Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

メモおよび注意

メモ: コンピュータを使いやすくするための重要な情報を説明しています。

注意: 手順に従わない場合は、ハードウェアの損傷やデータの損失の可能性があることを示しています。

2011 - 02

目次に戻る

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 1.60 ユーザーズガイド

本項では、RACADM コマンドラインインタフェースで使用できるサブコマンドについて説明します。

---

help

メモ: このコマンドを使うには、**DRAC 5 へのログイン** パーミッションが必要です。

表 A-1 に、**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**で使用できるすべてのサブコマンドをリストにし、それぞれの短い説明を表示します。

構文概要

```
racadm help

racadm help <サブコマンド>
```

説明

help サブコマンドは **racadm** コマンドで使用できるすべてのサブコマンドにそれぞれ一行の説明を付けて一覧表示します。**help** の後にサブコマンドを入力して、そ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 コマンドはすべての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だけの情報を表示します。

対応インタフェース

- ローカルRACADM
- リモートRACADM
- Telnet/SSH/シリアル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** パーミッションが必要です。

表 A-2 に、**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 エントリの追加や削除はできません。

構文概要

```
racadm arp
```

対応インタフェース

- リモート RACADM
- Telnet/SSH/シリアル RACADM

---

clearasrscreen

メモ: このサブコマンドを使用するには、**ログのクリア** パーミッションが必要です。

表 A-3 に、**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	メモリにある最後のクラッシュ画面をクリアします。

構文概要

```
racadm clearasrscreen
```

対応インタフェース

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/シリアル RACADM

---

config

メモ: **getconfig** コマンドを使うには、**DRAC 5へのログイン** パーミッションが必要です。

表 A-4に、**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 の設定データを取得します。

構文概要

```
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

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/シリアル RACADM

説明

config サブコマンドでは、ユーザーは DRAC 5 設定パラメータを個別に設定したり、設定ファイルの一部として一括して設定することができます。データが異なる場合は、その DRAC 5 オブジェクトが新しい値で書き込まれます。

入力

表 A-5 に、**config** サブコマンドオプションについて説明します。

メモ: **-f** と **-p** オプションは、シリアル/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*>**オプションは、**config** が **<*ファイル名*>**で指定したファイルの内容を読み込んでDRAC 5を設定するようにします。ファイルの内容は 構文解析規則 で指定した形式のデータである必要があります。
-p	**-p** （パスワード） オプションを使用すると、**config** は iDRAC6 の設定完了後に config 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を含むグループを指定します。
-o	**-o <*オブジェクト名*> <*Value*>** （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>で書き込まれる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グループのみに有効で、一意グループを指定できます。<*index*> は 1 ～ 16 の 10 進整数です。この場合、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し、ユーザーが **.cfg** ファイルの構文を解析して構文エラーを検出できるようにします。エラーが検出された場合は、その行番号とエラーの短い説明が表示されます。DRAC 5 への書き込みは行われません。このオプションはチェックのみです。

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。

- 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
- RACADM CLI エラー

このサブコマンドは、**.cfg** ファイル内にあったオブジェクトの総数のうち、そこから書き込まれた設定オブジェクトの数を示す値を返します。

例

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

  cfgNicIp アドレス 設定パラメータ（オブジェクト）の値を 10.35.10.110 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。

- `racadm config -f myrac.cfg`

  DRAC 5 を設定または再設定します。**myrac.cfg** ファイルは **getconfig** コマンドから作成できます。**myrac.cfg** ファイルは、構文解析ルールに従って手動で編集することもできます。

  メモ: **myrac.cfg** ファイルには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。設定時に **myrac.cfg** ファイルからパスワード情報を削除する場合は、**-p** オプションを使用します。

---

getconfig

getconfig サブコマンドの説明

getconfig サブコマンドを使うと、DRAC 5 設定パラメータを個別に取得することも、RAC 設定グループをすべて取得して 1 つのファイルに保存することもできます。

入力

表 A-6 に、**getconfig** サブコマンドオプションについて説明します。

メモ: ファイルを指定しないで **-f** オプションを使用すると、ファイルの内容が端末画面に出力されます。

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*>** オプションは、全 RAC 設定を設定ファイルに書き込むようにgetconfig に指示します。このファイルは **config** サブコマンドを使った一括設定用に使用できます。 **メモ: -f** オプションでは **cfgIpmiPet** と **cfgIpmiPef** グループのエントリは作成されません。**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**） オプションを使用すると、単一グループの設定を表示できます。**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付きグループの場合は、**-i** オプションを使用してください。
-h	**-h** （**ヘルプ**） オプションは、使用可能な設定グループすべてを表示します。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*> を指定しなければ、複数のエントリを含んだテーブルのグループに 1 の値が想定されます。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。
-o	オブジェクトオプションの -o **<*オブジェクト名*>** は、クエリで使用す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	ユーザー名オプションの **-u <*ユーザー名*>** （**ユーザー名**）オプションを使用すると、指定したユーザーの設定を表示できます。**<*ユーザー名*>** オプションはユーザーのログインユーザー名です。
-v	**-v** オプションは、プロパティの表示で追加の詳細情報を表示するために、**-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。

- 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
- racadm CLI トランスポートエラー

エラーが発生しなければ、指定した設定の内容が表示されます。

例

- `racadm getconfig -g cfgLanNetworking`

  cfgLanNetworking グループ内の設定プロパティ（オブジェクト）をすべて表示します。

- `racadm getconfig -f myfile.cfg`

  すべてのグループ設定オブジェクトを RAC から **myrac.cfg** に保存します。

- `racadm getconfig -h`

  DRAC 5 上で使用可能な設定グループのリストを表示します。

- `racadm getconfig -u root`

  `root` という名前のユーザーの設定プロパティを表示します。

- `racadm getconfig -g cfgUserAdmin -i 2 -v`

  インデックス 2 でのユーザーグループインスタンスを、プロパティ値の詳細情報と一緒に表示します。

構文概要

```
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

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル 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** パーミッションが必要です。

表 A-7 に、**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	最新の DRAC 5 コアダンプを表示します。

構文概要

```
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 情報はこれらの重要な問題の診断に使用できます。

使用可能な場合、coredump 情報は RAC の電源を切った後も、以下のどちらかの状態が発生するまで保持されます。

- **coredumpdelete** サブコマンドで coredump 情報がクリアされた。
- RAC で別の重要な問題が発生した この場合、coredump の内容は最後に発生した重大エラーに関するものとなります。

coredump のクリアの詳細については、**coredumpdelete** サブコマンドを参照してください。

対応インタフェース

- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

coredumpdelete

メモ: このコマンドを使用するには、**ログのクリア** または **デバッグコマンドの実行** パーミッションが必要です。

表 A-8 に、**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
coredumpdelete	DRAC 5 に保存されているコアダンプを削除します。

構文概要

```
racadm coredumpdelete
```

説明

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

メモ: **coredumpdelete** コマンドを発行したときに coredump が RAC に保存されていないと、成功したというメッセージが表示されます。これは正常な動作です。

coredump の表示に関する詳細は、**coredump** サブコマンドを参照してください。

対応インタフェース

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

fwupdate

メモ: このコマンドを使うには、**DRAC 5 の設定** パーミッションが必要です。

メモ: ファームウェアのアップデートを開始する前に、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 を参照してください。

表 A-9 に、**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
fwupdate	DRAC 5. 上のファームウェアのアップデート

構文概要

```
racadm fwupdate -s

racadm fwupdate -g -u -a <TFTP サーバーの IP アドレス> -d <パス>
```

```
racadm fwupdate -p -u -d <パス>
```

説明

fwupdate サブコマンドを使うと、DRAC 5 上のファームウェアをアップデートできます。ユーザーは以下のことができます。

- ファームウェアアップデートプロセスの状態を確認する
- IP アドレス（とパス）を指定することで TFTP サーバーから DRAC 5 ファームウェアをアップデートする
- ローカル RACADM を使ってローカルファイルから DRAC 5 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

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

入力

表 A-10 に **fwupdate** サブコマンド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およびリモート RACADM でサポートされています。シリアル/telnet/ssh コンソールではサポートされていません。**-p** オプションは Linux プラットフォーム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	**update** 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て、実際のアップデートプロセスを開始します。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。アップデートの終りに DRAC 5 はソフトリセットを実行します。
-s	**status** オプションはアップデートプロセスの現在の状態を返します。このオプションは、常に単独で使用します。
-g	**get** オプションは TFTP サーバーからファームウェア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。ユーザーは **-a** と **-d** オプションも指定する必要があります。**-a** オプションを指定しないと、プロパティ **cfgRhostsFwUpdateIpAddr** と **cfgRhostsFwUpdatePath** プロパティを使用して、グループ **cfgRemoteHosts** にあるプロパティからデフォルトが読み込まれます。
-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が保存されている TFTP サーバー上または 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、ファームウェアファイルを管理下システムからDRAC 5 にアップデートするために使用します。**-u** オプションを **-p** オプションと一緒に使用する必要があります。

出力

どの操作を実行中かを示すメッセージを表示します。

例

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

  この例では、**-g** オプションは、（**-d** で指定した）特定の IP アドレスにある TFTP サーバー上の（**-a** オプションで指定した）場所からファームウェア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をダウンロードした後、アップデートプロセスが開始されます。完了したら、DRAC 5 はリセットされます。

  ダウンロードに 15 分以上かかってタイムアウトした場合は、ファームウェアのフラッシュイメージをサーバー上のローカルドライブに転送します。その後、コンソールリダイレクトを使って、リモートシステムに接続し、ローカル `racadm` を使ってファームウェアをローカルにインストールします。

- `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込みます。

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

  この例では、アップデートの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。

- `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、RACADM は、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アップデートするために使用しています。このイメージは TFTP サーバーから取得します。

メモ： **-p** オプションはローカルおよびリモート RACADM でサポートされています。シリアル/telnet/ssh コンソールではサポートされていません。**-p** オプションは Linux プラットフォームではサポートされていません。

---

getssninfo

メモ： このコマンドを使うには、**DRAC 5 へのログイン** パーミッションが必要です。

表 A-11 に、**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 のセッションテーブルから、1 つまたは複数の現在アクティブまたは保留中のセッションの情報を取得します。

構文概要

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

説明

getssninfo コマンドは、DRAC に接続されているユーザーのリストを返します。概要情報では次の情報が表示されます。

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

対応インタフェース

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

入力

表 A-12 に、**getssninfo** サブコマンドオプションについて説明します。

表 A-12. getssninfo サブコマンドオプション

オプション	説明
-A	**-A** オプションを指定すると、データヘッダは印刷されません。
-u	**-u <ユーザー名 >** ユーザー名オプションは、印刷出力を特定のユーザー名の詳細セッション記録だけに限定します。ユーザー名として「*」記号を入力した場合は、すべてのユーザーが表示されます。このオプションを指定すると、概要情報は印刷されません。

例

- `racadm getssninfo`

表 A-13 に **racadm getssninfo** コマンド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	タイプ	コンソール
root	192.168.0.10	Telnet	仮想 KVM

- racadm getssninfo -A

  "root" 143.166.174.19 "Telnet" "NONE"

- racadm getssninfo -A -u *

  "root" "143.166.174.19" "Telnet" "NONE"

  "bob" "143.166.174.19" "GUI" "NONE"

---

getsysinfo

メモ: このコマンドを使うには、**DRAC 5 へのログイン** パーミッションが必要です。

表 A-14 に、**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
getsysinfo	DRAC 5 情報、システム情報、ウォッチドッグステータス情報を表示します。

構文概要

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

説明

getsysinfo サブコマンドは、RAC、管理下システム、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

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

入力

表 A-15 に、**getsysinfo** サブコマンド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
-d	DRAC 5 情報を表示します。
-s	システム情報を表示します。
-w	ウォッチドッグ情報を表示します。
-A	ヘッダ / ラベルを印刷しません。

-w オプションを指定しないと、その他のオプションがデフォルトとして使用されます。

出力

getsysinfo サブコマンドは、RAC、管理下システム、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 = Mon Oct 26 19:05:33 2009

Firmware Version = 1.50

Firmware Build = 09.10.21

Last Firmware Update = Wed Oct 21 21:57:33 2009

Hardware Version = A00

Current IP Address = 192.168.1.21

Current IP Gateway = 0.0.0.0

Current IP Address = 255.255.255.0

DHCP Enabled = 1

MAC Address = 00:1c:23:d7:1a:d9

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-297GP1S

Current DNS Domain =

System Information:

System Model = PowerEdge 2950

System Revision = [N/A]

System BIOS Version = 1.3.7

BMC Firmware Version = 02.28

Service Tag = 297GP1S

Express Service Tag = 4910296528

Host Name =

OS Name =

Power Status = ON

Watchidog Information:

Recovery Action = None

Present countdown value = 15 seconds

Initial countdown value = 15 seconds

Embedded NIC MACA dressess:

NIC1 Ethernet = 00:1A:A0:11:93:68

NIC2 Ethernet = 00:1A:A0:11:93:6A
```

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
Express Service Tag     = 48192
Express Service Tag     = 4910296528
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

Dell OpenManage が管理下システムにインストールされているときにのみ、**getsysinfo** の出力のホスト名と OS 名フィールドに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と、これらのフィールドには空白または不正確な値が表示されます。

---

getractime

メモ: このコマンドを使うには、**DRAC 5 へのログイン** パーミッションが必要です。

表 A-16 に、**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
getractime	リモートアクセスコントローラの現在の時刻を表示します。

構文概要

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

説明

オプションを指定しないと、**getractime** サブコマンドは時刻を一般的な可読形式で表示します。

-d オプションを指定すると、**getractime** は時刻を *yyyymmddhhmmss.mmmmmms* 形式で表示します。これは UNIX **date** コマンドで返されるのと同じ形式です。

出力

getractime サブコマンドは出力を 1 行で表示します。

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

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

ifconfig

メモ: このコマンドを使うには、**診断コマンドの実行** または **DRAC 5 の設定** パーミッションが必要です。

表 A-17 に、**ifconfig** サブコマンドについて説明します。

表 A-17. ifconfig

サブコマンド	定義
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。

構文概要

```
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** パーミッションが必要です。

表 A-18 に、**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	ルーティングテーブルと現在の接続を表示します。

構文概要

```
racadm netstat
```

対応インタフェース

- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

ping

メモ: このコマンドを使うには、**診断コマンドの実行** または **DRAC 5 の設定** パーミッションが必要です。

表 A-19 に、**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	現在のルーティングテーブルの内容を使って DRAC 5 から宛先 IP アドレスにアクセスできることを確認します。宛先 IP アドレスが必要です。ICMP エコーパケットが現在のルーティングテーブルの内容に基づいて、目的の IP アドレスに送信されます。

構文概要

```
racadm ping <IP アドレス>
```

対応インタフェース

- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

setniccfg

メモ: **setniccfg** コマンドを使うには、**DRAC 5 の設定** パーミッションが必要です。

表 A-20 に、**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 設定を指定します。

メモ: NIC と イーサネット管理ポートは同じ意味で使われる場合があります。

構文概要

```
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。

- **-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）。
- **-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、ゲートウェイを指定できます。指定しなければ、既存の静的な設定が使用されます。*<IP アドレス>*、*<ネットマスク>*、*<ゲートウェイ>* は文字列をドットで区切って入力する必要があります。

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

- **-o** オプションはイーサネット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>*、*<ゲートウェイ>* は文字列をドットで区切って入力する必要があります。

  ```
  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、操作に失敗した場合にエラーメッセージを表示します。成功した場合は、成功したことを知らせるメッセージが表示されます。

対応インタフェース

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

getniccfg

メモ: **getniccfg** コマンドを使うには、**DRAC 5 へのログイン** パーミッションが必要です。

表 A-21 に **setniccfg** と **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 設定を表示します。

構文概要

```
racadm getniccfg
```

説明

getniccfg サブコマンドは、現在のイーサネット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、操作に失敗した場合にエラーメッセージを表示します。成功した場合は、設定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

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

getsvctag

メモ: このコマンドを使うには、**DRAC 5 へのログイン** パーミッションが必要です。

表 A-22 に **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
getsvctag	サービスタグを表示します。

構文概要

```
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」と入力します。出力は次のように表示されます。

```
Y76TP0G
```

成功すると 0、エラーの場合はゼロ以外の値を返します。

対応インタフェース

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

racdump

メモ: このコマンドを使用するには、**デバッグ** パーミッションが必要です。

表 A-23 に **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 DRAC 5 の一般的な情報を表示します。

構文概要

```
racadm racdump
```

説明

racdump サブコマンドは、ダンプ、状態、DRAC 5 ボードの一般情報を取得する 1 つのコマンドを提供します。

racdump サブコマンドを実行すると、次の情報が表示されます。

- システム / RAC の一般情報
- コアダンプ
- セッション情報
- プロセス情報
- ファームウェアビルド情報

対応インタフェース

- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

racreset

メモ： このコマンドを使うには、**DRAC 5 の設定** パーミッションが必要です。

表 A-24 に、**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き、DRAC が使用可能な状態に戻るまでに 1 分間までかかることがあります。

構文概要

```
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 のログに書き込まれます。

ハードリセットは RAC のディープリセットを行います。ハードリセットは、RAC を回復するための最終手段としてのみ実行してください。

注意：DRAC 5 のハードリセットを行った後は、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 に、**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
hard	ハードリセットはリモートアクセスコントローラ（RAC）のディープリセットを行います。ハードリセットは、回復目的で の最終手段としてRACコントローラをリセットするためにのみ使用してください。
soft	ソフトリセットは RAC の正常な再起動を行います。

例

- `racadm racreset`

  DRAC 5 のソフトリセットシーケンスを開始します。

- `racadm racreset hard`

  DRAC 5 のハードリセットシーケンスを開始します。

対応インタフェース

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

racresetcfg

メモ： このコマンドを使うには、**DRAC 5 の設定** パーミッションが必要です。

表 A-26 に、**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 設定全体を工場出荷時のデフォルト値に戻します。

構文概要

```
racadm racresetcfg
```

対応インタフェース

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

説明

racresetcfg サブコマンドは、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。データベースのすべてのエントリには、カードを最初のデフォルト設定に戻すために使用するデフォルトのプロパティがあります。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 の現在の設定値を削除し、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名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（対応ウェブブラウザ、telnet/ssh、リモート RACADM など）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： このサブコマンドはまた、シリアルインタフェースもデフォルトボーレート（57600）と COM ポートに戻します。シリアルポートを通して RAC にアクセスするためにサーバー用の BIOS 設定画面でシリアル設定を再設定することが必要になる場合があります。

---

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** パーミッションが必要です。

表 A-27 に、**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
serveraction	管理下システムのリセットまたは電源オン / オフ / 入れ直しを実行します。

構文概要

```
racadm serveraction <アクション>
```

説明

serveraction サブコマンドを使うと、ホストシステムの電源管理を行うことができます。表 A-28 に、**serveraction** 電源管理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
<アクション>	処置を指定します。<アクション> の文字列のオプションは次のとおりです。 • **powerdown** — 管理下システムの電源を切ります。 • **powerup** — 管理下システムの電源を入れます。 • **powercycle** — 管理下システムの電源を入れ直します。このアクションは、システムのフロントパネルの電源ボタンを押してシステムの電源を入れ直すのと同様です。 • **powerstatus** — サーバーの現在の電源状態を表示します（「オン」または「オフ」）。 • **hardreset** — 管理下システムのリセット（再起動）を行います。

出力

serveraction サブコマンドは、要求された動作が実行できなかった場合にエラーメッセージを表示し、要求された動作が正常に完了した場合は成功のメッセージを表示します。

対応インタフェース

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

getraclog

メモ: このコマンドを使うには、**DRAC 5 へのログイン** パーミッションが必要です。

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
getraclog -i	DRAC 5 ログのエントリの数を表示します。
getraclog	DRAC 5 ログのエントリを表示します。

構文概要

```
racadm getraclog -i

racadm getraclog [-A] [-o] [-c 数] [-s 開始レコード] [-m]
```

説明

getraclog -i コマンドは DRAC 5 ログのエントリの数を表示します。

以下のオプションを使用すると、**getraclog** コマンドでエントリを読み込むことができます。

- **-A** — ヘッダーやラベルなしで出力を表示します。
- **-c** — 返されるエントリの最大数を指定します。
- **-m** — 一度に 1 画面分の情報を表示し、ユーザーに続行するように指示します（UNIXの **more** コマンドと同様）。

- **-o** — 出力を 1 行に表示します。
- **-s** — 表示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、すべてのログが表示されます。

出力

デフォルト出力には、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 0 時に始まり、システムが起動するまで増分されます。システムが起動した後は、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

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

clrraclog

メモ: このサブコマンドを使用するには、**ログのクリア** パーミッションが必要です。

構文概要

```
racadm clrraclog
```

説明

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

---

getsel

メモ: このコマンドを使うには、**DRAC 5 へのログイン** パーミッションが必要です。

表 A-30 に、**getsel** コマンドについて説明します。

表 A-30. getsel

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

構文概要

```
racadm getsel -i

racadm getsel [-E] [-R] [-A] [-o] [-c 数] [-s 数] [-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** オプションなし）はエントリの読み込みに使用します。

-A — ヘッダーとラベルなしで表示します。

-c — 返されるエントリの最大数を指定します。

-o — 出力を 1 行に表示します。

-s — 表示する開始レコードを指定します。

-E — 各行の終りに生の SEL を 16 バイトほど 16 進値で出力します。

-R — 生のデータのみ出力します。

-m — 一度に 1 画面分を表示し、ユーザーに続行するように指示します（UNIXの **more** コマンドと同様）。

メモ: 引数を何も指定しないと、ログ全体が表示されます。

出力

デフォルトの出力には、レコード番号、タイムスタンプ、重要度、説明が表示されます。

たとえば、次のとおりです。

```
Record:      1
Date/Time:   11/16/2005 22:40:43
Severity:    Ok
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/ シリアル RACADM

---

clrsel

メモ: このサブコマンドを使用するには、**ログのクリア** パーミッションが必要です。

構文概要

```
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

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

gettracelog

メモ: このコマンドを使うには、**DRAC 5 へのログイン** パーミッションが必要です。

表 A-31 に、**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
gettracelog -i	DRAC 5 トレースログのエントリの数を表示します。
gettracelog	DRAC 5 トレースログを表示します。

構文概要

```
racadm gettracelog -i

racadm gettracelog [-A] [-o] [-c 数] [-s 開始レコード] [-m]
```

説明

gettracelog （**-i** オプションなし）コマンドはエントリを読み込みます。以下の **gettracelog** エントリを使用してエントリを読み込みます。

-i — DRAC 5 トレースログのエントリの数を表示します。

-m — 1 度に 1 画面を表示し、ユーザーに続行を指示します（UNIXの **more** コマンドと同様）。

-o — 出力を 1 行に表示します。

-c — 表示するレコード数を指定します。

-s — 表示を開始するレコードを指定します。

-A — ヘッダーとラベルを表示しません。

出力

デフォルト出力には、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 0 時に始まり、システムが起動するまで増分されます。システムが起動した後は、システムのタイムスタンプが使用されます。

たとえば、次のとおりです。

```
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

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

sslcsrgen

メモ: このコマンドを使うには、**DRAC 5 の設定** パーミッションが必要です。

表 A-32 に、**sslcsrgen** サブコマンドについて説明します。

表 A-32. sslcsrgen

サブコマンド	説明
sslcsrgen	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。

構文概要

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

racadm sslcsrgen -s
```

説明

sslcsrgen サブコマンドを使用すると、CSR を生成して、クライアントのローカルファイルシステムにファイルをダウンロードできます。CSR は、RAC の SSL トランザクションに使用できるカスタム SSL 証明書の作成に使用できます。

オプション

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

表 A-33 に、**sslcsrgen** サブコマンドオプションについて説明します。

表 A-33. sslcsrgen サブコマンドオプション

オプション	説明
-g	新しい CSR を生成します。
-s	CSR 生成プロセスの状態を返します（生成中、アクティブ、なし）。
-f	CSR をダウンロードする先の場所の <ファイル名> を指定します。

メモ： **-f** オプションを指定しなければ、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、生成された CSR は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は使用できず、**-f** オプションは **-g** オプションと一緒にしか使用できません。

sslcsrgen -s サブコマンドは次のいずれかの状態コードを返します。

- CSR は正常に生成されました。
- CSR はありません。
- CSR の生成中です。

制限

sslcsrgen サブコマンドはローカルまたはリモート RACADM クライアントからしか実行できず、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 を生成する前に、CSR フィールドを RACADM **cfgRacSecurity** グループで設定する必要があります。例：racadm config -g cfgRacSecurity -o cfgRacSecCsrCommonName MyCompany

例

```
racadm sslcsrgen -s
```

または

```
racadm sslcsrgen -g -f c:\csr\csrtest.txt
```

対応インタフェース

- ローカル RACADM
- リモート RACADM

- Telnet/SSH/ シリアル RACADM

---

sslcertupload

メモ: このコマンドを使うには、**DRAC 5 の設定** パーミッションが必要です。

表 A-34 に、**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
sslcertupload	カスタム SSL サーバーまたは CA 証明書をクライアントから RAC にアップロードします。

構文概要

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

オプション

表 A-35 に、**sslccertupload** サブコマンド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
-t	アップロードする証明書のタイプが CA 証明書かサーバー証明書かを指定します。 1 = サーバー証明書 2 = CA 証明書
-f	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 **sslcert** ファイルが選択されます。

sslcertupload コマンドはアップロードに成功すると 0 を返し、成功しなければゼロ以外の値を返します。

制限

sslcertupload サブコマンドはローカルまたはリモート RACADM クライアントからしか実行できません。**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:\cert\cert.txt
```

対応インタフェース

- ローカル RACADM
- リモート RACADM

---

sslcertdownload

メモ: このコマンドを使うには、**DRAC 5 の設定** パーミッションが必要です。

表 A-36 に、**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
sslcertdownload	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。

構文概要

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

オプション

表 A-37 に、**sslccertdownload** サブコマンド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
-t	ダウンロードする証明書のタイプを Microsoft Active Directory 証明書またはサーバ証明書のいずれかに指定します。 1 = サーバー証明書 2 = Microsoft Active Directory 証明書
-f	アップロードする証明書のファイル名を指定します。**-f** オプションまたはファイル名が指定されていないと、現在のディレクトリ内の **sslcert** ファイルが選択されます。

sslcertdownload コマンドはダウンロードに成功すると 0 を返し、成功しなければゼロ以外の値を返します。

制限

sslcertdownload サブコマンドを実行できるのは、ローカルまたはリモートの RACADM クライアントからのみです。**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 sslcertdownload -t 1 -f c:\cert\cert.txt
```

対応インタフェース

- ローカル RACADM
- リモート RACADM

---

sslcertview

メモ: このコマンドを使うには、**DRAC 5 の設定** パーミッションが必要です。

表 A-38 に、**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

sslcertview	RAC にある SSL サーバーまたは CA 証明書を表示します。

構文概要

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

オプション

表 A-39 に、**sslccertview** サブコマンドオプションについて説明します。

表 A-39. sslcertview サブコマンドオプション

オプション	説明
-t	表示する証明書の種類が Microsoft Active Directory 証明書かサーバ証明書かを指定します。 1 = サーバー証明書 2 = Microsoft Active Directory 証明書
-A	ヘッダー / ラベルを印刷しません。

出力例

```
racadm sslcertview -t 1

Serial Number             : 00

Subject Information:
Country Code (CC)         : US
State (S)                 : Texas
Locality (L)              : Round Rock
Organizatoin (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
Organi©ation (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 Date                : Jul 7 16:21:56 2010 GMT

racadm sslcertview -t 1 -A

00
US
Texas
Round Rock
Dell Inc.
Remote Access Group
DRAC5 default certificate
US
Texas
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

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

sslkeyupload

メモ: このコマンドを使うには、**DRAC 5 の設定** パーミッションが必要です。

表 A-40 に、**sslkeyupload** サブコマンドについて説明します。

表 A-40. sslkeyupload

サブコマンド	説明
sslkeyupload	SSL キーをクライアントから DRAC 5 にアップロードします。

構文概要

```
racadm sslkeyupload -t <種類> [-f <ファイル名>]
```

オプション

表 A-41 に、**sslkeyupload** サブコマンドのオプションについて説明します。

表 A-41. sslkeyupload サブコマンドオプション

オプション	説明
-t	アップロードするキーを指定します。 1 = サーバー証明書
-f	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 **sslcert** ファイルが選択されます。

sslkeyupload コマンドはアップロードに成功すると 0 を返し、成功しなければゼロ以外の値を返します。

制限

sslkeyupload サブコマンドを実行できるのは、ローカルまたはリモートの RACADM クライアントからのみです。**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:\cert\cert.txt
```

対応インタフェース

- ローカル RACADM
- リモート RACADM

sslresetcfg

メモ: このコマンドを使うには、**DRAC 5 の設定** パーミッションが必要です。

表 A-42 は、**sslresetcfg** サブコマンドを説明します。

表 A-42. sslresetcfg

サブコマンド	説明
sslresetcfg	ウェブサーバー証明書を工場出荷時のデフォルトに復元し、ウェブサーバーを再起動します。コマンドを入力した 30秒後に、証明書の効力が発します。

構文概要

```
racadm sslresetcfg
```

例

```
$ racadm sslresetcfg
```

証明書の生成に成功し、ウェブサーバーを再起動しました。

対応インタフェース

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/シリアル

---

krbkeytabupload

メモ: このコマンドを使うには、**DRAC 5 の設定** パーミッションが必要です。

表 A-43 に、**krbkeytabupload** サブコマンドについて説明します。

表 A-43. kerbkeytabupload

サブコマンド	説明
krbkeytabupload	Kerberos keytab ファイルをアップロードします。

構文概要

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

オプション

表 A-44 に、**krbkeytabupload** サブコマンドのオプションについて説明します。

表 A-44. krbkeytabupload サブコマンドのオプション

オプション	説明
-f	アップロードする keytab 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 keytab ファイルが選択されます。

krbkeytabupload コマンドは、成功すると 0 を返し、失敗するとゼロ以外の数字を返します。

制限

krbkeytabupload サブコマンドを実行できるのは、ローカルまたはリモートの RACADM クライアントからのみです。

例

```
racadm krbkeytabupload -f c:\keytab\krbkeytab.tab
```

対応インタフェース

- ローカル RACADM
- リモート RACADM

---

testemail

表 A-45 に、**testemail** サブコマンドについて説明します。

表 A-45. testemail の設定

サブコマンド	説明
testemail	RAC の電子メールアラート機能をテストします。

構文概要

```
racadm testemail -i <インデックス>
```

説明

テスト電子メールを RAC から指定した宛先に送信します。

テスト電子メール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で、正しく設定されていることを確認してください。表 A-46 に、**cfgEmailAlert** グループのリストと関連コマンドを示します。

表 A-46. testemail の設定

アクション	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設定する	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 の IP アドレスが正しく設定されていることを確認します。	racadm config -g cfgRemoteHosts -o cfgRhostsSmptServerIpAddr 192.168.0.120
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 の数値です。

オプション

表 A-47 に、**testemail** サブコマンドオプションについて説明します。

表 A-47. 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

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

testtrap

メモ: このコマンドを使用するには、**警告のテスト** パーミッションが必要です。

表 A-48 に、**testtrap** サブコマンドについて説明します。

表 A-48. 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。

構文概要

```
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ーにテストトラップを送信することで 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 **cfgIpmiPet** グループ内の指定した索引が正しく設定されていることを確認してください。

表 A-49 に、**cfgIpmiPet** グループに関するコマンドを示します。

表 A-49. cfgEmailAlert コマンド

アクション	コマンド
警告を有効にする	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable 0 -i 1 1
宛先の電子メールの IP アドレスを設定する	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -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 cfgIpmiPet -i <インデックス> <インデックス> は 1 ～ 4 の数値です。

入力

表 A-50 に、**testtrap** サブコマンドオプションについて説明します。

表 A-50. 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

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

vmdisconnect

メモ: このサブコマンドを使用するには、**仮想メディアのアクセス** パーミッションが必要です。

表 A-51 に、**vmdisconnect** サブコマンドについて説明します。

表 A-51. vmdisconnect

サブコマンド	説明
vmdisconnect	開いている RAC 仮想メディア接続をリモートクライアントから閉じます。

構文概要

```
racadm vmdisconnect
```

説明

vmdisconnect サブコマンドを使用すると、他のユーザーの仮想メディアセッションを切断できます。切断すると、そのウェブベースのインタフェースに正しい接続状態が表示されます。これは、ローカルまたはリモート racadm を使ってのみ使用できます。

vmdisconnect サブコマンドを使うと、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に表示することも、racadm **getsysinfo** サブコマンドを使って表示することもできます。

対応インタフェース

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

vmkey

メモ: このサブコマンドを使用するには、**仮想メディアのアクセス** パーミッションが必要です。

表 A-52 に、**vmkey** サブコマンドについて説明します。

表 A-52. vmkey

サブコマンド	説明
vmkey	仮想メディアキー関連の操作を行います。

構文概要

racadm vmkey <アクション>

<アクション> を リセット に設定すると、仮想フラッシュメモリは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イメージを RAC にアップロードすると、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、キーを元のデフォルトサイズ（DRAC 5 上で 16 MB）に戻すために使用できます。

対応インタフェース

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

usercertupload

メモ: このコマンドを使うには、**DRAC 5 の設定** パーミッションが必要です。

表 A-53 に、**usercertupload** サブコマンドについて説明します。

表 A-53. usercertupload

サブコマンド	説明
usercertupload	ユーザー証明書またはユーザー CA 証明書をクライアントから DRAC にアップロードします。

構文概要

racadm usercertupload -t <タイプ> [-f <ファイル名>] -i <索引>

オプション

表 A-54 に、**usercertupload** サブコマンドオプションについて説明します。

表 A-54. usercertupload サブコマンドオプション

オプション	説明
-t	アップロードする証明書のタイプが CA 証明書かサーバー証明書かを指定します。 1 = ユーザー証明書 2 = ユーザー CA 証明書
-f	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 **sslcert** ファイルが選択されます。
-i	ユーザーのインデックス番号。有効な値は 1 ～ 16 です。

usercertupload コマンドはアップロードに成功すると 0 を返し、成功しなければゼロ以外の値を返します。

制限

usercertupload サブコマンドを実行できるのは、ローカルまたはリモートの RACADM クライアントからのみです。

例

```
racadm usercertupload -t 1 -f c:\cert\cert.txt -i 6
```

対応インタフェース

- ローカル RACADM
- リモート RACADM

---

usercertview

メモ: このコマンドを使うには、**DRAC 5 の設定** パーミッションが必要です。

表 A-55 に、**usercertview** サブコマンドを示します。

表 A-55. usercertview

サブコマンド	説明
usercertview	DRAC 上にあるユーザー証明書またはユーザー CA 証明書を表示します。

構文概要

```
racadm sslcertview -t <タイプ> [-A] -i <インデックス>
```

オプション

表 A-56 に、**sslccertview** サブコマンドオプションについて説明します。

表 A-56. sslcertview サブコマンドオプション

オプション	説明
-t	表示する証明書のタイプが ユーザー証明書かユーザー CA 証明書かを指定します。 1 = ユーザー証明書 2 = ユーザー CA 証明書
-A	ヘッダー / ラベルを印刷しません。
-i	ユーザーのインデックス番号。有効な値は 1 ～ 16 です。

対応インタフェース

- ローカル RACADM
- リモート RACADM
- Telnet/SSH/ シリアル RACADM

---

localConRedirDisable

メモ: このコマンドはローカル racadm ユーザーしか実行できません。

表 A-57 に、**localConRedirDisable**サブコマンドについて説明します。

表 A-57. localConRedirDisable

サブコマンド	説明
localConRedirDisable	管理ステーションへのコンソールリダイレクトを無効にします。

構文概要

```
racadm localConRedirDisable <オプション>
```

<*オプション*> を 1 に設定すると、コンソールリダイレクトが無効になります。

対応インタフェース

- ローカル RACADM

目次に戻る

目次に戻る

DRAC 5 プロパティデータベースの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 1.60 ユーザーズガイド

DRAC 5の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分類されています。本項には、プロパティデータベースでサポートされているグループとオブジェクトの ID のリストが掲載されています。

racadm ユーティリティでグループ ID とオブジェクト ID を使って DRAC 5 を設定します。次の各項で、それぞれの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か、書き込み可能か、またはその両方が可能であるかを示します。

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

表示可能文字には次の文字セットが含まれます。

```
abcdefghijklmnopqrstuvwxwz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

---

idRacInfo

このグループには、問い合わせを受けた DRAC 5 の詳細情報を提供する表示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できます。次の各項では、このグループの各オブジェクトについて説明します。

idRacProductInfo（読み取り専用）

有効値

最大 63 文字の 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）

有効値

最大 255 文字の 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 のタイプを説明するテキスト。

idRacVersionInfo（読み取り専用）

有効値

最大 63 文字の 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示す文字列。

idRacBuildInfo（読み取り専用）

有効値

最大 16 文字の 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示す文字列。

idRacName（読み取り専用）

有効値

最大 15 文字の 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

リモートアクセスコントローラの種類を DRAC 5 として識別します。

---

cfgLanNetworking

このグループには、DRAC 5 の NIC 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できます。このグループのすべてのオブジェクトでは DRAC 5 の NIC をリセットする必要があり、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 の IPアドレス設定を変更するオブジェクトによって、アクティブなユーザーセッションがすべて閉じられるため、ユーザーはアップデート後の IPアドレス設定を使って再び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 パーミッションが必要です。

有効値

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 DHCP サーバーから割り当て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 パーミッションが必要です。

有効値

最大 254 文字の ASCII 文字列。使用できる文字の種類は英数字、「-」、「.」です。

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）に設定されているときにのみ有効です。

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 パーミッションが必要です。

有効値

最大 63 文字の ASCII 文字列。

メモ: 一部の DNS サーバーは 31 文字以内の名前しか登録しません。

デフォルト

rac-*service tag*

説明

RAC 名 rac-*service tag* （デフォルト）を表示します。このパラメータは、**cfgDNSRegisterRac** が 1（TRUE） に設定されているときにのみ有効です。

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 パーミッションが必要です。

有効値

1（TRUE）

0（FALSE）

デフォルト

0

説明

DNS サーバー上に DRAC 5 名を登録します。

cfgTrapsSnmpFromDHCP（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 パーミッションが必要です。

有効値

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 パーミッションが必要です。

有効値

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: アドレスのスワップ中、**cfgDNSServer1** と **cfgDNSServer2** を同一値に設定することができます。

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 パーミッションが必要です。

有効値

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 の IP アドレスを取得します。このパラメータは、**cfgDNSServersFromDHCP** が 0（FALSE）に設定されているときにのみ有効です。

メモ: アドレスのスワップ中、**cfgDNSServer1** と **cfgDNSServer2** を同一値に設定することができます。

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** パーミッションが必要です。

有効値

1（TRUE）

0（FALSE）

デフォルト

0

説明

RAC の NIC（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なくなるので、RAC はシリアルまたはローカル RACADM インタフェースを通してしか利用できません。

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** パーミッションが必要です。このパラメータは、**cfgNicUseDhcp** パラメータが 0（FALSE）に設定されているときにのみ設定できます。

有効値

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** パーミッションが必要です。このパラメータは、**cfgNicUseDhcp** パラメータが 0（FALSE）に設定されているときにのみ設定できます。

有効値

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 IP アドレスの静的割り当てに使うサブネットマスク。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** パーミッションが必要です。このパラメータは、**cfgNicUseDhcp** パラメータが 0（FALSE）に設定されているときにのみ設定できます。

有効値

有効なゲートウェイ 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 IP アドレスの静的割り当てに使うゲートウェイ 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** パーミッションが必要です。

有効値

1（TRUE）

0（FALSE）

デフォルト

0

説明

RAC IP の割り当てに DHCP を使う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 IP アドレス、サブネットマスク、ゲートウェイはネットワーク上の 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、ゲートウェイは **cfgNicIpAddress**、**cfgNicNetmask**、**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にアップデートする場合は、**setniccfg** コマンドを使います。

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** パーミッションが必要です。

有効値

0（共有）

1（共有、フェールオーバー）

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）の現在の動作モードを指定します。表 B-1 に、サポートされているモードを示します。

表 B-1. cfgNicSelection でサポートされているモード

モード	説明
共有	ホストサーバーの組み込み NIC がホストサーバー上の RAC と共有されている場合に使用します。このモードでは、ネットワーク上でホストサーバーと RAC に共通にアクセスできるように、同じ IP アドレスを使用できます。
共有、フェールオーバー	ホストサーバー組み込み NIC 間でのチーム機能を有効にします。
専用	RAC NIC をリモートアクセス機能専用 NIC として使用するように指定します。

cfgNicMacAddress（読み取り専用）

有効値

RAC NIC MAC アドレスを表す文字列

デフォルト

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

説明

RACの NIC 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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

0～4094

デフォルト

0

説明

ネットワーク VLAN 設定用に 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** パーミッションが必要です。

有効値

0～7

デフォルト

0

説明

ネットワーク VLAN 設定用に VLAN の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

このグループでは、電子メール警告用の SMTP サーバーの設定やファームウェアアップデート用の TFTP サーバー IP アドレス設定を含む、各種リモートコンポーネントの設定が可能です。

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** パーミッションが必要です。

有効値

有効な SMTP サーバー 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。SMTP サーバーは、警告が設定されて有効になっていれば、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** パーミッションが必要です。

有効値

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 ファームウェアの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** パーミッションが必要です。

有効値

有効な TFTP サーバー 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に使うネットワーク TFTP サーバー 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** パーミッションが必要です。

有効値

文字列 最大 255 文字。

デフォルト

""

説明

TFTP サーバー上の RAC ファームウェアイメージファイルの TFTP パスを指定します。TFTP パスは、TFTP サーバー上の TFTP ルートパスの相対パスです。

メモ: それでもドライブを指定する必要があることがあります（例：**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経由での RAC へのアクセスが許可されているユーザーについての設定情報を提供します。

このユーザーグループの最大 16 のインスタンスが使用できます。各インスタンスは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** パーミッションが必要です。

有効値

2（ユーザー）

3（オペレータ）

4（Administrator: 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 チャネル上での最大権限。

cfgUserAdminIpmiSerialPrivilege（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** パーミッションが必要です。

有効値

2（ユーザー）

3（オペレータ）

4（Administrator: 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での最大権限。

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** パーミッションが必要です。

有効値

0x0000000～0x00001ff、0x0

デフォルト

0x0000000

説明

このプロパティでは、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、権限の組み合わせが可能なビットマスクとして表します。表 B-2 に使用可能なユーザー権限ビットマスクを示します。

表 B-2. ユーザー権限に応じたビットマスク

ユーザー権限	権限ビットマスク
DRAC 5 へのログイン	0x0000001
DRAC 5 の設定	0x0000002
ユーザーの設定	0x0000004
ログのクリア	0x0000008
サーバー制御コマンドの実行	0x0000010
コンソールリダイレクトへのアクセス	0x0000020
仮想メディアへのアクセス	0x0000040
テスト警告	0x0000080
デバッグコマンドの実行	0x0000100

例

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

表 B-3. ユーザー権限ビットマスクの例

ユーザー権限	権限ビットマスク
ユーザーは RAC にアクセスできません。	0x00000000
ユーザーは RAC にログインして RAC とサーバーの設定情報を表示することだけが許可されます。	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、仮想メディアにアクセスし、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** パーミッションが必要です。

有効値

文字列 最大 16 文字。

デフォルト

""

説明

このインデックスのユーザーの名前。インデックスが空の場合は、文字列をこの名前フィールドに書き込むと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、そのインデックスのユーザーが削除されます。この名前は変更できません。名前を削除してから再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）、「@」（アットマーク）、引用符を使用することはできません。

メモ: このプロパティ値はすべてのユーザーインスタンス間で一意でなければなりません。

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** パーミッションが必要です。

有効値

最大 20 文字の ASCII 文字列。

デフォルト

""

説明

このユーザーのパスワード。このユーザーパスワードは暗号化されるので、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** パーミッションが必要です。

有効値

1（TRUE）

0（FALSE）

デフォルト

0

説明

ユーザーを個別に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** パーミッションが必要です。

有効値

1（TRUE）

0（FALSE）

デフォルト

0

説明

シリアルオーバー LAN（SOL）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 電子メール警告機能を設定するためのパラメータが入っています。

次の各項では、このグループの各オブジェクトについて説明します。このグループは 4 つのインスタンスまで使用できます。

cfgEmailAlertIndex（読み取り専用）

有効値

1～4

デフォルト

このパラメータは既存のインスタンスに基づいて設定されます。

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）

有効値

1（TRUE）

0（FALSE）

デフォルト

0

説明

電子メール警告の送信先の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）

有効値

電子メールアドレス形式、最大 64 文字の ASCII 文字。

デフォルト

""

説明

警告元の電子メールアドレス。

cfgEmailAlertCustomMsg（読み取り専用）

有効値

文字列 最大 32 文字。

デフォルト

""

説明

警告と一緒に送信す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ています。

このグループでは 1 つのインスタンスが使用できます。次の各項では、このグループの各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** パーミッションが必要です。

有効値

1～2

デフォルト

2

説明

RAC で実行でき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** パーミッションが必要です。

有効値

10～1920

デフォルト

30

説明

リモート RACADM インタフェースの無動作タイムアウト待ち時間（秒）を指定します。リモート RACADM セッションが指定した時間以上非アクティブである場合、そのセッションは終了します。

