマウスポート番号	デフォルト = 5900
ビデオポート番号	デフォルト = 5901
ビデオ暗号化の有効	オン=有効、オフ=無効。

コンソールリダイレクト設定 ページでは、[表 7-3](#) に示したボタンを使用できます。

表 7-3. コンソールリダイレクト設定ページの情報

プロパティ	説明
印刷	コンソールリダイレクト ページを印刷します。
更新	コンソールリダイレクト ページを印刷します。
変更の適用	設定を保存します。

コンソールリダイレクトセッションの開始

コンソールリダイレクトのセッションを開くと、Dell Virtual KVM Viewer アプリケーションが起動し、リモートシステムのデスクトップがビューアに表示されます。この仮想 KVM アプリケーションを使用すると、ローカルまたはリモートの管理ステーションからシステムのマウスとキーボードの機能を制御できます。

コンソールリダイレクトセッションを開くには、次の手順を実行してください。

1. 管理ステーションで、対応 Web ブラウザを開いて DRAC 5 にログインします。詳細については、「[ウェブインタフェースへのアクセス](#)」を参照してください。
2. システム ツリーでは、**システム** をクリックし、**コンソール** タブの **コンソールリダイレクト** をクリックします。

 **メモ:** コンソールリダイレクトプラグインをインストールおよび実行するようセキュリティ警告プロンプトを受け取った場合、プラグインの信頼性を確認し、**はい** をクリックして、プラグインをインストールおよび実行します。Firefox を実行している場合は、ブラウザを再起動してから、[ステップ 1](#) に進みます。

3. **コンソールリダイレクト** ページで、[図 7-4](#) の情報を使用してコンソールリダイレクトセッションが利用可能であることを確認します。

表 7-4. コンソールリダイレクト設定ページの情報

プロパティ	説明
状態	接続または切断
最大セッション数	サポートしているコンソールリダイレクトの最大セッション数を表示します。
アクティブセッション	現在アクティブなコンソールリダイレクトのセッション数を表示します。
コンソールリダイレクトの有効	はい / いいえ
ビデオ暗号化の有効	はい / いいえ

コンソールリダイレクト ページでは、[表 7-5](#) に示したボタンを使用できます。

表 7-5. コンソールリダイレクト設定ページのボタン

ボタン	定義
更新	コンソールリダイレクト ページを印刷します。
接続	目的のリモートシステムのコンソールリダイレクトセッションを開きます。

4. コンソールリダイレクトセッションが使用可能であれば、**接続** をクリックします。

 **メモ:** アプリケーションが起動した後、複数のメッセージボックスが表示される場合があります。アプリケーションへの不正なアクセスを防ぐため、これらのメッセージボックスは 3 分以内に参照してください。そうでない場合は、アプリケーションの再起動プロンプトが表示されます。

 **メモ:** 以降の手順の途中で複数の **セキュリティ警告** ウィンドウが表示された場合は、その内容を読んでから、**はい** をクリックして続行します。

管理ステーションが DRAC 5 に接続し、リモートシステムのデスクトップに Dell Digital KVM Viewer アプリケーションが表示されます。

5. リモートシステムのデスクトップにマウスポインタが 2 つ表示された場合は、管理ステーションとリモートシステムのマウスポインタを同期します。「マウスポインタの同期」を参照してください。

Video Viewer の使用

Video Viewer は管理ステーションとリモートシステム間のユーザーインターフェイスを提供するので、管理ステーション側からリモートシステムのデスクトップを表示して、そのマウスやキーボード機能を制御できます。リモートシステムに接続すると、別のウィンドウで Video Viewer が開始します。

Video Viewer では、ビデオ補正、マウスアクセラレータ、スナップショットなど、さまざまな制御を調整できます。これらの機能の詳細については、**ヘルプ** をクリックしてください。

コンソールリダイレクトのセッションを開始し、Video Viewer が表示されたら、リモートシステムを正しく表示、制御するために、次のコントロールを調整する必要があります。これらの調整には以下が含まれます。

1. Viewer のメニューバーへのアクセス
1. ビデオ画質の調整
1. マウスポインタの同期

Viewer メニューバーへのアクセス

Viewer メニューバーは、非表示メニューバーです。メニューバーにアクセスするには、カーソルを Viewer のデスクトップウィンドウの上端中央部分に動かします。

デフォルトファンクションキー <F9> を押して、メニューバーを有効にすることもできます。このファンクションキーに新しい関数を再割り当てする場合は、次の手順を実行してください。

1. <F9> を押すか、またはマウスカーソルを Video Viewer の上部に動かします。
2. 「画鋏」を押して、Viewer メニューバーをロックします。
3. Viewer メニューバーの**ツール** をクリックして、**セッション** オプションを選択します。
4. **セッションオプション** ウィンドウで、**一般** タブをクリックします。
5. **メニューのアクティブ化キー入力** ボックスの **一般** タブウィンドウで、ドロップダウンメニューをクリックして他のファンクションキーを選択します。
6. **適用** をクリックし、次に **OK** をクリックします。

[表 7-6](#) で、Viewer メニューバーから使用できる主な機能について説明します。

表 7-6. Viewer メニューバーの選択

メニュー アイテム	アイテム	説明
ファイル	ファイルにキャプチャ	現在のリモートシステム画面をローカルシステムの .bmp (Windows) または .png (Linux) ファイルにキャプチャします。ダイアログボックスが表示されたら、ファイルを指定の場所に保存できます。
	終了	コンソールリダイレクト ページを終了します。
表示	更新	リモートシステム画面のビューポート全体をアップデート更新します。
	全画面表示	セッション画面を、ウィンドウから全画面表示に拡大します。
マクロ	各種キーボードショートカット	リモートシステムでキース入力のコンビネーションを実行します。 管理ステーションの キーボードをリモートシステムに接続してマクロを実行するには、次の手順を実行してください。 1. ツール をクリックします。

		<ol style="list-style-type: none"> 2. セッションオプション ウィンドウで、一般 タブをクリックします。 3. すべてのキー入力をターゲットにパスする を選択します。 4. OK をクリックします。 5. マクロ をクリックします。 6. マクロ メニューで、ターゲットシステムに実行するキー入力のコンビネーションをクリックします。
ツール	自動ビデオ調整	Session Viewer ビデオ出力を再調整します。
	手動ビデオ調整	Session Viewer ビデオ出力を手動で調整するための個別のコントロールがあります。 メモ: 水平位置を中央から外して調整すると、マウスポインタが非同期になります。
	セッションオプション	Session Viewer コントロールの調整を追加します。 マウス タブでは、使用しているオペレーティングシステムを選択して、コンソールリダイレクトのマウスの性能を最適化できます。 Windows、Linux、またはなし を選択します。 一般 タブには、次のオプションがあります。 <ol style="list-style-type: none"> 1. キーボードのパススルーモード — リモートシステムに管理ステーションのキー入力を渡すには、すべてのキー入力をターゲットにパスする を選択します。 1. メニューのアクティブ化キー入力 — Viewer のメニューバーをアクティブするファンクションキーを選択します。 ツールバー タブで、 ツールバーの非表示の遅延時間 の時間を 1 ~ 10 秒に調整できます。
ヘルプ	なし	ヘルプ メニューをアクティブにします。

ビデオ画質の調整

Video Viewer にはビデオ画像の調整機能があり、これを使用してビデオ画像の表示を最適化できます。詳細については、**ヘルプ** をクリックしてください。

自動にビデオ画質を調整するには、次の手順を実行してください。

1. Viewer のメニューバーにアクセスします。「[Viewer メニューバーへのアクセス](#)」を参照してください。
2. **ツール** をクリックして、**自動ビデオ調整** を選択します。

ビデオ画質が再調整されて、Session Viewer が再度表示されます。

手動でビデオ画質を調整するには、次の手順を実行してください。

1. Viewer のメニューバーにアクセスします。「[Viewer メニューバーへのアクセス](#)」を参照してください。
2. **ツール** をクリックして、**手動ビデオ調整** を選択します。
3. **ビデオ調整** ウィンドウで、必要に応じて個々のビデオ調整ボタンをクリックしてコントロールを調整します。

ビデオ画質を手動で調整するときは、次のガイドラインに従ってください。

1. マウスポインタが非同期になるのを防ぐには、水平設定を調整して、リモートシステムのデスクトップをセッションウィンドウの中央に配置します。
1. ピクセル異音率の設定を 0 に減少すると、複数のビデオ更新コマンドが発行されて、ネットワークトラフィックが過剰になり、Video Viewer でビデオのちらつきが生じます。ネットワークトラフィックを最小限に抑えながら、システムパフォーマンスとピクセル効果が最適化されるレベルに [ピクセル異音比] 設定を調整することをお勧めします。

マウスポインタの同期

コンソールリダイレクトを使用してリモートの PowerEdge システムに接続すると、リモートシステムのマウススピードが管理ステーションのマウスポインタと同期していないために、Video Viewer ウィンドウにマウスポインタが 2 個表示される場合があります。

マウスポインタを同期するは、次の手順を実行してください。

1. Viewer のメニューバーにアクセスします。「[Viewer メニューバーへのアクセス](#)」を参照してください。
2. **ツール** をクリックして、**セッションオプション** を選択します。
3. **マウス** タブをクリックし、管理ステーションのオペレーティングシステムを選択して、**OK** をクリックします。
4. **ツール** をクリックして、**手動ビデオ調整** を選択します。
5. 水平コントロールを調整して、セッションウィンドウの中央にリモートシステムデスクトップが表示されるようにします。

6. OK をクリックします。

Linux (Red Hat or Novell) を使用している場合、オペレーティングシステムのデフォルトマウス設定は、DRAC 5 コンソールリダイレクト画面のマウスの矢印の制御に使用されています。マウスの同期化問題を回避するために、すべてのユーザーはデフォルトのマウス設定を使用するようにしてください。

よくあるお問い合わせ (FAQ)

表 7-7 に、よくあるお問い合わせ (FAQ) とその回答を示します。

表 7-7. コンソールリダイレクトの使用:よくあるお問い合わせ (FAQ)

