Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00 ユーザーズガイド

メモと注意

メモ: コンピュータを使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータ損失の可能性と、その危険を回避するための方法が記載されています。

2008 年 27 月、Rev. A01

目次ページに戻る

RACADM サブコマンドの概要

Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00
ユーザーズガイド

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

---

help

表 A-1 で help コマンドについて説明します。

表 A-1. help コマンド

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

概要

```
racadm help

racadm help <サブコマンド>
```

説明

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

出力

racadm help コマンドはサブコマンドのリストを表示します。

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

対応インタフェース

- ローカル RACADM

---

config

表 A-2 で config および getconfig サブコマンドについて説明します。

表 A-2. config / getconfig

サブコマンド	定義

config	iDRAC を設定します。
getconfig	iDRAC 設定データを取得します。

概要

```
racadm config [-c|-p] -f <ファイル名>

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

対応インタフェース

- ローカル RACADM

説明

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

入力

表 A-3 で config サブコマンドのオプションについて説明します。

表A-3. config サブコマンドオプションと説明

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

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 エラー

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

例

- `racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.110`

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

- `racadm config -f myrac.cfg`

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

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

getconfig

getconfig サブコマンドを使うと、個別の iDRAC 設定パラメータを取得するか、すべての iDRAC 設定グループを取得してファイルに保存できます。

入力

表 A-4 で getconfig サブコマンドのオプションについて説明します。

メモ: ファイルを指定せずに -f オプションを使用すると、ファイルの内容がターミナル画面に表示されます。

表 A-4. getconfig サブコマンドオプション

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

出力

このサブコマンドは、次の場合にエラー出力を生成します。

- 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 転送エラー

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

例

- `racadm getconfig -g cfgLanNetworking`

  cfgLanNetworking グループに含まれている設定プロパティ(オブジェクト)をすべて表示します。

- `racadm getconfig -f myrac.cfg`

  iDRAC のグループ設定オブジェクトすべてを myrac.cfg に保存します。

- `racadm getconfig -h`

  iDRAC 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 のユーザーグループインスタンスと、プロパティ値の詳細情報を表示します。

概要

```
racadm getconfig -f <ファイル名>

racadm getconfig -g <グループ名> [-i <インデックス>]
```

```
racadm getconfig -u <ユーザー名>

racadm getconfig -h
```

対応インタフェース

- ローカル RACADM

---

getssninfo

表 A-5 で getssninfo サブコマンドについて説明します。

表 -5. getssinfo サブコマンド

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

概要

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

説明

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

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

対応インタフェース

- ローカル RACADM

入力

表 A-6 で **testemail** サブコマンドのオプションについて説明します。

表 A-6. getssninfo サブコマンドのオプション

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

例

- racadm getssninfo

表 A-7 に **racadm getssninfo** コマンドからの出力例を示します。

表 A-7. getssninfo サブコマンド出力例

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

- 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

表 A-8 で **racadm getsysinfo** サブコマンドについて説明します。

表 A-8. getsysinfo

コマンド	定義
getsysinfo	iDRAC 情報、システム情報、ウォッチドッグ状態情報を表示します。

概要

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

説明

getsysinfo サブコマンドは、iDRAC、管理下サーバー、およびウォッチドッグ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

入力

表 A-9 で **getssinfo** サブコマンドのオプションについて説明します。

表 A-9. getsysinfo サブコマンドオプション

オプション	説明
-d	iDRAC 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 / ラベルの印刷を削除します。

出力

getsysinfo サブコマンドは、iDRAC、管理下サーバー、およびウォッチドッグ設定に関連する情報を表示します。

出力例

```
RAC Information:
RAC Date/Time            = Wed Aug 22 20:01:33 2007
Firmware Version         = 0.32
Firmware Build           = 13661
Last Firmware Update     = Mon Aug 20 08:09:36 2007

Hardware Version         = NA
Current IP Address       = 192.168.0.120
Current IP Gateway       = 192.168.0.1
Current IP Netmask       = 255.255.255.0
DHCP Enabled             = 1
MAC Address              = 00:14:22:18:cd:f9
Current DNS Server 1     = 10.32.60.4
Current DNS Server 2     = 10.32.60.5
DNS Servers from DHCP    = 1
Reister DNS RAC Name     = 1
DNS RAC Name             = iDRAC-783932693338
Current DNS Domain       = us.dell.com

System Information:
System Model             = PowerEdge M600
System BIOS Version      = 0.2.1
BMC Firmware Version     = 0.32
Service Tag              = 48192
Host Name                = dell-x92i38xc2n
OS Name                  =
Power Status             = OFF

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

例

- `racadm getsysinfo -A -s`

  `System Information:" "PowerEdge M600" "0.2.1" "0.32" "48192" "dell-x92i38xc2n" "" "ON`

- `racadm getsysinfo -w -s`

```
System Information:
System Model             = PowerEdge M600
System BIOS Version      = 0.2.1
BMC Firmware Version     = 0.32
Service Tag              = 48192
Host Name                = dell-x92i38xc2n
OS Name                  =
Power Status             = ON


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

制限

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

---

getractime

表 A-10 で **getractime** サブコマンドについて説明します。

表 A-10. getractime

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

概要

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

説明

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

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

出力

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

出力例

```
racadm getractime

Thu Dec 8 20:15:26 2005

racadm getractime -d

20071208201542.000000
```

対応インタフェース

- ローカル RACADM

---

setniccfg

表 A-11 で **setniccfg** サブコマンドについて説明します。

表 A-11. setniccfg

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

概要