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** パーミッションが必要です。

有効値

60～1920

デフォルト

300

説明

ウェブサーバーのタイムアウト時間を指定します。このプロパティでは、アイドル状態が何秒続くと、接続がタイムアウトになるかを指定します。このプロパティで設定した制限時間が過ぎると、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、現在のセッションには影響しません（新しい設定を有効にするには、ログアウトしてログインする必要があります）。

ウェブサーバーセッションが時間切れになると、現在のセッションからログアウトされます。

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** パーミッションが必要です。

有効値

0（タイムアウトなし）

60～1920

デフォルト

300

説明

セキュアシェルの無動作タイムアウト時間を指定します。このプロパティでは、アイドル状態が何秒続くと、接続がタイムアウトになるかを指定します。このプロパティで設定した制限時間が過ぎると、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、現在のセッションには影響しません（新しい設定を有効にするには、ログアウトしてログインする必要があります）。

セキュアシェルセッションが時間切れになった後<Enter> を押すと、次のエラーメッセージが表示されます。

警告：セッションは有効でなくなりました。タイムアウトになった可能性があります。

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** パーミッションが必要です。

有効値

0（タイムアウトなし）

60～1920

デフォルト

0

説明

Telnet の無動作タイムアウト時間を指定します。このプロパティでは、アイドル状態が何秒続くと、接続がタイムアウトになるかを指定します。このプロパティで設定した制限時間が過ぎると、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、現在のセッションには影響しません（新しい設定を有効にするには、ログアウトしてログインする必要があります）。

Telnet が時間切れになった後<Enter> キーを押すと、次のエラーメッセージが表示されます。

警告：セッションは有効でなくなりました。タイムアウトになった可能性があります。

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 シリアルポート用設定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できます。次の各項では、このグループの各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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

文字列

MaxLen = 2

デフォルト

^\ (<Ctrl><\>)

メモ: 「^」は <Ctrl> キーを示します。

説明

connect com2 コマンドを使用しているとき、にこのキーまたはキーの組み合わせによってテキストコンソールリダイレクトを終了できます。**cfgSerialConsoleQuitKey** の値は次のように表すことができます。

- ASCII 値 — 例:「^a」

  ASCII 値は、次のエスケープキーコードを使って表すことができます。

  (a) ^ と任意の英字（a-z, A-Z）

  (b) ^ と特殊文字 [ ] \ ^ _

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** パーミッションが必要です。

有効値

0 = タイムアウトなし

60～1920

デフォルト

300

説明

アイドル状態が続いたときに、セッションが切断されるまでの最大待ち時間を秒で指定します。

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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

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す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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

1（TRUE）

0（FALSE）

デフォルト

1

説明

DRAC 5 上でのセキュアシェル (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** パーミッションが必要です。

有効値

1（TRUE）

0（FALSE）

デフォルト

0

説明

RAC 上の 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** パーミッションが必要です。

デフォルト

1

有効値

1（TRUE）

0（FALSE）

説明

COM 2 ポートリダイレクト用のコンソールを有効または無効にします。

---

cfgNetTuning

このグループを使用して、RAC NIC ネットワークインタフェースの詳細パラメータを設定できます。新しい設定が有効になるまで、最大 1 分かかります。

注意： このグループのプロパティを変更する際は特別な注意が必要です。このグループのプロパティを不当に変更すると、RAC NIC が動作できなくなることがあります。

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** パーミッションが必要です。

有効値

1（有効）

0（無効）

デフォルト

1

説明

物理リンクの速度とデュプレックスのオートネゴシエーションを有効にします。有効にした場合、オートネゴシエーションは、**cfgNetTuningNic100MB** オブジェクトと **cfgNetTuningNicFullDuplex** オブジェクトで設定した値に優先されます。

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** パーミッションが必要です。

有効値

0（10 メガビット）

1（100 メガビット）

デフォルト

1

説明

RAC NIC に使用する速度を指定します。このプロパティは、**cfgNetTuningNicAutoNeg** が **1**（有効）に設定されている場合には使用できません。

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** パーミッションが必要です。

有効値

0（半二重）

1（全二重）

デフォルト

1

説明

RAC NIC のデュプレックス設定を指定します。このプロパティは、**cfgNetTuningNicAutoNeg** が **1**（有効）に設定されている場合には使用できません。

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** パーミッションが必要です。

有効値

576～1500

デフォルト

1500

説明

DRAC 5 NIC で使う最大送信単位のサイズ（バイト）

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** パーミッションが必要です。

有効値

6～384

デフォルト

6

説明

TCP 再送信ラウンドトリップタイムのスムーズラウンドトリップタイムベースのデフォルト値（1/2 秒単位）。（値は16 進数で入力します。）

---

cfgOobSnmp

このグループには、DRAC 5 の SNMP エージェントとトラップの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できます。次の各項では、このグループの各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** パーミッションが必要です。

有効値

文字列 最大 31 文字。

デフォルト

public

説明

SNMP トラップに使う 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** パーミッションが必要です。

有効値

1（TRUE）

0（FALSE）

デフォルト

0

説明

RAC で 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各種の RAC 設定プロパティの設定に使用します。

cfgRacTunePluginType

メモ: このプロパティを変更するには、**DRAC 5 の設定** パーミッションが必要です。

有効値

1（TRUE）— Java プラグイン

0（FALSE）— ネイティブプラグイン

デフォルト

0

説明

仮想 KVM（vKVM）プラグインタイプを設定します。

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** パーミッションが必要です。

有効値

10～65535

デフォルト

80

説明

RAC との HTTP ネットワーク通信に使う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** パーミッションが必要です。

有効値

10～65535

デフォルト

443

説明

RAC との HTTPS ネットワーク通信に使う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** パーミッションが必要です。

有効値

1（TRUE）

0（FALSE）

デフォルト

0

説明

RAC の IP アドレス範囲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** パーミッションが必要です。

有効値

IP アドレス形式の文字列。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（**cfgRacTuneIpRangeMask**）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

メモ: このプロパティを変更するには、**DRAC 5 の設定** パーミッションが必要です。

有効値

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

IP アドレス形式の文字列。例：255.255.255.0

cfgRacTuneIpBlkEnable

メモ: このプロパティを変更するには、**DRAC 5 の設定** パーミッションが必要です。

有効値

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。

cfgRacTuneIpBlkFailcount

メモ: このプロパティを変更するには、**DRAC 5 の設定** パーミッションが必要です。

有効値

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を拒否する前に、時間枠内で許可するログイン失敗の最大回数。

cfgRacTuneIpBlkFailWindow

メモ: このプロパティを変更するには、**DRAC 5 の設定** パーミッションが必要です。

有効値

2～65535

デフォルト

60

説明

ログイン失敗数を数える時間枠を秒で定義します。最後にログイン試行が失敗してからこの制限時間がたつと、失敗数カウントはゼロにリセットされます。

cfgRacTuneIpBlkPenaltyTime

メモ: このプロパティを変更するには、**DRAC 5 の設定** パーミッションが必要です。

有効値

2～65535

デフォルト

300

説明

ログイン失敗数が制限値を超えた 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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

1～65535

デフォルト

5901

説明

RAC のコンソールリダイレクト動作中、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: このオブジェクトをアクティブにする前に 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** パーミッションが必要です。

有効値

1～65535

デフォルト

5901

説明

RAC のコンソールリダイレクト動作中、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: このオブジェクトをアクティブにする前に 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** パーミッションが必要です。

有効値

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: このオブジェクトをアクティブにする前に 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** パーミッションが必要です。

有効値

0～60

デフォルト

0

説明

RAC 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** パーミッションが必要です。

有効値

-720～780

デフォルト

0

説明

RAC 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次に示します。

-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** パーミッションが必要です。

有効値

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。

cfgRacTuneLocalServerVideo（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** パーミッションが必要です。

有効値

1（有効）

0（無効）

デフォルト

1

説明

ローカルサービデオを有効（スイッチオン）または無効（スイッチオフ）にします。

cfgRacTuneLocalConfigDisable

メモ: このプロパティを変更するには、**DRAC 5 の設定** パーミッションが必要です。

有効値

1（TRUE）

0（FALSE）

デフォルト

0

説明

ローカルユーザーがローカル racadm または Dell OpenManage Server 管理ユーティリティを使って DRAC 5 を設定する機能を有効または無効にします。

cfgRacTuneCtrlEConfigDisable

メモ: このプロパティを変更するには、**DRAC 5 の設定** パーミッションが必要です。

有効値

1（TRUE）

0（FALSE）

デフォルト

0

説明

ローカルユーザーが BIOS POST オプション ROM から DRAC 5 を設定できる機能を無効にする機能を有効または無効にします。

cfgRacTuneVirtualConsoleAuthorizeMultipleSessions（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** パーミッションが必要です。このオブジェクトはリモートまたはファームウェア（SSH または Telnet）RACADM でのみ使用可能であり、ローカル RACADM または旧バージョンの DRAC 製品では使用できません。

有効値

0（最初のセッションのユーザーが、次のユーザーによるセッション共有要求に応答しない場合、次のユーザーにはデフォルトのタイムアウト値である 30 秒の後に、アクセス拒否エラーが与えられます。）

1（最初のセッションのユーザーが、次のユーザーによるセッション共有要求に応答しない場合、次のユーザーにはデフォルトのタイムアウト値である 30 秒の後に、アクセス拒否エラーが与えられます。）

2（最初のセッションのユーザーが、次のユーザーによるセッション共有要求に応答しない場合、次のユーザーにはデフォルトのタイムアウト値である 30 秒の後に、アクセス拒否エラーが与えられます。）

デフォルト

0

説明

最初のユーザーが仮想コンソールをすでに使用している場合、このオブジェクトの値は、30 秒のタイムアウト後に、次のユーザーの共有要求対して与えられる権限に影響します。

---

ifcRacManagedNodeOs

このグループには、管理下サーバーのオペレーティングシステムを記述するプロパティが格納されています。

このグループでは 1 つのインスタンスが使用できます。次の各項では、このグループの各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** パーミッションが必要です。

有効値

文字列 最大 255 文字。

デフォルト

""

説明

管理下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** パーミッションが必要です。

有効値

文字列 最大 255 文字。

デフォルト

""

説明

管理下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。

証明書署名要求の生成の詳細については、RACADM **sslcsrgen** サブコマンドを参照してください。

cfgRacSecCsrCommonName（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** パーミッションが必要です。

有効値

文字列 最大 254 文字。

デフォルト

""

説明

CSR 共通名（コモンネーム: CN）を指定します。

cfgRacSecCsrOrganizationName（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** パーミッションが必要です。

有効値

文字列 最大 254 文字。

デフォルト

""

説明

CSR 組織名（O）を指定します。

cfgRacSecCsrOrganizationUnit（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** パーミッションが必要です。

有効値

文字列 最大 254 文字。

デフォルト

""

説明

CSR 部門名（OU）を指定します。

cfgRacSecCsrLocalityName（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** パーミッションが必要です。

有効値

文字列 最大 254 文字。

デフォルト

""

説明

CSR 地域（L）を指定します。

cfgRacSecCsrStateName（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** パーミッションが必要です。

有効値

文字列 最大 254 文字。

デフォルト

""

説明

CSR 都道府県名（S）を指定します。

cfgRacSecCsrCountryCode（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** パーミッションが必要です。

有効値

文字列 最大 2 文字。

デフォルト

""

説明

CSR 国番号（CC）を指定します。

cfgRacSecCsrEmailAddr（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** パーミッションが必要です。

有効値

文字列 最大 254 文字。

デフォルト

""

説明

CSR の電子メールアドレスを指定します。

cfgRacSecCsrKeySize（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** パーミッションが必要です。

有効値

1024

2048

4096

デフォルト

1024

説明

CSR の SSL 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できます。次の各項では、このグループの各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 パーミッションが必要です。

有効値

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連結するために使用されます。デバイスを連結すると、サーバーはシステムに連結している有効な 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 USB CDROM/ フロッピードライブをシステムの USB ポートに連結する場合と同じです。デバイスを連結すると、DRAC5 の ウェブ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、デバイスは USB バスから切断されます。

メモ: 変更を有効にするには、システムを再起動する必要があります。

cfgVirAtapiSvrPort（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** パーミッションが必要です。

有効値

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。

cfgVirAtapiSvrPortSsl（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** パーミッションが必要です。

有効値

未使用のポート番号 0～65535（10 進数）。

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** パーミッションが必要です。

有効値

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。

cfgVirMediaPluginTypr（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** パーミッションが必要です。

有効値

1（Java プラグイン）

0（ネイティブプラグイン）

デフォルト

0

説明

仮想メディアのプラグインタイプを設定します。

cfgVirtualBootOnce（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** パーミッションが必要です。

有効値

0 — Disable：このオプションを無効にします。

1 — Virtual Flash/Virtual Media：仮想フラッシュまたは仮想メディアデバイスから起動します。

2 — Virtual Floppy：仮想フロッピーデバイスから起動します。

3 — Virtual CD/DVD/ISO：仮想 CD/DVD/ISO から起動します。

4 — PXE：PXE（ネットワーク）がサーバーを起動します。

5 — Hard drive：デフォルトのハードディスクから起動します。

6 — Utility Partition：ユーティリティパーティションに起動します。ユーティリティパーティションが存在する必要があります。

7 — Default CD/DVD：サーバーのデフォルト CD/DVD ドライブ。

8 — BIOS Setup：BIOS 設定画面。

9 — Primary Removable Media：ブータブルフロッピーとしてエミュレートされる USB リムーバブルメディアから起動します。

デフォルト

0

説明

ブートワンスデバイスを設定します。このプロパティが対応デバイスに設定されている場合にホストサーバーを再起動すると、選択したデバイスから起動を試みます（デバイスに適切なメディアが搭載されている場合）。

メモ: 仮想フラッシュデバイスのブートワンス機能を有効にするには、システムの再起動中に BIOS 設定に移動し、手動で起動順序を変更します。

メモ: 仮想仮想フラッシュ（1）、PXE（4）、および Disable（0）以外のブートワンスデバイスは、BIOS とベースボード管理コントローラ（BMC）のサポートされているバージョンを備えた一部のシステムでのみサポートされています。ご使用のシステムがブートワンスデバイスのすべてをサポートしているかどうかについては、デルのウェブサイト **www.dell.com** を参照してください。

メモ: 仮想仮想フロッピーと仮想 CD/DVD/ISOをサポートしていないシステムでは、「1」（仮想フラッシュ / 仮想メディア）を使用して 仮想フロッピーか、仮想CD/DVD/ISOまたは 仮想フラッシュにブートワンスを実行してください。この場合、BIOS 設定で、必要な仮想デバイスを最初の起動デバイスとして設定します。DRAC 5 では、システムがデバイスを再起動すると、自動的にこのデバイスが切断され、別の再起動がこのシステムに適用されます。

メモ: 仮想フロッピーと仮想I CD/DVD/ISOを別々のオプションとしてサポートしているシステムでは、ブートワンスの後、仮想メディアの接続は自動的に切断または分離されません。

cfgFloppyEmulation（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** パーミッションが必要です。

有効値

1（True）

0（False）

デフォルト

0

説明

0 に設定されている場合、仮想フロッピードライブは Windows 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して認識されます。Windows オペレーティングシステムは列挙中に C：以降のドライブ文字を割り当てます。1 に設定すると、仮想フロッピードライブは Windows オペレーティングシステムでフロッピードライブとして認識されます。Windows オペレーティングシステムは A：または B：のドライブ文字を割り当てます。

---

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** パーミッションが必要です。

有効値

空白文字を含まない印刷可能なテキスト文字列。最大 254 文字。

デフォルト

""

説明

DRAC が置かれている 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** パーミッションが必要です。

有効値

空白文字を含まない印刷可能なテキスト文字列。最大 254 文字。

デフォルト

""

説明

Active Directory フォレストに記録されている 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** パーミッションが必要です。

有効値

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。

cfgADSpecifyServerEnable（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** パーミッションが必要です。

有効値

1 または 0（TRUE または FALSE）

デフォルト

0

説明

1（True）を選択すると、LDAP または グローバルカタログサーバーを指定できます。0（False）を選択すると、これを指定できません。

cfgADDomainController（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** パーミッションが必要です。

有効値

有効な IP アドレスまたは完全修飾ドメイン名（FQDN）

デフォルト

デフォルト値なし

説明

DRAC 5 はここで指定した値を使って LDAP サーバーでユーザー名を探します。

cfgADGlobalCatalog（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** パーミッションが必要です。

有効値

有効な IP アドレスまたは FQDN

デフォルト

デフォルト値なし

説明

DRAC 5 はここで指定した値を使ってグローバルカタログサーバーでユーザー名を探します。

cfgAODomain（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** パーミッションが必要です。

有効値

有効な IP アドレスまたは FQDN

形式

<ドメイン>:<IP または FQDN>

デフォルト

デフォルト値なし

説明

DRAC 5 では、ここで指定した値からユーザー名の関連オブジェクトが検索されます。

cfgADSmartCardLogonEnable（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** パーミッションが必要です。

有効値

1（TRUE）

0（FALSE）

デフォルト

0

説明

DRAC 5 へのスマートカードによるログオンを有効または無効にします。

cfgADCRLEnable（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** パーミッションが必要です。

有効値

1（TRUE）

0（FALSE）

デフォルト

0

説明

Active Directory ベースのスマートカードユーザー用の証明書失効リスト（CRL）を有効または無効にします。

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** パーミッションが必要です。

有効値

15～300

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** パーミッションが必要です。

有効値

空白文字を含まない印刷可能なテキスト文字列。最大 254 文字。

デフォルト

""

説明

ドメインフォレストのルートドメイン。

cfgADType（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** パーミッションが必要です。

有効値

1 = Active Directory で拡張スキーマを有効にします。

2 = Active Directory で標準スキーマを有効にします。

デフォルト

1 = 拡張スキーマ

説明

Active Directory と併用するスキーマタイプを指定します。

cfgADSSOEnable（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** パーミッションが必要です。

有効値

1（TRUE）

0（FALSE）

デフォルト

0

説明

RAC で Active Directory のシングルサインオン認証を有効または無効にします。

---

cfgStandardSchema

このグループには標準スキーマ設定値を設定するためのパラメータが含まれています。

cfgSSADRoleGroupIndex（読み取り専用）

有効値

1～5 の整数。

説明

Active Directory で記録した役割グループのインデックス。

cfgSSADRoleGroupName（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** パーミッションが必要です。

有効値

空白文字を含まない印刷可能なテキスト文字列。最大 254 文字。

デフォルト

（空白）

説明

Active Directory フォレストで記録した役割グループの名前。

cfgSSADRoleGroupDomain（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** パーミッションが必要です。

有効値

空白文字を含まない印刷可能なテキスト文字列。最大 254 文字。

デフォルト

（空白）

説明

役割グループが置かれている Active Directory ドメイン。

cfgSSADRoleGroupPrivilege（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** パーミッションが必要です。

有効値

0x00000000～**0x000001ff**

デフォルト

（空白）

説明

表 B-4 のビットマスク番号を使用して、役割グループの役割ベースの権限を設定します。

表 B-4. ロール（役割）グループの権限のビットマスク

役割グループの権限	ビットマスク
DRAC 5 へのログイン	0x00000001
DRAC 5 の設定	0x00000002
ユーザーの設定	0x00000004
ログのクリア	0x00000008
サーバー制御コマンドの実行	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
テスト警告	0x00000080
デバッグコマンドの実行	0x00000100

---

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す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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

2（ユーザー）

3（オペレータ）

4（Administrator: システム管理者）

デフォルト

4

説明

IPMI シリアルチャネルで許可される最大権限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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

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エコー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** パーミッションが必要です。

有効値

0（なし）

1（CR-LF）

2（NULL）

3（<CR>）

4（<LF-CR>）

5（<LF>）

デフォルト

1

説明

IPMI シリアルインタフェースの改行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** パーミッションが必要です。

有効値

0（<ENTER>）

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改行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**パーミッションが必要です。

有効値

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**パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

2（ユーザー）

3（オペレータ）

4（Administrator: システム管理者）

デフォルト

4

説明

シリアルオーバー LAN アクセスに必要な最小限の権限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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

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** パーミッションが必要です。

有効値

0（FALSE）

1（TRUE）

デフォルト

1

説明

IPMI オーバー LAN インタフェース 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** パーミッションが必要です。

有効値

2（ユーザー）

3（オペレータ）

4（Administrator: システム管理者）

デフォルト

0

説明

IPMI オーバー LAN アクセスに許可される最大権限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** パーミッションが必要です。

有効値

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 / 無効の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: このプロパティを変更するには、**DRAC 5の設定** パーミッションとシステム管理者権限が必要です。

有効値

空白文字を含まない 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**パーミッションが必要です。

有効値

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イベントフィルタ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）

有効値

文字列 最大255文字。

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）

有効値

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。

cfgIpmiPefAction（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** パーミッションが必要です。

有効値

0（なし）

1（電源を切る）

2（リセット）

3（電源を入れ直す）

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する処置を指定します。

cfgIpmiPefEnable（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** パーミッションが必要です。

有効値

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。

---

cfgIpmiPet

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。

cfgIpmiPetIndex（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** パーミッションが必要です。

有効値

1～4

デフォルト

適切な索引値。

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** パーミッションが必要です。

有効値

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

ネットワーク上でのトラップレシーバの送信先 IP アドレスを指定します。トラップレシーバは、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** パーミッションが必要です。

有効値

0（FALSE）

1（TRUE）

デフォルト

1

説明

個々のトラップを有効または無効にします。

---

cfgLogging

このグループは OEM イベントログフィルタを有効または無効化するために使用されます。

cfgLoggingSELOEMEventFilterEnable（読み取り / 書き込み）

有効値

0（SEL ログフィルタが無効）

1（SEL ログフィルタが有効）

デフォルト

0

説明

SEL ログフィルタの有効化または無効化

目次に戻る

目次に戻る

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 1.60 ユーザーズガイド

以下の表に、RACADM のサブコマンドと、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示します。

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	✔	✘	✔
clearasrscreen	✔	✔	✔
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	✔	✔	✔
sslkeyupload	✘	✔	✔
sslresetcfg	✔	✔	✔
testemail	✔	✔	✔
testtrap	✔	✔	✔
vmdisconnect	✔	✔	✔
vmkey	✔	✔	✔

usercertupload	✗	✓	✓
usercertview	✓	✓	✓
localConRedirDisable	✗	✓	✗
✓ = サポートされている ✗ =サポートされていない			

目次に戻る

目次に戻る

DRAC 5 概要

Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

Dell Remote Access Controller 5(DRAC 5)は、Dell システム向けのリモート管理機能、クラッシュしたシステムのリカバリ、および電源制御機能を提供するシステム管理ハードウェアおよびソフトウェアソリューションです。

DRAC 5 を取り付けると、システムのベースボード管理コントローラ(BMC)と通信することで、電圧、温度、侵入、ファン速度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。また、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しているシステムのみ)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。

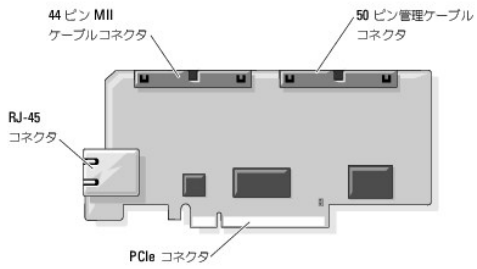
DRAC 5 には独自のマイクロプロセッサとメモリが搭載されており、電源は取り付け先のシステムから取り込みます。DRAC 5 はシステムに既に組み込まれている場合と、キットとして別途配布される場合があります。

DRAC 5 の使用を開始するには、DRAC 5 - はじめにを参照してください。

DRAC 5 仕様と機能

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



DRAC 5 仕様

電源仕様

表 1-1に DRAC 5 の電源要件を示します。

表 1-1. DRAC 5 の電源仕様

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

コネクタ

メモ: DRAC 5 ハードウェアの取り付け手順については、システムに付属の『 リモートアクセスカードの取り付け 』マニュアルまたは『取り付けと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、50 ピン管理ケーブル、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 ピン管理ケーブルは DRAC へのメインインタフェースで、USB、シリアル、ビデオ、内蔵回路(12C)バスに接続しています。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するために使用します。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 を接続するために使用します。

管理ケーブルと MII ケーブルを使用すると、必要に応じて DRAC を 3 通りのモードに設定できます。詳細については、DRAC 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。この情報は、ファイアウォールを開いて DRAC 5 にリモートアクセスするときに必要です。

表 1-2. DRAC 5 サーバー受信ポート

ポート番号	機能
22*	セキュアシェル(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 は接続機能のリストです。

表 1-4. 対応リモートアクセス接続

接続	機能
DRAC 5 NIC	• 10/100 Mbps イーサネット • DHCP のサポート • SNMP トラップと電子メールによるイベント通知 • 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 • 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	• 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シリアルコンソールおよび RACADM CLI コマンドに対応 • 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 の標準機能

DRAC は次の機能を提供しています。

- スマートカードログオンによる 2 要素認証。2 要素認証は、ユーザーが持つもの(スマートカード)とユーザーが知っているもの (PIN) に基づきます。
- Microsoft Active Directory(オプション)またはハードウェアに保存されているユーザー ID とパスワードによるユーザー認証。
- システム管理者が各ユーザーに特定の権限を設定できる役割ベースの権限。
- ウェブベースの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。
- 動的ドメイン名サービス (DNS) 登録。
- ウェブベースのインタフェース、シリアル、リモート RACADM または telnet 接続によるリモートシステム管理および監視機能。
- Active Directory 認証のサポート - 標準スキーマと拡張スキーマの使用によって DRAC 5 ユーザー ID とパスワードをすべて一元化。
- コンソールリダイレクト - リモートシステムキーボード、ビデオ、マウス機能の提供。
- 仮想メディア- 管理下システムから管理ステーション上のメディアドライブへのアクセスを提供。
- 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 ログ、オペレーティングシステム状態とは独立なシステムのクラッシュまたは無応答状態の最新クラッシュ画面へのアクセスを提供。
- Dell OpenManage ソフトウェアとの連携 - DRAC5 ウェブベースのインタフェースを Dell OpenManage Server Administrator または IT Assistant から起動可能。
- RAC 警告 - **専用、フェイルオーバー機能付き共有**、または **共有** NIC 設定を使って電子メールメッセージまたはSNMP トラップにより管理下ノードに関する問題を通知。
- ローカルおよびリモート設定 - RACADM コマンドラインユーティリティを使ってローカルおよびリモート設定が可能。
- リモート電源管理 - 管理コンソールからシャットダウンやリセットなどのリモート電源管理機能を提供。
- IPMI 対応。
- LAN と SM-CLP 上で IPMI を使用する規格ベースの管理。
- 消費電力を監視するセンサー。DRAC 5 はこのデータを使用してシステムの消費電力をグラフや統計で表します。
- セキュアソケットレイヤー (SSL) 暗号化 - ウェブベースのインタフェースを介したセキュアなリモートシステム管理を提供。
- 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無許可のアクセスを防止。
- 役割ベースの権限 - さまざまなシステム管理タスクの権限を割り当て。

その他の必要マニュアル

この『ユーザーズガイド』に加えて、次のマニュアルにもシステムの DRAC 5 のセットアップと操作に関する情報が記載されています。

- DRAC オンラインヘルプは、ウェブベースのインタフェースの使い方を説明しています。
- 『Dell OpenManage IT Assistant ユーザーズガイド』には、IT Assistant に関する情報が記載されています。
- 『Dell OpenManage Server Administrator ユーザーズガイド』には、Server Administrator のインストールと使用方法について記載されています。
- 『Dell OpenManage Server Administrator SNMP リファレンスガイド』では、Server Administrator SNMP の管理情報ベース(MIB)について説明しています。MIB は、標準の MIB を拡張してシステム管理エージェントの機能を指定する変数を定義します。
- 『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』 には、ベースボード管理コントローラ (BMC)の設定方法、BMC 管理ユーティリティを使った管理下システムの設定方法、BMC に関する追加情報が記載されています。
- 『Dell アップデートパッケージユーザーズガイド』では、システムアップデート戦略の一部として使用するDell アップデートパッケージの入手方法と使用法に関する情報を記載しています。
- 『Dell システムソフトウェアサポートマトリックス』では、各種の Dell システム、各システムでサポートされているオペレーティングシステム、各システムにインストールできる Dell OpenManage コンポーネントについて説明しています。
- デルサポートサイトに記載されている用語集は、本書で使用される用語に関する情報が説明されています。

次のシステムマニュアルにも、DRAC 5 がインストールされているシステムに関する詳細情報が記載されています。

- システムに同梱の「安全にお使いいただくために」には、安全および規制に関する重要な情報が記載されています。規制の詳細については、**www.dell.com / regulatory_compliance** にある法規制の順守のホームページを参照してください。保証情報は、このマニュアルに含まれている場合と、別の文書として付属する場合があります。
- システムをラックに取り付ける方法については、ラックに付属の『ラック取り付けガイド』に説明があります。
- 『はじめに』では、システムの機能、システムのセットアップ、および仕様の概要を説明しています。
- 『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、トラブルシューティングの方法、およびコンポーネントの取り付け方や交換方法について説明しています。
- システム管理ソフトウェアのマニュアルでは、システム管理ソフトウェアの機能、動作要件、インストール、および基本操作について説明しています。
- 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手順(必要な場合)や設定方法、および使い方について説明しています。
- 別途購入されたコンポーネントのマニュアルでは、これらのオプション装置の取り付けや設定について説明しています。
- システム、ソフトウェア、またはマニュアルの変更について記載されたアップデート情報がシステムに付属していることがあります。

  メモ: このアップデート情報には他の文書の内容を差し替える情報が含まれていることがあるので、必ず最初にお読みください。

- リリースノートや readme ファイルには、システムやマニュアルに加えられたアップデートの情報や、上級ユーザーや技術者のための高度な技術情報が記載されています。

目次に戻る

目次に戻る

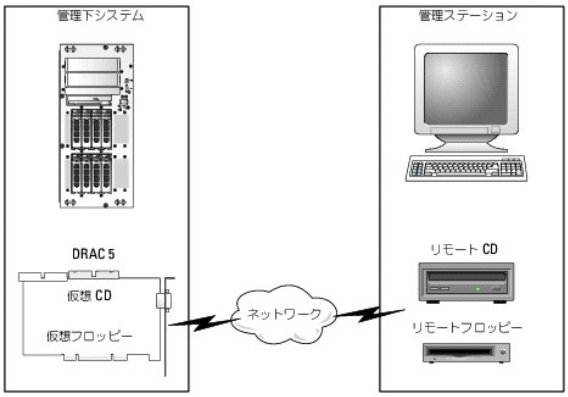
仮想メディアの使い方と設定

Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

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を使用できる仮想 CD ドライブを管理下システムに提供します。図 11-1 に、仮想メディアの全体的なアーキテクチャを示します。

図 11-1. 仮想メディアの全体的なアーキテクチャ



仮想メディアを使うと、リモートからの管理下システムの起動、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から新しいオペレーティングシステムのインストールまで、システム管理者はリモートの仮想 CD/DVD とディスケットドライブから実行することができます。

メモ: 仮想メディアは 128 Kbps 以上のネットワーク帯域幅を必要とします。

管理下システムには DRAC 5 カードが取り付けられています。DRAC 5 には仮想 CD とフロッピードライブが組み込まれており、これらは DRAC 5 ファームウェアで制御されます。これらの 2 つのデバイスは、仮想メディアが接続されているか切断されているかにかかわらず、常に管理下システムのオペレーティングシステムと BIOS にあります。

管理ステーションは、物理メディアまたはイメージファイルをネットワーク経由で提供します。RAC ブラウザを最初に起動して仮想メディアページにアクセスするとき、仮想メディアプラグインが DRAC 5 ウェブサーバーからダウンロードされ、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機能するためには、管理ステーションに仮想メディアプラグインがインストールされていることが必要です。

仮想メディアを接続すると、管理下システムからの仮想 CD/フロッピードライブへのアクセス要求はすべてネットワーク経由で管理ステーションへ送られます。仮想メディアの接続は、仮想デバイスにメディアを挿入する場合と全く同等です。仮想メディアが接続されていないときは、管理下システム上の仮想デバイスはドライブにメディアを取り付けることなく 2 台のドライブとして動作します。

メモ: 仮想メディアに接続するには、ブラウザのプラグインまたは Java プラグインを使用します。

表 11-1 に、仮想フロッピーと仮想光学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: 接続したままで仮想メディアを変更すると、システム起動手順が停止する場合があります。

表 11-1. 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光学ドライブ接続
レガシー 1.44 フロッピードライブ(1.44 フロッピーディスケット)	CD-ROM、DVD、CDRW、CD-ROM メディアとのコンボドライブ
USB フロッピードライブ(1.44 フロッピーディスケット)	CD-ROM イメージファイル(ISO9660 形式)
1.44 フロッピーイメージ	USB CD-ROM ドライブ(CD-ROM メディア)

仮想メディアブラウザのプラグインのインストール

仮想メディア機能を使用するには、管理ステーションに仮想メディアブラウザのプラグインがインストールされていることが必要です。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開くと、ブラウザが自動的にプラグインをダウンロードします（必要な場合）。プラグインが正常にインストールされると、仮想ドライブに接続しているフロッピーディスクと光ディスクのリストが仮想メディアページに表示されます。

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、対応バージョンの Internet Explorer と ActiveX Control 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** 以下に設定し、Internet Explorer が署名付き 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。

仮想メディア機能をインストールして使用するには、管理者権限も必要です。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を実行するには、表示されるセキュリティ警告に答えて ActiveX コントロールを許可します。

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システムで仮想メディア機能を実行するには、対応バージョンの Mozilla または Firefox をインストールします。仮想メディアプラグインがインストールされていないか、またはより新しいバージョンがあれば、インストール中に管理ステーションにこのプラグインをインストールしてよいか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がブラウザのディレクトリツリーに書き込む権限があることを確認してください。ユーザー ID が書き込み権限を持たない場合は、仮想メディアプラグインをインストールできません。

詳細については、デルサポートサイト **support.dell.com / manuals** にある『Dell システムソフトウェアサポートマトリックス』を参照してください。

仮想メディアの実行

△ **注意：仮想メディアセッションの実行 中は、racreset コマンドを使 用しないでください。データの喪 失を始め、望ましくない結 果が起きる可 能 性があります。**

仮想メディアを使用すると、フロッピーイメージやドライブを「仮想化」して、管理コンソールのフロッピーイメージ、フロッピードライブ、または光学ドライブをリモートシステム上で使用可能なドライブにすることができます。仮想メディアに接続するには、ブラウザのプラグインまたは Java プラグインを使用します。Java プラグインを使用している場合は、管理システムに Java Runtime Environment (JRE) 1.6 以降がインストールされていることを確認してください。

サポートされている仮想メディア設定

フロッピードライブと光学ドライブ 1 台ずつの仮想メディアを有効にできます。1 度に仮想化できるのは各メディアタイプにつきドライブ 1 台のみです。

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 つまたは空きフロッピードライブ 1 台があります。サポートされている光学ドライブには、最大 1 台の空き光学ドライブまたは 1 つの ISO イメージファイルがあります。

ウェブユーザーインタフェースを使った仮想メディアの実行

ネイティブプラグインを使 用した仮想メディアの接続

1. 管理ステーションで対応ウェブブラウザを開きます。対応ウェブブラウザのリストについては、デルサポートウェブサイト **support.dell.com / manuals** で『Dell システムソフトウェアサポートマトリックス』を参照してください。

   △ **注意：コンソールリダイレクトと 仮想メディア がサポートしているのは 32 ビットのウェブブラウザのみです。64 ビットのウェブブラウザを使 用すると、予 期しない結 果やエラーが生じることがあります。**

2. DRAC 5 に接続し、ログインします。詳細については、ウェブベース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 ページが開いて、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：フロップーイメージファイルは仮想フロッピーとして仮想化できるので、**フロッピードライブ** の下の **フロッピーイメージファイル** が表示されることがあります（該当する場合）。1 台の光学ドライブと 1 台のフロッピーを同時に選択するか、1 台のドライブだけを選択することができます。

   メモ：管理下システム上の仮想デバイスドライブ文字は、管理ステーション上の物理ドライブ文字とは一致しません。

4. 仮想メディアプラグインをインストールするように指示されたら、指示に従ってインストールしてください。

5. **属性** ボックスで、次の手順を実行します。

   a. **値** 列で、**接続 / 切断** 状態値が **接続** になっていることを確認します。

値が **切断** であれば、次の手順を実行します。

- **メディア** タブで、**設定** をクリックします。
- **値** 列で、**仮想メディアの接続** チェックボックスが選択されていることを確認します。
- **変更の適用** をクリックします。
- **仮想メディア** タブで、**仮想メディア** をクリックします。
- **値** 列で、**接続 / 切断** 状態値が **接続** になっていることを確認します。

メモ: 仮想メディアが接続されると、起動順序は RACADM を通してのみ変更可能となり、**設定** ページでは起動順序デバイスの設定変更はできなくなります。

b. **現在の状態** 値が **未接続** であ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は、再接続する前にイメージまたはドライブから切断する必要があります。この状態は、現在のウェブベースインタフェース上での仮想メディア接続の状態のみを示すものです。

c. **アクティブセッション** の値が **使用可能** であることを確認します。**値** フィールドに **使用中** と表示されている場合は、リモートアクセス の セッション管理 タブからアクティブな仮想メディア セッションを停止することで既存の仮想メディアセッションが解除または停止されるまで待つ必要があります。

1 度に 1 つの仮想メディアセッションのみ許可されます。このセッションは、ウェブベースインタフェースまたはVM-CLI ユーティリティ によって作成された可能性があります。

d. **暗号化を有効にする** チェックボックスを選択して、リモートシステムと管理ステーション間の暗号化接続を確立します（暗号化したい場合）。

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名を入力するか参照します。

フロッピーディスクまたは光学ドライブを仮想化する場合は、仮想化するドライブの隣にあるボタンを選択します。

7. **接続** をクリックします。

接続が認証されると、接続状態は **接続** になり、接続されている全ドライブのリストが表示されます。選択したすべての使用可能なフロッピーイメージとドライブが、管理下システムのコンソールから実際のドライブのように使用可能になります。

メモ: 割り当てられた仮想ドライブ文字（Microsoft Windows システム）またはデバイスの特別ファイル（Linux システム）は管理コンソールに表示されるドライブ文字と同じではない場合があります。

メモ: Internet Explorer の拡張セキュリティが設定されている Windows オペレーティングシステムクライアントでは、仮想メディアが正しく機能しないことがあります。この問題を解決するには、Microsoft オペレーティングシステムのマニュアルを参照するか、システム管理者にお問い合わせください。

仮想メディアの切断

仮想化されたイメージおよびドライブをすべて管理ステーションから切断するには **切断** をクリックします。**すべて**の仮想化イメージとドライブが管理下システムから切断され、使用できなくなります。

Java プラグインを使用した仮想メディアの接続

1. 管理ステーションで対応ウェブブラウザを開きます。対応ウェブブラウザのリストについては、デルサポートウェブサイト **support.dell.com / manuals** で『Dell システムソフトウェアサポートマトリックス』を参照してください。

2. DRAC 5 に接続し、ログインします。詳細については、ウェブベース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 ページが開いて、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: 仮想メディアに接続できるプラグインは、**設定** タブで選択したプラグインタイプにより異なります。

4. **属性** ボックスで、次の手順を実行します。

a. **値** 列で、**接続 / 切断** 状態値が **接続** になっていることを確認します。

値が **切断** であれば、次の手順を実行します。

- **メディア** タブで、**設定** をクリックします。
- **値** 列で、**仮想メディアの接続** チェックボックスの接続が選択されていることを確認します。
- **値** 列で、**Java プラグイン** を **プラグインタイプ** に選択します。
- **変更の適用** をクリックします。
- **仮想メディア** タブで、**仮想メディア** をクリックします。

メモ: JRE 1.6 以降が管理システムにインストールされていることを確認します。

b. **アクティブセッション** の値が **0** であることを確認します。**値** フィールドが **1** の場合は、**リモートアクセス** の **セッション管理** タブにアクセスして、既存の仮想メディアセッションが解除されるか、終了するまで待機します。1 度に 1 つの仮想メディアセッションのみ許可されます。このセッションは、ウェブベースインタフェースまたは VM-CLI ユーティリティ によって作

成された可能性があります。

5. **VM の起動** をクリックします。

   仮想メディア セッションのポップアップウィンドウが表示されます。ポップアップウィンドウに、仮想化できるドライバが表示されます。

6. デバイスが既に仮想化されている場合は、ドライバに関連付けられた **マップ** チェックボックスをオフにして切断します。

7. フロッピーイメージまたは ISO イメージを仮想化するには、**イメージの追加** をクリックしてイメージを選択します。

8. 接続するドライバまたはイメージに関連付けられた **マップ** チェックボックスをクリックします。

   ドライバまたはイメージが接続された管理下システムのデバイスが、**詳細**テーブルに表示されます。

仮想メディアの切断

ドライバまたはイメージに関連付けられた **マップ** チェックボックスをオフにします。

仮想メディア機能の接続と切断

DRAC 5 仮想メディア機能は USB テクノロジに基づくもので、USB プラグアンドプレイ機能を利用できます。DRAC 5 によって、仮想デバイスを USB バスに接続、切断するオプションが使用できるようになります。デバイスの接続が切断されているときは、オペレーティングシステムや BIOS は接続されているデバイスを認識できません。仮想デバイスが接続されると、デバイスが認識されます。デバイスが次回の起動時にしか有効 / 無効にできない DRAC 4 とは異なり、DRAC 5 では仮想デバイスは常に接続 / 切断できます。

仮想デバイスは、ウェブブラウザ、ローカル racadm、リモート racadm、telnet、またはシリアルポートを使って接続 / 切断できます。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** ページに移動して、設定を変更し、変更を適用します。**仮想メディアポート番号** と **仮想メディア SSL ポート番号** を指定することもできます。また、仮想フラッシュとブートワンス機能も有効または無効にできます。ブートワンス機能の情報ついては、cfgVirtualBootOnce(読み取り / 書き込み) を参照してください。このプロパティが対応デバイスに設定されている場合、ホストサーバーを再起動すると、選択したデバイスから起動を試みます(デバイスに適切なメディアが搭載されている場合)。

仮想メディアの自動接続

DRAC 5 ファームウェアのバージョン 1.30 以降では、仮想メディアの自動接続機能がサポートされています。この機能を有効にすると、DRAC 5 はサポートされているクライアント上でデバイスが仮想化(接続)されたときにのみ自動的に仮想デバイスをシステムに接続します。

仮想メディアのセッションが切断されると、DRAC 5 は仮想メディアデバイスの接続を解除します。

ウェブブラウザを使った仮想メディアの接続、自動接続、切断

仮想メディアで設定可能なステータスには、接続、自動接続、または切断があります。このステータスに基づいて、リモートシステムのデバイスが DRAC 5 GUI に表示されます。

- **接続** - リモートシステムのすべてのデバイスがサーバーに自動接続されます。サーバーに接続する場合は、リモートシステムで使用できるデバイスが DRAC 5 GUI に表示されます。
- **自動接続** - デバイスが仮想化されている場合にのみ、デバイスがサーバーに接続されます。たとえば、CD ドライブが付いたリモートマシンからサーバーに接続する場合は、CD を使って仮想化されている場合にのみ、CD ドライブが表示されます。そうでない場合、CD ドライブは DRAC 5 GUI に表示されません。
- **切断** - 仮想デバイスはサーバーに表示されません。

仮想メディア機能を接続するには、次の手順を行います。

1. **システム→ メディア→ 設定** の順にクリックします。
2. **仮想メディアの接続** の値を **接続** に変更します。
3. **変更の適用** をクリックします。

仮想メディア機能を切断するには、次の手順を行います。

1. **システム→ メディア→ 設定** の順にクリックします。
2. **仮想メディアの接続** の値を **切断** に変更します。
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接続、自動接続、切断

仮想メディア機能を接続するには、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 cfgVirMediaAttached 1
```

仮想メディア機能を切断するには、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 cfgVirMediaAttached 0
```