質問	回答
スクリーンにビデオの破損が見られます。この不具合はどのように修正しますか?	<p>コンソールリダイレクト ウィンドウで 更新 をクリックして画面をリフレッシュします。</p> <p>メモ: 場合によっては、ビデオの破損が修正されるまで、数回 更新 をクリックする必要があります。</p>
コンソールリダイレクト中に、Windows 2000 システムが休止状態から回復する時にキーボードとマウスがロックされます。この原因は何ですか?	この問題を解決するには、 racadm racreset コマンドを実行して DRAC 5 をリセットする必要があります。
コンソールリダイレクトウィンドウで、システム画面の底部が見えませんか。	管理ステーションのモニター解像度が 1280x1024 に設定されているか確認します。
コンソールリダイレクト中に、Windows Server 2003 システムが休止状態から回復する時にマウスがロックされます。原因は何ですか?	<p>この問題を解決するには、Windows 以外のオペレーティングシステム用のマウスアクセラレータを仮想 KVM (vKVM) ウィンドウのプルダウンメニューから選択し、5 ~ 10 秒ほど待ってから Windows を再選択します。問題が解決されない場合は、racadm racreset コマンドを実行して DRAC 5 をリセットする必要があります。</p> <p>これで解決しない場合は、racadm racreset hard コマンドを実行して DRAC 5 をリセットする必要があります。</p>
vKVM キーボードとマウスが動作していないのはなぜですか?	管理下システムの BIOS 設定で、USB コントローラを BIOS サポートでオン に設定する必要があります。管理下システムを再起動し、<F2> を押してセットアップに入ります。 オンボードデバイス を選択してから、 USB コントローラ を選択します。変更を保存し、システムを再起動します。
Windows の画面が青くなると、管理下システムのコンソール画面に何も表示されなくなるのはなぜですか?	管理下システムに正しい ATI ビデオドライバがありません。『Dell PowerEdge Installation and Server Management CD』を使って、ビデオドライバをアップデートする必要があります。
Windows 2000 のインストールが完了した後で、リモートコンソールの画面に何も表示されないのはなぜですか?	管理下システムに正しい ATI ビデオドライバがありません。DRAC 5 コンソールリダイレクトは、Windows 2000 の配布 CD に含まれている SVGA ビデオドライバでは、正しく実行しません。『Dell PowerEdge Installation and Server Management CD』を使って Windows 2000 をインストールし、管理下システムで最新の対応ドライバが使用されていることを確認する必要があります。
Windows 2000 オペレーティングシステムをロードする場合に、管理下システムの画面に何も表示されないのはなぜですか?	管理下システムに正しい ATI ビデオドライバがありません。『Dell PowerEdge Installation and Server Management CD』を使って、ビデオドライバをアップデートする必要があります。
Windows の全画面 DOS ウィンドウにおいて管理下システムで画面に何も表示されないのはなぜですか?	管理下システムに正しい ATI ビデオドライバがありません。『Dell PowerEdge Installation and Server Management CD』を使って、ビデオドライバをアップデートする必要があります。
<F2> キーを押しても BIOS 設定が表示されないのはなぜですか?	この動作は Windows 環境でよく見られます。マウスを使ってコンソールリダイレクトウィンドウの領域をクリックして、焦点を調整します。焦点をコンソールリダイレクト ウィンドウの下のメニューバーに移動するには、下のメニューバーのオブジェクトの 1 つをマウスでクリックします。
『Dell PowerEdge Installation and Server Management CD』を使ってリモートでオペレーティングシステムをインストールする場合に、vKVM マウスが同期しないのはなぜですか?	<p>ターゲットシステムで実行しているオペレーティングシステムにコンソールリダイレクトを設定します。</p> <ol style="list-style-type: none"> 1. vKVM ツールバーメニューの ツール をクリックして、セッションオプション オプションを選択します。 2. セッションオプション ウィンドウで、マウス タブをクリックします。 3. マウスアクセラレータ ボックスで、ターゲットシステムで実行しているオペレーティングシステムを選択して、OK をクリックします。
Windows システムで休止状態から再開したあとで、vKVM マウスが同期しないのはなぜですか?	<p>vKVM ウィンドウのプルダウンメニューの マウスアクセラレータ で、別のオペレーティングシステムを選択します。次に、元のオペレーティングシステムに戻って、USB マウスデバイスを起動します。</p> <ol style="list-style-type: none"> 1. vKVM ツールバーの ツール をクリックして、セッションオプション を選択します。 2. セッションオプション ウィンドウで、マウス タブをクリックします。 3. マウスアクセラレータ ボックスのその他のオペレーティングシステムを選択して OK をクリックします。 4. USB マウスデバイスを初期化します。
コンソールリダイレクトの実行時に DOS でマウスが同期しないのはなぜですか?	Dell BIOS はマウスドライバを PS/2 マウスとしてエミュレートしています。設計上、PS/2 マウスはマウスポインタに対して相対的な位置を使用するため、同期化で遅れが生じます。DRAC 5 には USB マウスドライバがついているため、絶対的な位置を使用しマウスポインタを細かく追跡できます。DRAC 5 が USB の絶対的なマウスの位置を Dell BIOS に渡しても、BIOS エミュレーションによって相対的な位置に戻されるため、動作は変わりません。
Linux テキストコンソールでマウスが同期しないのはなぜですか?	仮想 KVM には USB マウスドライバが必要ですが、USB マウスドライバは X-Windows オペレーティングシステムでしか使用できません。
まだマウスの同期に不具合があります。	<p>コンソールリダイレクトウィンドウのターゲットシステムデスクトップが中央にあることを確認してください。</p> <ol style="list-style-type: none"> 1. vKVM ツールバーメニューの ツール をクリックして、手動ビデオ調整 オプションを選択します。 2. 垂直と水平のコントロールを調整して、コンソールリダイレクトウィンドウのデスクトップの位置合わせをします。 3. 閉じる をクリックします。 4. ターゲットシステムのマウスカーソルをコンソールリダイレクトウィンドウの左上隅に移動して、カーソルをウィンドウの中央に戻します。 5. 両方のカーソルが同期するまでステップ 2 ~ 4 を繰り返します。
別のオペレーティングシステム用にマウスアクセラレータを変更すると、vKVM マウスとキーボードが動作しないのはなぜですか?	USB vKVM キーボードとマウスは、マウスアクセラレータを変更してから 5 ~ 10 秒間は使用できません。ネットワーク負荷によって、この操作に通常よりも時間がかかることがあります (10 秒を超える)。

<p>vKVM ウィンドウからサーバー画面の下部が見えないのはなぜですか？</p>	<p>サーバー画面の解像度が 128 色、60 Hz、1280 x 1024 ピクセルになっていることを確認してください。</p>
<p>DRAC5 のコンソールリダイレクトを使って Microsoft® オペレーティングシステムをリモートでインストールする間、キーボードやマウスを使用できないのはなぜですか？</p>	<p>BIOS でコンソールリダイレクトが有効になっているシステムで、Microsoft の対応オペレーティングシステムをリモートでインストールするとき、EMS 接続メッセージが表示され、続行する前に OK を選択するように要求されます。リモートでマウスを使って OK を選択することはできません。ローカルシステムで OK を選択するか、リモートで管理下システムを再起動し、再インストールしてから、BIOS のコンソールリダイレクトをオフにする必要があります。</p> <p>このメッセージは Microsoft によって生成され、コンソールリダイレクトが有効であることをユーザーに警告します。このメッセージが表示されないようにするには、常に BIOS でコンソールリダイレクトをオフにしてから、オペレーティングシステムをリモートでインストールしてください。</p>
<p>Microsoft Windows 2000 の中国語、日本語、および韓国語バージョンでは、コンソールリダイレクトを使ってオペレーティングシステムの起動メニューを表示できないのはなぜですか？</p>	<p>複数のオペレーティングシステムを起動できる Windows 2000 を実行しているシステムでは、次の手順に従ってデフォルトの起動オペレーティングシステムを変更します。</p> <ol style="list-style-type: none"> 1. マイコンピュータ アイコンを右クリックして、プロパティ を選択します。 2. 詳細 タブをクリックします。 3. スタートアップと回復設定 をクリックします。 4. 起動 リストから新しいデフォルトのオペレーティングシステムを選択します。 5. ボックスの オペレーティングシステムの一覧を表示する リストで、デフォルトのオペレーティングシステムが自動的に起動するまでにオペレーティングシステムの選択リストを表示する秒数を入力します。
<p>管理ステーションの Num Lock インジケータがリモートサーバーの Num Lock 状態を反映しないのはなぜですか？</p>	<p>DRAC 5 からアクセスした場合、管理ステーションの Num Lock インジケータは必ずしもリモートサーバーの Num Lock の状態と一致するとは限りません。Num Lock の状態は、リモートセッションが接続するときのリモートサーバーの設定によって決まり、管理ステーションの Num Lock の状態とは関係ありません。</p>
<p>コンソールリダイレクトセッションを確立すると、複数の Session Viewer ウィンドウが表示されるのはなぜですか？</p>	<p>コンソールリダイレクトセッションをローカルシステムに設定しています。リモートシステムにセッションを再構成してください。</p>
<p>コンソールリダイレクトセッションを実行中、ローカルユーザーがリモートシステムにアクセスする場合、警告メッセージを受信しますか？</p>	<p>いいえ。システムにローカルユーザーがアクセスする場合、そのユーザーは警告なしに処置をオーバーライドできます。</p>
<p>コンソールリダイレクトセッションを実行するのに必要な帯域幅はどのくらいですか？</p>	<p>良いパフォーマンスを得るには、5 MB/sec の接続をお勧めします。最小限のパフォーマンスは、1 MB/sec の接続で実現可能です。</p>
<p>コンソールリダイレクトを実行する管理ステーションのシステム最小要件は何ですか？</p>	<p>管理ステーションには、256 MB 以上の RAM を搭載した Intel Pentium III 500 MHz プロセッサが必要です。</p>
<p>リモートシステムでコンソールリダイレクトセッションは最大いくつまで実行できますか？</p>	<p>DRAC 5 では、同時コンソールリダイレクトセッションを 2 つまでサポートできます。</p>

[目次ページに戻る](#)

[目次ページに戻る](#)

仮想メディアの使用と設定

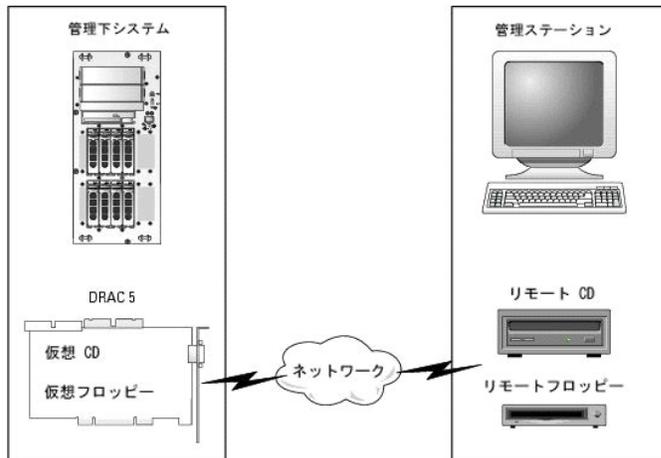
Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

- [概要](#)
- [管理下システムでのオペレーティングシステムの要件](#)
- [仮想メディアプラグインのインストール](#)
- [仮想メディアの実行](#)
- [仮想フラッシュの使用](#)
- [仮想メディアコマンドラインインタフェースユーティリティの使用](#)
- [よくあるお問い合わせ \(FAQ\)](#)

概要

仮想メディア機能は、ネットワーク上のどこからでも標準メディアとして使用できる仮想 CD ドライブを管理下システムに提供します。図 8-1 は仮想メディアのアーキテクチャの概要を示しています。

図 8-1. 仮想メディアのアーキテクチャのアーキテクチャの概要



仮想メディアを使用すると、管理下システムの起動から、アプリケーションのインストール、ドライバのアップデート、新しいオペレーティングシステムのインストールまで、CD/DVD やディスクドライブからリモートで実行することができます。

メモ: 仮想メディアでは、128 Kbps 以上のネットワーク帯域幅が必要です。

管理下システムは DRAC 5 カードを使用して構成されています。仮想 CD とフロッピードライブは DRAC 5 に内蔵された 2 つの電子デバイスで、DRAC 5 ファームウェアによって制御されます。これら 2 つのデバイスは、仮想メディアの接続の有無にかかわらず、管理下システムのオペレーティングシステムと BIOS に常駐します。

管理ステーションは、物理メディアやイメージファイルをネットワーク経由で提供します。RAC ブラウザを初めて起動して仮想メディアページにアクセスすると、DRAC 5 Web Server から仮想メディアプラグインがダウンロードされ、管理ステーションに自動的にインストールされます。仮想メディア機能が正しく動作するには、仮想メディアプラグインが管理ステーションにインストールされている必要があります。

仮想メディアが接続していると、管理下システムからの仮想 CD/フロッピードライブのアクセス要求がすべてネットワーク経由で管理ステーションに向けられます。仮想メディアを接続するのは、メディアを仮想デバイスに挿入する操作と同じです。仮想メディアが接続していないとき、管理下システムの仮想デバイスは、ドライブにメディアがインストールされていない 2 台のドライブに見えます。

表 8-1 に、仮想フロッピーと仮想オプティカルドライブでサポートされているドライブ接続を示します。

メモ: 接続中に仮想メディアを変更すると、システム起動シーケンスが停止する場合があります。

表 8-1. サポートされているドライブ接続

サポートされている仮想フロッピードライブ接続	サポートされている仮想オプティカルドライブ接続
1.44 フロッピーディスク使用のレガシー 1.44 フロッピードライブ	CD-ROM メディアのある CD-ROM、DVD、CDRW、コンピネーションドライブ
1.44 フロッピー ディスクを使用の UBC フロッピードライブ	ISO9660 フォーマットの CD-ROM イメージファイル
1.44 フロッピーイメージ	CD-ROM メディアのある USB CD-ROMドライブ

管理下システムのオペレーティングシステムの要件

仮想メディアは次のオペレーティングシステムを実行しているシステムでサポートされています。

- 1 Microsoft® Windows® 2000 Server Service (Pack 4)
- 1 Windows Server™ 2003
- 1 Red Hat® Enterprise Linux AS, ES, WS (バージョン 3.0)
- 1 Red Hat Enterprise Linux AS, ES, WS (バージョン 4)
- 1 Intel EM64T 用 SUSE® Linux Enterprise Server (バージョン 9)、Service Pack 2 (SP2)
- 1 SUSE Linux Enterprise Server (バージョン 10) (Intel EM64T 用)

最新のオペレーティングシステムの詳細については、『DRAC 5 Readme』および『Dell OpenManage™ Server Administrator 互換性ガイド』を参照してください。

仮想メディアプラグインのインストール

仮想メディアブラウザが動作するには、仮想メディアプラグインが管理ステーションにインストールされている必要があります。DRAC 5 ユーザーインタフェースを開いて仮想メディアページを起動すると、ブラウザが必要に応じてプラグインのダウンロードを自動的に開始します。プラグインが正常にインストールされた場合は、仮想メディアページに仮想ドライブが接続できるフロッピーとオプティカルディスクのリストが表示されます。