```
racadm setniccfg -d

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

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

説明

setniccfg サブコマンドは、iDRAC の IPアドレスを設定します。

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

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

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

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

出力

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

対応インタフェース

- ローカル RACADM

---

getniccfg

表 A-12 で **getniccfg** サブコマンドについて説明します。

表 A-12. getniccfg

サブコマンド	定義
getniccfg	iDRAC の現在の IP 設定を表示します。

概要

```
racadm getniccfg
```

説明

getniccfg サブコマンドは、現在の NIC 設定を表示します。

出力例

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

```
NIC Enabled     = 1

DHCP Enabled    = 1

IP Address      = 192.168.0.1

Subnet Mask     = 255.255.255.0

Gateway         = 192.168.0.1
```

対応インタフェース

- ローカル RACADM

---

getsvctag

表 A-13 で **getsvctag** サブコマンドについて説明します。

表 A-13. getsvctag

サブコマンド	定義
getsvctag	サービスタグを表示します。

概要

```
racadm getsvctag
```

説明

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

例

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

```
Y76TP0G
```

どちらのコマンドも成功すると *0* を、エラーの場合はゼロ以外を返します。

対応インタフェース

- ローカル RACADM

---

racreset

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

表 A-14. racreset

サブコマンド	定義
racreset	iDRAC をリセットします。

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

概要

```
racadm racreset
```

説明

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

例

- `racadm racreset`

  iDRAC のソフトリセットの手順を開始します。

対応インタフェース

- ローカル RACADM

---

racresetcfg

表 A-15 で **racresetcfg** サブコマンドについて説明します。

表 A-15. racresetcfg

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

概要

```
racadm racresetcfg
```

対応インタフェース

- ローカル RACADM

説明

racresetcfg コマンドは、ユーザーによって設定されるデータベースプロパティのすべてのエントリを削除します。データベースには、iDRAC を元のデフォルト設定に戻すデフォルトのプロパティがすべてのエントリにあります。

注意:このコマンドは現在の iDRAC の設定を削除し、iDRAC 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、デフォルトの名前およびパスワードはそれぞれ、**root** と **calvin** になり、IP アドレスは **192.168.0.120** にシャーシに存在するサーバーのスロット番号を加えた値になります。

---

serveraction

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

表 A-16. serveraction

サブコマンド	定義
serveraction	管理下サーバーのリセットまたはパワーオン / オフ / サイクルを実行します。

概要

```
racadm serveraction <action>
```

説明

serveraction サブコマンドを使用すると、ホストシステムに電力の管理操作を実行できます。表 A-17 で **serveraction** 電源制御のオプションについて説明します。

表 A-17. fserveraction サブコマンドオプション

文字列	定義
<処置**>**	処置を指定します。<処置> の文字列のオプションを次に示します。 - **powerdown** — 管理下サーバーの電源を切ります。 - **powerup** — 管理下サーバーの電源を入れます。 - **powercycle** — 管理下サーバーのパワーサイクル処理を発行します。この処理は、システムの前面パネルにある電源ボタンを押して電源を切ってから電源を入れ直す操作に似ています。 - **powerstatus** — サーバーの現在の電源状態(**オン** か **オフ** を表示します)。 - **hardreset** — 管理下サーバーのリセット(再起動)を実行します。

出力

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

対応インタフェース

- ローカル RACADM

---

getraclog

表 A-18 に **racadm getraclog** コマンドについて説明します。

表 A-18. getraclog

コマンド	定義
getraclog -i	iDRAC ログ内のエントリ数を表示します。
getraclog	iDRAC のログエントリを表示します。

概要

```
racadm getraclog -i

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

説明

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

メモ: オプションを指定しなければ、全部のログが表示されます。

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

表 A-19. getraclog サブコマンドオプション

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

出力

デフォルトの出力表示では、レコード番号、タイムスタンプ、ソース、説明が表示されます。タイムスタンプは、1 月 1 日の午前零時に開始し、管理下サーバー起動時まで増加します。管理下サーバー起動後、タイムスタンプには管理下サーバーのシステム時間が使用されます。

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

---

clrraclog

概要

```
racadm clrraclog
```

説明

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

---

getsel

表 A-20 で **getse** コマンドについて説明します。

表 A-20. 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。

概要

```
racadm getsel -i
```

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

説明

getsel -i コマンドは、SEL 内のエントリ数を表示します。

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

メモ: 引数を指定しなければ、全部のログが表示されます。

表 A-21. getsel サブコマンドオプション

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

出力

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

例:

```
Record:      1
Date/Time:   11/16/2005 22:40:43
Severity:    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

---

clrsel

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

---

gettracelog

表 A-22 で **gettracelog** サブコマンドについて説明します。

表 A-22. gettracelog

コマンド	定義
gettracelog -i	**iDRAC トレースログ** 内のエントリ数を表示します。
gettracelog	**iDRAC トレースログ** を表示します。

概要

```
racadm gettracelog -i

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

説明

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

表 A-23. gettracelog サブコマンドオプション

オプション	説明
-i	**iDRAC トレースログ** 内のエントリ数を表示します。
-m	一度に 1 画面で情報を表示して、ユーザーに続行のプロンプトを表示します(UNIX の **more** コマンドに類似)。
-o	出力を 1 行で表示します。
-c	表示するレコード数を指定します。
-s	表示する開始レコードを指定します。

-A	ヘッダーやラベルを表示しません。

出力

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

例:

```
Record: 1

Date/Time: Dec 8 08:21:30

Source: ssnmgrd[175]

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

対応インタフェース

- ローカル RACADM

---

sslcsrgen

表 A-24 で **sslcsrgen** サブコマンドについて説明します。

表 A-24. 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。

概要

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

racadm sslcsrgen -s
```

説明

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

オプション

表 A-25 で **sslcsrgen**サブコマンドのオプションについて説明します。

表 A-25. 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 生成処理の状態を返します(生成中、アクティブ、なし)。
-f	<ファイル名> の場所を指定します。ここに CSR がダウンロードされます。

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

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

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

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

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

例