仮想メディア機能を自動接続するには、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 cfgVirMediaAttached 2
```

仮想メディアからの起動

RACADM対応するシステムのシステム BIOS 上では、仮想光学ドライブまたは仮想フロッピードライブからの起動が可能です。POST 中、BIOS セットアップウィンドウを開き、仮想ドライブが有効になっており、正しい順序で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:

1. 管理下システムを起動します。
2. <F2> キーを押して BIOS 設定ウィンドウを開きます。
3. 起動順序をスクロールして、<Enter> キーを押します。

   ポップアップウィンドウに、仮想光デバイス と仮想フロッピードライブのリストがその他の標準起動デバイスと共に表示されます。
4. 仮想ドライブが有効で、起動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てください。必要に応じて、画面の指示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、変更された起動順序にもとづいて、起動デバイスからの起動を試みます。仮想デバイスが接続されており、ブータブルメディアが存在する場合、システムはこの仮想デバイスから起動します。それ以外の場合は、ブータブルメディアのない物理デバイスの場合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

本項では、管理ステーションに手動でインタラクティブにオペレーティングシステムをインストールする方法について説明します。完了までに数時間かかる場合があります。仮想メディア を使用し、スクリプトでオペレーティングシステムをインストールする手順では 15 分以内で完了します。詳細については、VM-CLI を使ってオペレーティングシステムを展開する を参照してください。

1. 次の点を確認します。
   - 管理ステーションの CD ドライブにオペレーティングシステムのインストール CD が挿入されている。
   - ローカル CD ドライブが選択されている。
   - 仮想ドライブが接続されている。
2. 仮想メディアからの起動 の項にある仮想メディアからの起動手順に従って、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されていることを確認してください。
3. 画面の指示に従って、インストール作業を完了します。

サーバーのオペレーティングシステムが実行しているときの仮想メディアの使い方

Windows ベースシステム

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与えられます。

Windows での仮想ドライブの使い方は、物理ドライブの場合とほぼ同じです。管理ステーションでメディアに接続すると、そのメディアはドライブをクリックしてその内容を参照するだけでそのシステムでの使用が可能になります。

Linux ベースシステム

Linux システムでは、仮想メディアドライブにはドライブ文字は与えられません。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は自動マウントされません。ドライブが自動マウントされない場合は、手動でマウントしてください。

仮想フラッシュの使い方

DRAC 5 には持続的な仮想フラッシュ- DRAC 5 ファイルシステムに常駐し持続ストレージとしてシステムからアクセスできる 16 MB のフラッシュメモリ-があります。仮想フラッシュは有効にされると 3 つ目の仮想ドライブとして設定され、BIOS 起動順に表示されて、ユーザーは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には、仮想フラッシュイメージがブータブルイメージでなければなりません。

ホストシステムに外部クライアント接続または機能デバイスが必要な CD やフロッピードライブとは異なり、仮想フラッシュの実装には DRAC 5 の持続仮想フラッシュ機能しか必要ありません。ホスト環境では、16 MB のフラッシュメモリがフォーマット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際、次のガイドラインに従ってください。

- 仮想フラッシュの接続 / 切断によって USB が再列挙され、これによってすべての仮想メディアデバイスが接続 / 切断されます(CD ドライブ、フロッピードライブなど)。
- 仮想フラッシュを有効または無効にしても、仮想メディア CD / フロッピードライブの接続状態は変化しません。

注意: 接続 / 切断によって、アクティブな仮想メディアの読み取り / 書き込み操作が中断されます。

仮想フラッシュを有効にする

仮想フラッシュを有効にするには、コマンドプロンプトを開いて次のコマンドを入力し、Enter を押します。

```
racadm config -g cfgRacVirtual -o cfgVirMediaKeyEnable 1
```

仮想フラッシュを無効にする

仮想フラッシュを無効にするには、コマンドプロンプトを開いて次のコマンドを入力し、Enter を押します。

```
racadm config -gcfgRacVirtual -o cfgVirMediaKeyEnable 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** や**fdisk** といったシステムツールを使うことで USB のパーティションとフォーマットが可能です。

イメージを RAC ウェブブラウザから仮想フラッシュに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てください。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度有効にすると、システムと BIOS がその仮想フラッシュを認識するようになります。

起動仮想フラッシュの設定

1. フロッピードライブに起動ディスクを挿入するか、起動 CD を光学ドライブに挿入します。
2. システムを再起動して、選択したメディアドライブから起動します。
3. 仮想フラッシュにパーティションを追加して、パーティションの設定を有効にします。

   仮想フラッシュをハードディスクに列挙する場合は、**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は、仮想フラッシュはフロッピー列挙となるので、仮想フラッシュを起動ドライブとして設定するためのパーティションは不要です。
4. **format** コマンドを使ってドライブを **/s** スイッチ付きでフォーマットし、システムファイルを仮想フラッシュに転送します。

   たとえば、次のとおりです。

   ```
   format /s x
   ```

   ここで、x は仮想フラッシュに割り当てるドライブ文字です。
5. システムをシャットダウンして、起動フロッピーまたは CD をドライブから取り出します。
6. システムに電源を入れて、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い方

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、スクリプト可能コマンドラインインタフェースで管理ステーションからリモートシステムの DRAC 5 への仮想メディア機能を提供します。

VM-CLI は次の機能を持ちます。

- 複数アクティブセッションを同時にサポートする。

  メモ: 読み取り専用のイメージファイルを仮想化するとき、複数セッションで同じイメージメディアを共有できる。物理ドライブを仮想化すると、その物理ドライブには一度に 1 つのセッションしかアクセスできなくなる。

- 仮想メディアプラグインと互換性のあるリムーバブルデバイスまたはイメージファイル
- DRAC ファームウェアの Boot Once オプションが有効になっている場合の自動終了
- Secure Sockets Layer (SSL) 使用による DRAC 5 へのセキュア通信

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 に対する仮想メディアユーザー権限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管理者権限、オペレーティングシステム固有の権限、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、VM-CLI コマンドを実行するために管理者権限Iも必要です。

クライアントシステムの管理者は、ユーザーグループと権限を制御するので、このユーティリティを実行できるユーザーも制御することになります。

Windows システムでは、VM-CLI ユーティリティを実行するためにはパワーユーザー権限が必要です。

Linux システムでは、**sudo** コマンドを使うことで管理者権限なしで VM-CLI コマンドにアクセスできます。このコマンドは、一元管理下でシステム管理者以外にアクセス権を与え、すべてのユーザーコマンドをログに記録します。VM-CLI グループへのユーザーの追加や編集を行う場合、システム管理者は **visudo** コマンドを使用します。管理者権限を持たないユーザーは、**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）のプレフィックスとして追加することでリモートシステムの DRAC 5 へのアクセス権を取得し、このユーティリティを実行できます。

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 システム管理ソフトウェアキットに含まれている『Dell Systems Management Tools and Documentation DVD』に収録されています。ユーティリティをインストールするには、『Dell Systems Management Tools and Documentation DVD』をシステムの DVD ドライブに挿入して画面に表示される指示に従ってください。

『Dell Systems Management Tools and Documentation DVD』には、診断、ストレージ管理、リモートアクセスサービス、RACADM ユーティリティなど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。この DVD には、システム管理ソフトウェアに関する最新の製品情報を記載した Readme ファイルも入っています。

『Dell Systems Management Tools and Documentation DVD』にはまた、**vmdeploy**-VM-CLI と RACADM ユーティリティを使ってソフトウェアを複数のリモートシステムに導入する方法を示すサンプルスクリプト-も収録されています。詳細については、VM-CLI を使ってオペレーティングシステムを展開する 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 システムで全く同じです。このユーティリティのオプションは RACADM ユーティリティのオプションと同じです。たとえば、DRAC 5 IP アドレスを指定するオプションは RACADM と VM-CLI ユーティリティと同じ構文を使用します。

VM-CLI コマンド形式は次のとおりです。

```
racvmcli [パラメータ] [オペレーティングシステムのシェルオプション]
```

メモ: `racvmcli` コマンドを実行するには、**管理者** 権限が必要です。

コマンドラインの構文ではすべて、大文字と小文字の区別がなされます。詳細については、VM-CLI パラメータを参照してください。

リモートシステムがコマンドを受け入れて DRAC 5 が 接続を認証すると、次のいずれかが発生するまでコマンドは実行され続けます。

- 何らかの理由で VM-CLI 接続が切られる。
- オペレーティングシステムのコントロールを使用して処理を手動で中止した。たとえば、Windows ではタスク マネージャを使用して処理を中止できます。

VM-CLI パラメータ

DRAC 5 IP アドレス

`-r <RAC の IP アドレス>[:<RAC の SSL ポート>]`

ここで、*<RAC の IP アドレス>* は DRAC 5 Dynamic Domain Naming System（DDNS）名の有効な一意 IP アドレスです（サポートされている場合）。

このパラメータは DRAC 5 IP アドレスと SSL ポートを指定します。VM-CLI ユーティリティは、対象 DRAC 5 との仮想メディア接続を確立するためにこの情報を必要とします。無効な IP アドレスまたは DDNS 名を入力すると、エラーメッセージが表示されてコマンドが終了します。

<RAC の SSL ポート> を省略すると、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 ポートを変更しない限り、オプションの SSL ポートは不要です。

DRAC 5 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 ユーザー名を指定します。

<*DRAC ユーザー名*> は次の属性を持つものであることが必要です。

- 有効なユーザー名
- 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て、コマンドが終了します。

DRAC ユーザーパスワード

`-p <DRAC ユーザーパスワード>`

このパラメータは、特定の DRAC 5 ユーザーのパスワードを指定します。

DRAC 5 の認証に失敗すると、エラーメッセージが表示されてコマンドは終了します。

フロッピー / ディスクデバイスまたはイメージファイル

`-f {<デバイス名> | <イメージファイル>}`

ここで、<*デバイス名*> は有効なドライブ文字（Windows システム）（または Linux システムの場合には）、マウント可能ファイルシステムパーティション番号など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提供するデバイスまたはファイルを指定します。

たとえば、イメージファイルは次のように指定します。

`-f c:\temp\myfloppy.img`（Windows システム）

`-f /tmp/myfloppy.img`（Linux システム）

イメージファイルが書き込み保護されていない場合は、仮想メディアがそのファイルに書き込むことができます。上書きしてはならないフロッピーイメージファイルへの書き込みを禁止するように、オペレーティングシステムを設定してください。

たとえば、デバイスは次のように指定します。

`-f a:\`（Windows システム）

`-f /dev/sdb4 # デバイス上の 4 番目のパーティション /dev/sdb`（Linux システム）

デバイスに書き込み保護機能がある場合は、その機能を使用して、仮想メディアがメディアに書き込めないようにしてください。

なお、フロッピーメディアを仮想化しない場合はこのパラメータは指定しないでください。無効な値が検出されたら、エラーメッセージが表示されて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>}`

ここで、<*デバイス名*> は有効な CD/DVD ドライブ文字 (Windows システム) または有効な 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 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 CD/DVD-ROM メディアを提供するデバイスまたはファイルを指定します。

たとえば、イメージファイルは次のように指定します。

`-c c:\temp\mydvd.img`（Windows システム）

`-c /tmp/mydvd.img`（Linux システム）

たとえば、デバイスは次のように指定します。

`-c d:\`（Windows システム）

`-c /dev/cdrom`（Linux システム）

なお、CD/DVD メディアを仮想化しない場合はこのパラメータは指定しないでください。無効な値が検出されたら、エラーメッセージが表示されてコマンドが終了します。

スイッチオプションしかない場合を除いて、このコマンドで少なくとも 1 つメディアタイプ（フロッピーまたは CD/DVD ドライブ）を指定します。指定しないと、エラーメッセージが表示されてコマンドが終了します。

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。その他の非スイッチオプションが提供されていない場合、コマンドはエラーメッセージなしで終了します。

ヘルプの表示

-h

このパラメータは、VM-CLI ユーティリティパラメータの概要を示します。その他の非スイッチオプションが提供されていない場合、コマンドはエラーなしで終了します。

暗号化データ

-e

このパラメータがコマンドラインに含まれている場合は、VM-CLI ユーティリティは SSL暗号化チャネルを使って管理ステーションとリモートシステムの DRAC 5 間のデータの転送を行います。このパラメータがコマンドラインに含まれていない場合は、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シェルオプション

VM-CLI コマンドラインでは次のオペレーティングシステム機能が使用できます。

- stderr/stdout redirection - 印刷されたユーティリティの出力をファイルにリダイレクトします。

  たとえば、「より大」の不等号(>)にファイル名を続けると、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されます。

  メモ: VM-CLI ユーティリティは標準入力(**stdin**)からは読み込みません。したがって、**stdin** リダイレクトは不要です。

- バックグラウンドでの実行- デフォルトで VM-CLI ユーティリティはフォアグラウンドで実行されます。オペレーティングシステムのコマンドシェル機能を使用すると、ユーティリティをバックグラウンドで実行できます。たとえば、Linux オペレーティングシステムの場合、コマンドの直後にアンパーサンド(&)を指定すると、プログラムが新しいバックグラウンドプロセスとして起動します。

後者の手法は、VM-CLI コマンドに対して新しいプロセスが開始された後にスクリプトを処理できるのでスクリプトプログラムの場合に便利です(この手法を使わないと、スクリプトは VM-CLI プログラムが終了するまでブロックされます)。複数の VM-CLI インスタンスがこの方法で開始され、1 つまたは複数のコマンドインスタンスを手動で終了しなければならない場合、プロセスを一覧表示して終了するためのオペレーティングシステムによって異なる機能を使用します。

VM-CLI 戻りコード

0 = エラーなし

1 = 接続できない

2 = VM-CLI コマンドラインエラー

3 = RAC ファームウェア接続の切断

エラーが発生した場合は、標準エラー出力に英語のみのテキストメッセージも表示されます。

VM-CLI を使ってオペレーティングシステムを展開する

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、コマンドラインインタフェースで管理ステーションからリモートシステムの DRAC 5 への仮想メディア機能を提供します。VM-CLI とスクリプトの使用によって、オペレーティングシステムをネットワーク上の複数のリモートシステムに展開できます。

ここでは、VM-CLI ユーティリティを会社のネットワークに組み込む方法について説明します。

作業を開始する前に

VM-CLI ユーティリティを使う前に、対象となるリモートシステムと会社のネットワークが次の項に記載する要件を満たしている ことを確認してください。

リモートシステム要件

- 各リモートシステムにDRAC 5 カードが装備されている。
- 各リモートシステムの仮想デバイスは Bios 起動順序の最初のデバイスです。

Dell Custom Factory Integration(CFI)

Dell Custom Factory Integration(CFI)オプションを利用して Dell システムを注文すると、デルはそのシステムにDDNS 名、および仮想メディア用に有効化されている設定済みのシステム BIOS を含む DRAC 5 カードを事前に組み込むことができます。この設定を使うと、システムは会社のネットワークに接続次第、仮想メディアから 起動できます。

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

ネットワーク要件

次を含むネットワーク共有フォルダが必要です。

- オペレーティングシステムファイル
- 必要なドライバ
- オペレーティングシステムの起動イメージファイル

  イメージファイルは業界標準起動フォーマットのフロッピーイメージまたは CD/DVD ISO イメージである必要があります。

ブータブルイメージファイルの作成

イメージファイルをリモートシステムに導入する前に、サポートされているシステムがそのファイルから起動でき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 のウェブユーザーインタフェースを使って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。

次の項では、Linux と Windows システム用のイメージファイルの作成方法について説明します。

Linux システムのイメージファイルの作成

Data Duplicator ユーティリティを使って、Linux システム用の起動イメージファイルを作成します。

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いて次のように入力します。

```
dd if=<入力デバイス> of=<出力ファイル>
```

たとえば、次のとおりです。

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

Windows システムのイメージファイルの作成

Windows イメージファイル用のデータ複製ユーティリティを選択するときには、イメージファイルと CD/DVD のブートセクターをコピーするユーティリティを選んでください。

導入の準備

リモートシステムの設定

1. 管理ステーションからアクセスできるネットワーク共有フォルダを作成します。
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フォルダにコピーします。
3. オペレーティングシステムをリモートシステムに導入する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、この手順をスキップしてください。

   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、このファイルを作成します。オペレーティングシステムの展開手順に使用するプログラムとスクリプトをすべて含めます。

   たとえば、Microsoft Windows オペレーティングシステムを導入する場合、イメージファイルには Microsoft Systems Management Server（SMS）で使用される導入方法と同様のプログラムを含めることができます。

   イメージファイルを作成するとき、次を確認してください。

   - 標準的なネットワークベースのインストール手順に従う
   - 対象システムのそれぞれが同じ導入プロシージャを起動して実行するように、展開イメージを「読み取り専用」とマークする
4. 次のいずれかの手順を実行してください。

   - 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展開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展開アプリケーションに統合するとき、サンプル展開スクリプトをガイドとして使用してください。
   - 既存の **vmdeploy** スクリプトを使ってオペレーティングシステムを展開します。

オペレーティングシステムの展開

VM-CLI ユーティリティとそのユーティリティに含まれている **vmdeploy** スクリプトを使って、リモートシステムにオペレーティングシステムを展開します。

始める前に、VM-CLI ユーティリティに含まれているサンプル **vmdeploy** スクリプトを見直してください。このスクリプトは、ネットワーク上のリモートシステムにオペレーティングシステムを展開するための詳細な要件が含まれています。

次の手順は、対象となるリモートシステム上にオペレーティングシステムを展開する作業の高レベルな概要です。

1. 展開するリモートシステムを識別する。
2. 対象リモートシステムのDRAC 5 の名前と IP アドレスを記録する。
3. 各対象リモートシステムで次の手順を実行する。
    a. 対象システム用の次のパラメータを含む VM-CLI プロセスを設定する。
        - DRAC 5 IP アドレスまたは DDNS 名
        - 起動可能展開イメージファイル名
        - DRAC 5 ユーザー名
        - DRAC 5 ユーザーパスワード
    b. RACADM を使って、対象 DRAC 5 **boot once** オプションを設定します。
    c. RACADM を使って、DRAC 5 システムを再起動します。

よくあるお問い合わせ（FAQ）

時々、仮想メディアクライアントの接続が切れることがあります。どうしてでしょうか?

ネットワークのタイムアウトが起きた場合、DRAC 5 ファームウェアは接続を切るので、サーバーと仮想ドライブ間の接続が切れることになります。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。

どのオペレーティングシステムが DRAC 5 をサポートしますか?

サポートされているオペレーティングシステムの一覧は、デルサポートサイト **support.dell.com / manuals** で『Dell システムソフトウェアサポートマトリックス』を参照してください。

どのウェブブラウザが DRAC 5 をサポートしていますか?

サポートされているウェブブラウザの一覧は、デルサポートサイト **support.dell.com / manuals** で『Dell システムソフトウェアサポートマトリックス』を参照してください。

時々クライアントの接続が切れるのはなぜですか?

- ネットワークが低速であるか、クライアントシステムの CD ドライブ内の CD を交換した場合は、クライアントの接続が途切れることがあります。たとえば、クライアントシステムの CD ドライブ内の CD を交換した場合、新しい CD に自動起動機能が備わっていることがあります。この場合、クライアントシステムが CD の読み込み準備に時間がかかりすぎて、ファームウェアがタイムアウトになり、接続が途切れることがあります。接続が途切れた場合は、GUI から再接続して、その前の操作を続けることができます。
- ネットワークのタイムアウトが起きた場合、DRAC 5 ファームウェアは接続を切るので、サーバーと仮想ドライブ間の接続が切れることになります。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 と Service Pack 4 が正しくインストールされない場合どうしますか?

Virtual Media とWindows 2000 オペレーティングシステム CD を使って Windows 2000 と Service Pack 4 をインストールする場合は、インストール中に CD ドライブとの接続が一時とだえてオペレーティングシステムが正しくインストールされないことがあります。この問題を解決するには、Microsoft のサポートウェブサイト **support.microsoft.com** から **usbstor.sys** from the ファイルをダウンロードして、問題があるシステムでのみこのプログラムを実行してください。詳細については、Microsoft の技術情報記事 237853 を参照してください。

Windows 2000 をローカルにもリモートにもインストールできないのはなぜでしょうか?

この問題は通常、仮想フラッシュが有効になったが、有効なイメージを含まないとき、たとえば、仮想フラッシュに破損したかランダムなイメージが含まれるときに起こります。この場合には、Windows 2000 をローカルにもリモートにもインストールできません。この問題を解決するには、仮想フラッシュに有効なイメージをインストールするか、インストール手順で仮想フラッシュを使わない場合は仮想フラッシュを無効にしてください。

共有 NIC モードで設定した場合に仮想メディア接続が切れるのはどうしてでしょうか?

サーバー上にネットワークとチップセットドライバをインストールすると、共有 NIC モードで設定した場合に仮想メディア接続が切れることがあります。ネットワークやチップセットドライバをインストールすると、LOM がリセットし、ネットワークパケットがタイムアウトして仮想メディア接続がタイムアウトによって切れます。この問題を避けるには、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てください。仮想メディア接続が切れることによってドライバのインストールが影響を受けることを避けるには、ドライバのインストールを直接サーバーから行ってください。

Windows オペレーティングシステムのインストールに時間がかかりすぎるようです。どうしてでしょうか。

『Dell Systems Management Tools and Documentation DVD』を使用して Windows オペレーティングシステムをインストールするときにネットワーク接続が低速な場合は、ネットワークの遅延により DRAC 5 ウェブベースインタフェースへのアクセスに時間がかかることがあります。インストールウィンドウにインストールの進行状況が表示されませんが、インストールプロセスは進行しています。

フロッピードライブまたは USB メモリキーの内容を見ているのですが、同じドライブを使っ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て再試行を求められます。どうしてでしょうか。

仮想フロッピードライブへの同時アクセスはできません。ドライブの仮想化を試みる前にドライブの内容を表示するアプリケーションを閉じてください。

仮想デバイスを起動デバイスとして設定するにはどうしますか。

管理下システムで、BIOS セットアップにアクセスして起動メニューに移動してください。仮想 CD、仮想フロッピー、または仮想フラッシュを見つけて、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、その CD ドライブを起動順序の最初のドライブとして設定してください。

どのタイプのメディアから起動できますか。

DRAC 5 を使うと、次の起動メディアから起動できます。

- 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がリムーバブルディスクとして認識した USB キー
- USB キーイメージ

USB キーをブータブルにするには、どうしますか。

仮想フロッピーから起動できるには Windows 98 DOS を持つ USB キーのみです。独自の起動 USB キーを設定するには、Windows 98 起動ディスクから起動して、システムファイルを起動ディスクから USB キーにコピーしてください。たとえば、DOS プロンプトで次のコマンドを入力します。

```
sys a: x: /s
```

ここで、「x:」は起動可能にする USB キーです。

Dell 起動ユーティリティを使用して、ブータブル USB キーを作成することもできます。このユーティリティは Dell ブランドの USB キーとしか互換性がありません。ユーティリティをダウンロードするには、サポートされているウェブブラウザを開いて、デルサポートサイト **support.dell.com** に移動し、「R122672.exe」を検索します。

ActiveX プラグインをインストールするには管理者権限が必要ですか?

仮想メディアプラグインをインストールするには、Windows システムの管理者またはパワーユーザーの権限が必要です。

Red Hat Linux の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し使用するにはどの権限が必要ですか?

仮想メディアプラグインをインストールするためには、ブラウザのディレクトリツリーへの 書き込み 権限が必要です。

Red Hat Enterprise Linux または SUSE Linux オペレーティングシステムを実行しているシステムで仮想フロッピーデバイスを見つけることができません。仮想メディアが連結しているのに、リモートフロッピーに接続してしまいます。どうすればよいでしょうか。

一部の Linux バージョンは仮想フロッピードライブと仮想 CD ドライブを同じ方法で自動マウントしません。仮想フロッピードライブをマウントするために、Linux が仮想フロッピードライブに割り当てるデバイスノードを見つけてください。仮想フロッピードライブを見つけてマウントするには、次の手順を実行してください。

1. Linux コマンドプロンプトウィンドウを開き、次のコマンドを入力します。

   ```
   grep "Virtual Floppy" /var/log/messages
   ```

2. そのメッセージの最後のエントリを探し、その時刻を書きとめます。

3. Linux のプロンプトで次のコマンドを実行します。

   ```
   grep "hh:mm:ss" /var/log/messages
   ```
   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。

4. 手順3 で、grep コマンドの結果を読み込んで、「Dell Virtual Floppy」に与えられたデバイス名を検索します。

5. 仮想フロッピードライブに連結されて接続されていることを確認します。

6. Linux のプロンプトで次のコマンドを実行します。

   ```
   mount /dev/sdx /mnt/floppy
   ```

   ここで、

   /dev/sdx は手順 4 で見つけたデバイス名です。

   /mnt/floppy はマウントポイントです。

仮想フロッピードライブまたは仮想フラッシュでは、どのタイプのファイルシステムがサポートされていますか?

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のは FAT16 または FAT32 ファイルシステムです。

DRAC 5 のウェブベースインタフェースを使ってファームウェアをリモートにアップデートしたときにサーバー上にある私の仮想ドライブが削除されました。どうしてでしょうか。

ファームウェアのアップデートすると、DRAC 5 はリモート接続のリセット、切断、および仮想ドライブのマウント解除を行います。このドライブはDRAC リセットが完了したときに再度表示されます。

仮想フラッシュを有効または無効にするとき、仮想ドライブがすべて表示から消えてから再び表示されます。どうしてでしょうか。

仮想フラッシュの有効と無効を切り替えると USB のリセットが発生し、すべての仮想ドライブが USB バスから切断された後、再接続されます。

ファイルシステムが読み取り専用の管理ステーションにウェブブラウザをインストールするにはどうしますか?

Linux を実行しており、管理ステーションに読み取り専用のファイルシステムがある場合は、ブラウザを DRAC 5 への接続を必要とすることなくクライアントシステムにインストールできます。ネイティブのプラグインインストールパッケージを使用すると、クライアントのセットアップ段階でブラウザを手動でインストールできます。

△ **注意:** **読み取り専用のクライアント環境では、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と、インストールされている仮想メディア プラグインは動作しなくなります。これは、ファームウェアに新しいプラグインバージョンがある場合、古いプラグイン機能は使用できなくなるためです。この場合、プラグインをインストールするように求められます。ファイルシステムは読み取り専用であるため、インストールに失敗して、プラグインの機能は使用できなくなります。**

プラグインインストールパッケージを取得するには、次の手順を実行します。

1. 既存の DRAC 5 にログインします。
2. ブラウザのアドレスバーで URL を変更してください。

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

   →

   `https://<RAC_IP>/plugins/ # 最後のスラッシュ (/) を付け忘れないでください。`
3. 2 つのサブディレクトリ vm と vkvm を見つけてください。適切なサブディレクトリに移動して、rac5XXX.xpi ファイルを右クリックし、**リンクのターゲットに名前を付けて保存...** 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の保存場所を選択します。

プラグインインストールパッケージをインストールするには、次の手順を実行します。

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の共有フォルダにコピーします。
2. クライアントシステム上で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にプラグインインストールパッケージのファイルパスを入力します。たとえば、次のとおりです。

   `file:///tmp/rac5vm.xpi`
4. ブラウザに表示される指示に従ってプラグインをインストールします。

いったんインストールすると、対象となる DRAC 5 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る場合を除いて、再びプラグインのインストールが求められることはありません。

目次に戻る

目次に戻る

セキュリティ機能の設定

Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

DRAC 5 は次のセキュリティ機能を備えています。

- DRAC 管理者用の高度なセキュリティオプション
  - コンソールリダイレクトを無効にするオプションを使用すると、ローカルシステムユーザーは DRAC 5 コンソールリダイレクト機能によるコンソールリダイレクトを無効にできます。
  - ローカル設定を無効にする機能を使用すると、リモートDRAC 管理者は以下からの DRAC 5 の設定能力を無効にすることができます。
    - BIOS POST オプション ROM
    - ローカル RACADM および Dell OpenManage Server Administrator ユーティリティを使用するオペレーティングシステム
- 128 ビットSSL暗号化と40ビットSSL暗号化(128 ビットが許可されていない国)をサポートするRACADM CLIとウェブベースインタフェース操作

  メモ: Telnet は SSL 暗号化をサポートしていません。
- ウェブインタフェースまたはRACADM CLIを使用したセッションタイムアウトの設定(分単位)
- 設定可能な IP ポート(該当する場合)
- 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セキュアシェル(SSH)
- IP アドレスごとのログイン失敗数の制限により制限を超えたIPアドレスのログインを阻止
- DRAC 5 に接続するクライアントの IPアドレス範囲を限定

DRAC Administrator のセキュリティオプション

DRAC 5 ローカル設定を無効にする

システム管理者は、**リモートアクセス→ 設定→ サービス** を選択することで、DRAC 5 グラフィカルユーザーインタフェース(GUI)を通してのローカル設定を無効にできます。**オプション ROM を使用した DRAC のローカル設定を無効にする** チェックボックスを選択すると、リモートアクセス設定ユーティリティ-システム起動時に Ctrl+E を押してアクセス-は読み取り専用モードで作動し、ローカルユーザーがデバイスを設定できなくします。システム管理者が **RACADM を使用した DRAC のローカル設定を無効にする** チェックボックスを選択すると、ローカルユーザーは DRAC 5 の設定を読み取ることはできるが、racadm ユーティリティや Dell OpenManage Server Administrator を使って設定を変更できなくなります。

システム管理者はこれらのオプションのいずれか一方、または両方を同時に有効にできます。GUI を使用するほかに、ローカル racadm コマンドを使って有効にすることもできます。

システム再起動中のローカル設定の無効化

この機能は、システムの再起動中に管理下システムのユーザーが DRAC 5 を設定できなくします。

```
racadm config -g cfgRacTune -o

cfgRacTuneCtrlEConfigDisable 1
```

メモ: このオプションは、Remote Access Configuration Utility バージョン 1.13 以降でしかサポートされていません。このバージョンにアップグレードするには、『Dell Server Updates DVD』またはデルサポートサイト**support.dell.com**から BIOS アップデートパッケージを使用して BIOS をアップグレードしてください。

ローカル racadm からのローカル設定を無効にする

この機能は、管理下システムのユーザーがローカル racadm または Dell OpenManage Server 管理ユーティリティを使って DRAC 5 を設定する機能を無効にします。

```
racadm config -g cfgRacTune -o cfgRacTuneLocalConfigDisable 1
```

注意: これらの機能は、ローカルユーザーがローカルシステムから DRAC 5 を設定する能力(デフォルト設定に戻す能力も含む)を著しく制限します。これらの機能を慎重に使用し、一度に 1 つのインターフェイスのみを無効にして、ログイン権限を完全に失うことを避けることをお勧めします。

メモ: 詳細については、デルサポートサイト **support.dell.com / manuals** にあるホワイトペーパー「DRAC のローカル設定とリモート仮想 KVM を無効にする」を参照してください。

システム管理者はローカル racadm コマンドを使ってローカル設定オプションを設定できますが、セキュリティ上の理由で、リセットは帯域外の DRAC 5 GUI またはコマンドラインインターフェイスからのみできるようになっています。システムの電源投入時自己診断テストが完了し、オペレーティングシステムが起動したら、cfgRacTuneLocalConfigDisable オプションが適用されます。オペレーテ

ィングシステムとしては、ローカル RACADM コマンドを実行できる Microsoft Windows Server または Enterprise Linux オペレーティングシステム、あるいは Dell OpenManage Deployment Toolkit のローカル RACADM コマンド を実行するために限定的に使用される Microsoft Windows Preinstallation Environment や vmlinux などが挙げられます。

次のような場合には、システム管理者がローカル設定を無効にする必要があります。たとえば、サーバーやリモートアクセスデバイスの管理者が複数人いるデータセンターでは、サーバーのソフトウェアスタックの保守担当者はリモートアクセスデバイスへの管理者権限を必要としない場合があります。同様に、技術者はシステムの定期保守作業中、サーバーへの物理的なアクセス権限を持ち、この間、システムを再起動し、パスワード保護されている BIOS にもアクセスできますが、リモートアクセスデバイスの設定はできないようにする必要があります。このような状況では、リモートアクセスデバイスの管理者がローカル設定を無効にすることができます。

管理者は、ローカル設定を無効にすると、DRAC 5 をそのデフォルト設定に戻す能力を含めてローカル設定権限が著しく制限されるので、これらのオプションは必要なときのみ使用してください。普段は、一度に 1 つだけのインターフェイスを無効にし、ログイン権限を完全に失わないようにしてください。たとえば、管理者がローカル DRAC 5 ユーザー全員を無効にし、Microsoft Active Directory ディレクトリサービスユーザーだけが DRAC 5 にログインできるようにすると、Active Directory の認証インフラストラクチャに不具合が生じ、管理者自身がログインできなくなる可能性があります。同様に、管理者がすべてのローカル設定を無効にし、Dynamic Host Configuration Protocol(DHCP)サーバーを含むネットワークに静的 IP アドレスを使って DRAC 5 を置いた後、DHCP サーバーが DRAC 5 の IP アドレスをネットワーク上の別のデバイスに割り当てると、その競合によって DRAC の帯域外の接続が無効になり、管理者がシリアル接続を通してファームウェアをデフォルト設定に戻すことが必要になります。

DRAC 5 リモート仮想 KVM を無効にする

管理者は DRAC 5 リモート KVM を選択的に無効にすることで、コンソールリダイレクトを通して他のユーザーから見られることなくローカルユーザーがシステムを操作するための柔軟でセキュアなメカニズムを提供できます。この機能を使用するには、サーバーに DRAC 管理下ノードソフトウェアをインストールする必要があります。管理者は次のコマンドを使って、リモート vKVM を無効にできます。

```
racadm LocalConRedirDisable 1
```

LocalConRedirDisable コマンドは、引数 1 を使って実行すると既存のリモート vKVM セッションウィンドウを無効にします。

リモートユーザーがローカルユーザーの設定を上書きするのを防ぐために、このコマンドはローカル racadm でのみ使用可能です。管理者は、Microsoft Windows Server 2003 および SUSE Linux Enterprise Server 10 など、ローカル racadm 対応のオペレーティングシステムで使用できます。このコマンドはシステム再起動後も有効であるため、リモート vKVM を再度有効にするには、システム管理者がこのコマンドを無効にする必要があります。これには、次のように引数 0 を使用します。

```
racadm LocalConRedirDisable 0
```

次のように、DRAC 5 リモート vKVM を無効にする必要が生じる状態がいくつかあります。たとえば、管理者は自分が設定した BIOS 設定をリモート DRAC 5 ユーザーに見られたくない場合、LocalConRedirDisable コマンドを使ってシステム POST 中にリモート vKVM を無効にできます。また、システム管理者がシステムにログインするたびにリモート vKVM を自動的に無効にすることでセキュリティを強化できます。これには、ユーザーログオンスクリプトから LocalConRedirDisable コマンドを実行します。

メモ: 詳細については、デルサポートサイト **support.dell.com / manuals** にあるホワイトペーパー「DRAC のローカル設定とリモート仮想 KVM を無効にする」を参照してください。

ログオンスクリプトの詳細については、**technet2.microsoft.com / windowsserver / en / library / 31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx** を参照してください。

SSL とデジタル証明書を使って DRAC 5 通信をセキュリティ保護する

この項では、DRAC 5 に組み込まれている次のデータセキュリティ機能について説明します。

SSL(セキュアソケットレイヤー)

DRAC には、業界標準 SSL セキュリティプロトコルを使って暗号化されたデータをインターネット経由で転送するように設定されたウェブサーバーが含まれます。公開鍵と秘密鍵の暗号技術に基づく SSL は、クライアントとサーバー間に認証と暗号化を備えた通信を提供して、ネットワーク上の盗聴を防止するセキュリティ方式として広く受け入れられています。

SSL に対応したシステムの特徴。

- SSL 対応のクライアントに対して自己認証する
- クライアントがサーバーに対して認証できるようにする
- 両方のシステムが暗号化された接続を確立できる

この暗号処理は高度なデータ保護を提供します。DRAC は、インターネットブラウザで一般的に使用できる暗号化のうち、北米で使用されている暗号規格のうち最も安全な形式のである 128 ビット SSL 暗号規格を採用しています。

DRAC ウェブサーバーには、デルによって自己署名された SSL デジタル証明書(サーバー ID)があります。インターネット上での高度なセキュリティを確保するために、新しい証明書署名要求(CSR)を生成する要求を DRAC に送信することでウェブサーバー SSL 証明書を置き換えます。

証明書署名要求(CSR)

CSR は、認証局(CA)に対してセキュアサーバー証明書の発行を求めるデジタル要求です。セキュアサーバー証明書は、リモートシステムの身元を保護して、リモート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できないようにします。DRAC のセキュリティを確保するため、CSR を生成して CSR を 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。

CA は、信頼性の高いスクリーニング、身分証明、その他の重要なセキュリティ条件を満たすことが IT 業界で認められている事業体です。CA には、Thawte や VeriSign などがあります。CA は CSR を受け取ると、CSR に含まれている情報を確認します。応募者が CA のセキュリティ標準を満たしていると、CA はネットワークおよびインターネットを介したトランザクションに対して、応募者を一意に識別する証明書を発行します。

CA が CSR を承認して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されている CSR 情報が、証明書に含まれている情報と一致する必要があります。

SSL メインメニューへのアクセス

1. **システム** ツリーを拡張し、**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、**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 12-1を参照) を使って、CA に送る CSR を生成します。CSR の情報は、DRAC 5 のファームウェアに保存されます。表 12-2 に、**SSL メインメニュー** ページ上のボタンを示します。

表 12-1. SSL メインメニューオプション

フィールド	説明
新規証明書署名要求(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、ファームウェアにある以前の CSR を上書きします。CA が CSR を受け入れるためには、ファームウェアにある CSR が CA から返された証明書に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	会社が所有権を持ち、DRAC 5 へのアクセス制御に使用している既存の証明書をアップロードするには、**次へ** をクリックします。 △ **注意: DRAC 5 では、X509、Base 64 符号化証明書のみが受け入れられます。DER によって符号化された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して、 DRAC 5 に付属のデフォルト証明書を置き換えてください。**
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 12-2. SSL メインメニューボタン

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	次のページに移動します。

新しい証明書署名要求の生成

メモ: 新しい CSR は、ファームウェアにある古い CSR を上書きします。CA が CSR を受け入れるためには、ファームウェアにある CSR が CA から返された証明書に一致する必要があります。一致しないと、DRAC 5 は証明書をアップロードしません。

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 属性の値を入力します。

   表 12-3に、**証明書署名要求(CSR)の生成** ページのオプションを示します。
3. **生成** をクリックして、CSR を保存または表示します。
4. **証明書署名要求(CSR)の生成** ページで適切なボタンをクリックして続行します。表 12-4 に、**証明書署名要求(CSR)の生成** で使用できるボタンを示します。

表 12-3. 証明書署名要求(CSR)の生成 ページのオプション

フィールド	説明
共通名	証明する名前（通常は、**www.xyzcompany.com** のようなウェブサーバーのドメイン名）。英数字、ハイフン、下線、ピリオドのみが有効です。スペースは使用できません。
組織名	この組織に関連付けられた名前（たとえば「XYZ Corporation」）。英数字、ハイフン、アンダースコア、ピリオド、スペースのみが有効です。
組織単位	部門など組織単位に関連付けられた名前（たとえば「エンタープライズグループ」）。英数字、ハイフン、アンダースコア、ピリオド、スペースのみが有効です。
地域	証明する会社が所在する都市や地域（たとえば「神戸」）。英数字とスペースのみが有効です。アンダースコアやその他の文字で単語を区切らないでください。
都道府県名	証明書を申請している組織の所在地（たとえば「東京」）。英数字とスペースのみが有効です。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所在する国の名前。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。
E-メール	CSR に関連付けられている E-メールアドレス。会社の E-メールアドレスや、CSR に関連付けたいその他の E-メールアドレスを入力できます。このフィールドは省略可能です。

表 12-4. 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 ページが開きます。

2. **ファイルパス** フィールドの **値** フィールドに証明書のパスを入力するか、**参照** をクリックして証明書ファイルに移動します。

メモ: アップロードする証明書の相対ファイルパスが **ファイルパス** の値に表示されます。フルパスと正しい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。

メモ: サーバー証明書をアップロードできるのは 1 回限りです。既に 1 回アップロードしたサーバー証明書をアップロードしようとすると、「有効な証明書が見つかりません」というエラーメッセージが表示されます。

3. **適用** をクリックします。

4. 適切なボタンをクリックして続行します。

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 12-5 に、**証明書** ウィンドウに表示されるフィールドと説明を示します。

2. **サーバー証明書の表示** ページの適切なボタンを押して続行します。

表 12-5. 証明書情報

フィールド	説明
シリアル番号	証明書のシリアル番号
タイトル情報	対象者によって入力された証明書の属性
発行者情報	発行者によって返された証明書の属性
有効期間の開始	証明書の発行日
有効期間の終了	証明書の失効日

セキュアシェル（SSH）の使い方

一度に最大 4 つの SSH セッションのみがサポートされます。セッションタイムアウトはDRAC 5 プロパティデータベースのグループとオブジェクトの定義 で説明されているとおり、`cfgSsnMgtSshIdleTimeout` プロパティによって制御されます。次のコマンドを使って、DRAC 5 上の SSH を有効にできます。

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

次のコマンドを使って、SSH ポートを変更できます。

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort
<ポート番号>
```

cfgSerialSshEnable と cfgRacTuneSshPort プロパティの詳細ついては、DRAC 5 プロパティデータベースの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 SSH の実装では、表 12-6 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 12-6. 暗号化スキーム

スキーマの種類	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)
対称暗号	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
メッセージの整合性	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
認証	• パスワード

メモ: SSHv1 はサポートされていません。

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、ユーザーが **root** としてログインしているときにのみ有効にできます。

1. **システム** ツリーを展開し、**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、**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。
   - ローカル設定(表 12-7)
   - ウェブサーバー(表 12-8)
   - SSH(表 12-9)
   - Telnet(表 12-10)
   - リモート RACADM(表 12-11)
   - SNMP エージェント(表 12-12)
   - 自動システムリカバリエージェント(表 12-13)

   自動システムリカバリエージェント を使用して、DRAC 5 の **前回のクラッシュ画面** 機能を有効にします。

   メモ: DRAC 5 で 前回クラッシュ画面 が機能するためには、**Server Administrator** をインストールするときに 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直す に設定して 自動回復 機能をアクティブに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 12-14 を参照してください。

表 12-7. ローカル設定

設定	説明
オプション ROM を使って DRAC ローカル設定を無効にする	オプション ROM を使って DRAC 5 のローカル設定を無効にします。システム再起動中に <Ctrl+E> を押してセットアップモジュールを開始するようにプロンプトが表示されます。
RACADM を使って DRAC ローカル設定を無効にする	ローカル RACADM を使って DRAC 5 のローカル設定を無効にします。

表 12-8. ウェブサーバーの設定

設定	説明
有効	ウェブサーバー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数	システムの現在のセッション数(**最大セッション数** 以下)。
タイムアウト	接続がアイドル状態を持続できる秒数。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。タイムアウト時間の範囲は 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** 秒です。
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** 秒です。

表 12-9. 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数	システムの現在のセッション数(**最大セッション数** 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 秒です。
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 秒です。

表 12-10. 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数	システムの現在のセッション数(**最大セッション数** 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 秒です。
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 秒です。

表 12-11. 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数	システムの現在のセッション数(**最大セッション数** 以下)。

表 12-12. 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 12-13. 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 12-14. 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。

DRAC 5 の追加の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。

- 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。
- IP アドレスブロック - 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>
```

これらの機能はまた、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も使用できます。

以下の各項で、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 フィルタは受信ログインの IP アドレスを、次の **cfgRacTuning** プロパティで指定する IP アドレス範囲と比較します。

- cfgRacTuneIpRangeAddr
- 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、着信ログイン要求の DRAC 5 へのアクセスが許可されます。この範囲外の IP アドレスからのログイン要求にはエラーが返されます。

次の式の値がゼロに等しい場合は、ログインに進みます。

```
cfgRacTuneIpRangeMask & (<着信 IP アドレス> ^ cfgRacTuneIpRangeAddr)
```

& は数量のビットワイズ AND で ^ はビットワイズ XOR です。

cfgRacTuneプロパティの全リストは、DRAC 5 プロパティデータベースのグループとオブジェクトの定義 を参照してください。

表 12-15. IP アドレスフィルタ(IpRange)のプロパティ

プロパティ	説明
cfgRacTuneIpRangeEnable	IP アドレスのチェック機能を有効にします。
cfgRacTuneIpRangeAddr	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が決まります。 許可する IP アドレスの上位部分を決定するため、このプロパティは **cfgRacTuneIpRangeMask** とビット単位で AND されます。上位部分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。各プロパティのデフォルト値は、IP アドレス範囲 192.168.1.0～192.168.1.255 から DRAC 5 セッションが確立できるように設定されています。
cfgRacTuneIpRangeMask	IP アドレスの有意ビット位置を定義します。サブネットマスクは、上位ビットがすべて 1 で、下位ビットがすべてゼロであるネットマスク形式です。

IP フィルタを有効にする

以下に、IP フィルタ設定のコマンド例を示します。

RACADM と RACADM コマンドの詳細については、RACADM のリモート使用 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)、次のようにフル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
```

連続する 4 つの IP アドレスにログインを限定するには(たとえば、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。

- **cfgRacTuneIpRangeMask** は必ずネットマスク形式で設定します。最上位ビットがすべて 1 で(これがマスクのサブネットを定義)、下位ビットはすべてゼロにします。
- 必要な範囲の基底アドレスを **cfgRacTuneIpRangeAddr** 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がすべてゼロになります。

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ときを動的に決定し、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。

- 許可するログイン失敗回数
- これらの失敗を数える時間枠(秒)
- ログイン失敗回数が所定の合計数を超えた IP アドレスからのセッション確立を防止する時間(秒)

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計数されます。ユーザーがログインに成功すると、失敗履歴がクリアされて、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 クライアントに「SSH ID: リモートホストが接続を閉じました」というメッセージが表示される場合があります。

cfgRacTuneプロパティの全リストは、DRAC 5 プロパティデータベースのグループとオブジェクトの定義 を参照してください。

表 12-16 に、ユーザー定義のパラメータを示します。

表 12-16. ログイン再試行制限のプロパティ

プロパティ	定義
cfgRacTuneIpBlkEnable	IP ブロック機能を有効にします。 一定時間内に**(cfgRacTuneIpBlkFailCount)** 1 つの IP アドレスからの失敗が連続すると**(cfgRacTuneIpBlkFailWindow)**、以降そのアドレスからのセッション確立試行が一定の時間**(cfgRacTuneIpBlkPenaltyTime)**拒否されます。
cfgRacTuneIpBlkFailCount	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。
cfgRacTuneIpBlkFailWindow	失敗回数を数える時間枠を秒で指定します。失敗回数がこの制限値を超えると、カウンタはリセットされます。
crgRacTuneIpBlkPenaltyTime	失敗回数が制限値を超えた 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阻止します。