Windows ベースの管理ステーション

Microsoft Windows オペレーティングシステムを実行している管理ステーションで仮想メディア機能を実行するには、サポートされている Internet Explorer のバージョンと ActiveX コントロールプラグインをインストールします。ブラウザのセキュリティを **中** またはそれ以下に設定し、Internet Explorer が ActiveX コントロールをダウンロードしてインストールできるようにします。

詳細については、「[対応 Web ブラウザ](#)」を参照してください。

仮想メディア機能をインストールして使用するには、管理者権限が必要です。ActiveX コントロールをインストールする前に、Internet Explorer でセキュリティ警告が表示される場合があります。ActiveX コントロールのインストール手順を完了するには、Internet Explorer でセキュリティ警告が表示されたときに ActiveX コントロールを受け入れる必要があります。

Linux ベースの管理ステーション

Linux オペレーティングシステムを実行している管理ステーションで仮想メディア機能を実行するには、Mozilla または Firefox のサポートされているバージョンをインストールします。プラグインがインストールされていない場合や、新しいバージョンがリリースされている場合は、管理ステーションでプラグインのインストールを確認するダイアログボックスが表示されます。ブラウザを実行しているユーザー ID に、ブラウザのディレクトリツリーへの書き込み権限があることを確認します。ユーザー ID に書き込み権限がない場合は、仮想メディアのプラグインをインストールできません。

詳細については、「[対応 Web ブラウザ](#)」を参照してください。

仮想メディアの実行

 **注意:** 仮想メディアのセッションを実行している間は、`racreset` コマンドを使用しないでください。使用すると、データ損失などの不測の結果が生じます。

仮想メディアを使用すると、ディスクイメージを「仮想化」して、管理コンソールでフロッピーイメージ、フロッピードライブ、オプティカルドライブなどをリモートシステムの使用可能なドライブとして有効にできます。

サポートされている仮想メディアの設定

フロッピードライブ 1 つとオプティカルドライブ 1 つを仮想メディアとして有効にできます。各メディアタイプにつき一度に 1 つのドライブだけを仮想化できます。

サポートされているフロッピードライブには、フロッピーイメージ 1 つと使用可能なフロッピードライブ 1 つがあります。サポートされているオプティカルドライブには、使用可能なオプティカルドライブ最大 1 つまたは ISO イメージファイル 1 つがあります。

ウェブインタフェースを使用した仮想メディアの実行

仮想メディアの接続

1. 管理ステーションで対応 Web ブラウザを開きます。「[対応 Web ブラウザ](#)」を参照してください。

 **注意:** コンソールリダイレクトおよび仮想メディアは、32 ビットウェブブラウザのみをサポートしています。64 ビットウェブブラウザの使用は、予期しない結果や故障の原因となる可能性があります。

2. DRAC 5 に接続してログインします。詳細については、「[ウェブインタフェースへのアクセス](#)」を参照してください。

3. **メディア** タブをクリックして、**仮想メディア** をクリックします。

仮想メディア ページに、仮想化できるクライアントドライブが表示されます。

 **メモ:** フロッピードライブ(該当する場合)の **フロッピーイメージファイル** が表示される場合は、このデバイスを仮想フロッピーとして仮想化できます。オプティカルドライブ 1 つとフロッピー 1 つを同時に選択するか、単一ドライブを選択できます。

 **メモ:** 管理下システムの仮想デバイスドライブ文字と、管理ステーションの物理ドライブ文字とは一致しません。

4. プロンプトが表示されたら、画面の説明に従って仮想メディアプラグインをインストールします。

5. **属性** ボックスで、次の手順を実行します。

a. 値 列で、**連結 / 分離** 状態の値が **連結** になっていることを確認します。

値が **分離** の場合は、次の手順を実行します。

- i. **メディア** タブの **設定** をクリックします。
- ii. 値 行の **連結仮想メディア** チェックボックスがオンになっていることを確認します。
- iii. **変更の適用** をクリックします。
- iv. **仮想メディア** タブで、**仮想メディア** をクリックします。
- v. 値 列で、**連結 / 分離** 状態の値が **連結** になっていることを確認します。

b. **現在の状態** 値が **未接続** になっていることを確認します。値 フィールドに接続と表示されている場合、再接続する前にイメージまたはドライブの接続を解除する必要があります。

c. リモートシステムと管理ステーション間に暗号化された接続を確立するには、**暗号化の有効** チェックボックスをリモートシステムと管理ステーション間に暗号化された接続を確立するには、暗号化の有効 チェックボックスをオンにします。

6. フロッピーイメージまたは ISO イメージを仮想化する場合は、**フロッピー イメージファイル** または **ISO イメージファイル** を選択して、仮想化するイメージファイルを入力するか、そのファイルまで参照します。

フロッピードライブまたはオプティカルドライブを仮想化する場合は、仮想化するドライブの横のボタンを選択します。

7. **接続** をクリックします。

この接続が認証されたら、接続状態が **接続済み** となり、接続しているドライブがすべて表示されます。選択したディスクイメージやドライブすべてが管理下システムのコンソールで実際のドライブのように使用できるようになります。

 **メモ:** 割り当てられているドライブ文字 (Microsoft® Windows® システムの場合) またはデバイスの特殊ファイル (Linux システムの場合) は、管理コンソールのドライブ文字と異なる場合があります。

 **メモ:** Internet Explorer 拡張セキュリティを設定した Windows オペレーティングシステムでは、仮想メディアは正しく機能しない可能性があります。この不具合を解決するには、Microsoft オペレーティングシステムマニュアルを参照するか、またはシステム管理者に問い合わせてください。

仮想メディアの接続解除

接続 をクリックすると、仮想化したイメージとドライブがすべて管理ステーションから切断されます。**すべての** 仮想化イメージとドライブが切断され、管理下システムで使用不可になります。

仮想メディア機能の有効と無効

DRAC 5 仮想メディア機能は USB テクノロジーを基盤とし、USB のプラグアンドプレイ機能を活用できます。DRAC 5 を使用すると、USB バスに仮想デバイスを接続したりバスから分離したりできるオプションが追加されます。デバイスを分離すると、オペレーティングシステムや BIOS には、連結されたドライブが見えません。仮想デバイスを接続すると、ドライブが見えるようになります。ドライブは次のシステム起動時のみ有効または無効にできる DRAC 4 と異なり、DRAC 5 の仮想デバイスはいつでも連結や分離ができます。

仮想デバイスは、Web ブラウザ、ローカル racadm、リモート racadm、telnet、およびシリアルポートを使用して連結または分離できます。ウェブブラウザを使用して仮想メディアを設定するには、**メディア** ページから、**設定** ページへ進むと、そこで設定を変更および適用できます。また、**仮想メディアのポート番号** および **仮想メディア SSL ポート番号** を指定することもできます。さらに、**仮想フラッシュ** および **1 度だけ起動** 機能を有効化または無効化ができます。

ウェブブラウザを使用した仮想メディアの連結と分離

仮想メディア機能を連結するには、以下の手続きに従ってください。

1. **システム** > **メディア** > **設定** の順にクリックします。
2. **仮想メディアの連結** の値 チェックボックスを選択します。
3. **変更の適用** をクリックします。

仮想メディア機能を分離するには、次の手順を実行してください。

1. システム->メディア->設定 をクリックします。
2. 仮想メディアの連結 用の値 チェックボックスを選択します。
3. 変更の適用 をクリックします。

RACADM を使った仮想メディアの連結と分離

仮想メディア機能を連結するには、コマンドプロンプトを開き、次のコマンドを入力して <Enter> を押します。

```
racadm config -g cfgRacVirtual -o cfgFloppyEmulation 1
```

仮想メディア機能を分離するには、コマンドプロンプトを開き、次のコマンドを入力して <Enter> を押します。

```
racadm config -g cfgRacVirtual -o cfgFloppyEmulation 0
```

仮想メディアからの起動

サポートしているシステムでは、システム BIOS によって、仮想オプティカルドライブまたは仮想フロッピードライブから起動できるようになります。POST 中に、BIOS 設定ウィンドウで仮想メディアが有効になり、正しい順序でリストに表示されていることを確認します。

BIOS 設定を変更するには、次の手順を実行してください。

1. 管理下システムを起動します。
2. <F2> を押して BIOS 設定ウィンドウに進みます。
3. 起動順序にスクロールして <Enter> を押します。

ポップアップウィンドウに、仮想オプティカルドライブと仮想フロッピードライブが、標準的な起動デバイスと一緒にリストに表示されます。

4. 仮想ドライブが有効になり、ブータブルメディアの最初のデバイスとして表示されていることを確認します。必要に応じて、画面の説明に従って起動順序を変更します。
5. 変更を保存して終了します。

管理下システムが再起動します。

管理下システムは起動順序に基づいて、起動可能なデバイスから起動しようとします。仮想デバイスが接続済みでブート可能なメディアが存在している場合、システムはこの仮想デバイスで起動します。ここからブートできない場合、ブート可能メディアのない物理デバイスと同様に、このデバイスは無視されます。

仮想メディアを使用したオペレーティングシステムのインストール

この項では、オペレーティングシステムをインタラクティブな方法で管理ステーションに手動でインストールする方法を説明します。完了に数時間かかる可能性があります。仮想メディアを使う場合、スクリーンに記述されたオペレーティングシステムのインストール手順では、15 分以内で完了します。詳細については、「[VM-CLIを使用したオペレーティングシステムの導入](#)」を参照してください。

1. 以下を確認します。
 - 1 オペレーティングシステムのインストール CD が管理ステーションの CD ドライブに挿入されている。
 - 1 ローカル CD ドライブが選択されている。
 - 1 仮想ドライブに接続している。
2. 「[仮想メディアからの起動](#)」の説明に従って、BIOS がインストール元の CD ドライブから起動するように設定します。
3. 画面の説明に従ってインストールを完了します。

サーバーのオペレーティングシステムが実行中の仮想メディアの使用

Windows ベースのシステム

Windows システムでは、仮想メディアドライブは自動的にマウントされてドライブ文字が設定されます。

Windows 内から仮想ドライブを使用する操作は、物理ドライブを使用する場合と似ています。管理ステーションでメディアに接続すると、ドライブをクリックしてその内容を参照すると、そのシステムでメディアが使用できるようになります。

Linux ベースのシステム

Linux システムでは、仮想メディアドライブにドライブ文字が設定されません。システムにインストールされているソフトウェアによっては、仮想メディアドライブが自動的にマウントされない場合もあります。ドライブが自動的にマウントされていない場合は、手動で行います。

仮想フラッシュの使用

DRAC 5 には持続的な仮想フラッシュが備わっています。DRAC 5 のファイルシステムに常駐する 16 MB のフラッシュメモリは、持続的なストレージとして使用でき、システムからアクセスできます。有効にすると、仮想フラッシュは第 3 の仮想ドライブとして設定されて BIOS の起動順序に表示されるので、ユーザーはこの仮想フラッシュから起動することができます。

 **メモ:** 仮想フラッシュから起動する場合は、仮想フラッシュのイメージはブータブルイメージでなければいけません。

ホストシステムに外部のクライアント接続や実動デバイスが必要な CD またはフロッピードライブと異なり、仮想フラッシュの実装には、DRAC 5 の持続的な仮想フラッシュ機能が必要なだけです。16 MB のフラッシュメモリは、ホスト環境では初期化されていないリムーバブル USB ドライブとして表示されます。

仮想フラッシュを実装するときには、次のガイドラインに従ってください。

- 1 仮想フラッシュの接続または分離は、すべての仮想メディアデバイスを接続および分離する USB 再記数法を実行します(例: CD ドライブとフロッピードライブ)。
- 1 仮想フラッシュを有効または無効にすると、仮想メディア CD/ フロッピードライブの接続状態は変わりません。

 **注意:** 分離と接続を実行すると、アクティブな仮想メディアの読み書きの操作が中断します。

仮想フラッシュの有効

仮想メディア機能を有効にするには、コマンドプロンプトを開き、次のコマンドを入力して <Enter> を押します。

```
racadm config -g cfgRacVirtual -o cfgFloppyEmulation 1
```

仮想フラッシュの無効

仮想メディア機能を無効にするには、コマンドプロンプトを開き、次のコマンドを入力して <Enter> を押します。

```
racadm config -g cfgRacVirtual -o cfgFloppyEmulation 0
```

仮想フラッシュへのイメージの保存

仮想フラッシュは、管理下ホストからフォーマットできます。Windows オペレーティングシステムを実行している場合は、ドライブのアイコンを右クリックして **フォーマット** を選択します。Linux を実行している場合は、**format** および **fdisk** などのシステムツールを使用すると、USB のパーティションとフォーマットができます。