```
racadm 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

---

sslcertupload

表 -26 で **sslcertupload** サブコマンドについて説明します。

表 A-26. sslcertupload

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

概要

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

オプション

表 A-27 で **sslcertupload** サブコマンドのオプションについて説明します。

表 A-27. sslcertupload サブコマンドオプション

オプション	説明
-t	CA 証明書かサーバ証明書か、アップロードする証明書のタイプを指定します。 1 = サーバー証明書 2 = CA 証明書
-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 コマンドは成功すると 0 を返し、成功しないと非ゼロの数字を返します。

例

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

対応インタフェース

- ローカル RACADM

---

sslcertdownload

表 A-28 で **sslcertdownload** サブコマンドについて説明します。

表 A-28. 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。

概要

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

オプション

表 A-29 で **sslcertdownload** サブコマンドのオプションについて説明します。

表 A-29. sslcertdownload サブコマンドオプション

オプション	説明
-t	Microsoft® Active Directory® 証明書かサーバー証明書か、ダウンロードする証明書の種類を指定します。 1 = サーバー証明書 2 = Microsoft Active Directory 証明書
-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。

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

例

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

対応インタフェース

- ローカル RACADM

---

sslcertview

表 A-30 で **sslcertview** サブコマンドについて説明します。

表 A-30. sslcertview

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

概要

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

オプション

表 A-31 で **sslcertview** サブコマンドのオプションについて説明します。

表 A-31. sslcertview サブコマンドオプション

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

出力例

```
racadm sslcertview -t 1

Serial Number             : 00

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

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

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

racadm sslcertview -t 1 A

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

---

testemail

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

表 A-32. testemail の設定

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

概要

```
racadm testemail -i <インデックス>
```

説明

iDRAC から指定の宛先へテスト電子メールを送信します。

testemail コマンドを実行する前に、RACADM **cfgEmailAlert** グループ内の指定され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-33 に **cfgEmailAlert** グループのコマンド例を示します。

表 A-33. testemail の設定

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

オプション

表 A-34 で **testemail** サブコマンドのオプションについて説明します。

表 A-34. testemail サブコマンドオプション

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

---

testtrap

表 A-35 で **testtrap** サブコマンドについて説明します。

表 A-35. testtrap

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

概要

```
racadm testtrap -i <インデックス>
```

説明

testtrap サブコマンドは、iDRAC からネットワーク上の指定した宛先トラップリスナにテストトラップを送信して、iDRAC 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インデックスが正しく設定されていることを確認してください。

表 A-36 に **cfgIpmiPet** グループのリストと関連コマンドを示します。

表 A-36. cfg 電子メール警告コマンド

処置	コマンド
警告を有効にする	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
宛先の電子メール 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 の数字

入力

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

表 A-37. 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

---

vmdisconnect

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

表 A-38. vmdisconnect

サブコマンド	説明
vmdisconnect	すべての開いているリモートクライアントからの iDRAC 仮想メディア接続を閉じます。

概要

```
racadm vmdisconnect
```

説明

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

vmdisconnect サブコマンドを使用すると、iDRAC 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 のウェブインタフェースまたは RACADM **getsysinfo** サブコマンドを使用して表示できます。

対応インタフェース

- ローカル RACADM

目次ページに戻る

目次ページに戻る

iDRAC プロパティデータベースグループおよびオブジェクトの定義

Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00
ユーザーズガイド

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

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

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

表示可能な文字には以下のセットがあります。

```
abcdefghijklmnopqrstuvwxwz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

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

---

idRacInfo

このグループにはクエリされる iDRAC の特定の情報を提供するための表示パラメータがあります。

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

idRacProductInfo（読み取り専用）

正当値

最大 63 バイトの ASCII 文字列。

デフォルト

iDRAC（Integrated Dell Remote Access Controller）

説明

製品を識別するテキスト文字列。

idRacDescriptionInfo（読み取り専用）

正当値

最大 255 バイトの ASCII 文字列。

デフォルト

このシステムコンポーネントは Dell PowerEdge サーバーのリモート管理機能全一式を提供します。

説明

RAC の種類を説明するテキスト。

idRacVersionInfo（読み取り専用）

正当値

最大 63 バイトの ASCII 文字列。

デフォルト

1.0

説明

現在の製品ファームウェアバージョンを含む文字列。

idRacBuildInfo（読み取り専用）

正当値

最大 16 バイトの ASCII 文字列。

デフォルト

現在の RAC ファームウェアビルドバージョン。 例："05.12.06"

説明

現在の製品ビルドバージョンを含む文字列。

idRacName（読み取り専用）

正当値

最大 15 バイトの ASCII 文字列。

デフォルト

iDRAC

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

8

説明

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

---

cfgLanNetworking

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

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

cfgDNSDomainNameFromDHCP（読み取り / 書き込み）

正当値

1（TRUE）

0（FALSE）

デフォルト

0

説明

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

cfgDNSDomainName（読み取り / 書き込み）

正当値

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

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

デフォルト

""