```
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
```

DRAC 5 の GUI を使ったネットワークセキュリティの設定

メモ: 以下の手順を行うには、**DRAC 5 の設定** 権限が必要です。

1. **システム** ツリーの **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、**ネットワーク** をクリックします。
3. **ネットワークの設定** 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から **変更の適用** をクリックします。

   表 12-17 に、**ネットワークセキュリティ** ページの設定を示します。
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。**ネットワークセキュリティ** ページのボタンについては、表 12-18 を参照してください。

表 12-17. 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指定します。
IP 範囲のサブネットマスク	IP アドレスの有意ビット位置を定義します。サブネットマスクは、上位ビットがすべて 1 で、下位ビットがすべてゼロであるネットマスク形式です。 例: **255.255.255.0**
IP ブロック有効	事前に選択した時間枠で、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、それを超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	ここで指定した時間枠(秒)内に IP ブロックエラーカウントが制限値を超えると、IP ブロックペナルティ時間がトリガされます。
IP ブロックのペナルティ時間	ログイン失敗回数が制限値を超えた IP アドレスからのセッションをすべて拒否する時間を秒で指定します。

表 12-18. 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** ページ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。

目次に戻る

目次に戻る

DRAC 5 SM-CLP コマンドラインインタフェースの使い方

Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

ここでは、DRAC 5 に組み込まれている Server Management 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 仕様に精通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、Distributed Management Task Force (DMTF) のウェブサイト **www.dmtf.org** 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。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 はバーブとターゲットの概念を起用して、CLI によるシステム管理機能を提供しています。バーブは実行する処理を示し、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)を指定します。

下記は SM-CLP コマンドライン構文の例です。

<バーブ> [<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 13-1 と表 13-2 に記載したバーブを使って操作を実行できます。

表 13-1. システムでサポートされている CLI バーブ

バーブ	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、バーブ、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。

表 13-2. ファン、バッテリ、イントルージョン、ハードウェアパフォーマンス、電源装置、温度、および電圧でサポートされている CLI バーブ

バーブ	定義
CD	シェルを使用して MAP を移動します。
help	特定のターゲットのヘルプを表示します。
show	ターゲットのプロパティ、バーブ、およびサブターゲットを表示します。
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 の使い方

1. 正しい資格情報を使用して SSH(または telnet)で DRAC 5 に接続します。
2. コマンドプロンプトで、smclp と入力します。

   SMCLP プロンプト(->)が表示されます。

SM-CLP の管理操作とターゲット

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。

- 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
- 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

オプション

表 13-3 に、サポートしている SM-CLP オプションを示します。

表 13-3. サポートされている SM-CLP オプション

SM-CLP オプション	説明
-all	実行可能な機能のすべてを実行するようにバーブに指示します。
-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	コマンドバーブのヘルプを表示します。
-version	コマンドバーブのバージョンを表示します。

ターゲット

表 13-4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 13-4. 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。
/system1/pwrmgtsvc1	システムの電力管理サービス。
/system1/pwrmgtsvc1/pwrmgtcap1	システムの電力管理サービスの機能。
/system1/fan1	管理下システムのファンターゲット。
/system1/fan1/tachsensor1	管理下システムのファンターゲット上の個々のセンサーターゲット。
/system1/batteries1	管理下システムのバッテリターゲット。
/system1/batteries1/sensor1	管理下システムのバッテリターゲット上の個々のセンサーターゲット。
/system1/intrusion1	管理下システムのシャーシイントルージョンターゲット。
/system1/intrusion1/sensor1	管理下システムのシャーシイントルージョンターゲット上の個々のセンサーターゲット。
/system1/hardwareperformance1	管理下システムのハードウェアパフォーマンスターゲット。
/system1/hardwareperformance1/sensor1	管理下システムのハードウェアパフォーマンスターゲット上の個々のセンサーターゲット。
/system1/powersupplies1	管理下システムの電源装置ターゲット。
/system1/powersupplies1/sensor1	管理下システムの電源装置スターゲット上の個々のセンサーターゲット。
/system1/temperatures1	管理下システムの温度ターゲット。
/system1/temperatures1/tempsensor1	管理下システムの温度ターゲット上の個々のセンサーターゲット。
/system1/voltages1	管理下システムの電圧ターゲット。

/system1/voltages1/voltsensor1	管理下システムの電圧ターゲット上の個々のセンサーターゲット。
/system1/chassis1	システムの個々のシャーシターゲット。

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。

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

サーバーの電源管理

表 13-5 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 13-5. 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) 2004-2008 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 管理

表 13-6 は、SM-CLP を使用して、管理下システムで SEL 関連の操作を実行する例を示しています。

表 13-6. SEL の管理操作

操作	構文
SEL の表示	->show /system1/logs1/log1 /system1/logs1/log1 Targets: Record1 Record2 Record3 Record4 Record5 Properties: InstanceID = IPMI:BMC1 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
SEL レコードの表示	->show /system1/logs1/log1/record4 /system1/logs1/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
SEL のクリア	->delete /system1/logs1/log1/record* All records deleted successfully

バッテリの管理

表 13-7 に、SM-CLP を使用してバッテリを操作する例を示します。

表 13-7. バッテリ管理操作

操作	構文
バッテリ状態の表示	->show system1/batteries1/sensor1 /system1/batteries1/sensor1: Properties: SystemCreationClassName = CIM_ComputerSystem SystemName = F196P1S CreationClassName = CIM_Sensor DeviceID = BATTERY 1 SensorType = 1 PossibleStates = {"Good" "Bad" "Unknown"} CurrentState = good ElementName = System Board CMOS Battery OtherSensorTypeDescription = CMOS battery sensor. EnabledState = 1 Verbs: CD exit help show version

MAP ターゲットのナビゲーション

表 13-8 は、**cd** バーブを使用して MAP をナビゲートする例を示しています。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 13-8. 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	`->cd system1`
	`->reset`
	
	メモ: 現在のデフォルトターゲットは / です。

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	`->cd system1`
	`->cd logs1/log1`
	`->show`

	`->cd system1/logs1/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 13-9 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派生したプロパティです。

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 13-9. 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一意に識別する ID。 MaxLen = 256
	ElementName	システムのユーザーフレンドリな名前。 MaxLen = 64
	NameFormat	IName 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 20=ゲートウェイ 21=ストレージバーチャライザ 22=メディアライブラリ 23=拡張ノード 24=NAS ヘッド 25=内蔵型 NAS 26=UPS 27=IP フォン 28=管理コントローラ 29=シャーシマネージャ
	ResetCapability	システムで使用可能なリセット方法を定義します。 値: 1=その他 2=不明 3=無効 4=有効 5=実装されていない
	CreationClassName	このインスタンスの派生元スーパークラス
	EnabledState	システムの有効 / 無効の状態を示します。 値: 0=不明 1=その他 2=有効 3=無効 4=シャットダウン 5=該当なし 6=有効であるがオフライン 7=テスト中 8=保留 9=無活動 10=起動中
	EnabledDefault	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。

		値: 2=有効 3=無効 4=該当なし 5=有効であるがオフライン 6=デフォルトなし
	RequestedState	システムに最後に要求された状態を示します。 値: 2=有効 3=無効 4=シャットダウン 5=変更なし 6=オフライン 7=テスト 8=保留 9=無活動 10=再起動 11=リセット 12=該当なし
	HealthState	システムの現在の正常性を示します。 値: 0=不明 5=正常 10=低下 / 警告 15=小さいエラー 20=大きいエラー 30=重大なエラー 35=回復不能なエラー
	OperationalStatus	システムの現在の状態を示します。 値: 0=不明 1=その他 2=正常 3=低下 4=過負荷 5=予測エラー 6=エラー 7=回復不能なエラー 8=起動中 9=止中 10=停止 11=サービス提供中 12=接続なし

		13=通信切断 14=中止 15=休止中 16=補助エンティティのエラー 17=完了 18=電源モード
	Description	システムの状態を説明するテキスト。

ファンのプロパティ名、温度、電圧数、消費電力、センサーのアンペア数

ファンでサポートされているプロパティ名、温度、電圧数、消費電力、センサーのアンペア数

表 13-10. センサー

オブジェクト	プロパティ	説明
CIM_NumericSensor	SystemCreationClassName	システム作成クラス名 - CIM_ComputerSystem)。
	SystemName	企業環境に存在するシステムを固有に識別するためのシステムサービスタグ。
	CreationClassName	作成クラス名 -CIM_NumericSensor。
	DeviceID	システム内のセンサーの固有の ID。 fan1...n(tachsensor 用) temp 1...n(tempsensor 用) numeric voltage 1...n(numericsensor 用(電圧)(PMBus システムのみ)) power consumption 1...n(消費電力用(PMBus システムのみ)) amperage 1...n (アンペア数用(PMBus システムのみ))
	BaseUnits	センサーの測定単位 RPM= タコメーター(tachsensor 用) C= 温度(tempsensor 用) V= 電圧(numericsensor 用) ワット=消費電力(powerconsumption 用) Amp= アンペア数 (amperage 用)
	CurrentReading	センサーの現在の読み取り値。
	LowerThresholdNonCritical	非重要しきい値下限。
	UpperThresholdNonCritical	非重要しきい値上限。
	LowerThresholdCriti cal	重要しきい値下限。
	UpperThresholdCriti cal	重要しきい値上限。
	SupportedThreshold	センサーでサポートされているしきい値。 { "LowerThresholdCritical" } (for tachsensor) {"LowerThresholdNonCritical", "UpperThresholdNonCritical", "UpperThresholdCritical", "LowerThresholdCritical" } (for tempsensor) {} (for voltsensor (numeric sensor)) {"UpperThresholdNonCritical", "UpperThresholdCritical"} (for powerconsumption {} for amperage)
	Set表Threshold	センサーに設定可能なしきい値レベル。 { } (しきい値設定用センサーのサポートなし)
	SensorTypes	センサーのタイプ: 5= タコメーター(tachsensor 用) 2= 温度(temperature 用) 3= 電圧(voltage 用) 1= 消費電力(powerconsumption 用) 1= アンペア数(amperage 用)
	PossibleStates	センサーの可能な状態。 { "unknown", "warning", "failed", "non-recoverable" }
	CurrentState	センサーが報告する現在の状態。
	ElementName	センサーの名前。
	OtherSensorTypeDescription	sensortype プロパティに「1」(その他)の値が含まれている場合は、このプロパティによってそのセンサーについての補足説明が表

		示されます。 "Power consumption sensor." for powerconsumption "Amperage sensor." for amperage
	EnabledState	センサーが有効か無効かを示します。 1= 有効

電源装置センサーのプロパティ名

表 13-11. サポートされている電源装置センサーのプロパティ名

オブジェクト	プロパティ	説明
CIM_NumericSensor	SystemCreationClassName	システム作成クラス名 - CIM_ComputerSystem)。
	SystemName	企業環境に存在するシステムを固有に識別するためのシステムサービスタグ。
	CreationClassName	作成クラス名 -CIM_PowerSupply。
	DeviceID	システム内のセンサーの固有の ID。 pwrsupply 1...n
	TotalOutputPower	DRAC ユーザーインタフェースに表示される総出力電力。
	ElementName	特定のセンサーの名前。
	OperationalStatus	電源装置の現在の作動状態。
	HealthState	電源装置の正常性状態。
	EnabledState	センサーが有効か無効かを示します。 1= 有効

イントルージョン、バッテリ、電圧、ハードウェアパフォーマンスの各センサーのプロパティ名

表 13-12. イントルージョン、バッテリ、電圧、ハードウェアパフォーマンスの各センサーでサポートされているプロパティ名 。

オブジェクト	プロパティ	説明
CIM_NumericSensor	SystemCreationClassName	システム作成クラス名 - CIM_ComputerSystem)。
	SystemName	企業環境に存在するシステムを固有に識別するためのシステムサービスタグ。
	CreationClassName	作成クラス名 - CIM_Sensor。
	DeviceID	システム内のセンサーの固有 ID。 Intrusion1...n(イントルージョンセンサー用) Battery1...n(バッテリセンサー用) Voltage1...n(電圧センサー用) Hardware performance sensor1...n(ハードウェアパフォーマンスセンサー用)
	SensorType	1=その他 3= 電圧(電圧センサー用)
	PossibleStates	センサーの可能な状態。 { "no intrusion", "chassis intrusion," "drive bay intrusion," "I/O card area intrusion," "processor area intrusion," "LAN disconnect," "unauthorized dock," "FAN area intrusion" } (イントルージョンセンサー用) { "absent," "low," "failed," "good" }(バッテリセンサー用) { "good," "bad," "unknown" } (電圧センサー用) { "Normal," "Others," "Thermal Protection," "Cooling Capacity changed," "Power Capacity changed," "User Configuration" }(ハードウェアパフォーマンスセンサー用)
	CurrentState	センサーが報告する現在の状態。
	ElementName	センサーの名前。
	OtherSensorTypeDescription	sensortype プロパティに「1」(その他)の値が含まれている場合は、このプロパティによってそのセンサーについての補足説明が表示されます。 "Chassis intrusion sensor"(イントルージョンセンサー用)

		"CMOS battery sensor"(バッテリセンサー用) "Hardware performance sensor"(ハードウェアパフォーマンス用)
	EnabledState	センサーが有効か無効かを示します。 1= 有効(全センサー用)

ファンおよび電源装置冗長性設定センサーのプロパティ名

表 13-13. ファンおよび電源装置の冗長性設定センサーでサポートされているプロパティ名

オブジェクト	プロパティ	説明
CIM_RedundancySet	InstanceID	インスタンス番号。
	RedundancyStatus	冗長性状態。
	TypeOfSet	3= 負荷分散(ファンの冗長性用) 4= 予備(電源装置の冗長性用)
	MinNumberNeeded	0=不明。
	ElementName	センサーの名前。

シャーシセンサーのプロパティ名

表 13-14. シャーシセンサーでサポートされているプロパティ名

オブジェクト	プロパティ	説明
CIM_Chassis	CreationClassName	作成クラス名 -CIM_Chassis
	PackageType	パッケージのタイプ 3= シャーシ
	ChassisPackageType	シャーシのパッケージタイプ 17= メインシステムシャーシ
	Manufacturer	メーカー 「Dell」
	Model	システムのモデル名
	ElementName	要素名

電源管理サービスのプロパティ名

表 13-15. 電源管理サービスでサポートされているプロパティ名

オブジェクト	プロパティ	説明
CIM_PowerManagementService	CreationClassName	作成クラス名 - CIM_PowerManagementService
	Name	IPMI 電源サービス
	ElementName	Dell サーバー電源管理サービス
	powerstate	システムの現在の電源状態。 2= オン 6= オフ 以下の値に設定可能です。 2= 電源オン 6= 電源オフ

		5= 電源リセット 9= システムのパワーサイクル

setバーブを使用すると、システムの電源状態を設定できます。たとえば、システムがオフの場合にオンにするには、次のように入力します。

```
set powerstate=2
```

電源機能のプロパティ名

表 13-16. 電源機能でサポートされているプロパティ名

オブジェクト	プロパティ	説明
CIM_PowerManagementCapabilities	InstanceID	電源機能の固有のインスタンス ID
	PowerChangeCapabilities	3= 電源状態の設定が可能
	ElementName	Dell サーバー電源管理サービス
	PowerStatesSupported	2= 電源オン 6= 電源オフ 5= 電源リセット 9= システムのパワーサイクル

目次に戻る

目次に戻る

監視と警告管理

Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

ここでは、DRAC 5 の監視方法と、システムと DRAC 5 が警告を受け取るように設定する手順を説明します。

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

DRAC 5 が前回クラッシュ画面を取り込めるようにするには、管理下システムの次の必須項目を設定する必要があります。

1. 管理下システムソフトウェアをインストールします。管理下システムソフトウェアのインストールについては、『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** でオフにしてから、対応する Microsoft Windows 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（デフォルトでは無効）。

   ローカル RACADM を有効にするには、コマンドプロンプトで次のコマンドを入力します。

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

4. 自動回復タイマーを有効にして、**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。

   自動リカバリ の設定手順の詳細については、『Server Administrator ユーザーズガイド』を参照してください。前回のクラッシュ画面をキャプチャできるように、**自動回復** タイマーを 60 秒以上に設定してください。デフォルト設定は 480 秒です。

   自動リカバリ 動作が **シャットダウン** または **電源の入れ直し** に設定されている場合は管理下システムの電源がオフになったときに前回のクラッシュ画面は使用できません。

Windows の自動再起動オプションを無効にする

DRAC 5 ウェブベースインタフェースの前回クラッシュ画面機能が正しく動作するようにするために、Microsoft Windows Server 2003 と Windows 2000 Server を実行している管理下システム上の **自動回復** 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 **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. **起動と回復** 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 **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. **起動と回復 ...** 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。

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では、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応答して、選択した処置を実行するように指定できます。これらの動作には、再起動、電源の入れ直し、電源オフ、電力の低減、警告のトリガ(プラットフォームイベントトラップ [PET] や E-メール)などがあります。

フィルタ可能なプラットフォームイベントには、以下のようなイベントがあります。

- ファンプローブエラー
- バッテリプローブ警告
- バッテリプローブエラー
- 離散的電圧プローブエラー
- 温度プローブ警告
- 温度プローブエラー
- シャーシイントルージョン検出
- 冗長性低下
- 冗長性喪失
- プロセッサ警告
- プロセッサエラー
- プロセッサ不在
- PS/VRM/D2D 警告
- PS/VRM/D2D エラー
- 電源装置の不在
- ハードウェアログエラー
- 自動システム回復
- システム電源プローブ警告
- システム電源プローブエラー

プラットフォームイベント(ファンプローブエラーなど)が発生すると、システムイベントが生成されて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ベースインタフェースのプラットフォームイベントフィルタリストにあるプラットフォームイベントフィルタ(PEF)と一致し、このフィルタが警告(PET または E-メール)を生成するように設定されていると、PET または E-メール警告が 1 つまたは複数の宛先に送信されます。

同じプラットフォームイベントフィルタで別の動作(システムの再起動など)を実行するように設定すると、その動作が行われます。

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または E-メール警告を設定する前に、プラットフォームの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った PEF の設定

1. 対応ウェブブラウザを使ってリモートシステムにログインします。ウェブベース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** タブをクリックして、**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** をクリックして、**プラットフォームイベント** を選択します。
   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選択します。
4. **プラットフォームイベントフィルタの設定** 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選択して **変更の適用** をクリックします。
5. **プラットフォームイベントフィルタリスト** で、設定するフィルタをクリックします。
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た後、**変更の適用** をクリックします。

メモ: 設定されている有効な宛先(PET または E-メール)に警告を送信するためには、**警告の生成** を有効にする必要があります。

RACADM CLI を使った PEF の設定

1. PEF を有効にします。

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

```
racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i 1 1
```

1 と 1 は、それぞれ PEF のインデックスと、有効 / 無効の選択です。

PEF インデックス値は 1〜17 です。有効 / 無効の選択は、1(有効)または 0(無効)です。

たとえば、PEF をインデックス 5 で有効にするには、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て <Enter> を押します。

   ```
   racadm config -g cfgIpmiPef -i <インデックス> -o cfgIpmiPefAction <アクション>
   ```

   <処置> の値ビットは次のとおりです。

   - <動作> ビット 0 の値 - 1 = 警告を有効にする、0 = 警告を無効にする
   - <動作> ビット 1 の値 - 1 = 電源をオフにする、0 = 電源をオフにしない
   - <動作> ビット 2 の値 - 1 = 再起動する、0 = 再起動しない
   - <動作> ビット 3 の値 - 1 = 電源の入れ直しをする、0 = 電源の入れ直しをしない
   - <動作> ビット 4 の値 - 1 = 電力を低減する、0 = 電力を低減しない

   たとえば、PEF で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 インデックス、2 は PEF 処置を再起動に設定します。

PET の設定

ウェブインタフェースを使用した PET の設定

1. ウェブブラウザを使ってリモートシステムにログインします。ウェブベースインタフェースへのアクセス を参照してください。
2. ウェブユーザーインタフェースを使った PEF の設定 の手順に必ず従ってください。
3. PET 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. **宛先の設定** 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 宛先の IP アドレスを設定します。
   a. **宛先番号** 列で、宛先番号をクリックします。
   b. **宛先を有効にする** チェックボックスが選択されていることを確認します。
   c. **宛先の IP アドレス** フィールドに有効な PET 宛先 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. **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(テストしたい場合)。

   メモ: この手順を実行するには、ユーザーアカウントが **テスト警告** 権限を持っていることが必要です。表 5-4 を参照してください。

   f. 手順a から手順 e までを繰り返して、すべての宛先番号を設定します。

RACADM CLI を使った 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いて次のコマンドを入力し、<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以下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、それぞれ PET の送信先インデックスと、有効 / 無効の選択です。

PET の送信先インデックスは 1～4 です。有効 / 無効の選択は、1(有効)または 0(無効)です。

たとえば、PET をインデックス 4 で有効にするには、次のコマンドを入力します。

```
racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 0
```

3. PET 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て <Enter> を押します。

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i 1 <IP アドレス>
   ```

   ここで、1 は PET の宛先インデックスで *<IP アドレス>* はプラットフォームイベント警告の宛先の IP アドレスです。

4. コミュニティ名の文字列を設定します。

   コマンドプロンプトで、次のコマンドを入力します。

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName <名前>
   ```

E-メール警告の設定

ウェブユーザーインタフェースを使用したE-メール警告の設定

1. ウェブブラウザを使ってリモートシステムにログインします。ウェブベースインタフェースへのアクセス を参照してください。
2. ウェブユーザーインタフェースを使った PEF の設定 の手順に従うようにしてください。
3. E-メール警告設定を指定します。
   a. **警告管理** タブで **E-メール警告設定** をクリックします。
   b. **SMTP(E-メール)サーバーアドレス設定** で、**SMTP(E-メール)サーバーの IP アドレス** 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. E-メール警告の宛先を指定します。
   a. **E-メール警告番号** 列で、E-メール警告番号をクリックします。
   b. **E-メール警告を有効にする** チェックボックスが選択されていることを確認します。
   c. **宛先の E-メールアドレス** フィールドに有効な E-メールアドレスを入力します。
   d. **E-メールの説明** フィールドに説明を入力します(必要な場合)。
   e. **変更の適用** をクリックします。
   f. **テスト E-メールの送信** をクリックして、設定した警告をテストします(テストしたい場合)。

   メモ: この手順を実行するには、ユーザーアカウントが **テスト警告** 権限を持っていることが必要です。表 5-4 を参照してください。

   g. 残る E-メール警告設定に対して ステップ a から ステップ e 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** をクリックして、**プラットフォームイベント** を選択します。
   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選択します。

RACADM CLI を使った E-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いて次のコマンドを入力し、<Enter> を押します。

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

2. E-メール警告を有効にします。

   コマンドプロンプトで以下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、それぞれ E-メール送信先のインデックスと、有効 / 無効の選択です。

   E-メールの送信先インデックスは 1 ～ 4 の値が可能です。有効 / 無効の選択は、1(有効)または 0(無効)です。

   たとえば、PET をインデックス 4 で有効にするには、次のコマンドを入力します。

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 4 1
   ```

3. E-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て <Enter> を押します。

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <E-メールアドレス>
   ```

   1 は E-メール送信先のインデックスで、*<E-メールアドレス>* はプラットフォームイベント警告の送信先の E-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に次の内容を入力し、<Enter> を押します。

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 <カスタムメッセージ>
   ```

   ここで、1 は E-メール宛先インデックスで *<カスタムメッセージ>* はカスタムメッセージです。

E-メール警告のテスト

RAC E-メール警告機能を使用すると、ユーザーは管理下システムで重大なイベントが発生したときに E-メール警告を受信できます。次の例は、RAC がネットワークで正しく E-メール警告を送信できるかどうかを確認するために、E-メール警告機能をテストする方法を示しています。

```
racadm testemail -i 2
```

メモ: E-メール警告機能のテストを行う前に、**SMTP** と **E-メール警告** 設定が指定されていることを確認してください。詳細については、E-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、管理下システム上で発生したシステムイベントのトラップを SNMP トラップリスナー設定で受信できます。

次の例で、ユーザーが RAC の トラップ警告機能をテストする例を示します。

```
racadm testtrap -i 2
```

RAC 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く設定されていることを確認してください。これらの設定の指定方法については、testtrapと testemail のサブコマンドの説明を参照してください。

よくあるお問い合わせ(FAQ)

どうして次のメッセージが表 示されるのでしょうか?

リモートアクセス : SNMP 認証エラー

検出作業の一部として、IT Assistant はデバイスの get と set コミュニティ名の確認を試みます。IT Assistant には、**コミュニティ名 = public** 取得と **コミュニティ名 = private** の設定があります。DRAC5 エージェントのコミュニティ名はデフォルトで public です。IT Assistant が set 要求を送信するとき **community = public** からの要求しか受け入れないので、DRAC 5 エージェントは SNMP 認証エラーを生成します。

DRAC 5 コミュニティ名は RACADM を使って変更できます。

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。

```
racadm getconfig -g cfgOobSnmp
```

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。

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <コミュニティ名>
```

SNMP 認証トラップの生成を防止するには、エージェントに受け入れられるコミュニティ名を入力する必要があります。DRAC 5 では 1 つしかコミュニティ名を許可しないので、同じ **get** と **set** コミュニティ名をIT Assistant の検出設定用に使用しなければなりません。

目次に戻る

目次に戻る

Intelligent Platform Management Interface（IPMI）の設定

Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

IPMI の設定

ここでは、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。インタフェースには次が含まれます。

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

DRAC 5 は完全に IPMI 2.0 対応です。次を使用して DRAC IPMI を設定できます。

- ブラウザ
- ipmitool などのオープンソースユーティリティ
- Dell OpenManage IPMI シェルの **ipmish**
- RACADM

IPMI シェルの ipmish を使用するための詳細については、デルサポートサイト **support.dell.com / manuals** にある『Dell OpenManage BMC ユーザーズガイド』を参照してください。

RACADM の使い方の詳細については、RACADM のリモート使用 を参照してください。

ウェブベースインタフェースを使った IPMI の設定

1. ウェブブラウザを使ってリモートシステムにログインします。ウェブベース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** ツリーの **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、**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 チャネル権限を更新します。

   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。詳細については、IPMI 2.0 規格を参照してください。

   IPMI LAN 設定 で **チャネル権限レベルの制限** ドロップダウンメニューをクリックし、**管理者**、**オペレータ**、または **ユーザー** 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。

   暗号鍵フィールド の **IPMI LAN 設定** に暗号鍵を入力して、**変更の適用** をクリックします。

   メモ: 暗号鍵は 40 文字までの偶数の 16 進数で指定します。

3. IPMI シリアルオーバー LAN（SOL）を設定します。
   a. **システム** ツリーの **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 の設定** 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 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 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。

   e. **ボーレート** ドロップダウンメニューで、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。
   f. **最低限必要な権限 を更新します**。このプロパティは、**シリアルオーバー LAN** 機能を使うために最低限必要な権限を定義します。

チャネル権限レベルの制限 ドロップダウンメニューで、**ユーザー**、**オペレータ**、または **管理者** 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. **シリアルの設定** 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 の **接続モードの設定** ドロップダウンメニューで適切なモードを選択します。

c. IPMI シリアル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て、適切なボーレートを選択し、**変更の適用** をクリックします。

d. チャネル権限レベルの制限を設定します。

チャネル権限レベルの制限 ドロップダウンメニューで **管理者**、**オペレータ**、または **ユーザー** 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 セットアップ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 中に F2 を押して BIOS セットアッププログラムを起動します。
- **シリアル通信** に移動します。
- **シリアル接続** 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 セットアッププログラムを終了します。
- システムを再起動します。

IPMI シリアルが端末モードの場合は、次の設定を追加できます。

- 削除制御
- エコー制御
- 行編集
- 改行シーケンス
- 改行シーケンスの入力

これらのプロパティの詳細については、IPMI 2.0 規格を参照してください。

RACADM CLI を使った IPMI の設定

1. RACADM インタフェースを使ってリモートシステムにログインします。RACADM のリモート使用 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いて次のコマンドを入力し、<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。詳細については、IPMI 2.0 規格を参照してください。

a. IPMI チャネル権限を更新します。

コマンドプロンプトで、次のコマンドを入力して <Enter> を押します。

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

<*レベル*> は次のいずれかです。

- 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 チャネル権限を 2(ユーザー) に設定するには、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。詳細については、IPMI 2.0 規格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て <Enter> を押します。

```
racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <キー>
```

ここで、<キー> は有効な 16 進形式の 20 文字から成る暗号鍵です。

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て <Enter> を押します。

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

a. IPMI SOL の最小権限レベルを更新します。

注意: IPMI SOL 最小権限レベルは、IPMI SOL をアクティブにするために最低限必要な権限を決定します。詳細については、IPMI 2.0 規格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て <Enter> を押します。

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <レベル>
```

<*レベル*> は次のいずれかです。

- 2(ユーザー)
- 3(オペレータ)
- 4(システム管理者)

たとえば、IPMI 権限を 2(ユーザー)に設定するには、次のコマンドを入力します。

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2
```

b. IPMI SOL 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 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て <Enter> を押します。

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <ボーレート>
```

<*ボーレート*> は 9600、19200、57600、115200 bps のいずれかを指定します。

たとえば、次のとおりです。

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600
```

c. SOL を有効にします。

メモ: SOL は個々のユーザーに対して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て <Enter> を押します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <ID> 2
```

<*ID*> はユーザーの一意な 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て <Enter> を押します。

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

b. IPMI シリアルボーレートを設定します。

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

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <ボーレート>
```

<*ボーレート*> は 9600、19200、57600、115200 bps のいずれかを指定します。

たとえば、次のとおりです。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate 57600
```

c. IPMI シリアル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て <Enter> を押します。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1
```

d. IPMI シリアルチャネルの最小権限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て <Enter> を押します。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <レベル>
```

<*レベル*> は次のいずれかです。

- 2(ユーザー)
- 3(オペレータ)
- 4(システム管理者)

たとえば、IPMI シリアルチャネル権限を 2(ユーザー)に設定するには、次のコマンドを入力します。

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit 2
```

e. BIOS セットアップ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 中に F2 を押して BIOS セットアッププログラムを起動します。
- **シリアル通信** に移動します。
- **シリアル接続** 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 セットアッププログラムを終了します。
- システムを再起動します。

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** コマンドを使って次の設定を追加できます。

- 削除制御
- エコー制御
- 行編集
- 改行シーケンス
- 改行シーケンスの入力

これらのプロパティの詳細については、IPMI 2.0 規格を参照してください。

IPMI リモートアクセスシリアルインタフェースの使い方

IPMI シリアルインタフェースでは、次のモードを使用できます。

- **IPMI ターミナルモード** - シリアル端末から送信された ASCII コマンドをサポートします。コマンドセット内のコマンド(電源制御を含む)の数は限られていますが、16 進数の ASCII 文字で入力された生の IPMI コマンドをサポートしています。
- **IPMI 基本モード** - プログラムへのアクセス用に、Baseboard Management Utility (BMU) に含まれている IPMI シェル(IPMISH)など、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、次の手順に従います。

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、次のコマンドを入力します。

   ```
   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>
   ```

詳細については、DRAC 5 プロパティデータベースのグループとオブジェクトの定義 を参照してください。

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 Baseboard Management Controller ユーザーズガイド』を参照してください。

1. **システム** ツリーを拡張し、**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、**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 設定を指定します。

   表 15-1 に、**シリアルオーバー LAN の設定** ページの設定を示します。
4. **変更の適用** をクリックします。
5. 必要なら、詳細設定を指定します。または、**シリアルオーバー LAN 設定** ページの該当するボタンをクリックして続行します(表 15-2 を参照)。

   詳細設定を指定するには:

   a. **詳細設定** をクリックします。

   b. **シリアルオーバー LAN の設定 詳細設定** ページで、必要な詳細設定を指定します。表 15-3 を参照してください。

   c. **変更の適用** をクリックします。

   d. 適切な **シリアルオーバー LAN の設定 詳細設定** ページのボタンをクリックして続行します。表 15-4 または **シリアルオーバー LAN の設定 詳細設定** ページのボタンの説明を参照してください。

表 15-1. シリアルオーバー LAN の設定 ページの設定

設定	説明
シリアルオーバー LAN を有効にする	シリアルオーバー LAN を有効にします。オン=有効、オフ=無効。
ボーレート	IPMI データ速度。**9600 bps**、**19.2 kbps**、**57.6 kbps**、または **115.2 kbps** を選択します。
チャネル権限レベルの制限	IPMI シリアルオーバー LAN の最低ユーザー権限として **管理者**、**オペレータ**、または **ユーザー** を選択します。

表 15-2. シリアルオーバー LAN の設定 ページのボタン

ボタン	説明
印刷	**シリアルオーバー LAN の設定** ページを印刷します。
更新	**シリアルオーバー LAN の設定** ページを更新します。
詳細設定	**シリアルオーバー LAN の設定 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 の設定** ページの設定を適用します。

表 15-3. シリアルオーバー LAN の設定 詳細設定 ページの設定

設定	説明
文字累積間隔	SOL 文字データパッケージの一部を送信する前に通常 BMC が待機する時間。1 ベース 5ms 増分。
文字送信しきい値	この文字数(以上)が受け入れられ次第、BMC は文字を含む SOL 文字データパッケージを送信します。1 ベースユニット。

表 15-4. シリアルオーバー LAN の設定 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 の設定 詳細設定** ページを印刷します。
更新	**シリアルオーバー LAN の設定 詳細設定** ページを更新します。
シリアルオーバー LAN の設定ページに戻る	**シリアルオーバー LAN の設定** ページに戻ります。
変更の適用	**シリアルオーバー LAN の設定 詳細設定** ページの設定を適用します。

目次に戻る

目次に戻る

管理下システムのリカバリ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 1.60 ユーザーズガイド

ここでは、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を DRAC 5 のウェブインタフェースを使って実行する方法を説明します。

リモートシステムのトラブルシューティングで最初に行うこと

次は、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、突然オフになりましたか?

システムがクラッシュした場合は、最後ののクラッシュ画面を確認し(前回システムクラッシュ画面の表示 を参照)、コンソールリダイレクト(管理下システムでサポートされている画面解像度とリフレッシュレート を参照)とリモート電源管理(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て、その過程を確認します。

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アクション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。

- 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。
- 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: 電源管理アクションを実行するには、**サーバーアクションコマンドの実行** 権限が必要です。

DRAC 5 GUI からの電源制御アクションの選択

1. 次のいずれかの **電源制御アクション** を選択します。
   - **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)。
   - **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)。
   - **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のと同じ)。この機能に使っても電源はオフになりません。
   - **システムの電源を入れ直す**- 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. 電源の管理アクションを実行するには、**適用** をクリックします(電源を入れ直す場合など)。
3. **電源管理** ページの適切なボタンをクリックして続行します(表 16-1を参照)。

表 16-1. 電源管理ページのボタン(右上)

ボタン	アクション
印刷	**電源管理** ページを印刷します。
更新	**電源管理** ページを再ロードします。

DRAC 5 の CLI からの電源制御アクションの選択

`racadm serveraction` サブコマンドを使用すると、ホストシステムの電源を管理できます。

`racadm serveraction <アクション>`

<アクション> の文字列のオプションは以下のとおりです。

- **powerdown** - 管理下システムの電源を切ります。
- **powerup** - 管理下システムの電源を入れます。
- **powercycle** - 管理下システムの電源を入れ直します。これは、システムのフロントパネルの電源ボタンを押してシステムの電源を切ってから入れ直す操作に似ています。
- **powerstatus** - サーバーの現在の電源状態を表示します(「オン」または「オフ」)。
- **hardreset** - 管理下システムのリセット(再起動)を行います。

システム情報の表示

システム概要 ページには、次のシステムコンポーネントに関する情報が表示されます。

- メインシステムシャーシ
- Remote Access Controller
- 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 16-2 と 表 16-3 に、システムシャーシのプロパティを示します。

メモ: **ホスト名** と **オペレーティングシステム名** 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 16-2. 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 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
オペレーティングシステム名	システムで稼動しているオペレーティングシステム

表 16-3. 自動リカバリのフィールド

フィールド	説明
回復アクション	「システムハング」が検知されたときに、アクションが不要か、ハードリセット、電源を切る、電源を入れ直すなどのアクション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 が回復アクション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)。

表 16-4. 埋め込み NIC MAC アドレス

フィールド	説明

NIC 1 Ethernet	NIC 1 Ethernet アドレス
NIC 2 Ethernet	NIC 2 Ethernet アドレス

Remote Access Controller

表 16-5 に、リモートアクセスコントローラのプロパティを示します。

表 16-5. 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	リモートアクセスコントローラのカード 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 16-6 に、ベースボード管理コントローラのプロパティを示します。

表 16-6. 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最大セッション数
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総数
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 が有効か無効か

システムイベントログ(SEL)の使い方

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** ツリーの **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 ページには、イベントの重大度と、表 16-7 に示すようなその他の情報が表示されます。
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 16-8 を参照)。

表 16-7. 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(通常)ステータスを示します。
	感嘆符の入った黄色の三角形は、警告(非重要)ステータスを示します。
	赤い X は、重要(エラー)ステータスを示します。

	疑問符のアイコンは、不明なステータスを示します。
日時	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 時間制 mm/dd/yyyy hh:mm:ss の形式です。
説明	イベントの短い説明。

表 16-8. SEL ページのボタン

ボタン	アクション
印刷	**ウィンドウでの表示順に 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、選択したディレクトリに **SEL** を保存できます。 **メモ:** Internet Explorer を使用しているときに保存中に問題が発生した場合、Microsoft サポートウェブサイト support.microsoft.com から Internet Explorer 用の累積セキュリティ更新プログラムをダウンロードしてください。
更新	**SEL** ページを再ロードします。

コマンドラインを使ってシステムログを表示する

```
racadm getsel -i
```

getsel -i コマンドは SEL 内のエントリ数を表示します。

```
racadm getsel <オプション>
```

メモ: 引数を何も指定しないと、ログ全体が表示されます。

メモ: 使用できるオプションの詳細については、getsel を参照してください。

clrsel コマンドは SEL から既存のレコードをすべて削除します。

```
racadm clrsel
```

POST およびオペレーティングシステム起動キャプチャログの使い方

DRAC 5 のこの機能を使用すると、BIOS POST の最後の 3 つのインスタンスとオペレーティングシステム起動のストップモーションビデオを再生できます。

POST とオペレーティングシステム起動キャプチャログを表示するには

1. **システム** ツリーの **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、**起動キャプチャ** タブをクリックします。
3. POST または オペレーティングシステムの起動キャプチャ ログのログ番号を選択します。

   新しい画面にログのビデオが再生されます。
4. ビデオを停止するには、**停止** をクリックします。

前回システム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。

前回のクラッシュ画面 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最新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、リモートアクセスできます。

前回のクラッシュ画面 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** ツリーの **システム** をクリックします。
2. **ログ** タブをクリックして、**前回のクラッシュ** をクリックします。

前回のクラッシュ画面 ページの右上に以下のボタンがあります(「表 16-9」を参照)。

表 16-9. 前回のクラッシュ画面ページのボタン

ボタン	アクション
印刷	**前回のクラッシュ画面** 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	**前回のクラッシュ画面** ページを削除します。
更新	**前回のクラッシュ画面** 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、**前回のクラッシュ画面** をキャプチャできないことがあります。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、**前回のクラッシュ画面** 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。

目次に戻る

目次に戻る

DRAC 5 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 1.60 ユーザーズガイド

ここでは、クラッシュした DRAC 5 の回復とトラブルシューティングに関連するタスクを実行する方法を説明します。

DRAC 5 のトラブルシューティングには、以下のいずれかのツールを使用できます。

- RAC ログ
- 診断コンソール
- トレースログ
- racdump
- coredump

RAC ログの使い方

RAC ログ は持続的なログで、DRAC 5 ファームウェアで管理されます。ログにはユーザーの操作（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 が発行した警告のリストが含まれています。ログが一杯になると、最も古いエントリから上書きされます。

DRAC 5 ユーザーインタフェース (UI) から RAC ログにアクセスするには、次の手順を行います。

1. **システム** ツリーの **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。

RAC ログ には、表 17-1 に示す情報が記録されています。

表 17-1. RAC ログページ情報

フィールド	説明
日付 / 時刻	日付と時刻（12月19日16:55:47 など）。 DRAC 5 を最初に起動したときにまだ管理下システムと通信できない間は、時刻にはシステムの起動 と表示されます。
ソース	イベントを引き起こしたインタフェース
説明	イベントの短い説明と DRAC 5 にログインしていたユーザー名

RAC ログページのボタンの使い方

RAC ログ ページには、表 17-2 に示すボタンがあります。

表 17-2. RAC ログのボタン

ボタン	動作
印刷	**RAC ログ** ページを印刷します。
ログのクリア	**RAC ログ** のエントリを消去します。 **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、選択したディレクトリに **RAC ログ** を保存できます。

	メモ: Internet Explorer を使用しているときに保存中に問題が発生した場合、Microsoft サポートウェブサイト support.microsoft.com から Internet Explorer 用の累積セキュリティ更新プログラムをダウンロードしてください。
更新	**RAC ログ** ページを再ロードします。

コマンドラインの使い方

RAC ログのエントリを表示するには、getraclog コマンドを使用します。

```
racadm getraclog -i
```

getraclog -i コマンドは DRAC 5 ログのエントリの数を表示します。

```
racadm getraclog [オプション]
```

メモ: 詳細については、getraclog を参照してください。

clrraclog コマンドを使用して、RAC ログからすべてのエントリをクリアします。