RAC Web ブラウザから仮想フラッシュにイメージをアップロードする前に、イメージファイルのサイズが 1.44 ~ 16 MB で、仮想フラッシュが無効になっていることを確認します。イメージをダウンロードして仮想フラッシュドライブを再び有効にすると、システムと BIOS が仮想フラッシュを認識します。

ブータブル仮想フラッシュの設定

1. ブータブルディスクをディスクドライブに挿入するか、ブータブル CD をオプティカルドライブに挿入します。
2. システムを再起動すると、選択したメディアドライブが起動します。
3. 仮想フラッシュにパーティションを追加して、パーティションを有効にします。

仮想フラッシュがハードドライブでエミュレートしている場合は、**fdisk** を使用します。仮想フラッシュがドライブ B として設定されている場合、仮想フラッシュはフロッピーにエミュレートされて、パーティションをしなくてもブータブルドライブとして仮想フラッシュを設定できます。

4. **format** コマンドを使用して、**/s** スイッチでドライブをフォーマットして、システムファイルを仮想フラッシュに転送します。

例:

```
format /s x
```

x は、仮想フラッシュに割り当てたドライブ文字です。

5. システムをシャットダウンして、ブータブルフロッピーまたは CD をドライブから取り外します。
6. システムをオンにして、システムが仮想フラッシュから `C:\¥` または `A:\¥` プロンプトに起動することを確認します。

仮想メディアコマンドラインインタフェースユーティリティの使用

仮想メディアコマンドラインインタフェース (VM-CLI) ユーティリティは、管理ステーションからリモートシステムの DRAC 5 に仮想メディア機能を提供するスクリプト可能なコマンドラインインタフェースです。

VM-CLI ユーティリティは次の機能を提供します。

- 1 複数のアクティブセッションを同時にサポートします。



メモ: 読み取り専用のイメージファイルを仮想化する場合は、複数のセッションが同じイメージメディアを共有します。物理ドライブを仮想化する場合は、一度に 1 セッションだけが特定の物理ドライブにアクセスできます。

- 1 リムーバブルメディアデバイスまたはイメージファイルは、仮想メディアプラグインと一貫しています。
- 1 DRAC ファームウェアのブートワンス機能が有効の場合、自動終了オプションが有効になります。
- 1 Secure Sockets Layer (SSL) を使って DRAC 5 の通信をセキュリティ保護にします。

ユーティリティを実行する前に、リモートシステムの DRAC 5 に仮想メディアユーザー特権があることを確認してください。

オペレーティングシステムがシステム管理者特権、オペレーティングシステムに固有の特権またはグループメンバーシップをサポートしている場合は、VM-CLI コマンドを実行するためにもシステム管理者特権が必要です。

クライアントシステムのシステム管理者はユーザーグループと特権を制御するので、ユーティリティを実行できるユーザーを制御します。

Windows システムの場合は、VM-CLI ユーティリティのパワーユーザー特権が必要です。

Linux システムでは、システム管理者の特権がなくても、`sudo` コマンドを使って VM-CLI ユーティリティにアクセスできます。このコマンドは、システム管理者以外のアクセスを集中管理する方法で、すべてのユーザーコマンドをログに記録します。VM-CLI グループのユーザーを追加または編集するには、管理者が `visudo` コマンドを使用します。システム管理者特権のないユーザーは、`sudo` コマンドを VM-CLI コマンドライン (または VM-CLI スクリプト) の接頭辞として追加すると、リモートシステムの DRAC 5 にアクセスしてユーティリティを実行できます。

対応オペレーティングシステム

VM-CLI ユーティリティは、次のオペレーティングシステムをサポートします。

- 1 Windows XP
- 1 Windows 2000 Server と Service Pack 4
- 1 Windows Server 2003
- 1 Windows Server 2003 R2
- 1 Red Hat Enterprise Linux AS/ES (バージョン 3)
- 1 Red Hat Enterprise Linux AS/ES (バージョン 4)
- 1 SUSE Linux Enterprise Server Version 9 Service Pack 2 for Intel EM64T

最新情報については、デルのサポートウェブサイト support.dell.com で、『DRAC 5 Readme』および『Dell OpenManage™ Server Administrator 互換性ガイド』を参照してください。

ユーティリティのインストール

VM-CLI ユーティリティは、Dell OpenManage System Management ソフトウェアキットに付属の『Dell OpenManage™ Systems Management Consoles CD』に含まれています。ユーティリティをインストールするには、『System Management Consoles CD』をシステムの CD ドライブに挿入し、画面の指示に従います。

『Systems Management Consoles CD』には、診断、ストレージ管理、Remote Access Service、RACADM ユーティリティなど、最新の Systems Management Software 製品が入っています。また、Systems Management Software 製品に関する最新情報を記載した `readme` ファイルも含まれています。

さらに、『Systems Management Consoles CD』には `vmdeploy` が含まれています。これは、VM-CLI と RACADM ユーティリティを使用して複数のリモートシステムにソフトウェアを導入する方法を説明したサンプルスクリプトです。詳細については、『[VM-CLI を使用したオペレーティングシステムの導入](#)』を参照してください。

コマンドラインオプション

VM-CLI インタフェースは、Windows と Linux システムで共通しています。このユーティリティは、RACADM ユーティリティオプションと同じオプションを使用しています。たとえば、DRAC 5 IP アドレスを指定するオプションでは、`racadm` でも VM-CLI ユーティリティでも同じ構文が必要です。

VM-CLI コマンドの形式は以下のとおりです。

```
racvmcli [パラメーター] [オペレーティングシステムシェルオプション]
```

コマンドラインの構文は大文字と小文字が区別されます。詳細については、「[VM-CLIパラメーター](#)」を参照してください。

リモートシステムのコマンドが受け入れられ、DRAC 5 が接続を許可した場合は、次のどちらかが発生するまでコマンドの実行が続行します。

- 1 理由に関わらず VM-CLI 接続は終了します。
- 1 プロセスは、オペレーティングシステムのコントロールを使用して手動で終了します。たとえば、Windows ではタスクマネージャを使用してプロセスを終了します。

VM-CLI のパラメータ

DRAC 5 IP アドレス

-r <RAC IP アドレス>[:<RAC SSL ポート>]

<RAC IP アドレス> は有効な固有の IPアドレスまたは DRAC 5 ダイナミックドメインネームシステム(DDNS)名です(サポートしている場合)。

このパラメータは DRAC 5 IPアドレスと SSL ポートを提供します。VM-CLI ユーティリティはこの情報を使用して、目的の DRAC 5 と仮想メディア接続を確立します。無効な IP アドレスまたは DDNS 名を入力した場合は、エラーメッセージが表示され、コマンドは終了します。

<RAC SSL ポート> を省くと、ポート 443(デフォルトポート)が使用されます。DRAC 5 のデフォルト SSL ポートを変更していない限り、オプションの SSL ポートは不要です。

DRAC 5 のユーザー名

-u <DRAC ユーザー名>

このパラメータは仮想メディアを実行する DRAC 5 ユーザー名を提供します。

<DRAC ユーザー名> には次の属性が必要です。

- 1 有効なユーザー名
- 1 DRAC 仮想メディアユーザー権限

DRAC 5 の認証に失敗した場合は、エラーメッセージが表示され、コマンドが終了します。

DRAC ユーザーのパスワード

-p <DRAC ユーザーパスワード>

このパラメータは、指定した DRAC 5 ユーザーのパスワードを提供します。

DRAC 5 の認証に失敗した場合は、エラーメッセージが表示され、コマンドが終了します。

フロッピー / ディスクデバイスまたはイメージファイル

-c <デバイス名> | <イメージファイル>

<デバイス名> は、有効なドライブ文字(Windows システム)またはマウント可能なファイルシステムのパーティション数(Linux システム)を含む有効なデバイスファイル名です。<イメージファイル> は、有効なイメージファイルのファイル名とパスです。

このパラメータは、仮想フロッピー / ディスクメディアを供給するデバイスまたはファイルを指定します。

たとえば、以下のようにイメージファイルを指定します。

-f c:\temp\myfloppy.img(Windows システム)

-f /tmp/myfloppy.img(Linux システム)

ファイルが書き込み禁止でない場合は、仮想メディアがイメージファイルに書き込み可能性があります。オペレーションシステムを設定して、上書きしてはいけないフロッピーイメージを書き込み禁止にしてください。

たとえば、次のようにデバイスを指定します。

-f a:z(Windows システム)

-f /dev/sdb4 # 4th デバイスのパーティション /dev/sdb(Linux システム)

デバイスに書き込み保護の機能がある場合は、その機能を使って、仮想メディアからそのメディアへの書き込みを禁止してください。

さらに、フロッピーメディアを仮想化しない場合は、コマンドラインからこのパラメータを省きます。無効な値が検出された場合は、エラーメッセージが表示され、コマンドが終了します。

CD/DVD デバイスまたはイメージファイル

-c <デバイス名> | <イメージファイル>

<デバイス名> は、有効な CD/DVD (Windows システム) または CD/DVD デバイスファイル名 (Linux システム) で、<イメージファイル> は、有効な ISO-9660 のファイル名とパスです。

このパラメータは、仮想 CD/DVD-ROM メディアを供給するデバイスまたはファイルを指定します。

たとえば、以下のようにイメージファイルを指定します。

-c c:\temp\mydvd.img (Windows システム)

-c /tmp/mydvd.img (Linux システム)

たとえば、次のようにデバイスを指定します。

-c d:\ (Windows システム)

-c /dev/cdrom (Linux システム)

さらに、CD/DVD メディアを仮想化しない場合は、コマンドラインからこのパラメータを省きます。無効な値が検出された場合は、エラーメッセージが表示され、コマンドが終了します。

スイッチオプションだけが提供されている場合を除き、メディアの種類を少なくとも 1 つコマンドで指定します (フロッピーまたは CD/DVD ドライブ)。そうしないと、エラーメッセージが表示され、コマンドがエラーを生成して終了します。

バージョン表示

-v

このパラメータは、VM-CLI ユーティリティのバージョンを表示するために使用します。スイッチ以外の他のオプションが提供されていない場合は、エラーメッセージなしにコマンドが終了します。

ヘルプ表示

-h

このパラメータは、VM-CLI ユーティリティのパラメータの概要を表示します。スイッチ以外の他のオプションが提供されていない場合は、エラーなしにコマンドが終了します。

暗号化されたデータ

-e

このパラメータがコマンドラインに含まれていると、VM-CLI は SSL-暗号化チャネルを使用して、管理ステーションとリモートシステムの DRAC 5 の間でデータを転送します。このパラメータがコマンドラインにない場合、データ転送は暗号化されません。

VM-CLI オペレーティングシステムのシェルオプション

VM-CLI のコマンドラインでは次のオペレーティングシステムの機能を使用できます。

- 1 stderr/stdout リダイレクト — ファイルへ印刷されたユーティリティの出力をリダイレクトします。

たとえば、大なり記号 (>) の後にファイル名を入力すると、指定したファイルが VM-CLI ユーティリティの印刷出力で上書きに使用されます。

 **メモ:** VM-CLI ユーティリティは、スタンダード入力から読み取りできません (**stdin**)。その結果、**stdin** リダイレクトは必要ありません。

- 1 バックグラウンド実行 — VM-CLI ユーティリティはデフォルトではフォアグラウンドで実行します。ユーティリティ機能をバックグラウンドで実行させるには、オペレーティングシステムのコマンドシエルのバックグラウンド文字を使用します。たとえば、Linux オペレーティングシステムでは、アンバサンド文字 (&) の後にコマンドを入力すると、プログラムが新しいバックグラウンドプロセスとして始動します。

後者の方法はスクリプトプログラムで便利です。VM-CLI コマンドの新しいプロセスが開始した後、スクリプトが継続できます (そうでない場合は、VM-CLI プログラムが終了するまでスクリプトがブロックされます)。VM-CLI の複数のインスタンスがこの方法で開始し、コマンドインスタンスの 1 つまたは複数を手動で終了しなければならない場合は、オペレーティングシステムに固有の機能を使ってプロセスをリストにして終了します。

VM-CLI の戻りコード

0 = エラーなし

1 = 接続不能

2 = VM-CLI コマンドラインエラー

3 = RAC ファームウェア接続喪失

テキストメッセージ(英語のみ)も、エラーが発生するたびに標準的なエラー出力に発行されます。

よくあるお問い合わせ(FAQ)