説明

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

cfgDNSRacName（読み取り / 書き込み）

正当値

最大 63 バイトの ASCII 文字列。 少なくとも 1 文字は英字である必要があります。

メモ: 31 文字以内の名前しか登録できない DNS サーバーもあります。

デフォルト

rac-サービスタグ

説明

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

cfgDNSRegisterRac（読み取り / 書き込み）

正当値

1（TRUE）

0（FALSE）

デフォルト

0

説明

DNS サーバーに iDRAC 名を登録します。

cfgDNSServersFromDHCP（読み取り / 書き込み）

正当値

1（TRUE）

0（FALSE）

デフォルト

0

説明

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

cfgDNSServer1（読み取り / 書き込み）

正当値

有効な IP アドレスを表す文字列。 例：192.168.0.20

説明

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

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

cfgDNSServer2（読み取り / 書き込み）

正当値

有効な IP アドレスを表す文字列。 例：192.168.0.20

デフォルト

0.0.0.0

説明

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

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

cfgNicEnable（読み取り / 書き込み）

正当値

1（TRUE）

0（FALSE）

デフォルト

0

説明

iDRAC 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、iDRAC へのリモートネットワークインタフェースにアクセスできず、シリアルインタフェースかローカル RACADM インタフェースでしか iDRAC を使用できなくなります。

cfgNicIpAddress（読み取り / 書き込み）

メモ：このパラメータは **cfgNicUseDhcp** パラメータが 0（FALSE）に設定されている場合にのみ設定可能です。

正当値

有効な IP アドレスを表す文字列。 例：192.168.0.20

デフォルト

192.168.0.*n*

n は 120 にサーバーのスロット番号を加えた値です。

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： このパラメータは **cfgNicUseDhcp** パラメータが 0（FALSE）に設定されている場合にのみ設定可能です。

正当値

有効なサブネットマスクを表す文字列。 例：255.255.255.0

デフォルト

255.255.255.0

説明

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

cfgNicGateway（読み取り / 書き込み）

メモ： このパラメータは **cfgNicUseDhcp** パラメータが 0（FALSE）に設定されている場合にのみ設定可能です。

正当値

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

デフォルト

192.168.0.1

説明

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

cfgNicUseDhcp（読み取り / 書き込み）

正当値

1（TRUE）

0（FALSE）

デフォルト

0

説明

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

cfgNicMacAddress（読み取り専用）

正当値

RAC NIC の MAC アドレスを表す文字列。

デフォルト

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

説明

iDRAC NIC の MAC アドレス。

---

cfgUserAdmin

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

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

cfgUserAdminIpmiLanPrivilege（読み取り / 書き込み）

正当値

2（**ユーザー**）

3（**オペレータ**）

4（**システム管理者**）

15（**アクセスなし**）

デフォルト

4（ユーザー 2）

15（その他すべて）

説明

IPMI LAN チャネル上の最大特権。

cfgUserAdminPrivilege（読み取り / 書き込み）

正当値

0x00000000 ～ 0x000001ff

デフォルト

0x00000000

説明

このプロパティは、ユーザーの役割ベースの特権を指定します。値は、特権の値を自由に組み合わせることのできるビットマスクとして表します。表 B-1 でビットマスクの作成に結合できるユーザー権限のビット値について説明します。

表 B-1. ユーザー特権に応じたビットマスク

ユーザー特権	特権ビットマスク
iDRAC へのログイン	0x0000001
iDRAC の設定	0x0000002
ユーザーの設定	0x0000004
ログのクリア	0x0000008
サーバーコントロールコマンドの実行	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-2 に、1 つまたは複数の特権を持つユーザーの特権ビットマスクの例を示します。

表 B-2. ユーザー特権のビットマスクの例

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

cfgUserAdminUserName（読み取り / 書き込み）

正当値

文字列。 最大長 = 16。

デフォルト

""

説明

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

メモ: このプロパティ値は、ユーザー名において固有の値でなくてはなりません。

cfgUserAdminPassword（書き込み専用）

正当値

最大 20 バイトの ASCII 文字列。

デフォルト

""

説明

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

cfgUserAdminEnable

正当値

1（TRUE）

0（FALSE）

デフォルト

0

説明

個々のユーザーを有効または無効にします。

cfgUserAdminSolEnable

正当値

1（TRUE）

0（FALSE）

デフォルト

0

説明

シリアルオーバー LAN（SOL）のユーザーアクセスを有効または無効にします。

---

cfgEmailAlert

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

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

cfgEmailAlertIndex（読み取り専用）

正当値

1～4

デフォルト

このパラメータは既存のインスタンスを基に自動入力されます。

説明

警告インスタンスの固有のインデックス。

cfgEmailAlertEnable（読み取り / 書き込み）

正当値

1（TRUE）

0（FALSE）

デフォルト

0

説明

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

cfgEmailAlertAddress

正当値

最大 64 の長さの ASCII 文字を使用した電子メールアドレス形式。

デフォルト

""

説明

警告ソースの電子メールアドレス。

cfgEmailAlertCustomMsg

正当値

文字列。 最大長 = 32。

デフォルト

""

説明

警告と一緒に送信されるカスタムメッセージを指定します。

---

cfgSessionManagement

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

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

cfgSsnMgtConsRedirMaxSessions（読み取り / 書き込み）

正当値

1 ～ 2

デフォルト

2

説明

iDRAC で許可されるコンソールリダイレクトセッションの最大数を指定します。

cfgSsnMgtWebserverTimeout（読み取り / 書き込み）

正当値

60 ～ 1920

デフォルト

300

説明

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

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

cfgSsnMgtSshIdleTimeout（読み取り / 書き込み）

正当値

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

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

```
Warning: Session no longer valid, may have timed out
（警告：セッションが無効になりました。タイムアウトの可能性があります。）
```

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。

cfgSsnMgtTelnetIdleTimeout（読み取り / 書き込み）

正当値

0（タイムアウトなし）

60 ～ 1920

デフォルト

300

説明

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

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

```
Warning: Session no longer valid, may have timed out
（警告：セッションが無効になりました。タイムアウトの可能性があります。）
```