```
racadm clrraclog
```

診断コンソールの使い方

DRAC 5 には、Microsoft Windows や Linux ベースのシステムに含まれているものと似た、ネットワーク診断ツールが標準装備されています(表 17-3 を参照)。DRAC 5 ウェブベースのインタフェースを使うことで、これらのネットワーク診断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、次の手順を行います。

1. **システム** ツリーの **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 17-3 に、**診断コンソール** ページで使用できるオプションを示します。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 17-3. 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** オプションの右側のテキストフィールドにインタフェース番号をオプションで入力すると、インタフェースを通るトラフィック、バッファの使用率、その他のネットワークインタフェースに関する情報が印刷されます。
ping <IP アドレス>	現在のルーティングテーブルの内容を使って DRAC 5 から宛先 IP アドレスにアクセスできることを確認します。宛先 IP アドレスをこのオプションの右側のフィールドに入力してください。現在のルーティングテーブルの内容に基づいて、ICMP(インターネットコントロールメッセージプロトコル)エコーパケットが宛先 IP アドレスに送信されます。
gettracelog	DRAC 5 トレースログを表示します。詳細については、gettracelog を参照してください。

トレースログの使い方

DRAC 5 の内部トレースログは、システム管理者が DRAC 5 の警告およびネットワークに関する問題をデバッグするために使用します。

DRAC 5 ウェブベースユーザーインタフェースからトレースログにアクセスするには、次の手順を行います。

1. **システム** ツリーの **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。
3. **gettracelog** コマンドまたは **racadm gettracelog** コマンドを **コマンド** フィールドに入力します。

   メモ: このコマンドはコマンドラインインタフェースからも使用できます。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。

- DHCP - DHCP サーバーから送受信したパケットを追跡します。

- IP - 送受信した IP パケットを追跡します。

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。

---

racdump の使い方

racadm racdump コマンドは単一コマンドで、ダンプ、状態、DRAC 5 ボードの一般情報を取得します。

メモ: このコマンドは Telnet と SSH のインタフェースでのみ使用できます。詳細については、racdump コマンドを参照してください。

---

coredump の使い方

racadm coredump 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 情報はこれらの重要な問題の診断に使用できます。

使用可能な場合、coredump 情報は RAC の電源を切った後も、以下のどちらかの状態が発生するまで保持されます。

- **coredumpdelete** サブコマンドを使用して coredump 情報がクリアされた。
- RAC で別の重要な問題が発生した。この場合、coredump の内容は最後に発生した重大エラーに関するものとなります。

racadm coredumpdelete コマンドを使用すると、現在 RAC に保存されている **coredump** データを消去できます。

詳細については、coredump および coredumpdelete を参照してください。

目次に戻る

目次に戻る

センサー

Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

ハードウェアセンサーまたはプローブを使用すると、不安定なシステムや損傷などの障害に対して適切な処置を講じることができるため、ネットワーク上のシステムをさらに効率的に監視できます。

DRAC 5 を使用して、ハードウェアセンサーのバッテリ、ファンプローブ、シャーシイントルージョン、電源装置、消費電力、温度、電圧を監視できます。

バッテリプローブ

バッテリプローブは、システム基板 CMOS とストレージ ROMB（RAM on Motherboard）のバッテリに関する情報を提供します。

メモ: ストレージ ROMB のバッテリ設定は、システムに ROMB がある場合にのみ表示されます。

ファンプローブ

ファンプローブセンサーは次の関する情報を提供します。

- ファンの冗長性 - プライマリファンが事前に設定された速度で熱を放散しなくなると、セカンダリファンが取って代わる機能。
- ファンプローブリスト - システムのすべてのファンの速度についての情報を提供します。

シャーシイントルージョンプローブ

シャーシイントルージョンプローブは、シャーシが開いているか閉じているかというシャーシの状態を表示します。

電源装置プローブ

電源装置プローブは次に関する情報を提供します。

- 電源装置の状態（正常なしきい値内にあるか、しきい値を超えたか）。

  メモ: しきい値は Dell OpenManage Server Administrator からのみ設定可能です。詳細については、『Dell OpenManage Server Administrator ユーザーズガイド』を参照してください。

- 電源装置の冗長性（プライマリ電源が故障した場合に冗長電源が取って代わる機能）。

  メモ: システムに電源装置が1個しかない場合、電源の冗長性セクションは表示されません。

ハードウェアパフォーマンスプローブ

ハードウェアパフォーマンスセンサーは、CPU のパフォーマンス状態（低下しているか正常か）を表示します。ハードウェアパフォーマンスセンサーの状態は、CPU がスロットル状態のときに低下します。

電力監視プローブ

電力監視プローブは、リアルタイムの消費電力に関する情報をワットとアンペア単位で表示します。この情報は、ベースボード管理コントローラ（BMC）ファームウェアセンサーからDRAC 5 に提供されます。

メモ: この機能は一部の Dell PowerEdge *x*9*xx* システムと *xx*0*x* システムでのみサポートされています。

DRAC 5 は高度な電源管理機能を提供しています。次の機能が含まれます。

- 一定期間にわたるシステムの電力レベル（W）と電力供給（A）のグラフ表示。
- DRAC の現在時刻から遡って過去 1 週間、1 日、1 時間のシステム電力消費量の最大、最小、平均を W（ワット）と BTU/Hr（1 時間あたりのイギリス熱単位）で示した統計。

- システムが消費した電力（W）と各電源装置が消費した平均電流（A）。

グラフ情報

グラフ情報 ページには、一定期間にわたるシステムの電力レベル（W）と電力供給（A）が表示されます。このページは 1 分毎に自動更新されます。

メモ: データは DRAC 5 によって 5 分間隔で取得され、DRAC のリセット、AC 電源の入れ直し、またはファームウェア更新後に消失します。

メモ: システムの電源切断時や BMC のリセット時にはグラフが途切れる可能性があります。これは、この期間中、電力センサーが使用不可になるためです。

電力消費量（ワット）には、電力データが収集される期間が表示されます。このページのドロップダウンメニューから、X 軸の範囲を 1 時間、1 日、1 週間のいずれかに設定できます。期間は、DRAC に設定されている現在時刻からの時間です。Y 軸には、システムが消費した電力がワットで表示されます。

電力消費量（アンペア）には、電流データが収集される期間が表示されます。このページのドロップダウンメニューから、X 軸の範囲を 1 時間、1 日、1 週間のいずれかに設定できます。期間は、現在の DRAC の時刻からです。Y 軸には、電源装置が消費した電流がアンペアで表示されます。システムに複数の電源装置装置があり、読み取り値が同じ場合は、電流グラフが重なり合う可能性があります。

電力消費の情報

電力消費情報 ページには、システムが消費した電力がワットで表示され、各電源装置が消費した平均電流がアンペアで表示されます。

このページには、プローブの状態、プローブ名、消費電力量、警告とエラーアラートが生成される上限下限のしきい値、電源装置ユニットの場所、および各電源装置が消費する平均電流（アンペア）も表示されます。

電力統計

電力統計 ページには、DRAC の現在時刻から遡って 1 時間、1 日、1 週間のシステムの平均電力消費量と最大最小電力消費量の統計がワットと BTU/Hr（1 時間あたりのイギリス熱単位）が表示されます。データは DRAC 5 で取得され、DRAC が何らかの理由でリセットされた場合にはリセットされます。

温度プローブ

温度センサーは、システム基板の周辺温度についての情報を提供します。温度プローブは、プローブの状態が事前に設定された警告値と重要なしきい値の範囲内にあるかどうかを示します。

電圧プローブ

次は一般的な電圧プローブです。ご使用のシステムには、これら以外のものが使用されている可能性があります。

- CPU [n] VCORE
- システム基板 0.9V PG
- システム基板 1.5V ESB2 PG
- システム基板 1.5V PG
- システム基板 1.8V PG
- システム基板 3.3V PG
- システム基板 5V PG
- システム基板バックプレーン PG
- システム基板 CPU VTT
- システム基板リニア PG

電圧プローブは、プローブの状態が事前に設定された警告値および重要なしきい値の範囲内にあるかどうかを示します。

目次に戻る

目次に戻る

DRAC 5 - はじめに

Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

DRAC 5 を使うと、システムがダウンしていても Dell システムのリモート監視、トラブルシューティング、修復を行うことができます。DRAC 5 には、コンソールリダイレクト、仮想メディア、仮想 KVM、スマートカード認証を始め、豊富な機能が揃っています。

管理ステーションは、システム管理者が DRAC カードを搭載した Dell システムをリモート管理できるシステムです。管理ステーションから監視されるシステムを管理下システムといいます。

DRAC カードを使用するには、次の手順を行います。

1. お使いの Dell システムに DRAC 5 カードを取り付けます - DRAC 5 が事前に取り付けられている場合とキットとして別途購入する必要がある場合があります。

   メモ: この手順はシステムによって異なります。この手順の実行方法に関する正確な手順については、デルサポートサイト **support.dell.com / manuals** にある該当するシステムの『ハードウェア取扱説明書 』を参照してください。

   管理下システムだけでなく、管理ステーションにもDRAC 5 ソフトウェアをインストールする必要があります。管理下システムソフトウェアなしでは RACADM をローカルに使用できず、DRAC は前回のクラッシュ画面を取り込めません。

2. DRAC 5 のプロパティ、ネットワーク、ユーザーを設定します - DRAC 5 の設定には、リモートアクセス設定ユーティリティ、ウェブベースインタフェース、または RACADM を使用できます。

3. Microsoft Active Directory を DRAC 5 にアクセスできるように設定し、Active Directory ソフトウェア内で既存のユーザーの DRAC 5 ユーザー権限を追加したり制御することができるようにします。

4. スマートカード認証を設定します。スマートカードは企業のセキュリティを強化します。

5. コンソールリダイレクトや仮想 メディアなどのリモートアクセスポイントを設定します。

6. セキュリティ設定を指定します。

7. ネットワーク上のシステムを管理するには、標準ベースの管理 Server Management-Command Line Protocol(SM-CLP)を使用します。

8. システム管理機能の効率を上げるための警告を設定します。

9. 標準ベースの IPMI ツールを使用してネットワーク上のシステムを管理するには、DRAC 5 Intelligent Platform Management Interface(IPMI)の設定を指定します。

目次に戻る

目次に戻る

DRAC 5 の基本インストール

Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

ここでは、DRAC 5 のハードウェアの取り付けとソフトウェアのインストールおよび設定方法について説明します。

作業を開始する前に

DRAC 5 ソフトウェアをインストールして設定する前に、システムに含まれている次の項目についての情報を収集してください。

- DRAC 5 ハードウェア(組み込みかまたはオプションキットに同梱)
- DRAC 5 取り付け手順(この章内)
- 『Dell Systems Management Tools and Documentation DVD』

DRAC 5ハードウェアの取り付け

メモ: DRAC 5 接続は USB キーボード接続をエミュレートします。このため、システムを再起動したとき、キーボードが接続されていなくてもそのことを通知しません。

DRAC 5 はシステムに既に組み込まれている場合と、キットとして別途配布される場合があります。お使いのシステムにインストールされている DRAC 5 の使用を開始するには、ソフトウェアのインストールと設定の概要を参照してください。

DDRAC 5 がシステムに組み込まれていない場合は、DRAC 5 キットにある『Remote Access カードの取り付け』マニュアルを参照するか、お使いの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』に記載されているハードウェアの取り付け手順に従って取り付けを終えてください。

メモ: DRAC 5 の取り外しについては、お使いのシステムの『インストールおよびトラブルシューティングガイド』を参照してください。また、拡張スキーマを使用している場合は、取り外した DRAC 5 に関連する Microsoft Active Directory RAC プロパティをすべて見直して、セキュリティが適切であることを確認してください。

DRAC 5 使用のためのシステム設定

DRAC 5 を使用するためのシステム設定を行うには、Dell Remote Access 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。

Dell Remote Access 設定ユーティリティを実行するには、

1. システムの電源を入れるか、再起動します。
2. POST 中に画面の指示に従って <Ctrl><E> を押します。

   <Ctrl><E> キーを押す前にオペレーティングシステムのロードが開始された場合は、システムの起動が完了するのを待ってから、もう一度システムを再起動し、この手順を実行してください。
3. NIC を設定します。
   a. 下向き矢印を使って、**NIC の選択** を強調表示します。
   b. 左右の矢印キーを使って、次の NIC 選択肢から選択します。
      - **専用** - このオプションは、リモートアクセスデバイスから Remote Access Controller(RAC)上で使用可能な専用ネットワークインタフェースを使用できるようにする場合に選択します。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ことでアプリケーションのトラフィックから分離できます。このオプションは DRAC カードがシステムに取り付けられている場合にのみ使用できます。
      - **共有** - このオプションは、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場合に選択します。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 チームを設定すると、完全に機能します。リモートアクセスデバイスは、データの受信は NIC 1 と NIC 2 で行いますが、データの送信は NIC 1 からのみ行います。NIC 1 が故障すると、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** - このオプションは、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場合に選択します。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 チームを設定すると、完全に機能します。リモートアクセスデバイスは、データの受信は NIC 1 と NIC 2 で行いますが、データの送信は NIC 1 からのみ行います。NIC 1 が故障した場合、リモートアクセスデバイスはすべてのデータ送信を 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の送信に NIC 2 を引き続き使用します。NIC 2 が故障した場合、リモートアクセスデバイスはデータ伝送のすべてをまた 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. 下方向キーを使って、**LAN パラメータ** を選択し、<Enter> を押します。
   b. 上下の方向キーを使って、**IP アドレスソース** を選択します。

c. 左右の矢印キーを使って、**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**、**デフォルトゲートウェイ** をそれぞれ設定します。

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: 1 つの NIC を装備する Dell PowerEdge 1900 システムでウェブユーザーインタフェースを表示すると、NIC 設定ページに NIC が 2 つ(NIC 1 と NIC 2)表示されます。これは正常な動作です。PowerEdge 1900 システム(およびシングル LAN オンマザーボードの構成のその他の Dell システム)は NIC チーミング設定にできます。共有モードとチームモードは、これらのシステムでは互いに独立して動作します。

Dell Remote Access 設定ユーティリティの詳細については、『Dell OpenManage Baseboard Management Controller Utilities 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の概要

ここでは、DRAC 5 のソフトウェアのインストールと設定プロセスについて高水準の概要を提供します。ウェブベースインタフェース RACADM CLI またはシリアル/Telnet/SSH コンソールを使って DRAC 5 を設定します。

DRAC 5 のソフトウェアコンポーネントの詳細については、管理下システムへ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、次の手順を実行します。

1. ソフトウェアを管理下システムにインストールします。管理下システムへのソフトウェアのインストールを参照してください。
2. ソフトウェアを管理ステーションにインストールします。管理ステーションへ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、次の手順を実行します。

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

注意: 同時に複数の DRAC 5 を使用すると予測できない結果に終わることがあります。

2. DRAC 5 のネットワーク設定を指定します。DRAC 5 プロパティの設定を参照してください。
3. DRAC 5 ユーザーの追加や設定を行います。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ために、ウェブブラウザを設定します。対応ウェブ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 の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。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を参照してください。
7. ネットワークから DRAC 5 にアクセスします。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を参照してください。

管理下システムへのソフトウェアのインストール

管理下システムへのソフトウェアのインストールは省略可能です。管理下システムソフトウェアなしでは RACADM をローカルに使用できず、DRAC は前回のクラッシュ画面を取り込めません。

管理下システムソフトウェアをインストールするには、『Dell Systems Management Tools and Documentation DVD』で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。

管理下システムソフトウェアは、Dell OpenManage Server Administrator の適切なバージョンから、選択したコンポーネントを管理下システムにインストールします。

メモ: DRAC 5 管理ステーションソフトウェアと DRAC 5 管理下システムソフトウェアを同じシステムにインストールしないでください。

注意: 最新の DRAC ファームウェアは RACADM の最新バージョンのみをサポートしています。最新のファームウェアを使用している DRAC に、旧バージョンの RACADM を使用してクエリを発行すると、エラーが発生する可能性があります。最新の Dell OpenManage DVD メディアで配布されている RACADM バージョンをインストールしてください。

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の表示 や **自動回復** 機能は使用できません。

前回クラッシュ画面の詳細については、前回システムクラッシュ画面の表示を参照してください。

管理ステーションへのソフトウェアのインストール

システムには Dell OpenManage Systems Management Software Kit が含まれています。このキットには『Dell Systems Management Tools and Documentation DVD』やその他のメディアが含まれています。Server Administrator ソフトウェアについては、『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 Digital KVM Viewer を Red Hat Enterprise Linux(バージョン 4)管理ステーションで実行するには追加の設定が必要です。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、次の手順を実行してください。

- パッケージの追加または削除を求められたら、**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 Digital KVM Viewerを実行するため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。
- Dell Digital KVM Viewer 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いてください。
  - キーボードとマウスポート(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 が稼動する管理ステーションに RACADM をインストールします。

メモ:『Dell Systems Management Tools and Documentation DVD』で **セットアップ** を実行すると、サポートされているすべてのオペレーティングシステム用の 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、ルート権限でログオンします。
2. 必要に応じて、次のコマンドまたは同等のコマンド を使って、『Dell Systems Management Tools and Documentation DVD』をマウントします。

   ```
   mount /media/cdrom
   ```

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

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

RACADM コマンドに関するヘルプは、コマンドを入力した後「**racadm help**」と入力してください。

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する 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
```

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。

- ウェブインタフェース
- RACADM CLI
- Dell アップデートパッケージ

作業を開始する前に

ローカル RACADM またはDell アップデートパッケージを使って DRAC 5 をアップデートする前に、次の手順を実行してください。この手順を実行しないと、アップデートに失敗することがあります。

1. 適切な IPMI と管理下ノードのドライバをインストールして有効にします。
2. システムで Windows オペレーティングシステムが稼動している場合は、**Windows Management Instrumentation**(WMI)サービスを有効にして起動します。
3. システムで SUSE Linux Enterprise Server (バージョン 10) for Intel EM64T が実行されている場合は、**Raw** サービスを起動してください。
4. RAC 仮想フラッシュがマウント解除されており、オペレーティングシステムまたはその他のアプリケーションやユーザーによって使用されていないことを確認してください。
5. 仮想メディアを切断してマウント解除します。
6. USB が有効になっていることを確認してください。

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、デルサポートサイト **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。

- コンパイルされた DRAC 5 ファームウェアコードとデータ
- 拡張 ROM イメージ
- ウェブベースのインタフェース、JPEG、およびその他のユーザーインタフェースのデータファイル
- 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。ファームウェアのアップデートを実行する際に、アップデートは現在の DRAC 5 設定を保持します。

ウェブベースの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. ウェブベースのインタフェースを開いてリモートシステムにログインします。

   ウェブベース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、**Remote Access** をクリックして、**アップデート** タブをクリックします。
3. **ファームウェアのアップデート** ページの **ファームウェアイメージ** フィールドで、**support.dell.com** からダウンロードしたファームウェアイメージへのパスを入力するか **参照** をクリックしてイメージに移動します。

   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は表示されません。

   たとえば、次のとおりです。

   ```
   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。

   アップデートには完了まで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** をクリックしてセッションを閉じると、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。

racadm を使用した DRAC 5 ファームウェアのアップデート

CLI ベースの racadm ツールを使用して DRAC 5 ファームウェアをアップデートできます。管理下システムに Server Administrator をインストールしている場合は、ローカルの racadm を使用してファームウェアをアップデートしてください。

1. デルサポートサイト **support.dell.com** から DRAC 5 のファームウェアイメージを管理下システムにダウンロードします。

   たとえば、次のとおりです。

   ```
   C:\downloads\firmimg.d5
   ```

2. 次の racadm コマンドを実行します。

   ```
   racadm -pud c:\downloads\
   ```

   リモート racadm を使用してファームウェアをアップデートすることもできます。

   たとえば、次のとおりです。

   racadm -r <*DRAC5 IP アドレス*> U <*ユーザー名*> -p <*パスワード*> fwupdate -p -u -d <*パス*>

   パスは、管理下システムに **firmimg.d5** を保存した場所です。

サポートされている Windows および Linux オペレーティングシステム用の Dell Update Package を使用した DRAC 5 ファームウェアのアップデート

サポートされている Windows および Linux オペレーティングシステム用の Dell Update Package を **デルサポートサイト** support.dell.com からダウンロードして実行します。詳細については、『Dell Update Package ユーザーズガイド』を参照してください。

ブラウザキャッシュのクリア

ファームウェアアップグレード後、ウェブベースブラウザのキャッシュをクリアします。

詳細については、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。

対応ウェブブラウザの設定

次に、対応ウェブブラウザの設定手順を説明します。対応ウェブブラウザのリストについては、デルサポートウェブサイト **support.dell.com / manuals** で『Dell システムソフトウェアサポートマトリックス』を参照してください。

ウェブブラウザをウェブベースのインタフェースに接続できるように設定

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 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ウェブブラウザを設定する必要があります。

Internet Explorer ウェブブラウザをプロキシサーバーにアクセスするように設定するには、次の手順を実行します。

1. ウェブブラウザのウィンドウを開きます。
2. **ツール** をクリックして、**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)設定** で **LAN 設定** をクリックします。
5. **プロキシサーバーを使用** チェックボックスがオンになっている場合は、**ローカルアドレスにはプロキシサーバーを使用しない** チェックボックスをオンにします。
6. **OK** を 2 度クリックします。

信頼されているドメインのリスト

ウェブブラウザを使って DRAC 5 ウェブベースインタフェースにアクセスするとき、信頼されているドメインのリストにその IP アドレスがない場合はそのリストにDRAC 5 IP アドレスを追加するように求められます。追加し終えたら、更新をクリックするかウェブブラウザを再起動して、DRAC 5 ウェブベースインタフェースへの接続を再確立します。

32 ビットと 64 ビットのウェブブラウザ

DRAC 5 ウェブベースインタフェースは 64 ビットウェブブラウザではサポートされていません。64 ビットブラウザを開いた後、コンソールリダイレクトページにアクセスしてプラグインをインストールすると、インストールに失敗します。このエラーを確認しないでこの手順を繰り返すと、最初の試みでプラグインのインストールに失敗したにも関わらず、コンソールリダイレクトページがロードされます。これは、プラグインのインストールに失敗しても、ウェブブラウザがプロファイルディレクトリにプラグイン情報を保存するからです。この問題を解決するには、32 ビットの対応ウェブブラウザを実行して DRAC 5 にログインします。

ウェブインタフェースの日本語版の表示

Windows

DRAC 5 ウェブベース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。

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

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、次の手順に従います。

1. **ツール** をクリックして、**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を選択します。

   複数の言語を選択するには、<Ctrl> を押しながら選択します。
5. 優先言語を選択して**上に移動** をクリックし、その言語をリストの先頭に移動します。
6. **OK** をクリックします。
7. **言語設定** 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) クライアントで簡体字中国語の GUI を使ってコンソールリダイレクトを実行している場合は、ビューアのメニューとタイトルが字化けすることがあります。この問題は、Red Hat Enterprise Linux（バージョン 4）簡体字中国語オペレーティングシステムにおけるエンコードエラーによるものです。この問題を解決するには、次の手順で現在のエンコード設定にアクセスして変更してください。

1. コマンド端末を開きます。
2. 「locale」と入力して、<Enter> を押します。次の出力メッセージが表示されます。

```
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」が含まれている場合は、変更する必要はありません。値に「zh_CN.UTF-8」が含まれていない場合は、手順 4 に進んでください。
4. /etc/sysconfig/i18n ファイルに移動します。

5. ファイルに次の変更を加えます。

   現在のエントリ:

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

   アップデート後のエントリ:

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

6. オペレーティングシステムからログアウトしてログインします。

7. DRAC 5 を再起動します。

他の言語から簡体字中国語に切り替える場合は、この修正がまだ有効であることを確認してください。有効でない場合は、この手順を繰り返します。

DRAC 5 の詳細設定については、DRAC 5 の詳細設定を参照してください。

目次に戻る

目次に戻る

DRAC 5 の詳細設定

Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

ここでは、DRAC 5 の詳細設定について説明します。システム管理の知識が豊富なユーザーや、特定のニーズに応じて DRAC 環境をカスタマイズしたいユーザーにお勧めします。

作業を開始する前に

DRAC 5 ハードウェアとソフトウェアの基本インストールと設定が完了していることを前提とします。詳細については、DRAC 5 の基本インストールを参照してください。

DRAC 5 プロパティの設定

ウェブベースインタフェースまたは RACADM を使って DRAC 5 のプロパティ(ネットワーク、ユーザーなど)を設定できます。

DRAC 5 の ウェブベースインタフェースと RACADM(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、リモート管理下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には、DRAC 5 ウェブベースインタフェースを使用します。この章では、DRAC 5 ウェブベースインタフェースを使って一般的なシステム管理作業を行う方法について説明し、関連情報へのリンクを提供します。

ウェブベースインタフェースの設定作業は RACADM を使って行うこともできます。

ウェブインタフェースを使用した DRAC 5 の設定

各ウェブベースインタフェースページの状況依存の情報については DRAC 5 オンラインヘルプを参照してください。

ウェブベースインタフェースへのアクセス

DRAC 5 ウェブベースインタフェースにアクセスするには、次の手順を実行します。

1. サポートされているウェブブラウザのウィンドウを開きます。

   対応ウェブブラウザのリストについては、デルサポートウェブサイト **support.dell.com / manuals** で『Dell システムソフトウェアサポートマトリックス』を参照してください。

2. **アドレス** フィールドに次のテキストを入力し、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)が変更されている場合は、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 DRAC5 の IP アドレスで、<ポート番号> は HTTPS のポート番号です。

   DRAC 5 の **ログイン** ウィンドウが開きます。

メモ: Internet Explorer バージョン 6 SP2 またはバージョン 7 を使用して DRAC 5 のウェブ GUI にログインするとき、クライアントがプライベートネットワーク上にあってインターネットにアクセスできない場合は、最大 30 秒の遅延が生じる可能性があります。この問題を解決するには、次の手順を実行してください。

1. フィッシングフィルタを無効にします。

   https://phishingfilter.microsoft.com/faq.aspx.

2. CRL フェッチを無効にします。
    a. **ツール**→ **オプション**→ **詳細設定** タブ→ **セキュリティ**の順にクリックします。
    b. **パブリッシャーの証明書破棄をチェック** の選択を解除します。

ログイン

DRAC 5 ユーザーとして、または Microsoft Active Directory ユーザーとしての、どちらでもログインできます。デフォルトのユーザー名とパスワードはそれぞれ **root** と **calvin** です。

DRAC 5 にログインする前に、**DRAC 5 へのログイン** パーミッションがあることを確認してください。ご自分のアクセス権限を確認するには、組織の DRAC 管理者またはネットワーク管理者に問い合わせてください。

ログインするには、次の手順を実行します。

1. **ユーザー名** フィールドで、次のいずれかを入力します。
    - DRAC 5 ユーザー名。

      例: <*ユーザー名*>

      ローカルユーザーの DRAC 5 ユーザー名では、大文字と小文字が区別されます。
    - Active Directory ユーザー名。

      例: <*ドメイン*>\<*ユーザー名*>、<*ドメイン*>/<*ユーザー名*>、または <*ユーザー*>@<*ドメイン*>

      Active Directory ユーザー名の例: **dell.com\john_doe** または **john_doe@dell.com**。

      Active Directory ユーザー名では大文字と小文字の区別はされません。
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。

   このフィールドで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> キーを押します。

ログアウト

1. DRAC 5 ウェブベースインタフェースウィンドウの右上隅にある **ログアウト** をクリックして、セッションを閉じます。
2. ブラウザ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され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。そうしない場合、セッションはタイムアウトされるまで、アクティブ状態が続きます。

メモ: Microsoft Internet Explorer の右上にある 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ことがあります。この問題を解決するには、**support.microsoft.com** の Microsoft サポートウェブサイトから Internet Explorer 用の最新の累積セキュリティ更新プログラムをダウンロードしてください。

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指定と設定

次の項では、管理下システムでシリアル /telnet 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い方

connect com2 シリアルコマンドを使用するときは、次の設定が正しく指定されていることを確認してください。

- **BIOS セットアップ** プログラムの **シリアル通信**→ **シリアルポート** 設定
- DRAC 設定

DRAC 5 への telnet セッションが確立されたときにこれらの設定が正しくないと、**connect com2** にブランク画面が表示されることがあります。

管理下システムでシリアル接続 BIOS セットアッププログラムを設定する

出力をシリアルポートにリダイレクトするように**BIOS セットアップ** プログラムを設定するには、次の手順に従ってください。

メモ: **システムセットアップ** プログラムの設定は、**connect com2** コマンドと連携して行う必要があります。

1. システムの電源を入れるか、再起動します。
2. 次のメッセージが表示された直後に <F2> を押します。

   ```
   <F2> = System Setup
   ```

3. スクロールダウンし、**シリアル通信** を選択して <Enter> を押します。
4. **シリアル通信** 画面で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. **システムセットアップ** プログラムの設定を完了するには、<Esc> を押して **システムセットアップ** プログラムを終了します。

リモートアクセスシリアルインタフェースの使い方

RAC デバイスへのシリアル接続を確立するとき、次のインタフェースを使用できます。

- IPMI シリアルインタフェース。IPMI リモートアクセスシリアルインタフェースの使い方を参照してください。
- RAC シリアルインタフェース

RAC シリアルインタフェース

RAC ではまた、IPMI で定義されていない RAC 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)もサポートされています。システムに、**シリアルコンソール** が有効になっている RAC カードが含まれている場合、RAC カードは 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を表示します。

RAC シリアル端末インター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。

たとえば、次のとおりです。

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
```

詳細については、cfgSerialConsoleEnable(読み取り / 書き込み)を参照してください。

表 4-1 にシリアルインタフェース設定を示します。

表 4-1. シリアルインタフェース設定

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
端末	無効	IPMI 端末モード
端末	有効	RAC CLI

起動中におけるシリアルコンソールリダイレクトのための Linux の設定

次は、Linux GRand Unified Bootloader(GRUB)に固有の手順です。別のブートローダを使用する場合も、同様の変更が必要になる可能性があります。

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とき、リダイレクト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、テキストが正しく表示されるようにしてください。この設定を行わないと、一部のテキスト画面が文字化け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 全般設定 セクションを見つけて、次の 2 行を追加します。

   ```
   serial --unit=1 --speed=57600
   terminal --timeout=10 serial
   ```

2. カーネル行に次の 2 つにオプションを追加します。

```
kernel .............console=ttyS1,57600
```

3. **/etc/grub.conf** に splashimage ディレクティブがある場合は、コメントアウトします。

表 4-2 に、この手順で説明する変更を示したサンプル **/etc/grub.conf** ファイルがあります。

表 4-2. 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
# NOTICE:  You do not have a /boot partition. This means that
#          all kernel and initrd paths are relative to /, e.g.?
#          root (hd0,0)
#          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/sda1 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 (hd0,00)
   kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 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て、テキストベースの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. RAC シリアル接続を介してコンソールセッションを開始する GRUB オプションを複数有効にするには、すべてのオプションに次の行を追加します。

   ```
   console=ttyS1,57600
   ```

   表 4-2 に、console=ttyS1,57600 を最初のオプションにのみ追加した例を示します。

起動後のコンソールへのログインを有効にする

/etc/inittab ファイルを次のように編集します。

COM2 シリアルポートに agetty を設定する新しい行を追加します。

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

表 4-3 に、新しい行を追加したサンプルファイルを示します。

表 4-3. サンプルファイル: /etc/innitab

```
#
# inittab  This file describes how the INIT process should set up
#          the system in a certain run-level.
#
# Author :  Miquel van Smoorenburg
#          Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
# Default runlevel.The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have
#       networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
```

```
si::sysinit:/etc/rc.d/rc.sysinit
```

```
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
```

```
# Things to run in every runlevel.
ud::once:/sbin/update

# Trap 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.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

```

# Run gettys in standard runlevels
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
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

/etc/securetty ファイルを下記のように編集します。

COM2 用のシリアル tty の名前の新しい行を追加します。

```
ttyS1
```

表 4-4 に、新しい行を追加したサンプルファイルを示します。

表 4-4. サンプルファイル: /etc/securetty

```
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 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から有効にできます。

シリアル/Telnet/SSH コンソールをローカルに有効にする

メモ: この項の手順を行うには、ユーザーは **DRAC 5 の設定** 権限を持っている必要があります。

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、次のローカル RACADM コマンドをコマンドプロンプトで入力します。

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1

racadm config -g cfgSerial -o cfgSerialTelnetEnable 1

racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

Enabling the Serial / Telnet / SSH Console Remotely

シリアル/telnet/ssh コンソールをリモートから有効にするには、次のリモート **RACADM** コマンドをコマンドプロンプトで入力します。

```
racadm -u <ユーザー名> -p <パスワード> -r <DRAC 5 IP アドレス> config -g cfgSerial -o 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 -o cfgSerialTelnetEnable 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 -o cfgSerialSshEnable 1
```

メモ: Internet Explorer バージョン 6 SP2 またはバージョン 7 を使用してプライベートネットワーク上の管理下システムにログインするとき、インターネットアクセスがない場合は、リモート RACADM コマンドの使用中に最大 30 秒の遅延が生じる可能性があります。

RACADM コマンドを使ったシリアルコンソールと telnet コンソールの設定

この項では、シリアル/telnet/ssh コンソールリダイレクトのデフォルト設定を行う手順について説明します。

設定を行うには、その設定に適切なグループ、プロパティ、プロパティ値を指定した RACADM **config** コマンドを入力します。

RACADM コマンドはローカルにもリモートからでも入力できます。RACADM コマンドをリモートから使用する場合は、ユーザー名、パスワード、管理下システム DRAC 5 IP アドレスを含める必要があります。

RACADM をローカルに使用する

RACADM コマンドをローカル入力するには、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 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 のリモート使用

RACADM コマンドをリモート使用するには、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 IPアドレス> config -g <グループ> -o <プロパティ> <値>
```

RACADM をリモートから使用する前にウェブサーバーに DRAC 5 カードが装備されていることを確認してください。装備されていないと、RACADM はタイムアウトして次のメッセージが表示されます。

```
指定された IP アドレスで RAC に接続できません。
```

Secure Shell (SSH)、telnet、またはローカル RACADM を使ってウェブサーバーを有効にするには 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 config -g cfgRacTuning -o cfgRacTuneWebServerEnable 1
```

設定の表示

表 4-5 に、設定を表示するためのアクションと関連コマンドを示します。コマンドを実行するには、管理下システムのコマンドプロンプトを開いて、コマンドを入力し、<Enter> を押します。

表 4-5. 設定の表示

アクション	コマンド
使用可能なグループを一覧表示します。	racadm getconfig -h
特定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
特定グループの現在の設定をリモート表示します。	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、**cfgSerial** グループのすべての設定をリモート表示するには、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*>

シリアルまたは telnet コンソールの使い方

表 4-19 に示すシリアルコマンドは、RACADM を使うかシリアル/telnet/ssh コマンドプロンプトからリモートに実行できます。

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 管理下ノードの BIOS を設定した後、次の手順に従って DRAC にログインしてください。

1. 管理ステーションの端末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。

   DRAC 5 へのログインが完了しました。

テキストコンソールの起動

管理ステーションの端末ソフトウェアから telnet またはSSH を使って DRAC 5 にログインした後、telnet/SSH である **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。1 度に 1 つの **connect com2** クライアントのみサポートされています。

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 コマンドプロンプトを開いて(telnet または SSH セッションを通して表示)、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> を押すことで管理下システムのシリアルコンソールに接続できます。DRAC 5 をシリアルポートに再接続するには、<Esc><Shift><9> を押します。管理下ノード COM2 ポートと DRAC 5 のシリアルポートのボーレートは同じである必要があります。

connect -h com2 コマンドは、キーボードからの入力またはシリアルポートからの新しい文字を待つ前にシリアル履歴バッファの内容を表示します。

メモ: -h オプションを使うとき、クライアントとサーバーの端末エミュレーションタイプ (ANSI または VT100) は同じでなければなりません。同じでないと、出力が字化けします。さらに、クライアント端末行を **25** に設定します。

履歴バッファのデフォルト(最大)サイズは 8192 文字です。この値は、次のコマンドを使って小さくすることができます。

racadm config -g cfgSerial -o cfgSerialHistorySize <数値>

シリアルと端末モードの設定

IPMI と RAC シリアルの設定

1. **システム** ツリーを拡張し、**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、**シリアル** をクリックします。
3. IPMI のシリアル設定を指定します。

   IPMI シリアル設定については、表 4-6 を参照してください。
4. RAC のシリアル設定を指定します。

   RAC シリアル設定の説明は、表 4-7 を参照してください。

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。シリアル設定ページの設定については、表 4-8 を参照してください。

表 4-6. IPMI シリアル設定

設定	説明
接続モード設定	• ダイレクト接続基本モード - IPMI シリアル基本モード。 • 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**、または **115.2 kbps** から選択します。
フロー制御	• なし - ハードウェアフロー制御オフ。 • RTS/CTS - ハードウェアフロー制御オン。
チャネル権限レベルの制限	• 管理者 • オペレータ • ユーザー

表 4-7. 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。
最大セッション数	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最大アイドル時間(秒)。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 秒を使用します。
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**、または **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 ^\ 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。最大値およびデフォルト値 = 8192 文字。
ログインコマンド	有効なログイン後に実行する DRAC コマンドライン。

表 4-8. シリアル設定ページの設定

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 と 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。

ターミナルモードの設定

1. **システム** ツリーを拡張し、**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、**シリアル** をクリックします。

3. **シリアル設定** ページで **端末モードの設定** をクリックします。

4. ターミナルモード設定を指定します。

   ターミナルモードの設定の説明は、表 4-9 を参照してください。

5. **変更の適用** をクリックします。

6. **ターミナルモード設定** ページの適切なボタンをクリックして続行します。ターミナルモード設定 ページのボタンの説明は、表 4-10 を参照してください。

表 4-9. 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。 - **BMC は、<bksp> または <del> を受け取ると 、<bksp><sp><bksp> 文字を出 力します** - - **BMC は、<bksp> か <del>を受け取ると、<del>を出 力します** -
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	ハンドシェークを有効または無効にします。
新しいラインシーケンス	**None**、**<CR-LF>**、**<NULL>**、**<CR>**、**<LF-CR>**、または **<LF>** を選択します。
新しいラインシーケンスの入 力	**<CR>** または**<NULL>** を選択します。

表 4-10. 端末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。

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、システム上で DRAC 5 とシリアルポート間のアクセスを提供して、管理下システムの電源のオン、オフ、リセット、およびアクセスログを可能にします。

シリアルコンソールは、管理下システムの外部シリアルコネクタを通して DRAC で使用できます。1度にアクティブにできる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。telnet と SSH コンソールは、DRAC モードを介して DRAC 5 で使用できます(DRAC モードを参照)。1 度に 4 つまでの telnet クライアントシステムと 4 つまでの SSH クライアントを接続できます。管理ステーションの管理下システムのシリアルまたh telnet コンソールへの接続には、管理ステーション端末エミュレーションソフトウェアが必要です。詳細については、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の設定を参照してください。

次の項では、次の方法を使った管理ステーションから管理下システムへの接続について説明します。

- 端末ソフトウェアと DB-9 またはヌルモデムケーブルを使用した管理下システムの外部シリアルポート
- 管理下システムの DRAC 5 NIC または共有チーム NIC を通して端末ソフトウェアを使った telnet 接続

シリアルコンソールの DB-9 またはヌルモデムケーブルの接続

シリアルテキストコンソールを使って DRAC/MC にアクセスするには、管理下システム上の COM ポートに DB-9 ヌルモデムケーブルを接続します。DB-9 ケーブルのすべてが、この接続に必要なピン割り当て / 信号を持っているわけではありません。この接続に使用する DB-9 ケーブルは、表 4-11 仕様に従っ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 4-11. DB-9 ヌルモデムケーブルに必要なピン割り当て

信号名	DB-9 ピン (7 ピン)	DB-9 ピン (ワークスステーションピン)
FG(筐体接地)	-	-
TD(送信データ)	3	2
RD(受信データ)	2	3
RTS(送信要求)	7	8
CTS(送信可)	8	7
SG(信号用接地)	5	5
DSR(データセットレディ)	6	4
CD(データキャリア検出)	1	4
DTR(データ端末レディ)	4	1 と 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、次のいずれかの端末エミュレーションソフトウェアを実行している管理ステーションから、シリアルまたは telnet のテキストコンソールをサポートしています。

- Xterm の Linux Minicom
- Hilgraeve の HyperTerminal Private Edition(バージョン 6.3)
- Xterm の Linux Telnet
- Microsoft Telnet

使用するターミナルソフトウェアを設定するには、次の項の手順に従ってください。Microsoft Telnet を使用する場合、設定は不要です。

Linux Minicom にシリアルコンソールエミュレーションを設定する方法

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。次の手順は、Minicom のバージョン 2.0 に有効です。他のバージョンでは若干異なる場合がありますが、必要な基本設定は同じです。他のバージョンの Minicom の設定については、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 にシリアルコンソールエミュレーションを設定する方法

メモ: telnet コンソールを表示する場合は、テキストが正しく表示されるように、Linux のインストールによるデフォルトウィンドウでなく、Xterm ウィンドウの使用をお勧めします。

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、矢印キーをウィンドウの右下隅に移動してウィンドウのサイズを 80 x 25 に変更します。
3. Minicom の設定ファイルがない場合には、次の手順に進んでください。

   Minicom の設定ファイルがある場合は、`minicom <Minicom 設定ファイル名>` と入力し、手順 17 に進んでください。
4. Xterm コマンドプロンプトで、`minicom -s` と入力します。
5. **シリアルポートのセットアップ** を選択し、<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、**速度 / パリティ / ビット** 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. **シリアルポートの設定** メニューを終了するには、<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、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、それぞれの空白値を保存します。
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** を選択して、<Enter> を押します。
15. **Minicom から終了** を選択して、<Enter> を押します。
16. コマンドシェルプロンプトで、`minicom <Minicom 設定ファイル名>` 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のリダイレクトに Minicom を使用して管理下システムの BIOS を設定する場合は、Minicom で色をオンにすると便利です。色をオンにするには、`minicom -c on` コマンドを入力します。

Minicom ウィンドウに [DRAC 5\root]# のようなコマンドプロンプトが表示されることを確認します。コマンドプロンプトが表示されたら、接続が確立されて **connect** シリアルコマンドを使って管理下システムのコンソールに接続できることを意味します。

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

表 4-12 に従って Minicom を設定します。

表 4-12. 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

設定の説明	必要な設定
速度 / パリティ / ビット	57600 8N1
ハードウェアフロー制御	はい
ソフトウェアフロー制御	いいえ
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の設定	**初期化**、**リセット**、**接続**、**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）

シリアルコンソールリダイレクト用ハイパーターミナルの設定

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。

HyperTerminal にシリアルコンソールリダイレクトを設定するには、次の手順を実行してください。

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:**の隣で、DB-9 ヌ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 COM1）を選択し、**OK**をクリックします。
4. 表 4-13 に示した COM ポート設定を指定します。
5. **OK** をクリックします。
6. **ファイル**→ **プロパティ** をクリックして、**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、**画面の行数** を **26** に設定します。
9. **列数** を **80** に設定して、**OK** をクリックします。

表 4-13. 管理ステーション COM ポート設定

設定の説明	必要な設定
速度	57600
データビット	8
パリティ	なし
終了ビット	1
フロー制御	ハードウェア

HyperTerminal ウィンドウには [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、接続に成功し、**connect com2** シリアルコマンドを使って管理下システムのコンソールに接続できることを意味します。

Telnet コンソールリダイレクト用に Linux XTerm を設定する

この項で説明する手順を実行する際は、次のガイドラインに従ってください。

- telnet コンソールから **connect com2** コマンドを使って システムセットアップ 画面を表示する場合は、BIOS と telnet セッションで端末の種類を **ANSI** に設定してください。
- telnet コンソールを表示する場合は、テキストが正しく表示されるように、Linux のインストールによるデフォルトウィンドウでなく、Xterm ウィンドウの使用をお勧めします。

Linux で telnet を実行するには:

1. 新しい Xterm 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. XTerm ウィンドウの右下隅をクリックして、ウィンドウサイズを 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 IP アドレス>` と入力します。

Microsoft Telnet で Telnet コンソールリダイレクトを有効にする方法

メモ: Some telnet clients on Microsoft オペレーティングシステム上の一部の telnet クライアントでは、BIOS コンソールリダイレクトを VT100 エミュレーションに設定した場合に BISO セットアップ画面が正しく表示されないことがあります。この問題が発生した場合は、GIOS コンソールリダイレクトを ANSI モードに変更して表示を更新します。BIOS セットアップメニューでこの手順を実行するには、**Console Redirection**→ **リモート端末タイプ**→ **ANSI** を選択します。

1. **Windows コンポーネントサービス** 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いて次のテキストを入力し、<Enter> を押します。

   `telnet <IP アドレス>:<ポート番号>`

   ここで、IP アドレス は DRAC 5 の IP アドレスで、ポート番号は telnet ポート番号です(新しいポートを使う場合)。

Telnet セッション用の Backspace キーの設定

一部のTelnet クライアントでは、<Backspace> キーを使用すると予想外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 をエコーすることがあります。Microsoft と Linux の telnet クライアントではほとんどの場合、<Backspace> キーの使用を設定できます。

Microsoft telnet クライアントで <Backspace> キーを使用でき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. コマンドプロンプトで、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 が Delete として送信されます。`

Linux telnet セッションで <Backspace> キーを使用でき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いて、次のように入力します。

   `stty erase ^h`

2. コマンドプロンプトで、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

シリアル と **telnet** コマンド、および RACADM CLI は、シリアルまたは telnet コンソールから入力し、ローカルまたはリモートにサーバーから実行できます。ローカル RACADM CLI はルートユー

ザーのみがインストールできます。

Windows XP または Windows 2003 を使って telnet を実行する

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、DRAC 5 telnet セッションで文字に関する問題が発生する可能性があります。この場合、ログイン画面がフリーズして Enter キーが応答せず、パスワードプロンプトが表示されなくなります。

この問題を解決するには、Microsoft のサポートウェブサイト **support.microsoft.com** から修正プログラム hotfix 824810 をダウンロードします。詳細については、Microsoft 技術情報の記事 824810 を参照してください。

Windows 2000 での Telnet の実行

管理ステーションで Windows 2000 が稼動している場合は、<F2> キーを押して BIOS セットアップにアクセスすることはできません。この問題を解決するには、Microsoft が推奨する無償ダウンロードである、UNIX 3.5 用 Windows サービスに同梱の Telnet クライアントを使用します。**www.microsoft.com/downloads/** にアクセスして、「Windows Services for UNIX 3.5」を検索してください。

セキュアシェル(SSH)の使い方

システムのデバイスとデバイス管理がセキュアであることは不可欠です。組み込み接続デバイスは多くのビジネスプロセスの中核となっています。これらのデバイスが危険に曝されると、コマンドラインインタフェース (CLI) デバイス管理ソフトウェアの新しいセキュリティ要件を必要とするビジネスに支障が生じることになります。

Secure Shell(SSH)は telnet セッションと同じ機能を持つコマンドラインセッションですが、セキュリティ面で telnet より優れています。DRAC 5 では、パスワード認証を持つ SSH バージョン 2 をサポートしています。SSH は、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きに DRAC 5 で有効になります。

管理ステーション上では、PuTTY または OpenSSH を使用して、管理下システムの DRAC 5 に接続できます。ログイン中にエラーが発生すると、セキュアシェルクライアントでエラーメッセージが表示されます。メッセージの内容はクライアントによって異なり、DRAC 5 では制御されません。

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してください。Windows のコマンドプロンプトから OpenSSH を実行した場合は、一部の機能を使用できません(いくつかのキーが機能せず、グラフィックが表示されません)。

一度に最大 4 つの SSH セッションのみがサポートされます。DRAC 5 プロパティデータベースのグループとオブジェクトの定義で説明されるように、セッションタイムアウトは `cfgSsnMgtSshIdleTimeout` プロパティによって制御されます。