表 8-2 に、よくあるお問い合わせ(FAQ)とその回答を示します。

表 8-2. 仮想メディアの使い方: よくあるお問い合わせ(FAQ)

質問	回答
どのオペレーティングシステムがDRAC 5をサポートしていますか?	サポートしているオペレーティングシステムについては、「 対応オペレーティングシステム 」のリストを参照してください。
どの Web ブラウザがDRAC 5をサポートしていますか?	サポートしている Web ブラウザについては、「 対応 Web ブラウザ 」のリストを参照してください。
時々クライアントの接続が切断されるのはなぜですか?	<ol style="list-style-type: none">ネットワークが遅い場合や、クライアントシステムの CD ドライブの CD を交換した場合に、クライアントの接続を損失する場合があります。たとえば、クライアントシステムの CD ドライブの CD を交換すると、新しい CD に自動スタート機能があるかもしれません。このような場合、ファームウェアタイムアウトになり、CD の読み取りを開始するまでに時間がかかると、接続が失われることがあります。接続が失われた場合は、GUI から再接続して前の操作を続行してください。ネットワークタイムアウトが発生した場合、DRAC 5 ファームウェアはサーバーと仮想ドライブ間のリンクを切断し、接続を中断します。仮想ドライブに再接続するには、仮想メディア機能を使用します。
Windows 2000(Service Pack 4)の正常なインストールに失敗したらどうすればよいですか?	仮想メディアおよびWindows 2000 のオペレーティングシステム CD を使用してWindows 2000(Service Pack 4)をインストールする場合、インストール作業中にシステムから CD ドライブへの接続が一時的に途切れることがあり、オペレーティングシステムが正常なインストールに失敗する場合があります。この不具合は修正するには、support.microsoft.com のMicrosoft サポートウェブサイトから usbstor.sys ファイルをダウンロードし、この不具合が発生したシステム上でこのプログラムを実行します。詳細に関しては、Microsoft Knowledge Base の記事 823086 を参照してください。
Windows 2000 をローカルまたはリモートでインストールできないのですか?	仮想フラッシュが有効で、有効なイメージが含まれていない場合、例えば、仮想フラッシュに破損した画像、またはランダム画像が含まれている場合、Windows 2000 をローカルまたはリモートでインストールできない可能性があります。この不具合を修正するには、仮想フラッシュの有効なイメージをインストールするか、インストール作業の間仮想フラッシュを使用しない場合は、仮想フラッシュを無効にします。
共有 NIC モードで設定した場合、仮想メディア接続はなぜ中断してしまうのですか?	共有 NIC モードで設定した場合、サーバーへのネットワークおよびチップセットドライバを取り付けると仮想メディアの接続が中断します。ネットワークまたはチップセットドライバの取り付けにより LOM がリセットされ、ネットワークバケットがタイムアウトして仮想メディア接続もタイムアウトするため中断します。この不具合に対処するには、ドライバを仮想ドライブからサーバーのローカルハードドライブにコピーします。仮想メディア接続の喪失によるドライバインストール作業の中断を防ぐためには、ドライバのインストールを直接サーバーから開始します。
Windows オペレーティングシステムのインストールに非常に時間がかかるように思います。どうしてでしょうか?	Windows オペレーティングシステムのインストールに[Dell PowerEdge Installation and Server Management CD]を使用し、またネットワークの接続が遅い場合、ネットワーク待ち時間のために DRAC 5 ウェブインタフェースへのアクセスに時間かかる場合があります。インストールウィンドウにインストール進行状況が表示されない場合でも、インストール作業は進行しています。
フロッピードライブまたは USB メモリキーの内容を表示しています。同じドライブを使用して仮想メディア接続を確立しようとすると、接続エラーメッセージが表示され、再試行を要求されます。なぜですか?	仮想フロッピードライブへの同時アクセスは許可されません。ドライブを仮想化する前に、ドライブの内容表示に使用しているアプリケーションを閉じてください。
どのようにして仮想デバイスを起動デバイスとして設定するのですか?	管理下システムの [BIOS 設定] にアクセスし、起動メニューに進みます。仮想 CD、仮想フロッピー、または仮想フラッシュを探し、必要に応じてデバイスの起動順序を変更します。たとえば、CD ドライブから起動するには、CD ドライブを起動順序の最初に設定する必要があります。
どのようなメディアで起動できますか?	DRAC 5 では、以下の起動メディアで起動することができます。 <ul style="list-style-type: none">CDROM/DVD データメディアISO 9660 イメージ1.44 フロッピーディスクまたはフロッピーイメージDRAC 5 組み込み仮想フラッシュオペレーティングシステムによりリムーバブルディスクと認識された USB キーUSB キーイメージ
USB キーを起動可能にするにはどうしますか?	Windows 98 DOS でのみ USB キーを仮想フロッピーから起動できます。独自の起動可能な USB キーを設定するには、Windows 98 スタートアップディスクを起動し、スタートアップディスクからシステムファイルを USB キーにコピーします。例えば、DOS プロンプトから、次のコマンドを入力します。 <pre>sys a: x: /s</pre> ここで、"x:" は、起動可能にする USB キーです。
ActiveX プラグインをインストールするにはシステム管理者特権が必要ですか?	仮想メディア機能のインストールおよび使用には、Windows システムにおいて管理者権限またはパワーユーザー権限が必要です。
Red Hat Linux 管理ステーションで仮想メディアプラグインをインストールおよび使用するには、どの特権が必要ですか?	仮想メディアプラグインを正しくインストールするには、ブラウザのディレクトリツリーの書き込み特権が必要です。
Red Hat Enterprise Linux または SUSE Linux オペレーティングシステムを起動しているシステム上で、仮想フロッピーを検索できません。仮想メディアを取り付け、リモートフロッピーに接続しています。どうすべきですか?	Linux のバージョンによってはフロッピードライブと仮想 CD ドライブを同じようにオートマウントしません。仮想フロッピードライブをマウントするには、Linux が仮想フロッピーに割り当てたデバイスノードを検索します。次の手順を実行して仮想フロッピードライブを検索し、マウントします。 <ol style="list-style-type: none">Linux コマンドプロンプトを開き、次のコマンドを実行します。 <pre>grep "仮想フロッピー" /var/log/messages</pre>そのメッセージに対する最後のエントリを検索し、時間を記録します。Linux プロンプトで、次のコマンドを実行します。 <pre>grep "hh:mm:ss" /var/log/messages</pre> ここで hh:mm:ss は、手順 1 で grep から返されたメッセージのタイムスタンプです。

	<p>4. 手順 3 で、grep コマンドの結果を読み、"DELL 仮想フロッピー" に付けられたデバイス名を検索します。</p> <p>5. 仮想フロッピードライブが取り付けられ、接続されていることを確認します。</p> <p>6. Linux プロンプトで、次のコマンドを実行する。</p> <pre>mount /dev/sdx /mnt/floppy</pre> <p>ここで、 /dev/sdx は、手順 4 で検索されたデバイス名で、 /mnt/floppy は、マウントポイントです。</p>
仮想フロッピードライブまたは仮想フラッシュでサポートされているファイルシステムの種類は何ですか？	フロッピードライブおよび仮想フラッシュは、FAT16 または FAT32 ファイルシステムをサポートしています。
DRAC 5 ウェブインタフェースを使用して、ファームウェアのアップデートをリモートで実行した時に、サーバーの仮想ドライブが削除されました。なぜですか？	ファームウェアのアップデートにより DRAC 5 がリセットされ、リモート接続が切断して仮想ドライブがアンマウントされます。DRAC リセットが完了すると、ドライブは再表示されます。
仮想フラッシュを有効、または無効にした際、すべての仮想ドライブが消えて、また再表示されます。どうしてですか？なぜですか？	仮想フラッシュの有効、無効の操作で USB がリセットされます。それによってすべての仮想ドライブが USB バスから分離され、また接続されません。

[目次ページに戻る](#)

[目次ページに戻る](#)

RACADM コマンドラインインタフェースの使用

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

- [シリアルまたは telnet コンソールの使用](#)
- [RACADM の使用](#)
- [複数の DRAC 5 の設定](#)
- [Racadm ユーティリティを使用した DRAC 5 の設定](#)
- [よくあるお問い合わせ \(FAQ\)](#)

シリアル /telnet/ssh コンソールは、一連の racadm コマンドを提供しています。racadm コマンドを使用すると、DRAC 5 ウェブインタフェースでサポートされているテキストベースの機能にアクセスできます。

RACADM を使用すると、DRAC 5 をローカルまたはリモートで設定および管理できます。RACADM は、管理ステーションと管理下システムで実行します。RACADM は『Dell Systems Management Consoles CD』に入っています。

RACADM を使って自動的に複数の DRAC 5 を設定するスクリプトを書くことができます。複数 DRAC 5 の設定の詳細は、「[マルチプル DRAC 5 カードの設定](#)」を参照してください。

この項では次の情報を提供します。

- 1 シリアルおよび racadm コマンドの使用「[シリアルまたは Telnet コンソールの使用](#)」と「[RACADM の使用](#)」を参照してください。
- 1 racadm コマンドを使用した DRAC 5 の設定
- 1 racadm 設定ファイルを使用した複数の DRAC 5 カードの設定

シリアルまたは telnet コンソールの使用

RACADM を使用するか、/telnet/ssh コンソール コマンドプロンプトから、[表 9-1](#) にあるシリアルコマンドをリモートで実行できます。

DRAC 5 へのログイン

管理ステーションのターミナルエミュレータソフトウェアと管理下ノード BIOS を設定したら、次の手順に従って DRAC 5 にログインします。

1. 管理ステーションのターミナルエミュレーションソフトウェアを使って、DRAC 5 に接続します。
2. DRAC 5 のユーザー名を入力して、<Enter>を押します。

これで DRAC 5 にログインできます。

テキストコンソールの起動

telnet または SSH を使用して管理ステーションのターミナルソフトウェアから DRAC 5 にログインしたら、telnet/SSH コマンドの **connect com2** を使って管理下システムのテキストコンソールをリダイレクトできます。一度に 1 つの **connect com2** クライアントのみがサポートされます。

管理下システムのテキストコンソールに接続するには、DRAC 5 のコマンド プロンプト (telnet または SSH セッションから表示) と開いて、次のように入力します。

```
connect com2
```

シリアルセッションから、<Esc><Shift><Q> を押して管理下システムのシリアルコンソールに接続します。これは DRAC 5 をバイパスして管理下システムのシリアルポートからサーバーの COM2 ポートに直接接続します。DRAC 5 をシリアルポートに再度接続するには、<Esc><Shift><9> を押します。管理ノード COM2 ポートと DRAC 5 シリアルポートのボーレートが同じでなければなりません。

connect -h com2 コマンドは、キーボードからの入力やシリアルポートからの新しい文字を待たずに、シリアル履歴バッファの内容を表示します。

 **メモ:** -h オプションを使用する場合は、クライアントとサーバーターミナルエミュレーションタイプ (ANSI または VT100) が同じでないと、出力が文字化けする可能性があります。また、クライアントターミナルの行は 25 に設定してください。

履歴バッファのデフォルト (最大) サイズは、8192 文字です。次のコマンドを使用すると、この値を小さくすることができます。

```
racadm config -g cfgSerial -o cfgSerialHistorySize <番号>
```

RACADM の使用

Racadm RACADM コマンドは、シリアルまたは telnet コンソールコマンドプロンプトか、通常の DOS または Linux コマンドプロンプトから、ローカルまたはリモートで実行できます。

DRAC 5 プロパティの設定、リモート管理タスクの実行、クラッシュしたシステムの回復などの操作には、**racadm** コマンドを使用します。

RACADM を使用した racadm サブコマンドのリストを表示するには、次のように入力します。

```
racadm help
```

サブコマンドのリストには、DRAC 5 でサポートされるコマンドがすべて含まれています。

racadm コマンドには、オプションなしの一般的な使用情報が表示されます。racadm help と入力すると、使用可能なサブコマンドのリストが表示されます。racadm help <サブコマンド> を入力すると、サブコマンドの構文とコマンドラインオプションのリストが表示されます。

以下の項で、racadm コマンドの使い方を説明します。

Racadm をリモートで使用する方法

 **メモ:** racadm のリモート機能を使用する前に、DRAC 5 の IP アドレスを設定してください。DRAC 5 の設定の詳細と関連文書については、「[DRAC 5 のインストールとセットアップ](#)」を参照してください。

RACADM には、管理下システムに接続してリモートコンソールまたは管理ステーションから **RACADM** サブコマンドを実行できるリモート機能オプション(-r)があります。リモート機能を使用するには、有効なユーザー名(-u オプション)、パスワード(-p オプション)、および IP アドレスが必要です。