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、iDRAC サービスの設定パラメータが含まれます。

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

cfgSerialSshEnable（読み取り / 書き込み）

正当値

1（TRUE）

0（FALSE）

デフォルト

1

説明

iDRAC 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）

正当値

1（TRUE）

0（FALSE）

デフォルト

0

説明

iDRAC 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。

---

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、iDRAC の各種プロパティの設定に使用します。

cfgRacTuneHttpPort（読み取り / 書き込み）

正当値

10 ～ 65535

デフォルト

80

説明

RAC との HTTP ネットワーク通信に使用するポート番号を指定します。

cfgRacTuneHttpsPort（読み取り / 書き込み）

正当値

10 ～ 65535

デフォルト

443

説明

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

cfgRacTuneIpRangeEnable

正当値

1（TRUE）

0（FALSE）

デフォルト

0

説明

iDRAC の IP アドレス範囲の検証機能を有効または無効にします。

cfgRacTuneIpRangeAddr

正当値

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

デフォルト

192.168.1.1

説明

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

cfgRacTuneIpRangeMask

正当値

左寄せビットを使用した標準的な IP マスク値

デフォルト

255.255.255.0

説明

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

cfgRacTuneIpBlkEnable

正当値

1（TRUE）

0（FALSE）

デフォルト

0

説明

RAC の IP アドレスブロック機能を有効または無効にします。

cfgRacTuneIpBlkFailCount

正当値

2 ～ 16

デフォルト

5

説明

この IP アドレスからのログイン試行が拒否される前に、ウィンドウ（cfgRacTuneIpBlkFailWindow）内で発生するログイン失敗の最大回数。

cfgRacTuneIpBlkFailWindow

正当値

10 ～ 65535

デフォルト

60

説明

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

cfgRacTuneIpBlkPenaltyTime

正当値

10 ～ 65535

デフォルト

300

説明

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

cfgRacTuneSshPort（読み取り / 書き込み）

正当値

1 ～ 65535

デフォルト

22

説明

iDRAC 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）

正当値

1 ～ 65535

デフォルト

23

説明

iDRAC 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。

cfgRacTuneConRedirEncryptEnable（読み取り / 書き込み）

正当値

1（TRUE）

0（FALSE）

デフォルト

1

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）

正当値

1 ～ 65535

デフォルト

5900

説明

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

cfgRacTuneConRedirVideoPort（読み取り / 書き込み）

正当値

1 ～ 65535

デフォルト

5901

説明

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

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

cfgRacTuneAsrEnable（読み取り / 書き込み）

正当値

0（FALSE）

1（TRUE）

デフォルト

0

説明

iDRAC の前回クラッシュ画面キャプチャ機能を有効または無効にします。

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

cfgRacTuneWebserverEnable（読み取り / 書き込み）

正当値

0（FALSE）

1（TRUE）

デフォルト

1

説明

iDRAC Web Server 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、クライアントのウェブブラウザやリモート RACADM を使用して iDRAC にアクセスできなくなります。このプロパティは Telnet/SSH/ またはローカル RACADM インタフェースには影響しません。

cfgRacTuneLocalServerVideo（読み取り / 書き込み）

正当値

1（有効）

0（無効）

デフォルト

1

説明

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

---

ifcRacManagedNodeOs

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

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

ifcRacMnOsHostname（読み取り / 書き込み）

正当値

文字列。 最大長 = 255。

デフォルト

""

説明

管理下サーバーのホスト名。

ifcRacMnOsOsName（読み取り / 書き込み）

正当値

文字列。 最大長 = 255。

デフォルト

""

説明

管理下サーバーのオペレーティングシステム名。

---

cfgRacSecurity

このグループは、iDRAC 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、iDRAC から CSR を生成する前に設定する必要

があります。

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

cfgSecCsrCommonName（読み取り / 書き込み）

正当値

文字列。 最大長 = 254。

デフォルト

""

説明

CSR 共通名（CN）を指定します。

cfgSecCsrOrganizationName（読み取り / 書き込み）

正当値

文字列。 最大長 = 254。

デフォルト

""

説明

CSR 組織名（O）を指定します。

cfgSecCsrOrganizationUnit（読み取り / 書き込み）

正当値

文字列。 最大長 = 254。

デフォルト

""

説明

CSR 部門名（OU）を指定します。

cfgSecCsrLocalityName（読み取り / 書き込み）

正当値

文字列。 最大長 = 254。

デフォルト

""

説明

CSR 地域（L）を指定します。

cfgSecCsrStateName（読み取り / 書き込み）

正当値

文字列。 最大長 = 254。

デフォルト

""

説明

CSR 州名（S）を指定します。

cfgSecCsrCountryCode（読み取り / 書き込み）

正当値

文字列。 最大長 = 2。

デフォルト

""

説明

CSR 国番号（CC）を指定します。

cfgSecCsrEmailAddr（読み取り / 書き込み）

正当値

文字列。 最大長 = 254。

デフォルト

""

説明

CSR の電子メールアドレスを指定します。

cfgSecCsrKeySize（読み取り / 書き込み）

正当値

1024

2048

4096

デフォルト

1024

説明

CSR の非対称キーサイズを指定します。

---

cfgRacVirtual

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

cfgVirMediaAttached（読み取り / 書き込み）

正当値

1（TRUE）

0（FALSE）

デフォルト

1

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、ローカルの 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。デバイスが連結されると、iDRAC 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、デバイスが USB バスから切断されます。

メモ: 変更をすべて有効にするには、システムを再起動する必要があります。

cfgVirAtapiSrvPort（読み取り / 書き込み）

正当値

1 ～ 65535

デフォルト

3668

説明

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

cfgVirAtapiSrvPortSsl（読み取り / 書き込み）

正当値

0 ～ 65535 までの 10 進数で未使用のポート番号。

デフォルト

3670

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。

cfgVirMediaBootOnce（読み取り / 書き込み）

正当値

1（有効）

0（無効）

デフォルト

0

説明

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

cfgFloppyEmulation（読み取り / 書き込み）

正当値

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、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 iDRAC 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）

正当値

余白のない印刷可能なテキスト文字列。 最大長は 254 文字です。

デフォルト

""