DRAC 5 で SSH を有効にするには、次を入力します。

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

SSH ポートを変更するには、次のように入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort <ポート番号>
```

`cfgSerialSshEnable` と `cfgRacTuneSshPort` プロパティの詳細については、DRAC 5 プロパティデータベースの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 SSH の実装では、表 4-14 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 4-14. 暗号化スキーム

スキーマの種類	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)
対称暗号	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
メッセージの整合性	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
認証	• パスワード

メモ: SSHv1 はサポートされていません。

DRAC 5 のネットワーク設定の指定

注意: DRAC 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。

- ウェブベースのインタフェース - DRAC 5 NIC の設定を参照してください。
- RACADM CLI - cfgLanNetworkingを参照してください。
- Dell Remote Access 設定ユーティリティ - DRAC 5 使用のためのシステム設定を参照してください。

メモ: Linux 環境で DRAC 5 を展開する場合は、RACADM のインストールを参照してください。

DRAC 5 へのネットワークアクセス

DRAC 5 を設定した後、次のいずれかのインタフェースを使って管理下システムにリモートアクセスできます。

- ウェブインタフェース
- RACADM
- Telnet コンソール
- SSH
- IPMI

表 4-15 に、各 DRAC 5 インタフェースを示します。

表 4-15. DRAC 5 インタフェース

インタフェース	説明
ウェブインタフェース	グラフィカルユーザーインタフェースを使って DRAC 5 にリモートアクセスできます。ウェブベースのインタフェースは DRAC 5 ファームウェアに内蔵されており、管理ステーション上の対応ウェブブラウザから NIC インタフェースを通してアクセスします。 対応ウェブブラウザのリストについては、デルサポートウェブサイト **support.dell.com / manuals** で『Dell システムソフトウェアサポートマトリックス』を参照してください。
RACADM	コマンドラインインタフェースを使って DRAC 5 にリモートアクセスできます。RACADM は管理下システムの IP アドレスを使って RACADM コマンドを実行します（racadm リモート機能オプション [-r]）。 **メモ:** racadm リモート昨日は、管理ステーションだけでサポートされています。 **メモ:** racadm リモート機能を使うとき、ファイル操作を含む **racadm** サブコマンドを使用する対象となるフォルダへの書き込み権限が必要です。例: `racadm getconfig -f <ファイル名>` または `racadm sslcertupload -t 1 -f c:\cert\cert.txt` サブコマンド
Telnet コンソール	DRAC 5 NIC 経由でのサーバーの RAC ポートへのアクセス、DRAC 5 NIC 経由でのハードウェア管理インタフェースへのアクセス、および**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、すべてのデータ（パスワードも含めて）をテキスト形式で送信するプロトコルです。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用の暗号化トランスポート層を使った 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 を通してリモートシステムの基本管理機能にアクセスできます。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、シリアルオーバー LAN が含まれます。詳細については、『Dell OpenManage Baseboard Management Controllerユーザーズガイド』を参照してください。

メモ: DRAC 5 のデフォルトユーザー名は root でデフォルトパスワードはcalvin です。

対応ウェブブラウザ、または Server Administrator あるいは IT Assistant を使って DRAC NIC を通して DRAC 5 のウェブベースインタフェースにアクセスできます。

対応ウェブブラウザのリストについては、デルサポートウェブサイト **support.dell.com / manuals** で『Dell システムソフトウェアサポートマトリックス』を参照してください。

Server Administrator 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にあるシステムツリーで、**システム**→ **メインシステムシャーシ**→ **リモートアクセスコントローラ** の順にクリックします。詳細については、『Server Administrator ユーザーズガイド』を参照してください。

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 サーバーは、予約テーブルにクライアントの ID トークンを保存するためのサーバーを必要とします。クライアント(DRAC 5 など)は DHCP ネゴシエーション中にこのトークンを提供する必要があります。RAC に対しては、DRAC 5 が 1 バイトインタフェース番号(0)に続く 6 バイトの MAC アドレスを使用してクライアント ID 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 **共有とフェールオーバー** モードに設定されており、DRAC が Spanning Tree Protocol (STP) を有効にしたスイッチに接続されている場合、STP 収束中に管理ステーションの LOM リンク状態が変化するとネットワーククライアントは 20〜30 秒の接続の遅延を経験することがあります。

1. **システム** ツリーの **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、**ネットワーク** をクリックします。
3. **ネットワークの設定** ページで、DRAC 5 NIC 設定を指定します。

   表 4-16 と 表 4-17 に、**ネットワークの設定** ページの **ネットワーク設定** と **IPMI 設定** を示します。
4. 完了したら、**変更の適用** をクリックします。
5. **ネットワークの設定** ページの適切なボタンをクリックして続行します。表 4-18 を参照してください。

表 4-16. ネットワークの設定

設定	説明
NIC の選択	選択した NIC モードを表示します(**専用**、**共有とフェールオーバー**、または **共有**)。 デフォルトの設定は **専用** です。
MAC アドレス	DRAC 5 の MAC アドレスを表示します。
NIC を有効にする	DRAC 5 の 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。
NIC IP アドレスに DHCP を使用	Dell OpenManage Server Administrator を有効にして、Dynamic Host Configuration Protocol (DHCP) から DRAC 5 NIC IP アドレスを取得します。このチェックボックスを選択すると、**静的 IP アドレス**、**静的ゲートウェイ**、**静的サブネットマスク** コントロールが非アクティブになります。 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ておきます。
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ておきます。
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ておきます。
DHCP を使用して DNS サーバーアドレスを取得する	静的設定ではなく、DHCP サーバーから一次と二次の INS 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	一次 DNS サーバー IP アドレスは、**DHCP を使って DNS サーバーアドレス** が **選択されていない** であるときにだけ使用します。
静的代替 DNS サーバー	二次 DNS サーバー IP アドレスは、**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** 場合に使用します。代替 DNS サーバーがないときは、IP アドレス 0.0.0.0 を入力することができます。
DNS 上における DRAC の登録	DNS サーバー上に DRAC 5 名を登録します。 デフォルト設定は **無効** です。
DNS DRAC 名	**DNS に DRAC 5 を登録** を選択した場合は、DRAC 5 名のみが表示されます。デフォルト DRAC 5 名は RAC-サービスタグです。ここで、サービスタグは Dell サーバーのサービスタグ番号です(例:RAC-EK00002)。
DNS ドメイン名に DHCP を使用	デフォルトの DNS ドメイン名を使用します。ボックスを選択しないで **DNS に DRAC 5 を登録** オプションを選択すると、**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 ドメイン名として DHCP を使用** チェックボックスを選択すると、このオプションは灰色表示となり、このフィールドを変更することはできません。
オートネゴシエーション	DRAC 5 が一番近いルータ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** を手動で設定できるか(**オフ**)を指定できます。
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 10Mb 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 4-17. 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。
チャネル権限レベルの制限	LAN チャネル許可されるユーザーの最大権限を設定します。システム管理者、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	暗号鍵の文字形式を 16 進文字 0～20 文字(空白を含まない)で設定します。 デフォルト設定は 00000000000000000000 です。
VLAN ID 有効	VLAN ID を有効にします。有効にすると、一致する VLAN ID トラフィックしか受け入れられません。
VLAN ID	802.1g フィールドの VLAN ID フィールド。
優先度	802.1g フィールドの 優先度 フィールド。

表 4-18. 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	ネットワーク設定に加えた変更を保存します。 **メモ:** NIC の IPアドレス設定を変更すると、アクティブなユーザーセッションがすべて閉じられるため、ユーザーはアップデート後の IPアドレス設定を使って DRAC 5 ウェブベースインタフェースに再び接続する必要があります。その他の変更では NIC をリセットする必要があり、このため接続が一時的に途絶える場合があります。

詳細については、DRAC 5 の GUI を使ったネットワークセキュリティの設定を参照してください。

RACADM のリモート使用

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 の設定方法の詳細および関連文書一覧については、DRAC 5 の基本インストールを参照してください。

RACADM CLI には、管理下システムに接続し、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)、および管理対象システムの IP アドレスが必要です。

メモ: リモートシステムにアクセスしているシステムのデフォルト証明書ストアに DRAC 証明書がない場合は、racadm コマンドを入力したときにメッセージが表示されます。

```
セキュリティ警告 : 証明書が無効です - 証明書の名前が無効かサイト名と一致しません

実行を継続します。証明書関連のエラーが発生したときに racadm に実行を停止するには、-S オプションを使用します。

racadm はコマンドの実行を続行します。ただし、-S オプションを使用した場合は、racadm がコマンドの実行を停止し、次のメッセージを表示します。

セキュリティ警告 : 証明書が無効です - 証明書の名前が無効かサイト名と一致しません

Racadm はコマンドの実行を続行しません。

エラー : 指定した IP アドレスの RAC に接続できません。
```

メモ: racadm リモート機能は、管理ステーションだけでサポートされています。詳細については、デルサポートサイト support.dell.com/manuals にある『Dell システムソフトウェアサポートマトリックス』を参照してください。

メモ: racadm リモート機能を使うとき、ファイル操作を含む racadm サブコマンドを使用する対象となるフォルダへの書き込み権限が必要です。例:

```
racadm getconfig -f <ファイル名>

または

racadm sslcertupload -t 1 -f c:\cert\cert.txt サブコマンド
```

RACADM 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>
```

たとえば、次のとおりです。

```
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)以外のカスタムポートに変更した場合は、次の構文を使用します。

```
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 オプション

表 4-19 に、**racadm** コマンドのオプションを示します。

表 4-19. racadm コマンドオプション

オプション	説明
-r <*raclpAddr*> **-r <*raclpAddr*>:<*ポート番号*>**	コントローラのリモート IP アドレスを指定します。 DRAC 5 ポート番号がデフォルトポート(443)出ない場合は、:<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と、**-p** オプションも必要になり、**-i** オプション(インタラクティブ)は使用できなくなります。
-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なくなります。
-S	**racadm** が無効な証明書エラーをチェックするように指定します。**racadm** は無効な証明書を検出した場合にコマンドの実行を停止して、エラーメッセージを表示します。

RACADM リモート機能を有効または無効にする

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有効になっています。無効になっている場合は、次の racadm コマンドを入力して有効にします。

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

リモート機能を無効にするには、次のように入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0
```

RACADM サブコマンド

表 4-20 に、RACADM で実行できる各**racadm** サブコマンドを示します。構文と有効なエントリを含む **racadm** サブコマンドの詳細リストについては、RACADMサブコマンドの概要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 を前付けしてください。たとえば、次のとおりです。

```
racadm help
```

表 4-20. RACADM サブコマンド

コマンド	説明
help	DRAC 5 サブコマンドを一覧表示します。
help <サブコマンド>	指定したサブコマンドの使用ステートメントを一覧にします。

arp	ARP 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。
clearasrscreen	前回の ASR(クラッシュ)画面をクリアします(前回の青色画面)。
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間を示すエントリが 1 つ作成されます。
config	RAC を設定します。
getconfig	現在の RAC 設定プロパティを表示します。
coredump	最新の DRAC 5 コアダンプを表示します。
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の状態を実行または表示します。
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的な情報を表示します。
getractime	DRAC 5 の日時を表示します。
ifconfig	RAC の現在の IP 設定を表示します。
netstat	ルーティングテーブルと現在の接続を表示します。
ping	現在のルーティングテーブルの内容を使って DRAC 5 から宛先 IP アドレスにアクセスできることを確認します。
setniccfg	コントローラの IP 設定を指定します。
getniccfg	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 のステータスと状態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。
racresetcfg	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源管理を行います。
getraclog	RAC ログを表示します。
clrsel	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 トレースログを表示します。-i を指定すると、このコマンドは DRAC 5 トレースログのエントリの数を表示します。
sslcsrgen	SSL CSR を生成してダウンロードします。
sslcertupload	DRAC 5 で CA 証明書またはサーバ証明書を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	DRAC 5 で CA 証明書またはサーバ証明書を表示します。
sslresetcfg	ウェブサーバー証明書を工場出荷時のデフォルトに復元して、ウェブサーバーを再起動します。
testemail	E-メールの設定をチェックするには、DRAC 5 に DRAC 5 NIC 経由でテスト E-メールを送信させます。
testtrap	トラップの設定をチェックするには、DRAC 5 に DRAC 5 NIC 経由でテスト SNMP トラップを送信させます。
vmdisconnect	仮想メディア接続を強制終了します。
vmkey	仮想フラッシュサイズをデフォルトサイズ(16 MB)に戻します。

RACADM エラーメッセージについてよくあるお問い合わせ(FAQ)

(racadm racreset コマンドを使用して)DRAC 5 をリセットした後、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)

このメッセージは何を意味しますか?

別のコマンドを実行する前に、DRAC 5 がリセットを完了するのを待つ必要があります。

racadm コマンドやサブコマンドを使用すると、原因不明のエラーが発生します。

racadm コマンドやサブコマンドを使用するとき、次のようなエラーが 1 つまたは複数起きることがあります。

- ローカル racadm エラーメッセージ - 構文、入力ミス、名前の誤りなどの問題。
- リモート racadm エラーメッセージ - IP アドレスの誤り、ユーザー名の誤り、パスワードの誤りなどの問題。

システムから DRAC IP アドレスを ping した後、DRAC 5 カードを専用と共有モード間で切り替えると、応答が返りません。

システムの ARP テーブルをクリアしてください。

複数 DRAC 5 カードの設定

RACADM を使うと、同じプロパティを持つ DRAC 5 カードを 1 枚または複数枚設定できます。グループ ID とオブジェクト ID を使って特定の DRAC 5 カードを照会するとき、RACADM は取得した情報から **racadm.cfg** 設定ファイルを作成します。このファイルを DRAC 5 カード 1 枚または複数枚にエクスポートすることで、まったく同じプロパティを持つコントローラを最小限の時間で設定できます。

メモ: 一部の設定ファイルには固有の DRAC 5 情報（静的 IP アドレスなど）が含まれているので、そのファイルを他の DRAC 5 カードにエクスポートする前に、その情報を変更する必要があります。

複数の DRAC 5 カードを設定するには、次の手順を実行します。

1. RACADM を使って、適切な設定を持つターゲット DRAC 5 をクエリします。

   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ていません。

   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** を使った RAC 設定のファイルへのリダイレクトは、ローカルまたはリモート RACADM インタフェースでのみサポートされています。

2. テキストエディタを使用して、設定ファイルに変更を加えます（省略可能）。

3. 新しい設定ファイルを使って、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 getconfig -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 の設定を要求し、**racadm.cfg** ファイルを生成します。必要に応じて、ファイルに別の名前を付けることもできます。

getconfig コマンドを使用すると、次のようなアクションが行えます。

- 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）
- 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、ユーザーとパスワードのデータベースを Server Administrator と同期させます。

初期設定ファイルの **racadm.cfg** 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: このファイルはテキストエディタで編集することをお勧めします。racadm ユーティリティが使用する ASCII テキストパーサーは、フォーマットを認識せず RACADM データベースを破壊す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 <filename>.cfg` コマンドと一緒に使用されます。この設定ファイルを使って設定ファイルを作成し（**.ini** ファイルと同様）、このファイルから DRAC 5 を設定することができます。ファイル名は自由に指定でき、最後に **.cfg** を付ける必要もありません（ただし、この項ではその命名法を使用しています）。

.cfg ファイルは次の方法で用意できます。

- 作成する
- `racadm getconfig -f <ファイル名>.cfg` コマンドで取得する
- `racadm getconfig -f <ファイル名>.cfg` コマンドで取得してから編集する

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、最初に解析が行われ、有効なグループとオブジェクト名があるかどうか、いくつかの単純な構文規則が守られているかどうかが検証されます。エラーはエラーが検出された行番号でフラグ指定され、その問題を説明した簡単なメッセージがあります。ファイル全体の正確性について解析され、すべてのエラーが表示されます。エラーが **.cfg** ファイルで見つかっても、DRAC/MC には書き込まれません。設定する前に、すべてのエラーを訂正する必要があります。**-c** オプションは **config** サブコマンドで使用できます。これは構文のみを検証し、DRAC/MC への書き込みを行いません。

.cfg ファイルを作成するときは、次のガイドラインに従ってください。

- パーサーがインデックス付けされたグループを見つけた場合、さまざまなインデックスの違いはアンカー付きオブジェクトの値で示されます。

  パーサーは、DRAC/MC 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。そのグループ内のオブジェクトはすべて、DRAC 5 を設定したときに簡単な変更が加えられたものです。変更されたオブジェクトが新しいインデックスを表す場合、設定中にその DRAC 5 のインデックスが作成されます。

- **.cfg** ファイルでは、インデックスを選択して指定することはできません。

  インデックスは作成と削除が繰り返されるため、グループは次第に使用と未使用のインデックスで断片化してく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、管理されているすべての RAC 間で索引を正確に一致させる必要のない場合に、索引付きエントリを追加できるという柔軟性が得られます。新しいユーザーは、最初に使用可能なインデックスに追加されます。DRAC で正しく解析および実行される **.cfg** ファイルは、すべてのインデックスがいっぱいで、新しいユーザーが追加される場合、正しく実行されない場合があります。

- まったく同じプロパティを持つすべての DRAC 5 カードの設定には、**racresetcfg** サブコマンドを使います。

  racresetcfg サブコマンドを使って DRAC 5 を元のデフォルトに戻し、`racadm config -f <ファイル名>.cfg` を実行します。`command`.**.cfg** ファイルにすべての必要オブジェクト、ユーザー、インデックス、およびその他のパラメータが入っ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 は最初のデフォルト設定にリセットされ、すべてのユーザーとユーザー設定が削除されます。root（ルート）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。

構文解析規則

- 「#」で始まる行はすべてコメントとして扱われます。

  コメント行は一列目から記述する必要があります。その他の列にある「#」の文字は単に # という文字として扱われます。

  一部のモデムパラメータでは # をその文字列内に含むことができます。エスケープ文字は必要ありません。**.cfg** を `racadm getconfig -f <ファイル名>.cfg` コマンドから生成し、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:

  ```
  #

  # これはコメントです。

  [cfgUserAdmin]

  cfgUserAdminPageModemInitString=<Modem init # not a comment>
  ```

- 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。

  グループ名を示す開始の **[** 文字は一列目にある必要があります。このグループ名は、そのグループ内の他のオブジェクトよりも前に指定する必要があります。関連するグループ名が含まれていないオブジェクトは、エラーを生成します。DRAC 5 プロパティデータベースのグループとオブジェクトの定義で定義したように、設定データはグループに分類されています。

  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}
  ```

- すべてのパラメータは、「`object`（オブジェクト）」、「=」、または「`value`（値）」の間に空白を入れずに「`object=value`」のペアとして指定されます。

  値の後にある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変更されません。'=' 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、有効なモデムチャットスクリプト文字です。

  上記の例を参照してください。

- **.cfg** パーサーはインデックスオブジェクトエントリを無視します。

  ユーザーは、使用するインデックスを指定できません。索引がすでに存在する場合は、それが使用されます。索引がない場合は、そのグループで最初に使用可能な索引に新しい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置くため、ユーザーは使用されているコメントをここで参照できます。

メモ: 次のコマンドを使用すると、インデックスグループを手動で作成できます。`racadm config -g <グループ名> -o <アンカー付きオブジェクト> -i <インデックス 1 ～ 16> <固有アンカー名>`

- インデックスグループの行は、**.cfg** ファイルからは削除できません。

  次のコマンドを使用して、手動でインデックスオブジェクトを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/MC 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>
```

- 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 "[ ]" の組み合わせの後に出現する最初のオブジェクトである 必要 があります。次は、現在のインデックス付きグループの例です。

  ```
  [cfgUserAdmin]

  cfgUserAdminUserName=<ユーザー名>
  ```

  `racadm getconfig -f <myexample>.cfg` と入力すると、このコマンドは **.cfg** ファイルを現在の DRAC 5 設定にバインドします。この設定ファイルは、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 IP アドレスの変更

設定ファイルで DRAC 5 IP アドレスを変更するとき、不要な **<*変数*>=値** エントリをすべて削除します。IP アドレスの変更に関する **<*値*>=値** エントリを含む実際の変数グループのラベルと "[" と "]" だけが残ります。

たとえば、次のとおりです。

```
#

# 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、このファイルを解析して、行番号ごとにエラーを特定します。ファイルが正しければ、該当するエントリがその内容で更新されます。さらに、前の例の **getconfig** コマンドを使用して、更新を確認できます。

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、ネットワーク上で新しいシステムを設定したりできます。

メモ:「Anchor」は内部用語です。ファイルには使用しないでください。

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、次のコマンドを使って **cfgNicUseDhcp** オブジェクトを記述し、この機能を有効にします。

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 1
```

これらのコマンドは、起動時にオプション ROM で <Ctrl><e> を入力するように求められるのと同じ設定機能を持ちます。オプション ROM を使用したネットワークプロパティ設定の詳細については、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。

次に、LAN ネットワークプロパティを設定するコマンドの使用例を示します。

```
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 cfgDNSServer1 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 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に設定できます。

- 専用
- 共有
- 共有とフェイルオーバー

表 4-21 に、各モードについて説明します。

表 4-21. DRAC 5 NIC の設定

モード	説明
専用	DRAC は、ネットワークトラフィックに対して独自の NIC(RJ-45 コネクタ)と BMC MAC アドレスを使用します。
共有	DRAC はプレーナで Broadcom LOM1 を使用します。
共有とフェールオーバー	DRAC は Broadcom LOM1 と LOM2 をフェールオーバー用のチームとして使用します。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)

DRAC 5 の Web インタフェースにアクセスすると、SSL 証明書のホスト名が DRAC 5. のホスト名と一致しないというセキュリティ警告が表示されます。

ウェブインタフェースとリモート racadm 機能のネットワークセキュリティを確保するため、DRAC 5 にはデフォルトの DRAC 5 サーバー証明書が含まれています。デフォルトの証明書は、DRAC 5 のホスト名(たとえば IP アドレス)と一致しない **DRAC 5 デフォルト証明書**に発行されているため、この証明書を使用すると、ウェブブラウザにセキュリティ警告が表示されます。

このセキュリティ問題に対処するには、DRAC 5 デフォルト証明書 の IP アドレスに発行された DRAC 5 デフォルト証明書 サーバー証明書をアップロードします。証明書の発行に必要な CSR を生成するとき、CSR の共通名(CN)が DRAC 5 の IP アドレス(たとえば 192.168.0.120)または登録されている DNS DRAC 名と一致するように注意してください。

CSR が登録されている DNS DRAC 名に一致することを確認するには:

1. **システム** ツリーの **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、**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
   a. **DNS に DRAC を登録**チェックボックスを選択します。
   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。

CSR の生成と証明書の発行については、SSL とデジタル証明書を使って DRAC 5 通信をセキュリティ保護するを参照してください。

プロパティを変更した後、リモート racadm とウェブベースのサービスが使えなくなるのはどうしてですか?

DRAC 5 ウェブサーバーがリセットした後リモート RACADM サービスとウェブベースのインタフェースが使用できるようになるまでに幾分時間がかかることがあります。

DRAC 5 ウェブサーバーは次のような場合にリセットします。

- DRAC 5 ウェブユーザーインタフェースを使ってネットワーク設定またはネットワークセキュリティのプロパティが変更された
- **cfgRacTuneHttpsPort** プロパティが変更された(config -f <設定ファイル> によって変更された場合を含む)
- **racresetcfg** が使われた
- DRAC 5 がリセットされた
- 新しい SSL サーバー証明書がアップロードされた

DNS サーバーが DRAC 5 を登録しないのはどうしてですか?

一部の DNS サーバーは 31 文字以内の名前しか登録しません。

DRAC 5 の ウェブインタフェースにアクセスすると、SSL 証明書が信頼できない認証局(CA)から発行されたというセキュリティ警告が表示されます。

ウェブインタフェースとリモート racadm 機能のネットワークセキュリティを確保するため、DRAC 5 にはデフォルトの DRAC 5 サーバー証明書が含まれています。この証明書は信頼できる CA によ

って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、信頼できる CA（たとえば Thawte や Verisign）から発行された DRAC/MC サーバー証明書をアップロードしてください。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って DRAC 5 通信をセキュリティ保護するを参照してください。

目次に戻る

目次に戻る

DRAC 5 ユーザーの追加と設定

Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

- RACADM ユーティリティを使用した DRAC 5 ユーザーの設定

DRAC 5 でシステムを管理し、システムのセキュリティを保持するには、特定の管理パーミッションを持つ一意なユーザー(または役割ベースの権限)を作成します。セキュリティを強化するために、特定のシステムイベントが発生したときに特定のユーザーに E-メールで警告を送るように設定することもできます。

DRAC 5 ユーザーを追加して設定するには:

メモ: 次の手順を実行するには、DRAC 5 の設定パーミッションが必要です。

1. **システム** ツリーを拡張し、**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、**ユーザー** をクリックします。

   ユーザー ページが開いて、各ユーザーの **状態**、**ユーザー名**、**RAC 権限**、**IPMI LAN 権限**、**IPMI シリアル権限**、**シリアルオーバー LAN**が表示されます。
3. **ユーザー ID** 列で、ユーザー ID をクリックします。
4. **ユーザーメインメニュー** ページでは、ユーザーの設定し、ユーザー証明書のアップロード、既存のユーザー証明書の表示、信頼される認証局(CA)の証明書のアップロード、信頼される CA 証明書の表示を行うことができます。

   ユーザーの設定 を選択して **次へ** をクリックすると、ユーザー設定 ページが表示されます。詳細については、手順 5 を参照してください。

   スマートカードの設定 セクションのオプションを選択した場合は、表 5-1 を参照してください。
5. **ユーザーの設定** ページで、ユーザーのプロパティと権限を設定します。

   表 5-2 には、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 **全般** 設定を示します。

   表 5-3 には、ユーザーの LAN 権限を設定するための **IPMI ユーザー権限** を示します。

   表 5-4 には、**IPMI ユーザー権限** と **DRAC ユーザー権限を設定** するための **ユーザーグループパーミッション** を示します。

   表 5-5 には、**DRAC グループ** パーミッションを示します。管理者、パワーユーザー、ゲストユーザーに DRAC ユーザー権限を追加すると、**DRAC グループ** は **カスタム** グループに変更されます。
6. 完了したら、**変更の適用** をクリックします。
7. **ユーザーの設定** ページの適切なボタンをクリックして続行します。表 5-6 を参照してください。

表 5-1. スマートカード設定セクションのオプション

オプション	説明
ユーザー証明書のアップロード	ユーザー証明書を DRAC にアップロードしてユーザープロファイルにインポートできます。
ユーザー証明書の表示	DRAC にアップロードされたユーザー証明書のページを表示します。
信頼される CA 証明書のアップロード	信頼される CA 証明書を DRAC にアップロードしてユーザープロファイルにインポートできます。
信頼される CA 証明書の表示	DRAC にアップロードされた信頼される CA 証明書を表示します。信頼される CA 証明書は、ユーザーに証明書を発行することを許可されている CA が発行したものです。

表 5-2. 一般プロパティ

プロパティ	説明
ユーザー ID	16 ある設定済みユーザー ID から指定します。 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。
ユーザーを有効にする	ユーザーが DRAC 5 にアクセスできるようにします。選択しないと、ユーザー名を変更できません。
ユーザー名	DRAC 5 ユーザー名を 16 文字以内で指定します。各ユーザーは一意のユーザー名を持つ必要があります。

	メモ: ローカル DRAC 5 のユーザー名に **@(アットマーク)**、**\(バックスラッシュ)**、**"(二重引用符)**、**/** (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、新しい名前は次回のユーザーログイン時までユーザーインタフェースに表示されません。
パスワードの変更	**新しいパスワード** と **新しいパスワードの確認** フィールドを有効にします。選択しないと、ユーザーの **パスワード** を変更することはできません。
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するため、ここに再入力する必要があります。

表 5-3. IPMI ユーザー権限

プロパティ	**説明**
LAN ユーザーに許可する最大権限	IPMI LAN チャネル上でのユーザーの最高権限として、**管理者**、**オペレーター**、**ユーザー**、または**なし** のユーザーグループのいずれかを指定します。
許可する最大シリアルポートユーザー権限	IPMI シリアルチャネル上でのユーザーの最高権限として、**管理者**、**オペレーター**、**ユーザー**、または **なし** のいずれかを指定します。
シリアルオーバー LAN を有効にする	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。選択すると、この権限が有効になります。

表 5-4. DRAC ユーザー権限

プロパティ	**説明**
DRAC グループ	ユーザーの DRAC ユーザーの最高権限レベルを **管理者**、**パワーユーザー**、**ゲストユーザー**、**なし**、**カスタム** のいずれかに指定します。 **DRAC グループ** パーミッションについては、表 5-5 を参照してください。
DRAC へのログイン	ユーザーに DRAC へのログインを許可します。
DRAC の設定	ユーザーに DRAC の設定を許可します。
ユーザーの設定	ユーザが指定したユーザーのシステムアクセスを許可できるようにします。
ログのクリア	ユーザーに DRAC ログのクリアを許可します。
サーバー制御コマンドの実行	ユーザーに racadm コマンドの実行を許可します。
コンソールリダイレクトへのアクセス	ユーザーにコンソールリダイレクトの実行を許可します。
仮想メディアへのアクセス	ユーザーに仮想メディアの実行と使用を許可します。
テスト警告	ユーザーがテスト警告(電子メールと PET)を特定のユーザーに送信できるようにします。
診断コマンドの実行	ユーザーに診断コマンドの実行を許可します。

表 5-5. DRAC グループのパーミッション

ユーザーグループ	**許可するパーミッション**
管理者	**DRAC へのログイン**、**DRAC の設定**、**ユーザーの設定**、**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**、**警告のテスト**、**診断コマンドの実行。**
パワーユーザー	**DRAC 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**、**警告のテスト。**
ゲストユーザー	DRAC へのログイン。
カスタム	次のパーミッションから任意の組み合わせを選択:**DRAC へのログイン**、**DRAC の設定**、**ユーザーの設定**、**ログのクリア**、**サーバーアクションコマンドの実行**、**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**、**警告のテスト**、**診断コマンドの実行。**
なし	割り当てられたアクセス権はありません。

表 5-6. ユーザー設定ページのボタン

ボタン	**アクション**
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	ネットワーク設定に加えた変更を保存します。

RACADM ユーティリティを使用した DRAC 5 ユーザーの設定

メモ: リモート Linux システム上で RACADM コマンドを実行するには、**root** ユーザーとしてログインする必要があります。

DRAC 5 ウェブベースインタフェースは DRAC 5 を設定する最も高速な方法です。コマンドラインまたはスクリプトの設定を好む場合、または複数の DRAC 5 を設定する必要がある場合は、管理下システムに DRAC 5 といっしょにインストールされている RACADM を使用してください。

まったく同じ設定を複数の DRAC 5 に対して指定する場合は、次のいずれかの手順を行ってください。

- この項にある RACADM の例をガイドとして使って **racadm** コマンドのバッチファイルを作成し、各管理下システムでこのバッチファイルを実行します。
- RACADMサブコマンドの概要に説明されているとおりに DRAC 5 設定ファイルを作成し、各管理下システムで同じ設定ファイルを使って**racadm config** サブコマンドを実行します。

作業を開始する前に

DRAC 5 プロパティデータベースで 16 までのユーザーを設定できます。手動で DRAC 5 ユーザーを有効にする前に、現在のユーザーが存在することを確認してください。新しい DRAC 5 を設定する場合や **racadm racresetcfg** コマンドを実行する場合は、唯一の現在のユーザーはパスワードが `calvin` の `root` です。**racresetcfg** サブコマンドは DRAC 5 を最初のデフォルトにリセットします。

注意: **racresetcfg コマンドを使用する場合は、注意が必要です。すべての設定パラメータがデフォルト値に戻ります。それまでに行った変更がすべて失われます。**

メモ: ユーザーは経時的に有効にしたり、無効にしたりできます。このため、各 DRAC 5 上でユーザーは異なるインデックス番号を持つ可能性があります。

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がわかります。

```
racadm getconfig -u <ユーザー名>
```

または

1～16 までの各インデックスに、次のコマンドを 1 回ずつ入力することもできます。

```
racadm getconfig -g cfgUserAdmin -i <インデックス>
```

メモ: `racadm getconfig -f <myfile.cfg>` と入力して、DRAC 5 設定パラメータが入っている**myfile.cfg** ファイルを表示したり編集したりできます。

複数のパラメータとオブジェクト ID が現在値と一緒に表示されます。対象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その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る場合は、そのインデックスがそのユーザー名によって使用されています。

メモ: **rracadm config** サブコマンドを使用し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。前の例で示した **cfgUserAdminIndex** オブジェクトに '#' 文字が含まれていることに注目してください。**racadm config -f racadm.cfg** コマンドを使用して、書き込むグループ / オブジェクトの数を指定する場合、インデックスは指定できません。最初に 使用可能なインデックスに新しいユーザーが追加されます。この仕組みにより、同じ設定を持つ複数の DRAC 5 の設定が柔軟にできるようになります。

DRAC 5 ユーザーの追加

新しいユーザーを RAC 設定に追加するには、基本的なコマンドをいくつか使用できます。通常は、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. ユーザー権限を設定します。
4. ユーザーを有効にします。

例

次の例では、パスワード「`123456`」と LOGIN 権限を持つ新しいユーザー名「`John`」を RAC に追加します。

```
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、次のいずれかのコマンドを使用します。

```
racadm getconfig -u john

racadm getconfig -g cfgUserAdmin -i 2
```

DRAC 5 ユーザーの削除

RACADM を使用している場合は、ユーザーを手動で個別に無効にする必要があります。設定ファイルを使用してユーザーを削除することはできません。

次の例では、RAC ユーザーの削除に使用できるコマンド構文を示します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <インデックス> ""
```

二重引用符に囲んだヌル文字列 ("") は、DRAC 5 に指定したインデックスからユーザー設定を削除し、ユーザー設定を工場出荷時のデフォルトに戻すように指示します。

E-メール警告のテスト

RAC E-メール警告機能を使用すると、管理下システムで重大イベントが発生したときに E-メール警告を受信できます。次の例は、RAC がネットワークで正しく E-メール警告を送信できるかどうかを確認するために、E-メール警告機能をテストする方法を示しています。

```
racadm testemail -i 2
```

メモ: E-メール警告機能のテストを行う前に、**SMTP** と **E-メール警告** 設定が指定されていることを確認してください。詳細については、E-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うと、SNMP トラップリスナー設定で管理下システム上で発生したシステムイベントのトラップを受信することができます。

次の例で、ユーザーが RAC の トラップ警告機能をテストする例を示します。

```
racadm testtrap -i 2
```

RAC 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く設定されていることを確認してください。これらの設定の指定方法については、testtrap と testemail のサブコマンドの説明を参照してください。

DRAC 5 ユーザーにパーミッションを与える

特定のシステム管理許可（ロールベースの権限）を持つユーザーを有効にするには、まず 作業を開始する前にのステップを実行して使用可能なユーザーインデックスを探します。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: 特定のユーザー権限に有効なビットマスク値については、表 B-2 のリストを参照してください。デフォルトの権限値は 0 で、これはユーザーの権限が有効になっていないことを示します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <インデックス> <ユーザー権限ビットマスク値>
```

目次に戻る

目次に戻る

Microsoft Active Directory での DRAC 5 の使い方

Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

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管理します。貴社がすでに 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 へのアクセスを提供するようにソフトウェアを設定でき、これによって Active Directory ソフトウェアの既存のユーザーに対する DRAC 5 ユーザー権限の追加および制御を行うことが可能になります。

メモ: Active Directory を使用した iDRAC 5 ユーザーの認識は、Microsoft Windows 2000、Windows Server 2003 および Windows Server 2008 オペレーティングシステムでサポートされています。

Active Directory が DRAC 5 を認証できるようにするための前提条件

Active Directory で DRAC 5 を認証する機能を使用するには、Active Directory インフラストラクチャが既に作成されている必要があります。DRAC 5 の Active Directory 認証は、1 つのフォレストの複数のツリーに対する認証をサポートしています。ドメイン機能レベル、グループ、オブジェクトなどに関してサポートされている Active Directory の設定については、サポートされている Active Directory の設定 を参照してください。

Active Directory インフラストラクチャがまだない場合、その設定方法については、Microsoft のウェブサイトを参照してください。

DRAC 5 は標準の公開鍵インフラストラクチャ(PIK)機構を使って Active Directory に対して安全に認証するので、Active Directory インフラストラクチャへの統合 PKI も必要になります。

PKI の設定については、Microsoft のウェブサイトを参照してください。

すべてのドメインコントローラに対して正しく認証するには、ドメインコントローラ上で Secure Socket Layer(SSL)を有効にする必要もあります。その他特定の情報については、ドメインコントローラの SSL を有効にする を参照してください。

サポートされている Active Directory の認証機構

Active Directory を使って DRAC 5 でのユーザーアクセスを定義する方法には 2 通りあります。Active Directory グループオブジェクトのみを用いた標準スキーマソリューションがその 1 つで、もう 1 つは Dell 指定の Active Directory オブジェクトを追加するために Dell がカスタマイズした拡張スキーマソリューションです。これらのソリューションについては、次の各項を参照してください。

Active Directory を使って DRAC 5 をへのアクセスを設定する場合は、拡張スキーマか標準スキーマソリューションのいずれか 1 つを選択する必要があります。

標準スキーマソリューションを使用する場合の長所は次のとおりです。

- 標準スキーマでは Active Directory オブジェクトのみが使用されるためスキーマ拡張が不要。
- Active Directory 側の設定が簡単

拡張スキーマソリューションを使用する場合の利点は次のとおりです。

- アクセス制御オブジェクトのすべてを Active Directory で管理できます。
- 権限レベルがそれぞれ異なる DRAC 5 カードでユーザーアクセス設定を最大限に柔軟に行うことが可能

標準スキーマの Active Directory の概要

図 6-1 に示すように、Active Directory を統合するために標準スキーマを使用する場合は、Active Directory と DRAC 5 の両方で設定が必要となります。Active Directory 側では、標準グループオブジェクトが役割グループとして使用されます。DRAC 5 へのアクセス権を持つユーザーが役割グループのメンバーになります。このユーザーに特定の DRAC 5 カードへのアクセス件を与えるには、役割グループ名とそのドメイン名を指定の DRAC 5 カードで設定する必要があります。拡張スキーマソリューションとは異なり、役割と権限レベルは Active Directory でなく、各 DRAC 5 カードで定義されます。各 DRAC 5 で設定、定義できる役割グループの数は 5 つまでです。表 6-12 に役割グループの権限レベル、表 6-1 に役割グループのデフォルト設定を示します。

図 6-1. Microsoft Active Directory と標準スキーマによる DRAC 5 の設定

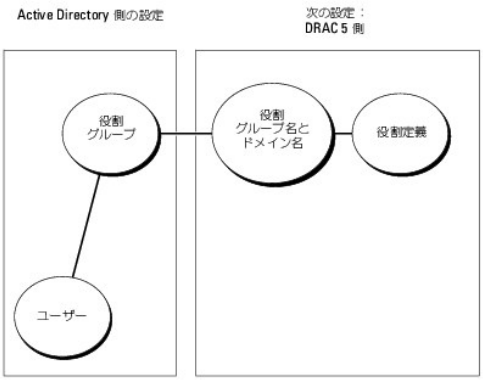


表 6-1. デフォルトの役割グループの権限

役割グループ	デフォルトの権限レベル	許可するパーミッション	ビットマスク
役割グループ 1	管理者	DRAC へのログイン、DRAC の設定、ユーザーの設定、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	0x000001ff
役割グループ 2	パワーユーザー	DRAC 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	0x000000f9
役割グループ 3	ゲストユーザー	DRAC へのログイン	0x00000001
役割グループ 4	なし	パーミッションの割り当てなし	0x00000000
役割グループ 5	なし	パーミッションの割り当てなし	0x00000000

メモ: ビットマスク値を使用するのは、RACADM で標準スキーマを設定する場合に限ります。

標準スキーマ Active Directory を有効にするには、次の 2 つの方法があります。

- DRAC 5 Web ベースのユーザーインタフェースを使用する。標準スキーマ Active Directory とウェブベースのインタフェースを用いた DRAC 5 の設定ウェブインタフェース を参照してください。
- RACADM CLI ツールの使用。標準スキーマ Active Directory と RACADM を用いた DRAC 5 の設定 を参照してください。

DRAC 5 にアクセスするための標準スキーマ Active Directory の設定

Active Directory ユーザーが DRAC 5 にアクセスできるようにするには、まず次の手順を実行し、Active Directory を設定する必要があります。

1. Active Directory サーバー(ドメインコントローラ)で、Active Directory ユーザーとコンピュータスナップイン を開きます。
2. グループを作成するか、既存のグループを選択します。グループ名およびドメイン名は、ウェブベースのインタフェースまたは RACADM のいずれかを使用して DRAC 5 で設定する必要があります(標準スキーマ Active Directory とウェブベースのインタフェースを用いた DRAC 5 の設定ウェブインタフェース または 標準スキーマ Active Directory と RACADM を用いた DRAC 5 の設定 を参照)。
3. DRAC 5 にアクセスするには、Active Directory ユーザーを Active Directory グループのメンバーに追加します。

標準スキーマ Active Directory とウェブベースのインタフェースを用いた DRAC 5 の設定ウェブインタフェース

1. サポートされているウェブ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** ツリーを拡張し、**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** ページで、**Active Directory の設定** を選択し、**次へ** をクリックします。

6. 共通設定セクションで以下の操作を行います。
   a. **Active Directory を有効にする** チェックボックスをオンにします。
   b. **ルートドメイン名** を入力します。**ルートドメイン名** はフォレストのルートドメインの完全修飾名です。
   c. **タイムアウト** の時間を秒単位で入力します。
7. Active Directory スキーマの選択セクションで **標準スキーマの使用** をクリックします。
8. **適用** をクリックして Active Directory の設定を保存します。
9. 標準スキーマ設定セクションの **役割グループ** 列で **役割グループ** をクリックします。

   役割グループの設定 ページが表示されます。このページには、役割グループの **グループ名**、**グループドメイン**、**役割グループの権限** が含まれています。
10. **グループ名** を入力します。このグループ名によって、DRAC 5 カードに関連した Active Directory の役割グループが識別されます。
11. **グループドメイン** を入力します。**グループドメイン** はフォレストのルートドメインの完全修飾名です。
12. **役割グループの権限** で、グループの権限を設定します。

    表 6-12 に **役割グループの権限** を示します。

    表 6-13 に **役割グループのパーミッション** を示します。パーミッションを変更すると、既存の **役割グループの権限**（システム管理者、パワーユーザー、ゲストユーザー）は、変更したパーミッションに基づいてカスタムグループまたは適切な役割グループの権限に変更されます。
13. **適用** をクリックして、役割グループの設定を保存します。
14. **Active Directory の設定と管理に戻る** をクリックします。
15. **Active Directory メインメニューに戻る** をクリックします。
16. ドメインフォーレストのルート CA 証明書を DRAC 5 へ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選択し、**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、証明書ファイルの場所まで移動します。

    メモ: アップロードする証明書の相対ファイルパスが **ファイルパス** の値に表示されます。フルパスと正しい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。

    ドメインコントローラの SSL 証明書はルート CA により署名されている必要があります。DRAC 5 にアクセスする管理ステーション上にルート CA 証明書があることを確認します（ドメインコントローラのルート CA 証明書を DRAC 5 にエクスポートする を参照）。
    c. **適用** をクリックします。

    適用 をクリックすると、DRAC 5 ウェブサーバーが自動的に再起動されます。
17. ログアウトしてからまた DRAC 5 にログインし、DRAC 5 Active Directory 機能の設定を完了します。
18. **システム** ツリーの **リモートアクセス** をクリックします。
19. **設定** タブをクリックし、**ネットワーク** をクリックします。

    ネットワーク設定 ページが開きます。
20. **ネットワーク設定** で **DHCP を使用（NIC IP アドレス用）**が選択されている場合、**DHCP を使用 を選択して DNS サーバーアドレスを取得** を選択します。

    DNS サーバーの IP アドレスを手動で入力するには、**DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスをオフにし、一次および代替 DNS サーバーの IP アドレスを入力します。
21. **変更の適用** をクリックします。

    これで、RAC 5 の標準スキーマ Active Directory 機能の設定が完了しました。

標準スキーマ Active Directory と RACADM を用いた DRAC 5 の設定

ウェブインタフェースではなく racadm CLI を使用した標準スキーマで 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。

1. 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 cfgADType 2

racadm config -g cfgActiveDirectory -o cfgADRootDomain <完全修飾ルートドメイン名>

racadm config -g cfgStandardSchema -i <インデックス> -o cfgSSADRoleGroipName <役割グループの共通名>

racadm config -g cfgStandardSchema -i <インデックス> -o cfgSSADRoleGroipDomain <完全修飾ルードメイン名>

racadm config -g cfgStandardSchema -i <インデックス> -o cfgSSADRoleGroupPrivilege <特定ユーザーパーミッション用のビットマスク番号>

racadm sslcertupload -t 0x2 -f <ADS ルート CA 証明書>

racadm sslcertdownload -t 0x1 -f <RAC SSL 証明書>
```

メモ: ビットマスク番号については、表 B-4 を参照してください。

2. DRAC/MC の DHCP が有効になっており、DHCP サーバーが提供する DNS を使用する場合は、次のコマンドを入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
```

3. 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 racadm コマンドを入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1 <プライマリ DNS IP アドレス>

racadm config -g cfgLanNetworking -o cfgDNSServer2 <セカンダリ DNS IP アドレス>
```

DRAC 5 に Active Directory サーバーを探させる代わりに、DRAC 5 の接続先サーバーを指定して、ユーザーを認証することもできます。サーバーを指定する RACADM コマンドについては、Active Directory 設定のためのサーバー指定 を参照してください。

拡張スキーマ Active Directory の概要

拡張スキーマ Active Directory を有効にするには、次の 2 つの方法があります。

- DRAC 5 Web ベースのユーザーインタフェースを使用する。拡張スキーマ Active Directory とウェブベースのインタフェースを用いた DRAC 5 の設定 を参照してください。
- RACADM CLI ツールの使用。拡張スキーマ Active Directory と RACADM を用いたDRAC 5 設定 を参照してください。

Active Directory スキーマ拡張

Active Directory データは、属性とクラスの分散データベースです。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。会社は、自社環境に特有のニーズを満たすための固有の属性とクラスを追加して、Active Directory データベースを拡張できます。デルでは、スキーマを拡張して、リモート管理の認証と許可をサポートするために必要な変更を含めました。

既存の Active Directory スキーマに追加した属性やクラスは、それぞれ固有の ID で定義する必要があります。業界で一意の ID を保持するため、Microsoft では Active Directory オブジェクト識別子（OID）のデータベースを管理して、会社がスキーマに拡張を追加する場合、それらが他社と重複しないようにしています。デルでは、Microsoft の Active Directory のスキーマを拡張できるように、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 を受け取っています。