 **メモ:** RACADM リモート機能は、Windows 2000 Server、Windows XP Professional、Windows 2000 Professional、Windows Server 2003、Windows Server 2003 R2、Red Hat Enterprise Linux (バージョン 3 とバージョン 4) および SUSE Linux オペレーティングシステムで実行している管理ステーションのみでサポートされます。

racadm の構文概要

```
racadm -r <RAC IP アドレス> -u <ユーザー名> -p <パスワード> <サブコマンド> <サブコマンドオプション>
```

```
racadm -i -r <RAC IP アドレス> <サブコマンド> <サブコマンドオプション>
```

例:

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo
```

```
racadm -i -r 192.168.0.120 getsysinfo
```

RAC の HTTPS ポート番号をデフォルトポート (443) からカスタムポートに変更した場合は、次の構文を使用する必要があります。

```
racadm -r <RAC IP アドレス>:<ポート> -u <ユーザー名> -p <パスワード> <サブコマンド> <サブコマンドオプション>
```

```
racadm -i -r <RAC IP アドレス>:<ポート> <サブコマンド> <サブコマンドオプション>
```

RACADM のオプション

表 9-1 は racadm コマンドのオプション一覧です。

表 9-1. racadm コマンドのオプション

オプション	説明
-r <racIpAddr>	コントローラのリモート IP アドレスを指定します。
-r <racIpAddr>:<ポート番号>	DRAC 5 のポート番号がデフォルトのポート (443) と異なる場合は、:<ポート番号> を使用します。
-i	インタラクティブにユーザーのユーザー名とパスワードを問い合わせるように racadm に指示します。
-u <ユーザー名>	コマンドのトランザクションの認証に使用するユーザー名を指定します。-u オプションを使用する場合は、-p オプションも使用し、-i オプション(インタラクティブ)は使用できません。
-p <パスワード>	コマンドのトランザクションを認証するパスワードを指定します。-p オプションを使用すると、-i オプションは使用できません。

RACADM リモート機能を有効または無効にする方法

 **メモ:** これらのコマンドはローカルシステムで実行することをお勧めします。

RACADM リモート機能はデフォルトでは有効になっています。無効になっている場合は、次のコマンドを使って有効にします。

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 1
```

リモート機能を無効にするには、次を入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0
```

RACADM サブコマンド

表 9-2 では、RACADM で実行できる `racadm` サブコマンドのそれぞれについて説明します。構文や有効なエントリなど、RACADM サブコマンドの詳細については、「[RACADM サブコマンドの概要](#)」のリストを参照してください。

RACADM サブコマンドを入力するときは、コマンドに `racadm` の接頭辞を付けます。例:

```
racadm help
```

表 9-2. RACADM サブコマンド

コマンド	説明
help	DRAC 5 のサブコマンドをリストにします。
help <サブコマンド>	指定したサブコマンドの使用法ステートメントをリストにします。
arp	ARP テーブルの内容を表示します。ARP テーブルエントリの追加や削除はできません。
clearasrscreen	前回 ASR (クラッシュ) 画面 (最後のブルー画面) をクリアします。
clrraclog	DRAC 5 のログをクリアします。ログがクリアされたときのユーザーと時刻を示すエントリが 1 つ作成されます。
config	RAC を設定します。
getconfig	現在の RAC 設定のプロパティを表示します。
coredump	前回の DRAC 5 coredump を表示します。
coredumpdelete	DRAC 5 に保存されているコアダンプを削除します。
fwupdate	DRAC 5 ファームウェアアップデートを実行するか、そのステータスを表示します。
getssninfo	アクティブセッションに関する情報を表示します。
getsysinfo	DRAC 5 とシステムに関する一般情報を表示します。
gettractime	DRAC 5 の時間を表示します。
ifconfig	現在の RAC IP 設定を表示します。
netstat	経路指定表および現在の接続を表示します。
ping	現在の経路指定表の内容を使用して、DRAC 5 から宛先 IP アドレスにアクセス可能であることを確認します。
setniccfq	コントローラの IP 設定を行います。
getniccfq	コントローラの現在の IP 設定を表示します。
getsvctag	サービスタグを表示します。
racdump	DRAC 5 状態と状況情報をデバッグ用にダンプします。
racreset	DRAC 5 をリセットします。
racresetcfq	DRAC 5 をデフォルト設定にリセットします。
serveraction	管理下システムの電力管理操作を実行します。
getraclog	RAC ログを表示します。
clrsef	システムイベントログのエントリをクリアします。
gettracelog	DRAC 5 ログを表示します。-i コマンドを使用すると、DRAC 5 トレースログ内のエントリ数を表示します。
sslcsrqaen	SSL CSR を生成してダウンロードします。
sslcertupload	CA 証明書またはサーバ証明書を DRAC 5 にアップロードします。
sslcertdownload	CA 証明書をダウンロードします。
sslcertview	CA 証明書またはサーバ証明書を DRAC 5 に表示します。
testemail	DRAC 5 NIC 経由で DRAC 5 に電子メールを送信させます。
testtrap	DRAC 5 NIC 経由で DRAC 5 に SNMP を送信させます。
vmdisconnect	仮想メディア接続を終了させます。
vmkey	仮想フラッシュサイズをデフォルトサイズ (16 MB) に再設定します。

RACADM エラーメッセージ

racadm CLI エラーメッセージの詳細については、この章の「[よくあるお問い合わせ \(FAQ\)](#)」を参照してください。

複数の DRAC 5 の設定

RACADM を使用すると、同じプロパティで 1 つ以上の DRAC 5 カードを設定できます。グループ ID とオブジェクト ID を使って特定の DRAC 5 をクエリすると、RACADM は取得した情報から `racadm.cfg` 設定ファイルを作成します。ファイルを 1 つ以上の DRAC 5 カードにエクスポートして、短い時間で同じプロパティのコントローラを設定できます。

 **メモ:** 一部の設定ファイルには、他の DRAC 5 カードにファイルをエクスポートする前に変更しなければならない固有の DRAC 5 情報 (静的 IP アドレスなど) が含まれています。

複数の DRAC 5 カードを設定するには、次の手順を実行してください。

1. 適切な設定を含むターゲット DRAC 5 に RACADM を使ってクエリします。

 **メモ:** 生成された .cfg ファイルにはユーザーパスワードは含まれません。

コマンドプロンプトを開いて、次のように入力します。

```
racadm getconfig -f myfile.cfg
```

 **メモ:** getconfig -f を使用して RAC の設定をファイルにリダイレクトする機能は、ローカルおよびリモートの RACADM インタフェースでのみサポートされています。

2. 簡単なテキストエディタ(オプション)を使用して設定ファイルを変更します。

3. 新しい設定ファイルを使用して、ターゲット RAC を変更します。

コマンドプロンプトで、次のように入力します。

```
racadm config -f myfile.cfg
```

4. 設定されたターゲット RAC をリセットします。

コマンドプロンプトで、次のように入力します。

```
racadm reset
```

getconfig -f racadm.cfg サブコマンドは DRAC 5 設定を要求して、racadm.cfg ファイルを生成します。必要に応じて、別の名前でファイルを設定できます。

getconfig コマンドを使用すると、次の処置を実行できます。

- 1 グループのすべての設定プロパティを表示する(グループ名とインデックスで指定)
- 1 ユーザーのすべての設定プロパティをユーザー名別に表示する

config サブコマンドは、情報を他の DRAC 5 にロードします。config を使用してユーザーおよびパスワードデータベースと Server Administrator を同期化します。

初期設定ファイルの racadm.cfg はユーザーが命名します。次の例では、設定ファイルの名前は myfile.cfg です。このファイルを作成するには、コマンドプロンプトで次のように入力します。

```
racadm getconfig -f myfile.cfg
```

 **注意:** 簡単なテキストエディタを使ってこのファイルを編集することをお勧めします。racadm ユーティリティは、ASCII テキストパーサーを使用しています。フォーマットすると、パーサーが混乱して、racadm データベースが壊れる可能性があります。

DRAC 5 設定ファイルの作成

DRAC 5 設定ファイル <ファイル名>.cfg は、racadm config -f<ファイル名>.cfg コマンドと一緒に使用されます。設定ファイルは、ユーザーが設定ファイル(.ini ファイルに類似)5 を構築して、このファイルから DRAC 4 を設定できるテキストファイルです。ファイル名は自由に指定できます。ここでは拡張子 .cfg を付けて説明していますが、その必要はありません。

.cfg ファイルには次の操作ができます。

- 1 作成する
- 1 racadm getconfig -f<ファイル名>.cfg コマンドから取得する
- 1 racadm getconfig -f<ファイル名>.cfg コマンドで取得して編集する

 **メモ:** getconfig コマンドの詳細については、「[getconfig](#)」を参照してください。

.cfg ファイルは、まずパーサーされ、有効なグループとオブジェクト名があるか、簡単な構文規則が守られているかが確認されます。エラーには、検出された行番号のフラグと、その問題を説明した簡単なメッセージが付きます。ファイル全体の整合性がパーサーされると、すべてのエラーが表示されます。エラーが .cfg ファイルに見つかった場合は、DRAC 5 への書き込みコマンドは送信されません。ユーザーは、設定前にすべてのエラーを修正する必要があります。config サブコマンドで -c オプションを使用できます。これは構文のみを検証し、DRAC 5 への書き込みは行いません。

.cfg ファイルを作成するときは、次のガイドラインに従います。

- 1 インデックス付けされたグループが検出された場合、これはさまざまなインデックスを区別するアンカー付きオブジェクトの値です。

パーサーは、DRAC 5 からそのグループのすべてのインデックスを読み取ります。グループ内のオブジェクトはすべて DRAC 5 が設定されたときに若干修正されたものです。収められたオブジェクトが新しいインデックスを表す場合、設定中 DRAC 5 にそのインデックスが作成されます。

- 1 ユーザーが .cfg ファイルのインデックスを自由に指定することはできません。

インデックスは作成や削除ができるため、グループは次第に使用中のインデックスと未使用のインデックスで断片化される可能性があります。インデックスが存在する場合は、変更されます。インデックスが存在しない場合は、最初に使用できるインデックスが使用されます。この方法では、管理しているすべての RAC 間で同じインデックスを作成する必要がないので、インデックスエントリを柔軟に追加できます。新しいユーザーは最初に使用できるインデックスに追加されます。1 つの DRAC 5 で正しくパーサーおよび実行される .cfg ファイルは、すべてのインデックスが一杯で新しいユーザーを追加しなければならない場合に、別の DRAC 5 で正しく実行されない場合があります。

- 1 **racresetcfg** サブコマンドを使用して、同じプロパティのすべての DRAC 5 カードを設定します。

racresetcfg サブコマンドを使って DRAC 5 をデフォルトにリセットして、`racadm config -f <ファイル名>.cfg` コマンドを実行します。**.cfg** ファイルに、必要なオブジェクト、ユーザー、インデックス、およびその他のパラメータがすべて含まれていることを確認します。

- ➡ **注意:** **racresetcfg** サブコマンドを使用すると、データベースと DRAC 5 NIC は元のデフォルトの設定にリセットされ、ユーザーおよびユーザー設定はすべて削除されます。root ユーザーは使用可能ですが、その他のユーザーの設定もデフォルトにリセットされます。

パースの規則

- 1 「#」で始まる行はすべてコメント扱いとなります。

コメント行は一列目から記述する必要があります。その他の列の「#」文字は単に # 文字として扱われます。

モデムパラメータでは文字列に # 文字が含まれている場合があります。エスケープ文字は必要ありません。`racadm getconfig -f <ファイル名>.cfg` コマンドから **.cfg** を生成し、エスケープ文字を追加せずに `racadm config -f <ファイル名>.cfg` コマンドを別の DRAC 5 に実行することをお勧めします。

例:

```
#  
  
# This is a comment  
  
[cfgUserAdmin]  
  
cfgUserAdminPageModemInitString=<モデムの初期文字列の # はコメントではありません>
```

- 1 すべてのグループエントリは「[」と「]」の文字で囲む必要があります。

グループ名を示すときの開始の「[」は一列目になければなりません。グループ名はそのグループ内のどのオブジェクトよりも前に指定する必要があります。オブジェクトに関係するグループ名がない場合、エラーが発生します。設定データは、「[DRAC 5 プロパティデータベースグループおよびオブジェクト定義](#)」に定義されるようにグループ分けされています。

次に、グループ名、オブジェクト、およびオブジェクトのプロパティ値の使用例を示します。

例:

```
[cfgLanNetworking] -(グループ名)  
  
cfgNicIpAddress=143.154.133.121 {オブジェクト名}
```

- 1 すべてのパラメータは、「object」、「=」、または「value」の間に空白を入れずに「object=value」のペアとして指定されます。

値の後の空白スペースは無視されます。値の文字列内にあるスペースはそのままにされます。「=」の右側の文字はそのまま使用されます (例 2 番目の '='、または '#', '[', ']', など)。これらの文字はモデムの設定に使われるチャットスクリプト文字です。

前項の例を参照してください。

- 1 **.cfg** パーサは、インデックスオブジェクトエントリを無視します。

どのインデックスを使用するかをユーザーが指定することはできません。インデックスがすでに存在している場合は、それが使用されます。インデックスがない場合は、そのグループで最初に使用可能なインデックスに新たなエントリが作成されます。

`racadm getconfig -f <ファイル名>.cfg` コマンドは、インデックスオブジェクトの前にコメントを配置するため、ここでコメントを確認できます。

- 📌 **メモ:** ユーザーは次のコマンドを使用して、インデックス付きグループを手動で作成できます。
`racadm config -g <グループ名> -o <アンカーオブジェクト> -i <インデックス 1-16> <固有のアンカー名>`

- 1 インデックスグループの行は **.cfg** ファイルから削除できません。

次のコマンドを使用して、インデックスオブジェクトを手動で削除する必要があります。

```
racadm config -g <グループ名> -o <オブジェクト名> -i <インデックス 1-16> ""
```

- 📌 **メモ:** NULL 文字列 (2 つの "" 文字) は、DRAC 5 に指定のグループのインデックスを削除するように指示します。

インデックス付きグループの内容を表示するには、次のコマンドを使用します。

```
racadm getconfig -g <グループ名> -i <インデックス 1~16>
```

- 1 インデックス付きグループの場合、オブジェクトアンカーは [] の組の後にくる最初のオブジェクトでなければなりません。次に、現在のインデックス付きグループの例を示します。

```
[cfgUserAdmin]  
  
cfgUserAdminUserName=<ユーザー名>
```

`racadm getconfig -f <myexample>.cfg` と入力すると、現在の DRAC 5 設定用の **.cfg** ファイルが構築されます。この設定ファイルを固有の **.cfg** ファイルの使用例または開始点として利用できます。

DRAC 5 の IP アドレスの変更

設定ファイルの DRAC 5 IP アドレスを変更するには、不要な <変数>=値 のエントリをすべて削除します。IP アドレス変更に関連する 2 つの <変数>=値 エントリを含む [と] が付いた実際の変数グループのラベルのみが残ります。

例:

```
#  
  
# Object Group "cfgLanNetworking"  
  
#  
[cfgLanNetworking]  
cfgNicIpAddress=10.35.10.110  
  
cfgNicGateway=10.35.10.1
```

このファイルは次のようにアップデートされます。

```
#  
  
# Object Group "cfgLanNetworking"  
  
#  
[cfgLanNetworking]  
cfgNicIpAddress=10.35.9.143  
  
# comment, the rest of this line is ignored  
  
cfgNicGateway=10.35.9.1
```

racadm config -f myfile.cfg コマンドは、このファイルをパースし、行番号ごとにエラーを探します。ファイルが正しければ、その内容で該当するエントリをアップデートします。さらに、前の例の **getconfig** コマンドを使用してアップデートを確認できます。

このファイルを使用して会社全体の変更をダウンロードしたり、ネットワークで新しいシステムを設定することができます。

 **メモ:**「アンカー」は内部の用語でファイルでは使用できません。

Racadm ユーティリティを使用した DRAC 5 の設定

 **メモ:** リモート Linux システムで RACADM コマンドを実行するには、**root** ユーザーとしてログインします。

DRAC 5 のウェブインタフェースは DRAC 5 を最短時間で設定する方法です。コマンドラインまたはスクリプト設定を使用したり、複数の DRAC 5 の設定をする場合は、管理下システムに DRAC 5 と一緒にインストールされる RACADM を使用してください。

複数の DRAC 5 を同じオプションで設定するには、次のいずれかの手順を実行します。

- 1 この項の Racadm CLI の使用例を参考に、バッチファイルまたは **racadm** コマンドを作成してから、そのバッチファイルをそれぞれの管理下システムで実行します。
- 1 [「racadm サブコマンドの概要」](#)の説明に従って DRAC 5 設定ファイルを作成し、同じ設定ファイルを使用して各管理下システムで **racadm config** サブコマンドを実行します。

はじめに

DRAC 5 のプロパティデータベースには 16 のユーザーを設定できます。DRAC 5 ユーザーを手動で有効にする前に、現在のユーザーが存在するか確認します。新しい DRAC 5 を設定している場合や、**racadm racresetcfg** コマンドを実行した場合、現在のユーザーは、パスワードが calvin の root だけです。**racresetcfg** サブコマンドは、DRAC 5 を元のデフォルトにリセットします。

 **注意:** **racreset.cfg** コマンドをすべての設定パラメータとして使用すると、元のデフォルトにリセットされるので注意してください。前の変更は喪失します。

 **メモ:** ユーザーは後日、有効 / 無効にできます。その結果、ユーザーは各 DRAC 5 に異なるインデックス番号を持つことになります。

コマンドプロンプトで、次のコマンドを入力すると、ユーザーが存在するかどうかを確認できます。

```
racadm getconfig -u <ユーザー名>
```

または

1~16 の各インデックスに 1 回ずつ次のコマンドを入力できます。

```
racadm getconfig -g cfgUserAdmin -i <インデックス>
```

 **メモ:** **racadm getconfig -f <myfile.cfg>** を入力して、DRAC 5 の設定パラメータすべてが入った **myfile.cfg** ファイルを表示または編集することもできます。

複数のパラメータとオブジェクト ID が現在の値と一緒に表示されます。オブジェクトは次の 2 つです。

```
# cfgUserAdminIndex=XX
```

cfgUserAdminUserName=

cfgUserAdminUserName オブジェクトに値がない場合は、cfgUserAdminIndex オブジェクトで示されるインデックス番号を使用できます。「=」の後に名前が表示されたら、そのインデックスはそのユーザー名が使用しています。

 **メモ:** racadm config サブコマンドを使ってユーザーを手動で追加または削除する場合は、-i オプションでインデックスを指定する必要があります。前の例に表示された cfgUserAdminIndex オブジェクトに '#' 文字があることに注意してください。また、racadm config -f racadm.cfg コマンドを使用して書き込むグループ / オブジェクトを指定する場合は、インデックスを指定できません。新しいユーザーは、最初に使用できるインデックスに追加されます。この動作により、複数の DRAC 5 を同じオプションで設定する際の柔軟性が得られます。

DRAC 5 ユーザーの追加

新しいユーザーを RAC 設定に追加する場合は、基本的なコマンドをいくつか使用できます。一般に、次の手順を実行してください。

1. ユーザー名を設定します。
2. パスワードを設定します。
3. ユーザー特権を設定します。
4. ユーザーを有効にします。

例

次の例は、パスワードが "123456" で RAC へのログイン特権を持つ "John" という新しいユーザーを追加する方法を示しています。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456
racadm config -g cfgUserAdmin -i 2 -o cfgUserPrivilege 0x00000001
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminEnable 1
```

確認するには、つぎのコマンドの 1 つを使用します。

```
racadm getconfig -u john
racadm getconfig -g cfgUserAdmin -i 2
```

DRAC 5 ユーザーの削除

RACADM を使用するとき、ユーザーは手動で個別に無効にする必要があります。設定ファイルを使ってユーザーを削除することはできません。

次の例は、RAC ユーザーを削除するときに使用できるコマンド構文です。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <インデックス> "
```

二重引用符 ("") のヌル文字列は、指定したインデックスのユーザー設定を削除して、出荷時のデフォルトリセットするように指示します。

電子メール警告のテスト

RAC 電子メール警告の機能を使用すると、管理下システムで重大なイベントが発生したときに、電子メールで警告を受け取ることができます。次の例は、RAC がネットワークを介して電子メール警告を正しく送信するかどうかを確認するため、電子メール警告の機能をテストする方法を示しています。

```
racadm testemail -i 2
```

 **メモ:** 電子メール警告の機能をテストする前に、SMTP と電子メールの設定を確認します。詳細については、「[電子メール警告の設定](#)」を参照してください。

RAC SNMP トラップ警告機能のテスト

RAC SNMP トラップ警告機能を使用すると、管理下システムで発生したシステムイベントを受信するための SNMP トラップリスナーを設定できます。

次の例は、RAC の SNMP トラップ警告機能をユーザーがテストする方法を示しています。

```
racadm testtrap -i 2
```

SNMP トラップ警告機能をテストする前に、SNMP とトラップの設定が正しいことを確認します。これらを設定するには、[testtrap](#) と [testemail](#) サブコマンドの説明を参照してください。

DRAC 5 ユーザーの権限を有効にする方法

特定の管理者権限(役割ベース認証)を持つユーザーを追加するには、最初に「はじめに」のステップを実行して、使用できるユーザーインデックスを見つけます。次に、新しいユーザー名とパスワードを使って次のコマンドラインを入力します。

 **メモ:** 特定のユーザー特権については、[表 B-2](#) で有効なビットマスクの値を参照してください。デフォルト特権の値は 0 で、この場合ユーザーに特権はありません。

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <インデックス> <ユーザー特権ビットマスク値>
```

DRAC 5 ネットワークプロパティの設定

使用可能なネットワークプロパティのリストを生成するには、次のように入力します。

```
racadm getconfig -g cfgLanNetworking
```

DHCP を使用して IP アドレスを取得するには、このコマンドでオブジェクト **cfgNicUseDhcp** を書き込んで、この機能を有効にします。

```
racadm config -g cfgLanNetworking -o cfgNicUseDhcp 1
```

コマンドは、起動時に <Ctrl><d> の入力を求められたときのオプション ROM と同じ設定機能を提供します。オプション ROM を使ってネットワークプロパティを設定する詳細については、「[DRAC 5 ネットワークプロパティの設定](#)」を参照してください。

次の例に、特定の LAN ネットワークプロパティを設定するときに使用できるコマンドの使い方を示します。

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1
racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0
racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicUseDhcp 0
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
racadm config -g cfgLanNetworking -o ccfgDNSServer1 192.168.0.5
racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6
racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1
racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002
racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

 **メモ:** **cfgNicEnable** を 0 に設定すると、DHCP が有効になっていても DRAC 5 LAN は無効になります。

DRAC モード

DRAC 5 は、次の 3 つのモードのいずれかで設定できます。

- 1 専用
- 1 共有
- 1 フェールオーバー付き共有

[表 9-3](#) で、各モードについて説明します。

表 9-3. DRAC 5 NIC 設定

モード	説明
専用	DRAC は、独自の NIC (RJ-45 コネクタ) と BMC MAC アドレスをネットトランフィックに使用します。
共有	DRAC は、プレーナで Broadcom LOM1 を使用します。
フェールオーバー付き共有	DRAC は、フェールオーバー用のチームとして Broadcom LOM1 と LOM2 を使用します。このチームは BMC MAC アドレスを使用します。

よくあるお問い合わせ(FAQ)

[表 9-4](#) に、よくあるお問い合わせ (FAQ) とその回答を示します。

表 9-4. シリアルおよび racadm コマンドの使用:よくあるお問い合わせ(FAQ)

質問	回答
racadm racreset コマンドを使用して DRAC 5 リセットを実行した後で、コマンドを発行すると次のメッセージが表示されます。 racadm <コマンド名> Transport: ERROR: (RC=-1) このメッセージはどのような意味ですか?	DRAC 5 のリセットが完了するまで待ってから、別のコマンドを発行してください。
racadm コマンドとサブコマンドを使用する場合に、不明のエラーが発生します。	racadm のコマンドとサブコマンドを使用するとき、次のエラーの 1 つまたは複数が発生する場合があります。 1 ローカルエラーメッセージ — 構文、タイプエラー、名前間違いなどの問題。 例: エラー: <メッセージ>
システムから DRAC の IP アドレスに ping してから、ping の応答中に DRAC カードを 専用 から 共有 モードに切り替えましたが、応答がありません。	システムの ARP テーブルをクリアしてください。

[目次ページに戻る](#)

[目次ページに戻る](#)

用語集

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

AGP

Accelerated Graphics Port の略語。AGPは、グラフィックカードによるメインシステムメモリへの高速なインタフェースを提供するバス仕様です。

ARP

Address Resolution Protocol(アドレス解決プロトコル)の頭字語。インターネットアドレスからホストの Ethernet アドレスを求める手法。