説明

DRAC が存在する Active Directory ドメイン。

cfgADRacName（読み取り / 書き込み）

正当値

余白のない印刷可能なテキスト文字列。 最大長は 254 文字です。

デフォルト

""

説明

Active Directory フォレストに記録された iDRAC 名。

cfgADEnable（読み取り / 書き込み）

正当値

1（TRUE）

0（FALSE）

デフォルト

0

説明

iDRAC 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 iDRAC 認証が使用されます。

cfgADAuthTimeout（読み取り / 書き込み）

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

正当値

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）

正当値

余白のない印刷可能なテキスト文字列。 最大長は 254 文字です。

デフォルト

""

説明

ドメインフォレストのルートドメイン。

cfgADSpecifyServerEnable（読み取り / 書き込み）

正当値

1 または 0（True または False）

デフォルト

0

説明

1（True）で、LDAP またはグローバルカタログサーバーを指定することができます。 0（False）で、このオプションが無効になります。

cfgADDomainController（読み取り / 書き込み）

有効な IP アドレスまたは完全修飾されたドメイン名（FQDN）

デフォルト

デフォルト値なし

説明

iDRAC は指定された値を使用して、LDAP サーバーからユーザー名を検索します。

cfgADGlobalCatalog（読み取り / 書き込み）

正当値

有効な IP アドレスまたは完全修飾されたドメイン名（FQDN）

デフォルト

デフォルト値なし

説明

iDDRAC は指定された値を使用してグローバルカタログサーバーでユーザー名を検索します。

cfgADType（読み取り / 書き込み）

正当値

1 = 拡張スキーマで Active Directory を有効にします。

2 = 標準スキーマで Active Directory 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特定します。

---

cfgStandardSchema

このグループには Active Directory 標準スキーマ設定を行うためのパラメータが含まれています。

cfgSSADRoleGroupIndex（読み取り専用）

正当値

1 ～ 5 までの整数。

説明

Active Directory で記録したロールグループのインデックス。

cfgSSADRoleGroupName（読み取り / 書き込み）

正当値

余白のない印刷可能なテキスト文字列。 最大長は 254 文字です。

デフォルト

（空白）

説明

Active Directory フォレストで記録したロールグループの名前。

cfgSSADRoleGroupDomain（読み取り / 書き込み）

正当値

余白のない印刷可能なテキスト文字列。 最大長は 254 文字です。

デフォルト

（空白）

説明

役割グループが存在する Active Directory ドメイン。

cfgSSADRoleGroupPrivilege（読み取り / 書き込み）

正当値

0x00000000 ～ **0x000001ff**

デフォルト

（空白）

説明

表 B-3のビットマスク番号を使って、役割グループの役割ベースの特権レベルを設定します。

表 B-3. 役割グループの特権のビットマスク

役割グループの特権	ビットマスク
iDRAC へのログイン	0x00000001
iDRAC の設定	0x00000002
ユーザーの設定	0x00000004
ログのクリア	0x00000008
サーバーコントロールコマンドの実行	0x00000010
コンソールリダイレクトへのアクセス	0x00000020
仮想メディアへのアクセス	0x00000040
テスト警告	0x00000080

デバッグコマンドの実行	0x00000100

---

cfgIpmiSol

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

cfgIpmiSolEnable（読み取り / 書き込み）

正当値

0（FALSE）

1（TRUE）

デフォルト

1

説明

SOL を有効または無効にします。

cfgIpmiSolBaudRate（読み取り / 書き込み）

正当値

19200、57600、115200

デフォルト

115200

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）

正当値

2（ユーザー）

3（オペレータ）

4（システム管理者）

デフォルト

4

説明

SOL アクセスに必要な最小特権を指定します。

cfgIpmiSolAccumulateInterval（読み取り / 書き込み）

正当値

1 ～ 255

デフォルト

10

説明

SOL 文字データパケットの一部を送信する前に通常 iDRAC 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）

正当値

1 ～ 255

デフォルト

255

説明

SOL しきい値の限界値。 SOL データパケット送信前にバッファする最大バイト数を指定します。

---

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）

正当値

0（FALSE）

1（TRUE）

デフォルト

0

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）

正当値

2（ユーザー）

3（オペレータ）

4（システム管理者）

デフォルト

4

説明

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

cfgIpmiLanAlertEnable（読み取り / 書き込み）

正当値

0（FALSE）

1（TRUE）

デフォルト

0

説明

グローバル電子メール警告を有効または無効にします。 このプロパティは個々の電子メール警告の有効 / 無効プロパティをすべて上書きします。

cfgIpmiEncryptionKey（読み取り / 書き込み）

正当値

スペースなしの 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）

正当値

最大 18 文字の文字列。

デフォルト

public

説明

トラップの SNMP コミュニティ名。

---

cfgIpmiPef

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

イベントフィルタは、管理下サーバー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）

正当値

文字列。 最大長 = 255。

デフォルト

インデックスフィルタの名前。

説明

プラットフォームイベントフィルタの名前を指定します。

cfgIpmiPefIndex（読み取り専用）

正当値

1 ～ 17

デフォルト

プラットフォームイベントフィルタオブジェクトのインデックス値。

説明

特定のプラットフォームイベントフィルタのインデックスを指定します。

cfgIpmiPefAction（読み取り / 書き込み）

正当値

0（なし）

1（電源を切る）

2（リセット）

3（パワーサイクル）

デフォルト

0

説明

警告がトリガされたときに管理下サーバーで実行される処置を指定します。

cfgIpmiPefEnable（読み取り / 書き込み）

正当値

0（FALSE）

1（TRUE）

デフォルト

1

説明

特定のプラットフォームイベントフィルタを有効または無効にします。

---

cfgIpmiPet

このグループは、管理下サーバー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）

正当値

1 ～ 4

デフォルト

適切なインデックス値。

説明

トラップに対応するインデックスの固有の識別子。

cfgIpmiPetAlertDestIpAddr（読み取り / 書き込み）

正当値

有効な IP アドレスを表す文字列。 例：192.168.0.67

デフォルト

0.0.0.0

説明

ネットワーク上でトラップレシーバの送信先 IP アドレスを指定します。 トラップレシーバは、管理下サーバー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）