Dell の拡張子：dell

Dell ベースの OID：1.2.840.113556.1.8000.1280

RAC LinkID の範囲：12070～12079

Microsoft が管理する Active Directory OID データベースは、**http://msdn.microsoft.com/certification/ADAcctInfo.asp** で拡張子 Dell を入力することで参照できます。

RAC スキーマ拡張の概要

デルでは、さまざまな顧客環境に柔軟に対応できるように、ユーザーが達成したい成果に応じて設定できるプロパティを用意しています。デルは、関連、デバイス、権限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、特定の権限セットを持つユーザーまたはグループを 1 台または複数台の 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 権限、およびネットワーク上の RAC デバイスを組み合わせる際に最大限の柔軟性が得られる一方、複雑になり過ぎることはありません。

Active Directory オブジェクトの概要

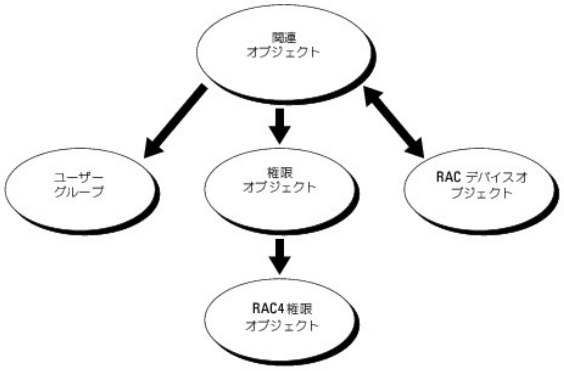
認証と許可のために Active Directory に統合するネットワーク上の物理 RAC の 1 台につき、少なくとも 1 個ずつ関連オブジェクトと RAC デバイスオブジェクトを作成しておきます。関連オブジェクトは必要なだけいくつでも作成でき、各関連オブジェクトにリンクできるユーザー、ユーザーグループ、RAC デバイスオブジェクトの数にも制限はありません。ユーザーと RAC デバイスオブジェクトは、企業内のどのドメインのメンバでもかまいません。

ただし、各関連オブジェクトは 1 つの権限オブジェクトにしかリンクできず、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 つの権限オブジェクトにしかリンクできません。この例では、システム管理者は特定の RAC で各ユーザーの権限を制御できます。

RAC デバイスオブジェクトは、Active Directory に照会して認証と許可を実行するための RAC ファームウェアへのリンクです。RAC をネットワークに追加した場合、システム管理者は RAC とそのデバイスオブジェクトをその Active Directory 名で設定して、ユーザーが Active Directory で認証と認可を実行できるようにする必要があります。さらに、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。

図 6-2 は、関連オブジェクトがすべての認証と認可に必要な関連付けを提供する仕組みを示しています。

図 6-2. Active Directory オブジェクトの標準的なセットアップ



メモ: RAC 権限オブジェクトは DRAC 4 と DRAC 5 の両方に適用されます。

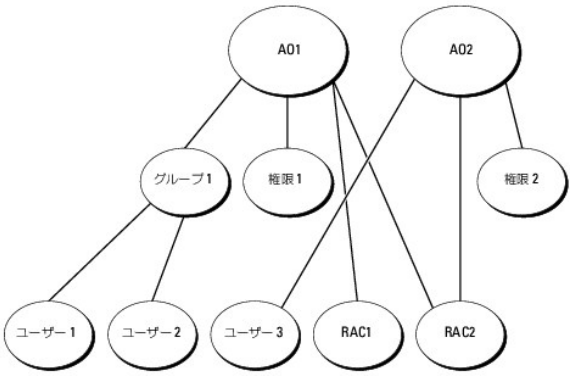
作成する関連オブジェクトの数に制限はありません。少なくとも 1 つは作成する必要があります。また、RAC(DRAC 5)を使って認証と承認ができるように Active Directory と統合するネットワーク上の各 RAC(DRAC 5)に RAC デバイスオブジェクトが 1 つ必要です。

関連オブジェクトに含むことができるユーザー、グループ、RAC デバイスオブジェクトの数に制限はありません。ただし、関連オブジェクトに含むことができる権限オブジェクトは、関連オブジェクト 1 つに 1 つだけです。関連オブジェクトは RAC(DRAC 5)に「権限」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、複数のドメインのいずれに設定することも可能です。たとえば、DRAC 5 カードが 2 枚(RAC1 と RAC2)あり、既存の Active Directory ユーザーが 3 人(ユーザー 1、ユーザー 2、ユーザー 3)いるとします。ユーザー 1 とユーザー 2 に両方の DRAC 5 カードの管理者権限を与え、ユーザー 3 に RAC2 カードへのログイン権限を与えたいとします。図 6-3 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、ユニバーサルスコープで関連オブジェクトを作成します。Dell Schema Extender ユーティリティで作成されたデフォルトの関連オブジェクトはドメインローカルグループであり、他のドメインからのユニバーサルグループとは連動しません。

図 6-3. 単一ドメインでの Active Directory オブジェクトの設定



単一ドメインのシナリオでオブジェクトを設定するには、次の手順に従います。

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 つの権限オブジェクト(権限 1 と権限 2) を作成し、権限 1 にはすべての権限(システム管理者)、権限 2 にはログイン権限を与えます。

4. ユーザー 1 とユーザー 2 をまとめてグループ 1 とします。

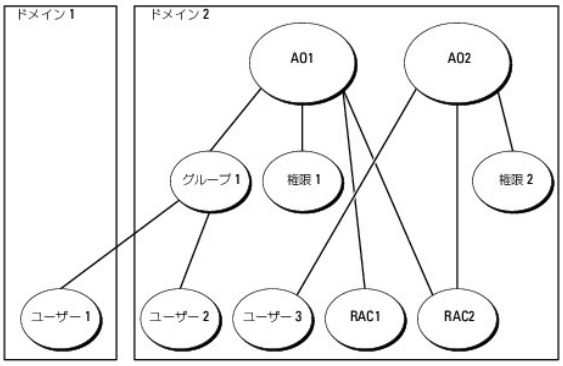
5. グループ 1 をメンバーとして関連オブジェクト 1(AO1)に、権限 1 を権限オブジェクトとして AO1 に、そして RAC1、RAC2 を RAC デバイスとして AO1 にそれぞれ追加します。

6. ユーザー 3 をメンバーとして関連オブジェクト 2(AO2)に、権限 2 を権限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。

詳細については、Active Directory への DRAC 5 ユーザーと権限の追加 を参照してください。

図 6-4 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)あり、既存の Active Directory ユーザーが 3 人(ユーザー 1、ユーザー 2、ユーザー 3)いるとします。ユーザー 1 はドメイン 1 に存在し、ユーザー 2 とユーザー 3 はドメイン 2 に存在しています。このシナリオでは、両方の DRAC 5 カードへの管理者権限を持つユーザー 1 とユーザー 2 を設定し、RAC2 カードへのログイン権限を持つユーザー 3 を設定します。

図 6-4. 複数ドメインでの Active Directory オブジェクトの設定



複数ドメインのシナリオでオブジェクトを設定するには、次の手順を実行してください。

1. ドメインのフォレスト機能がネイティブまたは Windows 2003 モードになっていることを確認します。

2. 2 つの関連オブジェクト (ユニバーサルスコープの)AO1 と AO2 をいずれかのドメインに作成します。

   図 6-4 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 つの権限オブジェクト(権限 1 と権限 2) を作成し、権限 1 にはすべての権限(システム管理者)、権限 2 にはログイン権限を与えます。

5. ユーザー 1 とユーザー 2 をまとめてグループ 1 とします。グループ 1 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. グループ 1 をメンバーとして関連オブジェクト 1(AO1)に、権限 1 を権限オブジェクトとして AO1 に、そして RAC1、RAC2 を RAC デバイスとして AO1 にそれぞれ追加します。

7. ユーザー 3 をメンバーとして関連オブジェクト 2(AO2)に、権限 2 を権限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拡張スキーマ 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 ユーザーおよびコンピュータのスナップイン 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 ユーザーとその権限を Active Directory に追加します(Active Directory への DRAC 5 ユーザーと権限の追加 を参照)。

4. SSL を各ドメインコントローラで有効にします(ドメインコントローラの SSL を有効にする を参照)。

5. DRAC 5 Active Directory プロパティを、DRAC 5 ウェブベースインタフェースまたは RACADM を使用して設定します(拡張スキーマ Active Directory とウェブベースのインタフェースを用いた DRAC 5 の設定 または 拡張スキーマ Active Directory と RACADM を用いたDRAC 5 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、デルの組織単位、スキーマのクラスと属性、サンプル権限、および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には、ドメインフォレストのスキーママスター FSMO(Flexible Single Master Operation)役割所有者のスキーマ Administrator 権限が必要です。

次のいずれかの方法を使用してスキーマを拡張できます。

- Dell Schema Extender ユーティリティ
- 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、Dell の組織単位はスキーマに追加されません。

LDIF ファイルと Dell Schema Extender はそれぞれ『Dell Systems Management Tools and Documentation DVD』の次のディレクトリに入っています。

- DVD **ドライブ:\support\OMActiveDirectory Tools\RAC4-5\LDIF_Files**
- DVD **ドライブ:\support\OMActiveDirectory Tools\RAC4-5\Schema_Extender**

LDIF ファイルを使用するには、**LDIF_Files** 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 Schema Extender の使い方 を参照してください。

Schema Extender または LDIF ファイルのコピーと実行はどの場所からでもできます。

Dell Schema Extender の使い方

△ **注意: Dell Schema Extender は、SchemaExtenderOem.ini ファイルを使用します。Dell Schema Extender ユーティリティが正しく機能するように、このファイルの名前と内容を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. **資格情報で現在のログオンを使用** を選択するか、スキーマ管理者権限でユーザー名とパスワードを入力します。
4. Dell Schema Extender を実行するには、**次へ** をクリックします。
5. **完了** をクリックします。

   スキーマが拡張されます。スキーマの拡張を確認するには、Microsoft Management Console(MMC)と Active Directory スキーマスナップインを使用して、次の存在を確認します。

   - クラス(表 6-2 ～ 表 6-7 を参照)
   - 属性(表 6-8)

   Active Directory スキーマの MMC スナップインを有効にして使用する方法の詳細については、Microsoft のマニュアルを参照してください。

表 6-2. 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	割り当てられた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 6-3. 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。この設定によって DRAC 5 が Lightweight Directory Access Protocol(LDAP)クエリを Active Directory に送信できるようになります。
クラスの種類	構造体クラス
SuperClasses	dellProduct
属性	**dellSchemaVersion** **dellRacType**

表 6-4. 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。この関連オブジェクトはユーザーとデバイスの間の接続を提供します。
クラスの種類	構造体クラス
SuperClasses	グループ
属性	**dellProductMembers** **dellPrivilegeMember**

表 6-5. dellRAC4Privileges クラス

OID	**1.2.840.113556.1.8000.1280.1.1.1.3**
説明	このクラスは DRAC 5 デバイスの権限(許可の権限)を定義するために使用されます。
クラスの種類	補助クラス
SuperClasses	なし
属性	**dellIsLoginUser** **dellIsCardConfigAdmin** **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsConsoleRedirectUser** **dellIsVirtualMediaUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin**

表 6-6. dellPrivileges クラス

OID	**1.2.840.113556.1.8000.1280.1.1.1.4**
説明	デルの権限(許可権限)のコンテナクラスとして使用されます。
クラスの種類	構造体クラス
SuperClasses	ユーザー
属性	**dellRAC4Privileges**

表 6-7. dellProduct クラス

OID	**1.2.840.113556.1.8000.1280.1.1.1.5**
説明	すべてのデル製品が派生するメインクラス。
クラスの種類	構造体クラス
SuperClasses	コンピュータ
属性	**dellAssociationMembers**

表 6-8. Active Directory スキーマに追加された属性のリスト

属性名 / 説明	**割り当てられた OID / 構文オブジェクト識別子**	**単一値**
dellPrivilegeMember	1.2.840.113556.1.8000.1280.1.1.2.1	FALSE

この属性に属する dellPrivilege オブジェクトのリスト。	識別名(LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
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 バックワードリンクへのフォワードリンクです。 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 ユーザーにデバイスへのログイン権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.3 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin ユーザーにデバイスのカード設定権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.4 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin ユーザーにデバイスのユーザー設定権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.5 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin ユーザーにデバイスのログクリア権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.6 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser ユーザーにデバイスのサーバーリセット権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.7 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser ユーザーにデバイスのコンソールリダイレクト権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.8 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser ユーザーにデバイスの仮想メディア権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.9 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser ユーザーにデバイスのテスト警告ユーザー権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.10 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin ユーザーにデバイスのデバッグコマンド管理権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.11 ブール(LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion スキーマのアップデートに現在のスキーマバージョンが使用されます。	1.2.840.113556.1.8000.1280.1.1.2.12 大文字小文字の区別無視の文字列 (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 タイプで dellAssociationObjectMembers フォワードリンクへのバックワードリンクです。	1.2.840.113556.1.8000.1280.1.1.2.13 大文字小文字の区別無視の文字列 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers この製品に属する dellAssociationObjectMembers オブジェクトのリスト。この属性は dellProductMembers リンク属性へのバックワードリンクです。 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スナップインへの Dell 拡張のインストール

Active Directory でスキーマを拡張した場合、Active Directory ユーザーとコンピュータのスナップインも拡張して、RAC(DRAC 5)デバイス、ユーザーおよびユーザーグループ、RAC 関連、および RAC 権限をシステム管理者が管理できるようにする必要があります。

『Dell Systems Management Tools and Documentation DVD』を使ってシステム管理ソフトウェアをインストールする場合、インストール手順中に **Dell Extension to the Active Directory User's and Computers Snap-In** を選択するとスナップインを拡張できます。システム管理ソフトウェアのインストールの手順については、『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する各システムに、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の開始 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開始

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。

1. ドメインコントローラにログインしている場合は、**スタート管理ツール**→ **Active Directory ユーザーとコンピュータ** 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**→ **実行** の順にクリックし、MMC と入力して <**Enter**> を押します。

   Microsoft Management Console(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**（または Windows 2000 が稼動するシステムでは **コンソール**）をクリックします。

3. **スナップインの 追加と削除** 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て **追加** をクリックします。

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 ユーザーと権限の追加

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、権限オブジェクトを作成すると、DRAC 5 ユーザーと権限を追加できます。各オブジェクトタイプを追加するには、次の手順に従います。

- RAC デバイスオブジェクトの作成
- 権限オブジェクトの作成
- 関連オブジェクトの作成
- 関連オブジェクトへのオブジェクトの追加

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**→ **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、拡張スキーマ Active Directory とウェブベースのインタフェースを用いた DRAC 5 の設定 の ステップ a で入力する DRAC 5 の名前と同じである必要があります。

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。

権限オブジェクトの作成

メモ: 権限オブジェクトは、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. **コンソールのルート**(MMC)ウィンドウでコンテナを右クリックします。

2. **新規**→ **Dell RAC オブジェクト** の順に選択します。

   新規オブジェクト 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. **権限オブジェクト** を選択します。

5. **OK** をクリックします。

6. 作成した権限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 権限** タブをクリックして、ユーザーに与える権限を選択します（詳細は 表 5-4 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。関連スコープは関連オブジェクトのセキュリティグループの種類を指定します。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している場合にのみ使用可能になります。

1. **コンソールのルート**（MMC）ウィンドウでコンテナを右クリックします。

2. **新規→ Dell RAC オブジェクト** の順に選択します。

   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、ユーザーまたはユーザーグループ、権限オブジェクト、RAC デバイスまたは RAC デバイスグループ間の関連付けができます。Windows 2000 モード以降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。

ユーザーおよび RAC デバイスのグループを追加できます。デル関連グループとデル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、**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** を選択します。

3. ユーザーまたはユーザーグループの名前を入力し、**OK** をクリックします。

権限オブジェクト タブをクリックして、RAC デバイスに認証するときにユーザーまたはユーザーグループの権限を定義する関連に、権限オブジェクトを追加します。関連オブジェクトに追加できる権限オブジェクトは 1 つだけです。

権限の追加

1. **権限オブジェクト** タブを選択し、**追加** をクリックします。

2. 権限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 台または複数台の 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、次の手順に従います。

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 デバイスグループの名前を入力し、**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。

拡張スキーマ Active Directory とウェブベースのインタフェースを用いた DRAC 5 の設定

1. サポートされているウェブ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** ツリーを拡張し、**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** ページで、**Active Directory の設定** を選択し、**次へ** をクリックします。
6. 共通設定 セクションで以下の操作を行います。
   a. **Active Directory を有効にする** チェックボックスをオンにします。
   b. **ルートドメイン名** を入力します。**ルートドメイン名** はフォレストのルートドメインの完全修飾名です。
   c. **タイムアウト** の時間を秒単位で入力します。
7. Active Directory スキーマの選択セクションで **拡張スキーマの使用** をクリックします。
8. 拡張スキーマの設定セクションで、以下の操作を行います。
   a. **DRAC 名** を入力します。この名前は、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ある必要があります（RAC デバイスオブジェクトの作成 の ステップ 3 を参照）。
   b. **DRAC ドメイン名**（drac5.com など）を入力します。NetBIOS 名を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。
9. **適用** をクリックして Active Directory の設定を保存します。
10. **Active Directory メインメニューに戻る** をクリックします。
11. ドメインフォーレストのルート CA 証明書を DRAC 5 へ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選択し、**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、証明書ファイルの場所まで移動します。

    メモ: アップロードする証明書の相対ファイルパスが **ファイルパス** の値に表示されます。フルパスと正しい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。

    ドメインコントローラの SSL 証明書はルート CA により署名されている必要があります。DRAC 5 にアクセスする管理ステーション上でルート CA 証明書を使用可能にします（ドメインコントローラのルート CA 証明書を DRAC 5 にエクスポートする を参照）。

    c. **適用** をクリックします。

    適用 をクリックすると、DRAC 5 ウェブサーバーが自動的に再起動されます。
12. ログアウトしてからまた DRAC 5 にログインし、DRAC 5 Active Directory 機能の設定を完了します。
13. **システム** ツリーの **リモートアクセス** をクリックします。
14. **設定** タブをクリックし、**ネットワーク** をクリックします。

    ネットワーク設定 ページが開きます。
15. **ネットワーク設定** で **DHCP を使用（NIC IP アドレス用）** が選択されている場合は、**DHCP を使用して DNS サーバーアドレスを取得** を選択します。

    DNS サーバーの IP アドレスを手動で入力するには、**DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスをオフにし、一次および代替 DNS サーバーの IP アドレスを入力します。
16. **変更の適用** をクリックします。

    これで、RAC 5 の拡張スキーマ Active Directory 機能の設定が完了しました。

拡張スキーマ Active Directory と RACADM を用いたDRAC 5 設定

ウェブインタフェースではなく racadm CLI を使用した拡張スキーマで 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。

1. 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 cfgADType 1

   racadm config -g cfgActiveDirectory -o cfgADRacDomain <完全修飾ルートドメイン名>

   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>
   ```

2. DRAC/MC の DHCP が有効になっており、DHCP サーバーが提供する DNS を使用する場合は、次のコマンドを入力します。

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
   ```

3. DRAC 5 で DHCP が無効になっている場合や、手動で DNS IP アドレスを入力する場合は、次の racadm コマンドを入力します。

   ```
   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 機能の設定を完了させます。

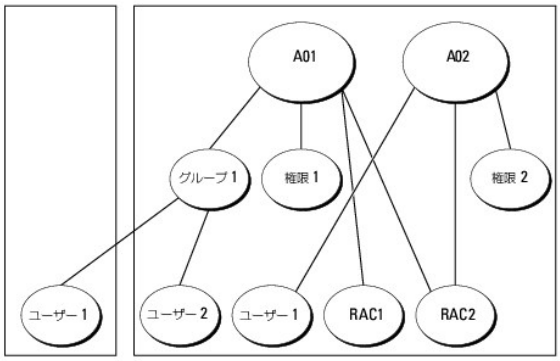
DRAC 5 に Active Directory サーバーを探させる代わりに、DRAC 5 の接続先サーバーを指定して、ユーザーを認証することもできます。サーバーを指定する RACADM コマンドについては、Active Directory 設定のためのサーバー指定 を参照してください。

拡張スキーマを使用した権限の蓄積

拡張スキーマ認証機構は、異なる関連オブジェクトを通して同じユーザーに関連付けられた異なる権限オブジェクトからの権限の蓄積をサポートしています。つまり、拡張スキーマ認証は権限を蓄積して、同じユーザーに関連付けられた異なる権限オブジェクトに対応して割り当てられた権限すべてのスーパーセットをユーザーに許可します。

図 6-5 に、拡張スキーマを使用した権限の蓄積例を示します。

図 6-5. ユーザーの権限の蓄積



この図には、A01 と A02 の 2 つの関連オブジェクトが示されています。これらの関連オブジェクトは、同じドメインまたは異なるドメインの一部とします。ユーザー 1 は、両方の関連オブジェクトを通して RAC1 と RAC2 に関連付けられています。このため、ユーザー 1 は、権限 1 と権限 2 のオブジェクトの権限セットを結合した蓄積権限を持つことになります。

たとえば、権限 1 にログイン、仮想メディア、ログのクリア権限が含まれ、権限 2 にはログイン、DRAC の設定、テストアラートの権限が含まれるとします。この場合、ユーザー 1 には、ログイン、仮想メディア、ログのクリア、DRAC の設定、テスト警告の権限、つまり、Priv1 と Priv2 を組合わせた権限セットが設定されます。

拡張スキーマ認証は、同じユーザーに関連付けられている異なる権限オブジェクトに割り当てられている権限を考慮してこのように権限を蓄積することでユーザーに最大限の権限を与えます。

Active Directory 設定のためのサーバー指定

DNS サーバーが返したサーバーを使用する代わりに LDAP、グローバルカタログサーバー、または関係オブジェクト（拡張スキーマのみに適用）のドメインを指定してユーザー名を検索する場合は、次のコマンドを入力して **サーバーの指定** オプションを有効にします。

```
racadm config -g cfgActive Directory -o cfgADSpecifyServer Enable 1
```

メモ: このオプションを使用すると、CA 証明書のホスト名は指定されたサーバーの名前と適合しません。IP アドレスだけでなくホスト名を入力できるため、これは DRAC システム管理者にとっては特に便利です。

サーバーの指定 オプションを有効にした後、LDAP サーバーまたはグローバルカタログサーバーを IP アドレスまたはサーバーの完全修飾ドメイン名(FQDN)を使用して指定できます。FQDN はサーバーのホスト名とドメイン名で構成されます。

メモ: Kerberos に基づく Active Directory 認証を使用する場合は、サーバーの完全修飾ドメイン名 のみを指定してください。IP アドレスはサポートされていません。詳細については、Kerberos 認証を有効にする方法 を参照してください。

コマンドラインインタフェース(CLI)を使用して LDAP サーバーを指定するには、次のように入力します。

```
racadm config -g cfgActive Directory -o cfgADDomainController <完全修飾されたドメイン名または IP アドレス>
```

コマンドラインインタフェース(CLI)を使用してグローバルカタログサーバーを指定するには、次のように入力します。

```
racadm config -g cfgActive Directory -o cfgGlobalCatalog <完全修飾されたドメイン名または IP アドレス>
```

関連オブジェクト(拡張スキーマのみに適用)のドメインを指定するには、CLI を使用して次のように入力します。

```
racadm config -g cfgActive Directory -o cfgAODomain <ドメイン>:<完全修飾ドメイン名または IP アドレス>
```

<domain> は関連オブジェクトが存在するドメインです。IP/FQDN は、DRAC 5 が接続する特定のホスト(ドメインのドメインコントローラ)の IP アドレスまたは完全修飾ドメイン名です。

関連オブジェクトを指定する場合は、グローバルカタログの IP アドレスまたは完全修飾ドメイン名も必ず入力してください。

メモ: IP アドレスを 0.0.0.0 と指定すると、DRAC 5 はサーバーの検索を実行しません。

LDAP、グローバルカタログサーバー、関連オブジェクトなどのリストをコンマで区切って指定できます。DRAC 5 では、最大 4 個の IP アドレスまたはホスト名を指定できます。

LDAPS がすべてのドメインおよびアプリケーションに対して正しく設定されていないと、DSAPS を有効にしたときに既存のアプリケーション / ドメインの 機能中に予期せぬ結果を招くことがあります。

拡張スキーマの場合は、関連オブジェクトと一緒にドメインコントローラまたはグローバルカタログを指定できます。グローバルカタログのみ、または関連オブジェクトのみの指定は拡張スキーマには適用されません。ドメインコントローラのみを指定する場合、ユーザー、グループ、RAC、権限、関連を含むすべてのオブジェクトが同じドメイン上にあることが必要です。これらのオブジェクトのいずれかが別のドメインにある場合は、関連オブジェクトオプションでグローバルカタログを使用してください。ドメインコントローラは最大 4 つ指定でき、これらのエントリすべてが同じドメインを指す必要があります。グローバルカタログサーバーは最大 4 つ指定できます。関連オブジェクトサーバーは最大 4 つ指定できます。これらすべてのエントリが同じドメインを指す必要があります。関連オブジェクトオプションを使用している場合は、ログインできるようにグローバルカタログオプションも設定する必要があります。ユーザーを作成したドメインコントローラの名前を指定します。IP アドレス または完全修飾ドメイン名もここで指定できます。

標準スキーマの場合は、ドメインコントローラとグローバルカタログのみを指定します。標準スキーマでは関連オブジェクトの指定は適用されません。ユーザー役割グループが作成されるドメインコントローラを指定できます。IP アドレスまたは完全修飾ドメイン名を指定します。ドメインコントローラは最大 4 つ指定できます。これらすべてのエントリが同じドメインを指す必要があります。ドメインコントローラのみを指定する場合は、ユーザーとグループが同じドメイン上にあることが必要です。役割グループが別のドメインにある場合は、グローバルカタログサーバーも指定する必要があります。グローバルカタログサーバーは最大 4 つ指定できます。IP アドレスまたは完全修飾ドメイン名もここで指定できます。グローバルカタログサーバーのみも指定できます。

Active Directory 証明書の設定と管理

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** ツリーを拡張し、**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** をクリックします。

表 6-9に、**Active Directory メインメニュー** ページのオプションを示します。

表 6-9. 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、Active Directory スキーマの選択、役割グループ設定を指定します。
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。

Active Directory の設定(標準スキーマと拡張スキーマ)

1. **Active Directory メインメニュー** ページで、**Active Directory の設定** を選択し、**次へ** をクリックします。

2. **Active Directory の設定と管理** ページで、Active Directoryの設定を入力します。

   表 6-10 に、**Active Directory の設定と管理** ページの設定を示します。

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 6-11 を参照してください。

5. Active Directory 標準スキーマの役割グループを設定するには、個々の役割グループ(1〜5)をクリックします。表 6-12 および 表 6-13 を参照してください。

   メモ: **Active Directory** の設定と管理 ページの設定を保存するには、カスタム役割グループ ページに進む前に 適用 をクリックします。

表 6-10. Active Directory の設定と管理 ページの設定

設定	説明
Active Directory を有効にする	Active Directory を有効にします。オン=有効、オフ=無効
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 **NULL** になっています。 名前はx.y からなる有効なドメイン名とします。ここで、x は空白を含まない 1〜254文字の 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)。最小値は 15 秒です。デフォルト値は 120 秒です。
標準スキーマを使用	Active Directory で標準スキーマを使用します。
拡張スキーマを使用	Active Directory で拡張スキーマを使用します。
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 **NULL** になっています。 名前には空白を含まない 1〜254 文字の ASCII 文字列を使用します。
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**NULL** になっています。 名前はx.y からなる有効なドメイン名とします。ここで、x は空白を含まない 1〜254文字の 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。
役割グループ	DRAC 5 カードに関連付けられている役割グループのリスト。 役割グループの設定を変更するには、役割グループリストでその役割グループの番号をクリックします。**役割グループの設定** ウィンドウが開きます。 **メモ:** **Active Directory の設定と管理** ページの設定を適用する前に役割グループのリンクをクリックすると、その設定は失われてしまいます。
グループ名	この名前によって、DRAC 5 カードに関連した Active Directory の役割グループが識別されます。
グループドメイン	グループが属するドメイン。
グループの権限	グループの権限レベル。

表 6-11. Active Directory の設定と管理 ページのボタン

ボタン	説明
印刷	**Active Directory の設定と管理** ページを印刷します。
適用	**Active Directory の設定と管理** ページに加えた変更を保存します。
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。

表 6-12. 役割グループの権限

設定	説明
役割グループの権限レベル	ユーザーの DRAC ユーザーの最高権限レベルを管理者、パワーユーザー、ゲストユーザー、なし、カスタムのいずれかに指定します。 **役割グループ** パーミッションについては、表 6-13 を参照してください。
DRAC へのログイン	ユーザーに DRAC へのログインを許可します。
DRAC の設定	ユーザーに DRAC の設定を許可します。
ユーザーの設定	ユーザが指定したユーザーのシステムアクセスを許可できるようにします。
ログのクリア	ユーザーに DRAC ログのクリアを許可します。

サーバー制御コマンドの実行	ユーザーに racadm コマンドの実行を許可します。
コンソールリダイレクトへのアクセス	ユーザーにコンソールリダイレクトの実行を許可します。
仮想メディアへのアクセス	ユーザーに仮想メディアの実行と使用を許可します。
テスト警告	ユーザーがテスト警告(E-メールと PET)を特定のユーザーに送信できるようにします。
診断コマンドの実行	ユーザーに診断コマンドの実行を許可します。

表 6-13. 役割グループのパーミッション

プロパティ	説明
管理者	DRAC へのログイン、DRAC の設定、ユーザーの設定、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 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 へのログイン
カスタム	次のパーミッションから任意の組み合わせを選択します。**DRAC へのログイン**、**DRAC の設定**、**ユーザーの設定**、**ログのクリア**、**サーバーアクションコマンドの実行**、**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	パーミッションの割り当てなし

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 証明書のアップロード** を選択し、**次へ** をクリックします。
2. **ファイルパス** フィールドの **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、**参照** をクリックして証明書ファイルに移動します。

   メモ: アップロードする証明書の相対ファイルパスが **ファイルパス** の値に表示されます。フルパスと正しい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 6-11 を参照してください。

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 **DRAC サーバー証明書のダウンロード** 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、ファイルをシステムのディレクトリに保存します。
3. **ダウンロードが完了しました** 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 ページを使って、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 証明書の表示** を選択し、**次へ** をクリックします。

   表 6-14 に、**証明書** ウィンドウに表示されるフィールドと説明を示します。

2. **Active Directory の CA 証明書** ページの適切なボタンをクリックして続行します。表 6-11 を参照してください。

表 6-14. Active Directory CA 証明書の情報

フィールド	説明
シリアル番号	証明書のシリアル番号です。
タイトル情報	タイトルによって入力された証明書の属性です。
発行者情報	発行者によって返された証明書の属性です。

有効期間の開始	証明書の発行日。
有効期間の終了	証明書の有効期限日。

ドメインコントローラの SSL を有効にする

DRAC 5 が Active Directory ドメインコントローラに対してユーザーを認証するとき、ドメインコントローラと SSL セッションを開始します。このとき、ドメインコントローラは認証局 (CA) によって署名された証明書を発行し、そのルート証明書も DRAC 5 にアップロードされます。つまり、DRAC 5 が(ルートか子ドメインコントローラかにかかわらず)どのドメインコントローラに対しても認証できるためには、そのドメインコントローラはそのドメインの CA によって署名された SSL 対応証明書を持っている必要があります。

Microsoft Enterprise のルート CA を使用して自動的にすべてのドメインコントローラ SSL 証明書を割り当てる場合は、次の手順で各ドメインコントローラの SSL を有効にする必要があります。

1. 各コントローラの SSL 証明書をインストールして、各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** をクリックします。
   b. **公開キーのポリシー** フォルダを展開し、**自動証明書要求の設定** を右クリックして **自動証明書要求** をクリックします。
   c. **自動証明書要求の設定ウィザード** 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、**完了** をクリックします。

ドメインコントローラのルート CA 証明書を DRAC 5 にエクスポートする

メモ: システムで Windows 2000 が稼動している場合は、次の手順が異なる可能性があります。

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**(または Windows 2000 マシンでは**コンソール**) をクリックし、**スナップインの追加と削除 を選択します**。
5. **スナップインの追加と削除** 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** を選択して **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て **次へ** をクリックします。
8. **ローカルコンピュータ** を選択して **完了** 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、**パーソナル** フォルダを展開して、**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** を選択してから **エクスポート...** を 選択 します。
12. **証明書のエクスポートウィザード** で **次へ** を選択し、**いいえ、秘密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、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、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 で保存した証明者を DRAC 5 に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場合は、拡張スキーマ Active Directory とウェブベースのインタフェースを用いた DRAC 5 の設定 を参照してください。

    ウェブベースのインタフェースを使って証明書をアップロードする場合は、次の手順を実行します。

    a. サポートされているウェブ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** ツリーを拡張し、**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、**セキュリティ** をクリックします。
    e. **セキュリティ証明書メインメニュー** ページで **サーバー証明書のアップロード** を選択して、**適用** をクリックします。
    f. **証明書のアップロード** 画面で、次のいずれかの手順を実行します。

- **参照** をクリックして、証明書を選択します。
- **値** フィールドで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 ファームウェアの SSL 証明書

メモ: Active Directory サーバーが SSL セッションの初期化段階でクライアントを認証する設定になっている場合、DRAC 5 サーバー証明書を Active Directory ドメインコントローラにもアップロードする必要があります。Active Directory サーバーが SSL セッションの開始段階でクライアントを認証しない場合、この手順は不要です。

DRAC 5 ファームウェア SSL 証明書をすべてのドメインコントローラの信頼できる証明書リストにインポートするには、次の手順を実行します。

メモ: システムで Windows 2000 が稼動している場合は、次の手順が異なる可能性があります。

メモ: DRAC 5 ファームウェアの SSL 証明書がよく知られた CA によって署名されている場合は、ここで説明する手順を省略できます。

DRAC 5 の SSL 証明書は DRAC 5 のウェブ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すべて、デフォルトの自己署名付き証明書が付いています。

DRAC 5 ウェブインタフェースを使用し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**→ **信頼できるルート認証局** 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 証明書ファイルまで参照します。
4. 各ドメインコントローラの **信頼できるルート認証局** に RAC SSL 証明書をインストールします。

   独自の証明書をインストールした場合は、その証明書に署名する CA が **信頼できるルート認証局** リストにあるかどうか確認してください。この認証局がリストにない場合は、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証明書の保存場所を Windows に自動的に選択させるか、保存する場所を指定します。
6. **完了** をクリックして **OK** をクリックします。

DRAC 5 上で SSL 時間を設定する

DRAC 5 が Active Directory ユーザーを認証するとき、DRAC 5 は DRAC が認証済みの Active Directory サーバーと通信していることを確認するために Active Directory サーバーによって発行された証明書の検証も行います。

この検証によって、DRAC 5 で指定した時間枠内で証明書が有効であることの確認もできます。ただし、証明書と DRAC 5 で指定されているタイムゾーンが一致しないことがあります。これは、DRAC 5 の時間がローカルシステム時間を反映しており、証明書が GMT 時間を反映している場合に起こり得ます。

証明書の時間と比較するためにDRAC 5 で GMT 時間を使用するには、タイムゾーンオフセットオブジェクトを設定する必要があります。

```
racadm config -g cfgRacTuning -o cfgRacTuneTimeZoneOffset
<オフセット値>
```

詳細については、cfgRacTuneTimezoneOffset(読み取り / 書き込み) を参照してください。

サポートされている Active Directory の設定

DRAC 5 の Active Directory クエリアルゴリズムは、1 つのフォレスト内の複数のツリーをサポートします。

DRAC 5 の Active Directory 認証は、混在モード(Microsoft Windows NT 4.0、Windows 2000、Windows Server 2003 などの異なるオペレーティングシステムを実行するフォレスト内のドメインコントローラ)をサポートします。ただし、DRAC 5 のクエリプロセスによって使用されるオブジェクト(ユーザー、RAC デバイスオブジェクト、関連オブジェクトなど)のすべてが 同じドメイン内に存在する必要があります。Dell 拡張の Active Directory Users and Computers スナップインはモードをチェックし、混在モードであれば、異なるドメインのオブジェクトを作成するためにユーザーを制限します。

DRAC 5 Active Directory は、ドメインフォレストの機能レベルがネイティブモードあるいは Windows 2003 モードの場合、複数のドメイン環境をサポートします。また、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)にあるグループはユニバーサルグループでなければなりません。

メモ: 関連オブジェクトと権限オブジェクトは同じドメインの中に置く必要があります。この 2 種類のオブジェクトは、Dell 拡張の Active Directory ユーザーとコンピュータのスナップインによって、強制的に同一のドメインに作成されます。その他のオブジェクトは別のドメインに作成することができます。

Active Directory を使用して DRAC 5 にログインする

次のいづれかの方法で、Active Directory を使って DRAC 5 へログインできます。

- 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、3 つの方法にすべて共通です。

<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>*/<*ユーザ名*>

ユーザー名 は 1～256 バイトの ASCII 文字列です。

ユーザー名またはドメイン名に空白スペースと特殊文字(\、/、@ など)は使用できません。

メモ: Americas 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。

スマートカードを使用して DRAC 5 にログインすることもできます。詳細については、スマートカードを使用した DRAC 5 へのログイン を参照してください。

Active Directory シングルサインオンの使い方

DRAC 5 で Kerberos(ネットワーク認証プロトコルの 1 つ)の使用を有効にすると、シングルサインオンで DRAC 5 にログインできるようになります。Active Directory シングルサインオン機能の使用のために DRAC 5 をセットアップする方法の詳細については、Kerberos 認証を有効にする方法 を参照してください。

DRAC 5 にシングルサインオンの使用を設定する方法

1. **リモートアクセス**→ **設定 タブ**→ **Active Directory** サブタブ→ に移動し、**Active Directory の設定** を選択します。
2. **Active Directory の設定と管理** ページで、**シングルサインオン** を選択します。

   このオプションを使用すると、ワークステーションにログインしてから直接 DRAC 5 にログインできます。

シングルサインオンを使用した DRAC 5 へのログイン

1. ネットワークアカウントを使用してワークステーションにログインします。
2. https を使用して DRAC ウェブページにアクセスします。

   https://*<IP アドレス>*

   デフォルトの HTTPS ポート番号(ポート 443)が変更されている場合は、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 DRAC5 の IP アドレスで、*<ポート番号>* は HTTPS のポート番号です。

   DRAC 5 シングルサインオンページが表示されます。
3. **ログイン** をクリックします。

   有効な Active Directory アカウントを使用してログインすると、オペレーティングシステムにキャッシュされている資格情報を使用して DRAC 5 にログインできます。

よくあるお問い合わせ(FAQ)

ドメインコントローラの SSL 設定に何か制限はありますか?

はい。信頼された CA SSL 証明書として DRAC/MC がアップロードを許可するのは 1 つに限られているため、フォレスト内にある Active Directory サーバーの SSL 証明書は、すべて同一の ルート CA によって署名されることが必要です。

新規に RAC 証明書を作成し、アップロードしたら、Web インタフェースが起動しなくなってしまいました。

RAC 証明書の生成に Microsoft 証明書サービスを使用している場合、証明書の作成時に **ウェブ証明書** ではなく誤って **ユーザー証明書** を選択してしまった可能性があります。

回復するには、CSR を生成した後、Microsoft Certificate Service から新しいウェブ証明書を作成し、以下の racadm コマンドを使うことで管理下システムから RACADM CLI を使ってロードしま

す。

```
racadm sslcsrgen [-g] [-u] [-f {filename}]
```

```
racadm sslcertupload -t 1 -f {web_sslcert}
```

Active Directory 認証を用いて DRAC 5 にログインできないのですが、どうすればよいでしょうか?この問題はどのようにトラブルシューティングできますか?

1. ログインに NetBIOS 名でなく、正しいユーザードメイン名が使用されていることを確認します。
2. ローカル DRAC ユーザーアカウントを持っている場合は、ローカル資格証明書を使って DRAC 5 にログインします。

   ログインした後、次を行います。

   a. DRAC 5 Active Directory 設定 ページの **Active Directory を有効にする** ボックスが選択済みであることを確認します。
   b. DRAC 5 ネットワーク設定ページの DNS 設定が正しく行われていることを確認します。
   c. 使用する Active Directory ルート CA から DRAC 5 へ Active Directory 証明書がアップロード済みであることを確認します。
   d. 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。
   e. **DRAC 名**、**ルートドメイン名**、および **DRAC/MC 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。
   f. DRAC 5 パスワードが 127 文字以内であることを確認します。DRAC 5 は 256 文字までのパスワードをサポートできますが、Active Directory は 127 文字までしかサポートしていません。

Windows 7 オペレーティングシステムでの Active Directory ユーザーによる SSO ログインに失敗します。これを解決するにはどうすればよいですか?

Windows 7 の暗号タイプを有効化する必要があります。暗号タイプを有効化するには、次の手順を実行します(標準および拡張スキーマ向け)。

1. システム管理者としてログインするか、管理者権限を持つユーザーとしてログインします。
2. **スタート** から **gpedit.msc** を実行します。

   ローカルグループポリシーエディタ ウィンドウが開きます。
3. **ローカルコンピュータ設定**→ **Windows 設定**→ **セキュリティ設定**→ **ローカルポリシー**→ **セキュリティオプション** の順に選択します。
4. **ネットワークセキュリティ: kerberos に許可される暗号化方式の設定** を右クリックして、**プロパティ** を選択します。
5. 全オプションを有効化して、**OK** をクリックします。

   これで、SSO を使用して iDRAC にログインできます。
6. **ローカルグループポリシーエディタ** ウィンドウで、**ローカルコンピュータの設定**→ **Windows 設定**→ **セキュリティ設定**→ **ローカルポリシー**→ **セキュリティオプション** の順に選択します。
7. **ネットワークセキュリティ: NTLM の制限 :リモートサーバーへの発信 NTLM トラフィック** を右クリックして **プロパティ** を選択します。
8. **すべて許可** を選択し、**OK** をクリックしてから、**ローカルグループポリシーエディタ** ウィンドウを閉じます。
9. **スタート** から **cmd** を実行します。

   コマンドプロンプト ウィンドウが表示されます。
10. `gpupdate /force` コマンドを実行します。

    グループポリシーが更新されます。
11. **コマンドプロンプト** ウィンドウを開きます。

拡張スキーマでは、次の追加設定を行います。

1. **スタート** から **regedit** を実行します。

   レジストリエディタ ウィンドウが表示されます。
2. **HKEY_LOCAL_MACHINE**→ **システム**→ **CurrentControlSet**→ **制御**→ **LSA** と移動します。
3. 右ペインで、**新規**→ **DWORD(32 ビット)値** を右クリックします。
4. 新しいキーを **SuppressExtendedProtection** と名付けます。

5. **SuppressExtendedProtection** を右クリックして、**変更** をクリックします。
6. **値データ** フィールドに **1** を入力して **OK** をクリックします。
7. **レジストリ エディタ** ウィンドウを閉じます。

   これで、SSO を使用して iDRAC にログインできます。

目次に戻る

目次に戻る

Kerberos 認証を有効にする方法

Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

Kerberos は、セキュリティ保護されていないネットワークでシステムが安全に通信できるようにするネットワーク認証プロトコルです。これは、システムが本物であることをシステム自体が証明できるようにすることで、達成されます。

Microsoft Windows 2000、Windows XP、Windows Server 2003、Windows Vista、および Windows Server 2008 では、Kerberos をデフォルト認証方式として採用しています。

DRAC 5 バージョン 1.40 以降、DRAC 5 は Kerberos を使用して 2 種類の認証メカニズム(シングルサインオンと Active Directory スマートカードログイン)をサポートしています。シングルサインオンでは、ユーザーが有効な Active Directory アカウントでログインした後、オペレーティングシステムにキャッシュされているユーザー資格情報が使用されます。

DRAC 5 バージョン 1.40 以降、Active Directory 認証では有効な資格情報として、ユーザー名とパスワードの組み合わせに加えて、スマートカードベースの 2 要素認証(TFA)も使用されます。

Kerberos 認証を設定するための前提条件

- DRAC 5 に Active Directory ログインを設定します。詳細については、Active Directory を使用して DRAC 5 にログインする を参照してください。
- Kerberos 認証を提供する Active Directory ユーザーに対しては、次のプロパティを設定します。
  - このアカウントに DES 暗号化を使用する
  - Kerberos の事前認証は不要
- Active Directory のルートドメインに DRAC 5 をコンピュータとして登録します。
  a. **リモートアクセス**→ **設定** タブ→ **ネットワーク** サブタブ→ **ネットワーク設定** に移動します。
  b. 有効な **使用する / 静的 DNS サーバー** の IP アドレスを入力します。この値は、ルートドメインの一部である DNS の IP アドレスで、ユーザーの Active Directory アカウントを認証します。
  c. **DNS に DRAC を登録する** を選択します。
  d. 有効な **DNS ドメイン名** を入力します。

  メモ: DNS 名が DNS サーバーによって解決されていることを確認します。

  詳細については、『DRAC 5 オンラインヘルプ』を参照してください。
- DRAC 5 の時刻設定を Active Directory ドメインコントローラの時刻設定と同期します。DRAC の時刻がドメインコントローラの時刻と異なる場合は、DRAC 5 の Kerberos 認証に失敗します。最大 5 分のオフセットが許可されています。認証に成功するには、サーバーの時刻をドメインコントローラの時刻と同期してから DRAC の時刻を **リセット** してください。

  次の RACADM タイムゾーンオフセットコマンドを使用して時刻を同期することもできます。