ASCII

American Standard Code for Information Interchange(情報交換用アメリカ標準コード)の頭字語。文字、数字、その他の記号の表示と印刷に使用されるコード表現体系。

BIOS

Basic Input/Output System の頭字語。周辺デバイスに最も低位レベルのインタフェースを提供し、オペレーティングシステムのメモリへのロードなど、システム起動処理の第一段階を制御するシステムソフトウェアの一部。

BMC

Baseboard Management Controller(ベースボード管理コントローラ)の略語。DRAC 5 と管理下システムの BMC 間のコントローラインタフェースです。

CA

認証局は、高水準で信頼できる審査、身元確認、その他の重要なセキュリティ要件を満たすことで IT 業界で認められているビジネス組織です。CA には、Thawte や VeriSign があります。CA は CSR を受信すると、その情報の確認と検証を行います。申請者が CA のセキュリティ水準を満たしている場合は、申請者に証明書を発行します。この証明書によって、ネットワークまたはインターネット上で行ったトランザクションに対して、申請者を一意に識別できます。

CD

Compact Disc(コンパクトディスク)の略語。

CHAP

Challenge-Handshake Authentication Protocol の頭字語。接続の発信元 ID を確認するために PPP サーバが使用する認証方法。

CIM

Common Information Model の頭字語。ネットワーク上でシステムを管理するためのプロトコル。

CLI

Command Line Interface の略語。

CLP

Command Line Interface の略語。

CSR

Certificate Signing Request(証明書署名要求)の略語。

DDNS

Dynamic Domain Naming System(ダイナミックドメインネーミングシステム)の略語。

DHCP

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

DLL

Dynamic Link Library の略語。小さいプログラムで構成されたライブラリ。システムで実行中の大きいプログラムが必要時にメモリに呼び出すことができます。この小さいプログラムは、大きいプログラムがプリンタやスキャナなど特定のデバイスと通信できるように、一般に DLL プログラム(または、DLL ファイル)としてパッケージ化されています。

DMTF

Distributed Management Task Force(分散管理タスクフォース)の略語。

DNS

Domain Name System(ドメイン名システム)の略語。

DRAC 5

Dell™ Remote Access Controller 5 の略語。

DSU

Disk Storage Unit(ディスクストレージユニット)の略語。

FQDN

Fully Qualified Domain Names(完全修飾ドメイン名)の頭字語。Microsoft® Active Directory® は 64 バイト以下の FQDN のみをサポートしています。

FSMO

Flexible Single Master Operation の頭字語。Microsoft の拡張操作で単独性を保証する方法。

GMT

Greenwich Mean Time(グリニッジ標準時)の略語。世界各地に共通する標準時刻。GMT はイギリスのロンドン郊外にあるグリニッジ天文台跡を通過する本初子午線(経度 0°)に基づく平均太陽時を反映しています。

GPIO

General Purpose Input/Output(汎用入力/出力)の略語。

GRUB

GRand Unified Bootloader の略語。一般的に使用されている新しい Linux ローダー。

GUI

Graphical User Interface(グラフィカルユーザーインターフェース)の略語。ユーザーとの対話がすべてテキストによって表示または入力されるコマンド表示メッセージインターフェースとは対照的に、ウィンドウ、ダイアログボックス、ボタンなどの要素を使用するコンピュータ表示インターフェースを指します。

ICMB

Intelligent Chassis Management Bus(インテリジェントシャーシ管理バス)の略語。

ICMP

Internet Control Message Protocol(インターネットコントロールメッセージプロトコル)の略語。

ID

identifier(識別子)の略語。一般に、ユーザー識別子(ユーザー ID)またはオブジェクト識別子(オブジェクト ID)を参照するときに使用されます。

IP

Internet Protocol(インターネットプロトコル)の略語。TCP/IP のネットワーク層。IP はパケットの経路指定、断片化、再構成などを提供します。

IPMB

Intelligent Platform Management Bus(インテリジェントプラットフォーム管理バス)の略語。システム管理テクノロジーで使用されるバス。

IPMI

Intelligent Platform Management Interface(インテリジェントプラットフォーム管理インタフェース)の略語。システム管理テクノロジーの一部。

Kbps

kilobits per second(キロビット/秒)の略語で、データ転送速度を表す単位。

LAN

Local Area Network(ローカルエリアネットワーク)の略語。

LDAP

Lightweight Directory Access Protocol の略語。

LED

Light-Emitting Diode(発光ダイオード)の略語。

LOM

Local area network On Motherboard の略語。

MAC

Media Access Control(メディアアクセスコントロール)の頭字語。ネットワークノードとネットワーク物理層の間のネットワークサブレイヤ。

MAC アドレス

Media Access Control アドレス。NIC の物理コンポーネントに組み込まれる固有アドレス。

MAP

Manageability Access Point の略語。

Mbps

megabits per second(メガビット/秒)の略語で、データ転送速度の単位。

MIB

Management Information Base(管理情報ベース)の略語。

MII

Media Independent Interface の略語。

NAS

Network Attached Storage の略語。

NIC

Network Interface Card(ネットワークインタフェースカード)の略語。アダプタ回路基板。コンピュータに搭載されて、ネットワークへの物理的な接続を提供します。

OID

Object Identifiers(オブジェクト識別子)の略語。

PCI

Peripheral Component Interconnect(周辺機器コンポーネント相互接続)の略語。周辺機器をシステムに接続し、それらの周辺機器と通信するための標準インタフェースおよびバス技術。

POST

Power-On Self-Test(電源投入セルフテスト)の頭字語。コンピュータの電源を入れると、システムで自動的に診断テストが実行されます。

PPP

Point-to-Point Protocol の略語。シリアルポイントツーポイントリンクを介してネットワークレイヤデータグラム(IP パケットなど)を転送するためのインターネット標準プロトコル。

RAC

Remote Access Controller の略語。

RAM

Random-Access Memory(ランダムアクセスメモリ)の頭字語。RAM は、システムおよび DRAC 5 の読み書き可能な汎用メモリです。

RAM ディスク

ハードディスクをエミュレートするメモリ常驻プログラム。DRAC 5 はメモリに RAM ディスクを保持しています。

ROM

Read-Only Memory(読み取り専用メモリ)の頭字語。データの読み取りはできますが、書き込みはできません。

RPM

Red Hat Package Manager の略語。Red Hat Enterprise Linux オペレーションシステム用のパッケージ管理システムで、ソフトウェアパッケージのインストールに使用します。インストールプログラムに似ています。

SAC

Microsoft の Special Administration Console の頭字語。

SAP

Manageability Access Point の略語。

SEL

System Event Log の頭字語。

SMI

Systems Management Interrupt(システム管理割り込み)の略語。

SMTP

Simple Mail Transfer Protocol の略語。システム間の電子メール転送に使用されるプロトコルで、通常はイーサネットで使用されます。

SMWG

Systems Management Working Group の略語。

SNMP

Simple Network Management Protocol(シンプルネットワーク管理プロトコル)の略語。IP ネットワーク上のノードを管理するためのプロトコル。DRAC 5 は SNMP が管理するデバイス(ノード)です。

SNMP トラップ

DRAC 5 または BMC によって生成される通知(イベント)。管理システムの状況変化やハードウェアの問題の可能性に関する情報が含まれています。

SSH

セキュア SHell(Secure Shell)の略語。

SSL

Secure Sockets Layer(セキュアソケットレイヤ)の略語。

TAP

Teletocator Alphanumeric Protocol の略語。ボケベルサービスに要求を送信するときに使用されるプロトコル。

TCP/IP

Transmission Control Protocol/Internet Protocol の略語。ネットワーク層とトランスポート層を含む標準イーサネットプロトコルのセットを表します。

TFTP

Trivial File Transfer Protocol の略語。ディスクデバイスやシステムに起動コードをダウンロードするために使用されるシンプルファイル転送プロトコルの一種。

UPS

無停電電源装置 (Uninterruptible power supply) の略語。

USB

ユニバーサルシリアルバス (Universal Serial Bus) の略語。

UTC

Universal Coordinated Time (協定世界時) の略語。「GMT」を参照してください。

VLAN

Virtual Local Area Network (仮想ローカルエリアネットワーク) の略語。

VNC

Virtual Network Computing (仮想ネットワークコンピューティング) の略語。

VT-100

Video Terminal 100 の略語。多くの共通端末エミュレーションプログラムで使用されています。

WAN

Wide Area Network (広域ネットワーク) の略語。

管理下システム

DRAC 5 がインストールされるか埋め込まれている管理下システム。

管理ステーション

リモートで DRAC 5 にアクセスするシステム。

コンソールリダイレクト

コンソールリダイレクトとは、管理システムのディスプレイ画面、マウス機能、キーボード機能などを管理ステーションの対応するデバイスに転送する機能のこと。この機能があれば、管理ステーションのシステムコンソールから管理下システムを制御できるようになります。

ハードウェアログ

DRAC 5 と BMC が生成するイベントを記録します。

バス

コンピュータ内の各種の機能単位を接続する伝導体のセット。バスは、それが運ぶデータの種別ごとに、データバス、アドレスバス、または PCI バス、などと命名されます。

[目次ページに戻る](#)

[目次ページに戻る](#)

Dell™ Remote Access Controller 5 ファームウェアバージョン 1.0 ユーザーズガイド

-  **メモ:** コンピュータの操作上、知っておくと便利な情報が記載されています。
-  **注意:** ハードウェアの損傷やデータ損失の可能性と、その危険を回避するための方法が記載されています。
-  **警告:** 物的損傷、負傷および死亡の危険性があることを示しています。

このマニュアルの情報は予告なしに変更されることがあります。
© 2006 すべての著作権は Dell Inc. にあります。

Dell Inc. からの書面による許可なく複製することは、いかなる手段によっても禁じられています。

このマニュアルで使用されている商標: Dell, DELL ロゴ, Dell OpenManage、および PowerEdge は Dell Inc. の商標です。Microsoft および Windows は Microsoft Corporation の登録商標で、Windows Server は Microsoft Corporation の商標です。Red Hat は、Red Hat, Inc. の登録商標です。Intel は、Intel Corporation の登録商標です。UNIX は Open Group の米国およびその他の国における登録商標です。

Copyright 1998-2006 The OpenLDAP Foundation. All rights reserved. 変更の有無にかかわらず、ソースおよびバイナリ形式の再配布と使用は、OpenLDAP パブリックライセンスによって認証されている場合に限り許可されます。このライセンスのコピーは、配布の最上位ディレクトリにある「ライセンス」ファイル、または <http://www.OpenLDAP.org/license.html> から入手できます。OpenLDAP は OpenLDAP Foundation の登録商標です。個々のファイルと提供されたパッケージの著作権は、他の著作権者が権利を有し、追加規制の対象となる場合があります。本書物はミシガン大学の LDAP v3.3 配布によるものです。本書物には公的ソースから入手した資料も含まれています。OpenLDAP に関する情報は、<http://www.openldap.org/> で入手できます。Portions Copyright 1998-2004 Kurt D. Zeilenga. Portions Copyright 1998-2004 Net Boolean Incorporated. Portions Copyright 2001-2004 IBM Corporation. All rights reserved. 変更の有無にかかわらず、ソースおよびバイナリ形式の再配布と使用は、OpenLDAP パブリックライセンスによって認証されている場合に限り許可されます。Portions Copyright 1999-2003 Howard Y.H. Chu. Portions Copyright 1999-2003 Symas Corporation. Portions Copyright 1998-2003 Halvard B. Furuseth. All rights reserved. 変更の有無にかかわらず、ソースおよびバイナリ形式の再配布および使用は、この通知が保護されるという条件の下で許可されます。著作権所有者の名称は、事前の書面による許可なく、本ソフトウェアから派生する製品を是認または促進する目的で使用してはなりません。本ソフトウェアは、明示または暗示の保証なしに「現状のまま」提供されるものとします。Portions Copyright (c) 1992-1996 Regents of the University of Michigan. All rights reserved. 変更の有無にかかわらず、ソースおよびバイナリ形式の再配布と使用は、この著作権の表示が維持され、それらがミシガン大学アーカイブに帰属するという条件の下で許可されます。大学名は、事前の書面による特定許可なく、本ソフトウェアから派生する製品を是認または促進する目的で使用してはなりません。本ソフトウェアは、明示または暗示の保証なしに「現状のまま」提供されるものとします。本書には、商標または製品の権利を主張する事業体を表すその他の商標および社名が使用されていることがあります。これらの商標や会社名は、Dell Inc. に所属するものではありません。

本書には、商標または製品の権利を主張する事業体を表すその他の商標および社名が使用されていることがあります。これらの商標や会社名は、Dell Inc. に所属するものではありません。

[目次ページに戻る](#)