正当値

0（FALSE）

1（TRUE）

デフォルト

1

説明

特定のトラップを有効または無効にします。

目次ページに戻る

目次ページに戻る

RACADM と SM-CLP の比較

Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00
ユーザーズガイド

表 C-1 は RACADM グループおよびオブジェクトと、同等の SM-CLP 場所（存在する場合）をSM-CLP マップ内にリストにしたものです。

表 C-1. RACADM と SM-CLP の比較

RACADM グループ	SM-CLP	説明
idRacInfo		
idRacName		最大 15 バイトの ASCII 文字列。デフォルト: **iDRAC**
idRacProductInfo		最大 63 バイトの ASCII 文字列。デフォルト: **Integrated Dell Remote Access Controller**
idRacDescriptionInfo		最大 255 バイトの ASCII 文字列。デフォルト: **このシステムコンポーネントは Dell PowerEdge サーバーのリモート管理機能全一式を提供しています。**
idRacVersionInfo		最大 63 バイトの ASCII 文字列。デフォルト: **1**
idRacBuildInfo		最大 16 バイトの ASCII 文字列。
idRacType		デフォルト: **8**
cfgActiveDirectory	**/system1/sp1/oemdell_adservice1**	
cfgADEnable	enablestate	無効にするには 0、有効にするには 1。デフォルト: **0**
cfgADRacName	oemdell_adracname	最大 254 バイトの文字列。
cfgADRacDomain	oemdell_adracdomain	最大 254 バイトの文字列。
cfgADRootDomain	oemdell_adrootdomain	最大 254 バイトの文字列。
cfgADAuthTimeout	oemdell_timeout	15 ～ 300 秒。デフォルト: **120**
cfgADType	oemdell_schematype	標準スキーマは 1、拡張スキーマは 2。デフォルト: **1**
cfgStandardSchema		
cfgSSADRoleGroupIndex	**/system1/sp1/group1** *through* **/system1/sp1/group5**	RACADM — グループインデックス ID（1-5）。 SM-CLP — アドレスパスで選択。
cfgSSADRoleGroupName	oemdell_groupname	最大 254 バイトの文字列。
cfgSSADRoleGroupDomain	oemdell_groupdomain	最大 254 バイトの文字列。
cfgSSADRoleGroupPrivilege	oemdell_groupprivilege	0x00000000 ～ 0x000001ff の値によるビットマスク。
cfgLanNetworking	**/system1/sp1/enetport1**	
cfgNicMacAddress	macaddress	インタフェースの MAC アドレス。編集不可。
	/system1/sp1/enetport1/lanendpt1/ipendpt1	
cfgNicEnable	oemdell_nicenable	NIC を無効にするには 0、NIC を有効にするには 1。デフォルト: **0**
cfgNicUseDHCP	oemdell_usedhcp	静的ネットワークアドレスを設定するには 0、DHCP を使用するには 1。デフォルト: **0**
cfgNicIpAddress	ipaddress	iDRAC の IP アドレス。デフォルト: **192.168.0.120** + サーバーのスロット番号。
cfgNicNetmask	subnetmask	iDRAC ネットワークのサブネットマスク。デフォルト: **255.255.255.0**
	committed	グループ値が変更されると、**committed** は 0 に設定され、新しい値は保存されていないことを示します。新しい設定を保存するには値を 1 に設定します。デフォルト: **1**
	/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1	
cfgDNSDomainName	oemdell_dnsdomainname	最大 254 バイトの ASCII 文字列。英字を少なくとも 1 文字含める必要があります。
cfgDNSDomainNameFromDHCP	oemdell_domainnamefromdhcp	DHCP からドメイン名を取得するには 1 に設定します。デフォルト: **0**
cfgDNSRacName	oemdell_dnsracname	最大 63 バイトの ASCII 文字列。英字を少なくとも 1 文字含める必要があります。デフォルト: **iDRAC-** + Dell サービスタグ