  ```
  racadm config -g cfgRacTuning -o

  cfgRacTuneTimeZoneOffset オフセット値
  ```

  Offset value には、オフセット時間(分単位)を指定します。
- クライアントシステムに Microsoft Visual C++ 2005 再配布可能パッケージをインストールします。
- Active Directory サーバーで **ktpass** ユーティリティを実行します。

  DRAC 5 は 非 Windows オペレーティングシステムのデバイスであるため、DRAC 5 を Active Directory のユーザーアカウントにマッピングするドメインコントローラ(Active Directory サーバー)で、**ktpass** ユーティリティ(Microsoft Windows の一部)を実行する必要があります。これには、次の操作を行います。

  a. Active Directory 管理ツールを起動します。
  b. **ユーザー** フォルダを右クリックし、**新規** を選択してから **ユーザー** をクリックします。
  c. Kerberos サポートを追加したい DRAC5 ホストの名前を入力します。
  d. ユーザーを保存します。
  e. コマンドプロンプトを開き、次のコマンドを入力します。

  ```
  C:\>ktpass -princ HOST/dracname.domain-name.com@DOMAIN-NAME.COM -mapuser account -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass
  password -out c:\krbkeytab
  ```

  ここで、

  - dracname は DRAC 5 の DNS 名です。
  - domain-name は、認証したい Active Directory ドメイン名です。これを、実際のドメイン名(大文字)と入れ替えてください。
  - account はユーザー名で、Active Directoryの 手順 b および手順 c で作成した有効なユーザーアカウントです。ユーザー名の入力形式は *domain-name.com/user-name* です。

- password はユーザーアカウント用のパスワードです。
- DES-CBC-MD5 は Kerberosis 認証のために DRAC 5 が使用する暗号タイプです。
- KRB5_NT_PRINCIPAL はプリンシパルタイプです。

f. これで生成したキータブファイルを DRAC 5 ホストにアップロードします。

メモ: 最新の **ktpass** ユーティリティを使用して keytab ファイルを作成することをお勧めします。

この手順によって、DRAC 5 にアップロードする keytab ファイルが生成されます。

メモ: keytab には暗号キーが含まれているため、安全な場所に保管してください。

ktpass ユーティリティの詳細については、次の Microsoft ウェブサイトを参照してください。**http://technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true**

DRAC 5 用の Kerberos 認証に使用する DRAC 5 を設定する方法

Active Directory のルートドメインから取得した keytab を DRAC 5 にアップロードします。

1. **リモートアクセス**→ **設定** タブ→ **Active Directory** サブタブと移動します。
2. **Kerberos Keytab のアップロード** を選択し、**次へ** をクリックします。
3. **Kerberos keytab のアップロード** ページで、アップロードする keytab ファイルを選択し、**適用** をクリックします。

目次に戻る

目次に戻る

シングルサインオンの有効化

Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

シングルサインオンを使用すると、有効な Active Directory アカウントを使ってオペレーティングシステムにログインした後で、資格情報を入力せずに DRAC にログインできます。この場合、DRAC はオペレーティングシステムにキャッシュされた資格情報を使用します。DRAC はシングルサインオン用のネットワーク認証プロトコル Kerberos を使用します。

シングルサインオンを設定するための前提条件

- DRAC 5 に Active Directory ログインを設定します。詳細については、Active Directory を使用して DRAC 5 にログインするを参照してください。
- DRAC 5 用の Kerberos 認証を設定します。詳細については、Kerberos 認証を有効にする方法を参照してください。

DRAC 5 にシングルサインオンの使用を設定する方法

1. **リモートアクセス**→ **設定** タブ→ **Active Directory** サブタブと移動し、**Active Directory の設定** を選択します。
2. **Active Directory の設定と管理** ページで、**シングルサインオン** を選択します。

   このオプションを使用すると、ワークステーションにログインしてから直接 DRAC 5 にログインできます。

シングルサインオンを使用した DRAC 5 へのログイン

メモ: DRAC 5 にログインするには、Microsoft Visual C++ 2005 Libraries の最新の実行時コンポーネントがあることを確認してください。詳細については、Microsoft のウェブサイトを参照してください。

1. Active Directory の有効なアカウントを使ってシステムにログインします。
2. ブラウザのアドレスバーに DRAC 5 のウェブアドレスを入力します。

   メモ: ブラウザの設定によっては、この機能を最初に使用するときに Single Sign-On ActiveX プラグインのダウンロードとインストールを要求される場合があります。

   DRAC 5 へのログインが完了しました。

目次に戻る

目次に戻る

スマートカード認証の設定

Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

Dell Remote Access Controller 5 (DRAC 5) バージョン 1.30 以降では、DRAC 5 のウェブインタフェースへのログイン用に 2 要素認証がサポートされています。このサポートは DRAC 5 の **スマートカードログオン** 機能によって提供されています。

従来の認証方式では、ユーザーの認証にユーザー名とパスワードを使用しますが、これは最小限のセキュリティしか提供しません。

一方、2 要素認証ではユーザーがパスワードまたは PIN とデジタル証明書用の秘密鍵を持っている必要があるので、高レベルのセキュリティを実現できます。

2 要素認証では、ユーザーが両方の要素を提供して身元を証明する必要があります。

DRAC 5 へのスマートカードログインの設定

リモートアクセス→ 設定→ スマートカード の順に選択して、DRAC 5 スマートカードログイン機能を有効にします。

- スマートカードの設定を **無効にする** 場合、Microsoft Active Directory またはローカルログオン用のユーザー名とパスワードの入力が要求されます。
- スマートカードを **有効 にする** または **リモート racadm で有効にする** 場合、GUI を使っての以降のログイン時にスマートカード を使うように求められます。

  有効にする を選択すると、telnet、ssh、シリアル、リモート racadm、IPMI オーバー LAN などのコマンドラインインタフェース (CLI) の帯域外インタフェースはすべて無効になります。これは、これらのサービスは単一要素認証しかサポートしないからです。

  リモート racadm で有効にする を選択すると、CLI 帯域外インタフェース(リモート racadm 以外)はすべて無効になります。

  メモ: デルでは、DRAC 5 管理者はリモート racadm コマンドを使ってスクリプトを実行する DRAC 5 ユーザーインタフェースにアクセスするときにのみ **リモート racadm で有効にする** 設定を使うことを推奨しています。リモート racadm を使用する必要がないときは、スマートカードログインを **有効にする** 設定を選択してください。また、DRAC 5 のローカルユーザー設定や Active Directory の設定が完了してから、**スマートカードログオン** を有効にしてください。

- **スマートカードログオン用CRL チェックを有効にする**:証明書失効リスト(CRL)配信サーバーからダウンロードしたユーザーの DRAC 証明書に照合してチェックします。

  メモ: CRL 配信サーバーのリストがユーザーのスマートカード証明書に表示されています。

スマートカードログイン用にローカル DRAC 5 ユーザーを設定する

ローカル DRAC 5 ユーザーがスマートカードを使って DRAC 5 にログインするように設定できます。**リモートアクセス→ 設定→ ユーザー** の順に選択します。

ただし、ユーザーがスマートカードを使用して DRAC 5 にログインするには、まずユーザーのスマートカード証明書と信頼されている認証局(CA)の証明書を DRAC 5 にアップロードする必要があります。

スマートカード証明書のエクスポート

カード管理ソフトウェア(CMS)を使ってスマートカード証明書をスマートカードから Base64 符号化形式ファイルにエクスポートすることでユーザーの証明書を取得できます。CMS は通常、スマートカードのベンダーから入手できます。この符号化ファイルをユーザーの証明書として DRAC 5 にアップロードしてください。スマートカードのユーザー証明書を発行する信頼される認証局も、CA 証明書を Base64 エンコード形式でファイルにエクスポートする必要があります。ユーザー用の信頼される CA 証明書としてこのファイルをアップロードします。スマートカード証明書内でユーザーのユーザープリンシプル名(UPN)を形成するユーザー名でユーザーを設定します。

メモ: DRAC 5 にログインするには、DRAC 5 で設定するユーザー名が、大文字と小文字の区別を含めてスマートカード証明書の User Principle Name(UPN) と同じでなければなりません。

たとえば、スマートカード証明書が「sampleuser@domain.com」というユーザーに発行された場合、ユーザー名は「sampleuser」となります。

スマートカードログイン用に Active Directory ユーザーを設定する

Active Directory ユーザーがスマートカードを使って DRAC 5 にログインできるように設定するには、DRAC 5 管理者は DNS サーバーを設定して、Active Directory CA 証明書を DRAC 5 にアップロードし、Active Directory ログオンを有効にします。Active Directory ユーザーの設定方法については、Microsoft Active Directory での DRAC 5 の使い方 を参照してください。

Active Directory と Kerberos を Smart Card Active Directory ログイン用に設定する必要があります。設定方法については、Microsoft Active Directory での DRAC 5 の使い方 と Kerberos 認証を有効にする方法 を参照してください。

ローカル DRAC ユーザーの場合は、適切な特権で DRAC にログインします。

次の場合は、適切な Microsoft Active Directory 特権で DRAC にログインします。

- Microsoft Active Directory のユーザーである
- DRAC で Active Directory ログインが設定されている
- DRAC で Kerberos Active Directory 認証が有効になっている

スマートカードの設定

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。

1. **システム** ツリーを拡張し、**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、**スマートカード** をクリックします。
3. スマートカードのログオン設定を指定します。

   表 9-1 に、**スマートカード** ページの設定を示します。
4. **変更の適用** をクリックします。

表 9-1. スマートカードの設定

設定	説明
スマートカードログオンの設定	- 無効 - スマートカードログオンを無効にします。以降、グラフィカルユーザーインタフェース（GUI）からログインすると、通常のログインページが表示されます。セキュアシェル（SSH）、Telnet、シリアル、リモート RACADM を含むすべての帯域外インタフェースはデフォルト状態に戻ります。 - 有効 - スマートカードログオンを有効にします。変更を適用した後、ログアウトし、スマートカードを挿入して PIN を入力し、**ログイン** をクリックして DRAC にログインします。スマートカードログインを有効にすると、SSH、Telnet、シリアル、リモート RACADM、IPMI オーバー LAN を含むすべての CLI 帯域外インタフェースにできなくなります。 - リモート RACADM と共に有効にする - スマートカードログオンとリモート RACADM を有効にします。その他の CLI 帯域外インタフェースがすべて無効になります。 **メモ:** スマートカードログインにはローカル DRAC ユーザーを適切な証明書で設定することが必要です。スマートカードログオンを Microsoft Active Directory ユーザーのログインに使用する場合は、そのユーザーの Active Directory ユーザー証明書を設定する必要があります。ユーザー証明書は、**ユーザー→ ユーザーメインメニュー** ページで設定できます。
スマートカードログオンの CRL チェックを有効にする	このチェックはスマートカードのローカルユーザーにのみ使用可能です。このオプションは、ユーザーのスマートカード証明書を失効させるために DRAC 5 で証明書失効リスト（CRL）をチェックする場合に選択します。CRL が機能するには、ネットワーク構成の過程で DRAC に DNS の有効な IP アドレスが設定されている必要があります。DRAC の **リモートアクセス→ 設定→ ネットワーク** で DNS の IP アドレスを設定できます。 以下の場合には、ユーザーはログインできません。 - ユーザー証明書が CRL ファイルのリストで失効となっている。 - DRAC が CRL 配信サーバーと通信できない。 - DRAC が CRL をダウンロードできない。 **メモ:** このチェックに成功するには、**設定→ ネットワーク** ページで DNS サーバーの IP アドレスを正しく設定する必要があります。

スマートカードを使用した DRAC 5 へのログイン

スマートカードログイン機能を有効にした場合は、DRAC 5 のウェブインタフェースに、スマートカードログインページが表示されます。

メモ: ユーザー用のスマートカードログオンを有効にする前に、DRAC 5 のローカルユーザーと Active Directory の設定が完了していることを確認してください。

メモ: ブラウザの設定によっては、この機能を初めて使うときに、スマートカードリーダー ActiveX プラグインをダウンロードしてインストールするように要求される場合があります。

1. https を使用して DRAC 5 のウェブページにアクセスします。

   `https://<IP アドレス>`

   デフォルトの HTTPS ポート番号（ポート 443）が変更されている場合は、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 DRAC5 の IP アドレスで、<ポート番号> は HTTPS のポート番号です。

DRAC 5 **ログイン** ページが表示され、スマートカードの挿入を要求されます。

2. スマートカードをリーダーに挿入し、スマートカードの PIN を入力します。
3. **ログイン** をクリックします。

メモ: Active Directory ユーザーで **スマートカードログオンの CTL チェックを有効にする** が選択されていれば、DRAC 5 はダウンロードを試みます。証明書が CRL に失効と表示されているか、何らかの理由で CRL をダウンロードできない場合は、Active Directory を通したログインに失敗します。スマートカードログオンは、Microsoft Internet Explorer でのみサポートされています。

Active Directory スマートカード認証を使用した DRAC 5 へのログイン

1. https を使用して DRAC 5 にログインします。

   https://*<IP アドレス>*

   デフォルトの HTTPS ポート番号(ポート 443)が変更されている場合は、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 DRAC5 の IP アドレスで、<ポート番号> は HTTPS のポート番号です。

   DRAC 5 ログイン ページが表示され、スマートカードの挿入を要求されます。

2. スマートカードをリーダーに挿入し、スマートカードの PIN を入力します。
3. **ログイン** をクリックします。

   Active Directory に設定した資格情報で DRAC 5 にログインします。詳細については、Kerberos 認証を有効にする方法 を参照してください。

DRAC 5 へのスマートカードログインのトラブルシューティング

以下は、スマートカードにアクセスできないときのデバッグに役立つヒントです。

ActiveX プラグインがスマートカードリーダーを検出しません

スマートカードが Microsoft Windows オペレーティングシステムでサポートされていることを確認します。Windows がサポートしているスマートカード暗号サービスプロバイダ(CSP)の数は限られています。

ヒント:スマートカード CSP が特定のクライアントに含まれているかどうかを確認する一般的なチェックとして、Windows のログオン(Ctrl-Alt-Del) 画面で、スマートカードをリーダーに挿入し、Windows でスマートカードが検出され、PIN ダイアログボックスが表示されるかどうかを調べます。

間違ったスマートカード PIN

間違った PIN でログインを試みた回数が多すぎるためにスマートカードがロックアウトされたかどうかをチェックします。このような場合は、新しいスマートカードの入手方法について、組織のスマートカード発行者に問い合わせてください。

ローカル DRAC 5 へのログインを無効にする

ローカル DRAC 5 ユーザーがログインできない場合、DRAC 5 にアップロードしたユーザー名とユーザー証明書をチェックします。DRAC 5 追跡ログによって、エラーに関する重要なログメッセージが得られることがあります。ただし、セキュリティ上の理由でエラーメッセージは内部的で、曖昧なものになっている場合があります。

Active Directory ユーザーとして DRAC 5 にログインできません

Active Directory ユーザーとして DRAC 5 にログインできない場合は、スマートカードログオンを有効にしないで DRAC 5 にログインしてみてください。CRL チェックを有効にしている場合は、CRL チェックを有効にしない状態で Active Directory にログインしてみてください。DRAC 5追跡ログには、CRL が失敗したときの重要なメッセージが入っています。

次のコマンドを使用してローカル racadm からスマートカードログオンを無効にすることもできます。

```
racadm config -g cfgActiveDirectory -o cfgADSmartCardLogonEnable 0
```

目次に戻る

目次に戻る

GUI コンソールリダイレクトの使い方

Dell Remote Access Controller 5 ファームウェアバージョン 1.60 ユーザーズガイド

ここでは、DRAC 5 コンソールリダイレクト機能の使用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うと、ローカルコンソールにグラフィックまたはテキストモードでリモートアクセスできます。コンソールリダイレクトを使うと、1 箇所から 1 つまたは複数の DRAC 5 対応システムを制御できます。

今日では高度なネットワークとインターネットの技術を利用することで、1 台 1 台サーバーの前に座って定期メンテナンスを実行する必要はなくなりました。別の町や地球の反対側にいても、デスクトップやラップトップからサーバーを管理できます。また、リモートから即座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い方

メモ: コンソールリダイレクトセッションを開始しても、管理下システムはそのコンソールがリダイレクトされていることを表示しません。

コンソールリダイレクト ページは、ローカル管理ステーション側のキーボード、ビデオ、マウスを使って、リモート管理下システム側の対応するデバイスを制御するリモートシステムを管理するためのものです。この機能を仮想メディア機能と併用すると、リモートでソフトウェアのインストールを実行できます。

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。

- 同時コンソールリダイレクトセッションは 4 セッションまでしかサポートされていません。
- コンソールリダイレクトセッションの接続可能な対象システムは 1 つだけです。
- ローカルシステムでコンソールリダイレクトセッションを設定することはできません。
- 1 MB/秒以上 のネットワーク帯域幅が必要です。

管理下システムでサポートされている画面解像度とリフレッシュレート

表 10-1 に、管理下システムで実行されているコンソールリダイレクトセッションでサポートされている画面解像度と対応するリフレッシュレートを示します。

表 10-1. サポートされている画面解像度と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。対応ウェブブラウザのリストについては、デルサポートウェブサイト **support.dell.com / manuals** で『Dell システムソフトウェアサポートマトリックス』を参照してください。

注意: コンソールリダイレクトと 仮想メディア がサポートしているのは 32 ビットのウェブブラウザのみです。64 ビットのウェブブラウザを使用すると、予期しない結果やエラーが生じることがあります。

- 対応ウェブブラウザの設定

2. モニターは、最低限解像度 1280 x 1024 ピクセル、60 Hz、128 色に設定してください。これ以下の設定では、**全画面モード** でコンソールを表示できないことがあります。
3. Java プラグインを使用して接続している場合は、システムに Java 仮想マシン(JVM)バージョン 1.6 アップデート 21 以降がインストールされていることを確認してください。

コンソールリダイレクトの設定

1. 管理ステーションで、対応ウェブブラウザを開いて DRAC 5 にログインします。詳細については、ウェブベース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** ツリーの **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、**設定** 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 10-2 の情報を使ってコンソールリダイレクトセッションを設定します。
5. DRAC 5 バージョン 1.40 以降では、**ネイティブ** またはインストールする **Java** プラグインタイプを選択できます。
6. **変更を適用** をクリックして設定を保存します。

メモ: 仮想コンソール設定の変更はいずれも、既存のユーザー仮想コンソールセッションに影響を及ぼすか、接続を切断します。

表 10-2. 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	使用可能なコンソールリダイレクトセッションの数が表示されます。
アクティブセッション数	現在アクティブなコンソールリダイレクトセッションの数が表示されます。
キーボードとマウスのポート番号	デフォルト = 5900
ビデオポート番号	デフォルト = 5901
ビデオ暗号化有効	オン = 有効、オフ = 無効
ローカルサーバービデオ有効	オン = 有効、オフ = 無効
プラグインタイプ	**ネイティブ**(Windows 用 ActiveX と Linux 用 XPI プラグイン)または **Java** プラグインを選択できます。 **メモ:** Java プラグインを選択する場合は、お使いのシステムに Java 仮想マシン(JVM)バージョン 1.6 アップデート 21 以降がインストールされていることを確認してください。
コンソール共有のためのデフォルトアクセス	1 番目のユーザーがコンソールに接続されている時に、コンソールへアクセスしようとする 2 番目のユーザーのコンソール共有要求に対する、コンソール共有アクセス権限のデフォルトタイプを選択します。アクセスのパーミッションは次の通りです。 • **アクセス不可** - 2 番目のユーザーにアクセスを許可しません。 • **読み取り専用アクセス** - 2 番目のユーザーに読み取り専用アクセスを許可します。 • **完全アクセス** - 2 番目のユーザーに完全なアクセスを許可します。

表 10-3 のボタンは **コンソールリダイレクト設定** ページにあります。

表 10-3. コンソールリダイレクトの設定ページのボタン

プロパティ	説明
印刷	**コンソールリダイレクト設定** ページを印刷します。
更新	**コンソールリダイレクト設定** ページを再ロードます。
変更の適用	設定を保存します。

メモ: DRAC 5 バージョン 1.30 以降では、リモートユーザーによるコンソールリダイレクトを無効にすることができます。詳細については、を参照してください。DRAC 5 リモート仮想 KVM を無効にする

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セッションを開くと、Dell デジタル KVM 表示アプリケーションが起動され、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。このデジタル KVM 表示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およびキーボード機能を制御することができます。

コンソールリダイレクトセッションを開始するには、次の手順を実行します。

1. 管理ステーションで、対応ウェブブラウザを開いて DRAC 5 にログインします。詳細については、ウェブベース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** をクリックして、**コンソール** タブで **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して実行することを指示するセキュリティ警告が表示された場合は、プラグインの真正性を確認した後 **はい** をクリックしてプラグインをインストールし、実行してください。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、表 10-4 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使用可能であることを確認します。

表 10-4. コンソールリダイレクトページの情報

プロパティ	説明
コンソールリダイレクト有効	はい / いいえ
ビデオ暗号化 有効	はい / いいえ
ローカルサーバービデオ有効	はい / いいえ
状態	接続または切断
最大セッション数	サポートされるコンソールリダイレクトセッションの最大数
アクティブセッション数	現在アクティブなコンソールリダイレクトセッションの数
プラグインタイプ	**コンソールコンソールリダイレクトの設定** ページで選択したプラグインタイプ。
コンソール共有のためのデフォルトアクセス	1 番目のユーザーがコンソールに接続されている時に、2 番目のユーザーの要求に対する、コンソール共有アクセス権限のデフォルトタイプです。アクセスのパーミッションは次の通りです。 • **アクセス不可** - 2 番目のユーザーにアクセスが拒否されることを示します。 • **読み取り専用アクセス** - 2 番目のユーザーに対する読み取り専用アクセスを示します。 • **完全アクセス** - 2 番目のユーザーに対する完全なアクセスを示します。

コンソールリダイレクト ページには、表 10-5 に示すボタンがあります。

表 10-5. コンソールリダイレクトページのボタン

ボタン	定義
更新	**コンソールリダイレクトの設定** ページを再ロードします。
接続	目的の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を開始します。
印刷	**コンソールリダイレクトの設定** ページを印刷します。

4. 新しいコンソールを開くには、**接続** をクリックします。

メモ: DRAC 5 は 4 つの同時コンソールリダイレクトをサポートします。セッションを開いているときに、別のユーザーが同じ管理下システムで別のセッションを開こうとすると、ユーザーにアクセス権限を付与するかどうかを求めるリクエストが送信されます。アクセス権限は許可または拒否できます。30 秒以内にアクセス権限を許可しないと、リクエストは無効になります。

Firefox ブラウザを使用している場合は、JNLP ファイルを開くか保存するように求められます。このファイルは、Java Web Start Launcher を使用して開くことができます。JNLP ファイルを保存する場合は、セッションを切断する前に手動で開きます。いったんセッションを切断すると、保存した JNLP ファイルを確認できません。Internet Explorer を使用している場合、JNLP ファイルはインターネット一時ファイルフォルダにキャッシュされ、Java Web Start Launcher を使用して自動的に実行されます。

メモ: 次の手順の途中で **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。

コンソールを使い終わり、(リモートシステムのログアウト手順を使用して)ログアウトすると、コンソールリダイレクトページで **切断** をクリックするかビューアを終了します。

管理ステーションが DRAC 5 に接続されて、リモートシステムのデスクトップが Dell デジタル KVM 表示アプリケーションに表示されます。

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させてください。マウスポインタの同期 を参照してください。

ローカルビデオを有効または無効にする

ローカルビデオを有効または無効にするには、次の手順を実行します。

1. 管理ステーションで、対応ウェブブラウザを開いて DRAC 5 にログインします。詳細については、ウェブベース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** ツリーの **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、**設定** をクリックします。
4. サーバー上でローカルビデオを有効にする(オンにする)には、**コンソールリダイレクトの設定** ページで **ローカルサーバービデオ有効** チェックボックスを選択してから **変更の適用** をクリックします。デフォルト値はオンです。
5. サーバー上でローカルビデオを無効にする(オフにする)には、**コンソールリダイレクトの設定** ページで **ローカルサーバービデオ有効** チェックボックスを選択解除してから **変更の適用** をクリックします。

コンソールリダイレクト ページにローカルサーバービデオのステータスが表示されます。

メモ: ローカルサーバービデオ有効機能は、PowerEdge SC1435 と 6950 以外のすべての x9xx PowerEdge システムでサポートされています。

メモ: サーバー上でローカルビデオを無効にする(オフにする)と、ローカルサーバーに接続されているモニターのみ無効になります。

メモ: DRAC 5 バージョン 1.30 以降では、リモートユーザーによるコンソールリダイレクトを無効にすることができます。詳細については、を参照してください。DRAC 5 リモート仮想 KVM を無効にする

ビデオビューアの使い方

ビデオビューアによって管理ステーションとリモートシステムの間のユーザーインタフェースを提供することで、管理ステーションからリモートシステムのデスクトップを表示し、そのマウスやキーボード機能を制御することができます。リモートシステムに接続すると、ビデオビューアが別のウィンドウで開きます。

ビデオビューアは、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、様々な制御調整機能を提供します。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セッションを開始し、ビデオビューア ウィンドウが表示されたら、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。調整内容には次が含まれます。

- ビューアメニューバーへのアクセス
- ビデオ画質の調整
- マウスポインタの同期

ビューアメニューバーへのアクセス

ビデオメニューバーは非表示のメニューバーです。このメニューバーにアクセスするには、カーソルをビューアのデスクトップウィンドウの上端の中央あたりに移動します。

また、デフォルトファンクションキー <F9> を押すことでもメニューバーをアクティブにすることができます。ファンクションキーに新しい機能を再割り当てするには、次の手順を実行します。

1. <F9> を押すか、カーソルをビデオビューアの上部に移動します。
2. 「押しピン」を押して、ビューアメニューバーをロックします。
3. ビューアメニューバーで、**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、**全般** タブをクリックします。
5. **全般** タブで **メニューアクティブ化キー** ボックスのドロップダウンメニューから別のファンクションキーを選択します。
6. **適用** をクリックして、**OK** をクリックします。

表 10-6 に、ビューアメニューバーで使用できる主な機能を示します。

表 10-6. ビューアメニューバーの選択項目

メニュー項目	項目	説明
ファイル	ファイルへの取り込み	現在のリモートシステム画面をローカルシステム上の **.bmp**(Windows)または **.png**(Linux)ファイルに取り込みます。ダイアログボックスが表示され、指定した場所にファイルを保存できます。
	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	リモートシステムの画面ビューポート全体を更新します。
	全画面	セッション画面をウィンドウから全画面に拡張します。
マクロ	各種のショート	リモートシステムでキーの組み合わせを実行します。

	カットキー	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、次の手順に従います。 1. **ツール** をクリックします。 2. **セッションオプション** ウィンドウで、**全般** タブをクリックします。 3. **全キー操作をターゲットに反映** 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で実行したいキーの組み合わせをクリックしてします。
ツール	ビデオの自動調整	セッションビューアビデオ出力を再調整します。
	ビデオの手動調整	セッションビューア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を提供します。 **メモ:** 水平位置を調整すると、マウスポインタとの同期がずれます。
	セッションオプション	追加のセッションビューアコントロールの調整を提供します。 **マウス** タブを使用すると、オペレーティングシステムに応じてマウスの性能を最適化できます。 単一カーソルモードを終了するには、ドロップダウンメニューからキーストロークの終了を選択します。**キーストロークの終了** オプションは、プラグインタイプが **Java** の場合に使用できます。 **全般** タブには次のオプションがあります。 • **キーボードパススルーモード - 全キー操作をターゲットに反映** を選択して、管理ステーションでのキー操作をリモートシステムに反映します。 • **メニューアクティブ化キー** - ビューアメニューバーをアクティブにするファンクションキーを選択します。 **ツールバーの非表示の遅延時間** リストボックスを使用すると、ニューバーのサムタックボタンをクリックしない場合に、マウスカーソルを削除してからメニューバーが非表示になるまでの時間を調整できます。このオプションは、プラグインタイプが **ネイティブ** の場合に使用できます。
ヘルプ	-	**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

ビデオビューアには、映像を最適化できるビデオ調整機能が備わっています。詳細については、**ヘルプ** をクリックしてください。

ビデオ画質を自動調整するには、次の手順を実行します。

1. ビューアメニューバーにアクセスします。ビューア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、**自動ビデオ調整**(**ネイティブ** プラグインの場合)または **ビデオ設定**(**Java** プラグインの場合)を選択すると、ビューアウィンドウのビデオ品質が動的に調整されます。

ビデオ画質を手動調整するには、次の手順を実行します。

1. ビューアメニューバーにアクセスします。ビューア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、**手動ビデオ調整**(**ネイティブ** プラグインの場合)または**ビデオ設定**(**Java** プラグインの場合)を選択します。
3. **手動ビデオ調整** ウィンドウで、必要に応じて各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。
4. 調整が終わったら、**閉じる** をクリックして **手動ビデオ調整** ダイアログボックスを終了します。

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。

- マウスポインタの同期がずれないように、水平設定は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に中央揃えした状態で調整します。
- ピクセルノイズ比 設定をゼロに下げると、ビデオ更新コマンドが多数発生し、ネットワークトラフィック量が過剰に増加するため、ビデオビューアウィンドウ 内のビデオ映像がちらつきます。システムパフォーマンスと画素効果を最適化しつつ、ネットワークトラフィックを最小限に抑えたレベルになるようにピクセルノイズ比の設定を調整するようにお勧めします。

マウスポインタの同期

コンソールリダイレクトを利用してリモートの Dell システムに接続した際、リモートシステムのマウスアクセラレータ速度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、ビデオビューアウィンドウ内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させるためには、次の手順を実行します。

1. ビューアメニューバーにアクセスします。ビューア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** タブをクリックして、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、**OK** をクリックします。

4. **ツール** をクリックして、**ビデオの手動調整** を選択します。

5. リモートシステムのデスクトップがセッションウィンドウの中央に来るように水平コントロールを調整します。

6. **OK** をクリックします。

Linux（Red Hat または Novell）を使用するときは、DRAC 5 コンソールダイレクト画面でのマウス矢印の制御にオペレーティングシステムのデフォルトマウス設定が使用されます。

メモ: Linux（Red Hat または Novell）システムでは、マウス矢印の同期に関する既知の問題があります。マウスの同期に関する問題を最小限に抑えるために、すべてのユーザーが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。

コンソールリダイレクトを無効にするための情報については、DRAC 5 リモート仮想 KVM を無効にする を参照してください。

電源制御オプションの使い方

電源制御オプションを使用すると、管理下システムで次の操作を実行できます。

- システムの電源をオンにする
- システムの電源を切る
- システムをリセットする
- システムの電源サイクルを行う

管理下システムで電源を制御するには、次の手順を実行します。

1. ビューアメニューバーにアクセスします。ビューア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** をクリックしてから **電源制御** をクリックします。

3. 表示されたいずれかのオプションをクリックします。
   - システムの電源をオンにします。
   - システムの電源を切ります。
   - システムをリセットします。電源を切らずにシステムを再起動します。
   - システムの電源サイクルを行います。電源を切ってからシステムを再起動します。

   ポップアップウィンドウが表示されます。

4. **はい** をクリックしてから **OK** をクリックします。

よくあるお問い合わせ（FAQ）

サーバー上のローカルビデオがオフになっているときに新しいリモートコンソールビデオセッションを開始できますか?

はい。

ローカルビデオをオフにする要求を出してからサーバー上のローカルビデオがオフになるまで 15 秒かかるのはどうしてですか?

ビデオがオフになる前に、ローカルユーザーが必要な操作を行う機会を与えるためです。

ローカルビデオをオンにするときにも遅延時間がありますか?

いいえ。DRAC 5 がローカルビデオをオンにする要求を受け取り次第ビデオはオンになります。

ローカルユーザーはビデオをオフにできますか?

はい。ローカルユーザーは racadm CLI（ローカル）を使ってビデオをオフにできます。

ローカルユーザーはビデオをオンにすることもできますか?

はい。ユーザーは racadm CLI がサーバーにインストールされており、ターミナルサービス、telnet、SSH などのRDP 接続を介してサーバーにアクセスできるときにのみできます。その後、ユーザーはサーバーにログオンし、racadm（ローカル）を実行してビデオをオンにできます。

私のローカルビデオはオフになっており、何らかの理由で DRAC 5 はリモートアクセスできません。またサーバーは RDP、telnet、SSH をつかってアクセスできません。ローカルビデオを復元するにはどうしますか?

この場合にローカルビデオを復元する唯一の方法は、サーバーから AC 電源ケーブルを抜いて逃げ電力を流出させてから AC 電源コードを再接続する方法で、これによってローカルビデオがサーバーモニターに復元されます。また、DRAC 5 の設定がローカルビデオオン（デフォルト）に変わります。ローカルビデオをオフにする場合は、DRAC 5 を再設定する必要があります。

ローカルビデオをオフにするとローカルキーボードとマウスもオフになりますか?

いいえ。ローカルビデオをオフにするとサーバーのモニター出力コネクタから送られるビデオ信号のみがオフになります。サーバーにローカル接続されているローカルキーボードとマウスはオフにはなりません。

ローカルサーバービデオをオフにするとリモート vKVM セッションのビデオもオフになりますか?

いいえ。ローカルビデオをオンまたはオフにすることは、リモートコンソールセッションからは独立して行われます。

DRAC5 ユーザーがローカルサーバービデオをオンまたはオフにするにはどの権限が必要ですか?

DRAC 5 設定権限を持つユーザーは誰でもローカルサーバービデオをオンまたはオフにできます。

ローカルサーバービデオの現在のステータスを取得するには、どのようにしますか?

状態は、DRAC 5 のウェブベースインタフェースの **コンソールリダイレクトの設定** ページに表示されます。racadm CLI コマンド `racadm getconfig -g cfgRacTuning` を使うと、状態を cfgRacTuneLocalServerVideo オブジェクトに表示できます。状態はまた、サーバーの LCD 画面に「Video OFF」または「Video OFF in 15」としても表示されます。

サーバーの LCD 画面に「Video OFF」または「Video OFF in 15」の状態表示がないことがあるのはどうしてですか?

ローカルビデオ状態は優先度の低いメッセージです。優先度の高いサーバーイベントが起きた場合はマスクされます。LCD メッセージは優先度に基づいて表示されます。優先度の高い LCD メッセージを解決するかクリアすると、次の優先レベルのメッセージが表示されます。LCD 画面に表示されるサーバービデオメッセージは情報通知です。

ローカルサーバービデオ機能に関する詳細情報はどこから入手できますか?

デルサポートサイト **support.dell.com / manuals** で、この機能に関するホワイトペーパーをお読みください。

画面でビデオの映像の乱れが起きます。どうすれば解消できますか?

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更新してください。

メモ: **更新** を数回クリックする必要があることがあります。

コンソールリダイレクト中、Windows 2000 システムのハイバネーション後キーボードとマウスがロックされます。この問題はどうして起きるのでしょうか?

この問題を解決するには、**racadm racreset** コマンドを実行して DRAC 5 をリセットしてください。

コンソールリダイレクトウィンドウからシステム画面の下部が見えません。

管理ステーションのモニターの解像度が 1280x1024 に設定されていることを確認してください。

コンソールリダイレクト中、Windows 2003 システムのハイバネーション後マウスがロックされます。どうしてでしょうか?

この問題を解決するには、マウスの加速用に仮想 KVM (vKVM) ウィンドウのプルダウンメニューから Windows 以外のオペレーティングシステムを選択し、5～10 秒待ってから Windows を選択してください。問題が解決しない場合は、**racadm racreset** コマンドを実行することで DRAC 5 をリセットする必要があります。

それでも問題が解決しない場合は、**racadm racreset hard** コマンドを実行することで DRAC 5 をリセットする必要があります。

vKVM キーボードとマウスが動かないのはどうしてでしょうか?

管理下システムの BIOS 設定で USB コントローラを **On with BIOS support** に設定してください。管理下システムを再起動した後、<F2> を押してセットアップを行います。**統合デバイス** を選択して、**USB コントローラ** を選択します。変更を保存してシステムを再起動します。

Windows の画面が青いときに管理下システムのコンソール画面がブランクになるのはどうしてでしょうか?

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 Systems Management Tools and Documentation DVD』でビデオドライバをアップデートしてください。

Windows 2000 のインストールを完了した後リモートコンソールの画面がブランクになりました。どうしてでしょうか?

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。windows 2000 の配布 CD にある SVGA ビデオドライバで DRAC 5 コンソールリダイレクトが正しく機能しません。管理下システムで最新の対応ドライバを使用するためには、『Dell Systems Management Tools and Documentation DVD』で Windows 2000 をインストールしてください。

Windows 2000 オペレーティングシステムをロードするときに管理下システムの画面がブランクになるのはどうしてですか?

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 Systems Management Tools and Documentation DVD』でビデオドライバをアップデートしてください。

Windows の DOS ウィンドウでは管理下システムの画面がブランクになるのはどうしてでしょうか?

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 Systems Management Tools and Documentation DVD』でビデオドライバをアップデートしてください。

<F2> キーを押して BIOS 設定にならないのはどうしてですか?

これは Windows 環境独特の操作です。マウスを使ってコンソールリダイレクトウィンドウ内部をクリックして焦点を調整してください。焦点をコンソールリダイレクトウィンドウの下部のメニューバーに移すには、マウスを使って下部のメニューバー上のオブジェクトを 1 つクリックします。

『Dell Systems Management Tools and Documentation DVD』を使ってオペレーティングシステムをリモートインストールするとき vKVM マウスが同期しないのはなぜでしょうか?

コンソールリダイレクトを対象システムで実行されているオペレーティングシステム用に設定してください。

1. vKVM ツールバーメニューで、**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. **マウスの加速** ボックスで、対象システムで実行され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 システムのハイバネーション後 vKVM マウスの同期が戻らないのはどうしてでしょうか?

マウス加速用に Windows 以外のオペレーティングシステムを vKVM ウィンドウのプルダウンメニューから選択してください。次に、Windows オペレーティングシステムに戻って USB マウスデバイスを初期化してください。

1. vKVM tツールバーで **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. **マウスの加速** ボックスで、別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を実行しているときに DOS でマウスが同期しないのはなぜでしょうか。

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。デザイン上、PS/2 マウスはマウスポインタの相対位置を使用するのでこれが同期のずれを引き起こします。DRAC 5 は USB マウスドライバを持っているので、マウスポインタの絶対位置とより近似した追跡が可能です。DRAC 5 が USB マウスの絶対位置をDell BIOS, に渡しても、BIOS エミュレーションはそれを相対位置に換算して動作を維持します。

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しょうか。

仮想 KVM は USB マウスドライバを必要としますが、USB マウスドライバは X-Window オペレーティングシステムでしか使用できません。。

マウスの同期の問題がまだ解決しません。

対象システムのデスクトップがコンソールリダイレクトウィンドウの中央に置かれていることを確認してください。

1. vKVM ツールバーで **ツール** をクリックして、**ビデオの手動調整** を選択します。
2. 必要に応じて水平と垂直コントロールを調整し、デスクトップをコンソールリダイレクトウィンドウの中央に合わせます。
3. **閉じる** をクリックします。
4. 対象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、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されるまで、手順 2 から 4 を繰り返します。

マウスの加速を別のオペレーていんぐシステムに変更したら vKVM マウスとキーボードが動かなくなるのはどうしてでしょうか?

USB vKVM キーボードとマウスはマウスの加速を変更した後 5 ～10 秒間動かなくなります。ネットワークの負荷によってこの時間が長くなることもあります（10 秒以上）。

vKVM ウィンドウからサーバー画面の下部が見えないのはどうしてですか?

サーバー画面の解像度設定が 1280 x 1024 ピクセル、60 Hz 、128 色であることを確認してください。

DRAC5 コンソールリダイレクトを使用してリモートで Microsoft オペレーティングシステムをインストール中に、キーボードやマウスを使用できないのはなぜですか。

サポートされている Microsoft オペレーティングシステムを BIOS でコンソールリダイレクトに対応しているシステムに リモートインストールするとき、EMS 接続メッセージを受け取るので作業を続行する前に**OK** を選択する必要があります。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、リモート管理下システムを再起動、再インストールしてからコンソールリダイレクトを BIOS でオフにする必要があります。

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になったことをユーザーに通知します。このメッセージが表示されないようにするには、オペレーティングシステムをリモートインストールする前に、必ずコンソールリダイレクトを BIOS でオフにしてください。

Microsoft Windows 2000 の中国語、日本語、韓国語バージョンでは、コンソールリダイレクトにオペレーティングシステムの起動メニューが表示されないのはどうしてですか?

複数のオペレーティングシステムで起動できるシステムが Windows 2000 を実行しているときに、デフォルトの起動オペレーティングシステムを次の手順で変更してください。

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. **起動と回復**をクリックします。
4. Select the new default operating system from the **起動システム** リストから新しいデフォルトオペレーティングシステムを選択します。
5. **オペレーティングシステムの一覧を表示する時間** ボックスで、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前に選択リストを表示する秒数を入力します。

管理ステーションの Num Lock インジケータにリモートサーバーの Num Lock のステータスが反映されないのはなぜですか。

DRAC 5 を介してアクセスした場合、管理ステーションの Num Lock インジケータはリモートサーバーの Num Lock の状態に一致するとは限りません。Num Lock の状態は、管理ステーションの Num Lock の状態にかかわらず、リモートセッションが接続されたときのリモートサーバーの設定に依存します。

1 つのコンソールリダイレクトセッションを確立したときに複数のセッションビューアウィンドウが開くのはどうしてでしょうか?

ローカルシステムにコンソールリダイレクトセッションを設定しているので、リモートシステムへのセッションを再設定してください。

1 つのコンソールリダイレクトセッションを実行しているときにローカルユーザーがリモートシステムにアクセスした場合、警告メッセージが表示されますか?

いいえ ローカルユーザーがシステムにアクセスする場合、あなたの操作は警告なしで上書きされます。

コンソールリダイレクトセッションを実行するために必要な帯域幅はどれくらいですか。

良好なパフォーマンスを得るためには、5 MB/秒の接続を推奨します。最低限必要なパフォーマンスを得るためには、1 MB/秒の接続が必要です。

管理ステーションでコンソールリダイレクトを実行するために最低限必要なシステム要件を教えてください。

管理ステーションには、Intel Pentium III 500 MHz プロセッサと最低限 256 MB の RAM が必要です。

リモートシステム上で実行できるコンソールリダイレクトセッションの最大数はいくつですか?

DRAC 5 は、同時に 2 つまでのコンソールリダイレクトセッションをサポートします。

マウスの同期の問題があるのはどうしてですか?

Linux(Red Hat または Novell)システムでは、マウス矢印の同期に関する既知の問題があります。マウスの同期に関する問題を最小限に抑えるために、すべてのユーザーが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。

ファイルシステムが読み取り専用の管理ステーションにウェブブラウザをインストールするにはどうしますか?

Linux を実行しており、ファイルシステムが読み取り専用の管理ステーションでは、DRAC 5 に接続する必要なくブラウザをクライアントシステムにインストールできます。ネイティブのプラグインインストールパッケージを使用すると、クライアントのセットアップ段階でブラウザを手動でインストールできます。

△ **注意: 読み取り専用のクライアント環境では、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と、インストールされている仮想メディア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バージョンがある場合、古いプラグイン機能は使用できなくなるためです。この場合、プラグインをインストールするように求められます。ファイルシステムは読み取り専用であるため、インストールに失敗して、プラグインの機能は使用できなくなります。**

プラグインインストールパッケージを取得するには、次の手順を実行します。

1. 既存の DRAC 5 にログインします。
2. ブラウザのアドレスバーで URL を変更してください。

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

   →

   `https://<RAC_IP>/plugins/ # 最後のスラッシュ (/) を付け忘れないでください。`
3. 2 つのサブディレクトリ vm と vkvm をご覧ください。適切なサブディレクトリに移動して、rac5XXX.xpi ファイルを右クリックし、**リンクのターゲットに名前を付けて保存....** 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の保存場所を選択します。

プラグインインストールパッケージをインストールするには、次の手順を実行します。

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の共有フォルダにコピーします。
2. クライアントシステム上で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にプラグインインストールパッケージのファイルパスを入力します。たとえば、次のとおりです。

   `file:///tmp/rac5vm.xpi`
4. ブラウザに表示される指示に従ってプラグインをインストールします。.

対象 DRAC 5 ファームウェアにそのプラグインの新バージョンが含まれる場合を除き、インストールしたプラグインのインストールが求められることはありません。

ターミナルを再起動すると、コンソールリダイレクトセッションが終了するのはなぜですか。

DRAC 5 の NIC 設定が「共有」または「フェールオーバーと共有」モードの場合にシステムをリセットすると、LAN On Motherboard(LOM)がリセットされます。Spanning Tree Protocol(STP)が有効になっているスイッチがあるネットワークでは、これによって 10〜15 秒後に管理ステーションとクライアント間の接続が再確立されます。その結果、リモートシステムの接続性が失われ、コンソールリダイレクトおよび仮想メディアクライアントに接続喪失エラーメッセージが表示されます。この時点で DRAC の GUI にアクセスすると、「ページが見つかりません」というエラーメッセージが表示されます。

この問題を回避するには、次の手順を実行します。

- ネットワークを介した接続に DRAC 5 専用の NIC を使用します。
- ネットワークのスイッチで STP を無効にします。

目次に戻る