cfgDNSRegisterRac	oemdell_dnsregisterrac	DNS の iDRAC 名を登録するには 1 に設定します。デフォルト:**0**
cfgDNSServersFromDHCP	oemdell_dnsserversfromdhcp	DHCP から DNS サーバーのアドレスを取得するには 1 に設定します。デフォルト:**0**
	/server1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap1	
cfgDNSServer1	dnsserveraddresses1	DNS サーバーの IP アドレスを表す文字列。
	/server1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1/remotesap1	
cfgDNSServer2	dnsserveraddresses2	DNS サーバーの IP アドレスを表す文字列。
	/server1/sp1/enetport1/lanendpt1/ipendpt1/remotesap1	
cfgNicGateway	defaultgatewayaddress	デフォルトゲートウェイの IP アドレスを表す文字列。デフォルト:**192.168.0.1**
cfgRacVirtual	**/server1/sp1/oemdell_vmservice1**	
cfgFloppyEmulation	oemdell_floppyemulation	フロッピーディスクのエミュレーションを有効にするには 1 に設定します。デフォルト:**0**
cfgVirMediaAttached	enabledstate	メディアを連結するには 1 (RACADM)/VMEDIA_ATTACH (SM-CLP)に設定します。デフォルト:1 (RACADM)/VMEDIA_ATTACH (SM-CLP)
cfgVirMediaBootOnce	oemdell_singleboot	選択したメディアから次回の起動を実行するには 1 に設定します。デフォルト:**0**
	/server1/sp1/oemdell_vmservice1/tcpendpt1	
	oemdell_sslenabled	1 つ目の仮想メディアデバイスに対して SSL が有効な場合は 1 に、そうでない場合は 0 に設定されます。編集不可。
cfgVirAtapiSvrPort	portnumber	1 つ目の仮想メディアデバイスに使用するポート。デフォルト:**3668**
	/server1/sp1/oemdell_vmservice1/tcendpt2	
	oemdell_sslenabled	2 つ目の仮想メディアデバイスに対して SSL が有効な場合は 1 に、そうでない場合は 0 に設定されます。編集不可。
cfgVirAtapiSvrPortSsl	portnumber	2 つ目の仮想メディアデバイスに使用するポート。デフォルト:**3670**
cfgUserAdmin	**/server1/sp1/oemdell_vmservice1/tcpendpt2**	
cfgUserAdminEnable	enabledstate	ユーザーを有効にするには 1 に設定します。デフォルト:**0**
cfgUserAdminIndex	userid	ユーザーインデックス、1 ～ 16。
cfgUserAdminIpmiLanPrivilege	oemdell_ipmilanprivileges	2(ユーザー)、3(オペレータ)、4(システム管理者)、15(アクセスなし)。デフォルト:**4**
cfgUserAdminPassword	password	最大 20 バイトの ASCII 文字列。
cfgUserAdminPrivilege	oemdell_extendedprivileges	0x00000000 ～ 0x000001ff のビットマスク値。デフォルト:**0x00000000**
cfgUserAdminSolEnable	solenabled	シリアルオーバー LAN を使用可能にするには 1 に設定します。デフォルト:**0**
cfgUserAdminUserName	username	最大 16 バイトの文字列。
cfgEmailAlert		
cfgEmailAlertAddress		電子メール送信先アドレス、最大 64 バイト。
cfgEmailAlertCustomMsg		電子メールで送信するメッセージ、最大 32 バイト。
cfgEmailAlertEnable		電子メール警告を有効にするには 1 に設定します。デフォルト:**0**
cfgEmailAlertIndex		電子メール警告インスタンスのインデックス。1 ～ 4 の番号。
cfgSessionManagement		
cfgSsnMgtConsRedirMaxSessions		現在許可されているコンソールリダイレクトセッションの数(1 または 2)。デフォルト:**2**
cfgSsnMgtSshIdleTimeout		SSH セッションタイムアウト前のアイドル時間(秒)。タイムアウトを無効にするには 0、もしくは 60 ～ 1920 秒。デフォルト:**300**
cfgSsnMgtTelnetIdleTimeout		Telnet セッションタイムアウト前のアイドル時間(秒)。タイムアウトを無効にするには 0、もしくは 60 ～ 1920 秒。デフォルト:**300**
cfgSsnMgtWebserverTimeout		ウェブインタフェースセッションタイムアウト前のアイドル時間(秒)。60 ～ 1920 秒。デフォルト:**300**
cfgRacTuning		
cfgRacTuneConRedirEnable		コンソールリダイレクトを有効にするには 1、無効にするには 0 に設定します。デフォルト:**1**

cfgRacTuneConRedirEncrypt Enable		コンソールリダイレクトネットワークトラフィックの暗号化を有効にするには 1、無効にするには 0 に設定します。デフォルト:**1**
cfgRacTuneConRedirPort		コンソールリダイレクトに使用するポート。デフォルト:**5900**
cfgRacTuneConRedirVideoPort		ビデオリダイレクトに使用するポート。 デフォルト:**5901**
cfgRacTuneHttpPort		ウェブインタフェース HTTP に使用するポート。デフォルト:**80**
cfgRacTuneHttpsPort		セキュアウェブインタフェース HTTPS に使用するポート。 デフォルト:**443**
cfgRacTuneIpBlkEnable		IP ブロック機能を有効にするには 1 に設定します。デフォルト:**0**
cfgRacTuneIpBlkFailCount		IP のブロック前にカウントされるログイン失敗回数(2 ～ 16)。デフォルト:**5**
cfgRacTuneIpBlkFailWindow		ログイン失敗回数をカウントする秒数(10 ～65535)。デフォルト:**60**
cfgRacTuneIpBlkPenaltyTime		ブロックされた IP がブロックされ続ける秒数(10 ～ 65535)。デフォルト:**300**
cfgRacTuneIpRangeAddr		IP 範囲フィルタの IP アドレス。デフォルト:**192.168.0.1**
cfgRacTuneIpRangeEnable		IP 範囲フィルタ許可するには 1 に設定します。デフォルト:0
cfgRacTuneIpRangeMask		有効な IP アドレスを選択するためにベースアドレスに適用されるビットマスク。デフォルト:**255.255.255.0**
cfgRacTuneLocalServerVideo		ローカル iKVM コンソールを有効にするには 1 に設定します。デフォルト:**1**
cfgRacTuneSshPort		SSH サービスに使用するポート。デフォルト:**22**
cfgRacTuneTelnetPort		Telnet サービスに使用するポート。 デフォルト:**23**
cfgRacTuneWebserverEnable		iDRAC ウェブインタフェースを有効にするには 1 に設定します。デフォルト:**1**
ifcRacManagedNodeOS		
ifcRacMnOsHostname		管理下サーバーのホスト名。最大 255 バイトの文字列。
ifcRacMnOsOsName		管理下サーバーのオペレーティングシステム名。最大 255 バイトの文字列。
cfgRacSecurity	**/system1/sp1/oemdell_racsecurity1**	
cfgRacSecCsrCommonName	commonname	Active Directory のコモンネーム(CN)。最大 254 バイトの文字列。
cfgRacSecCsrCountryCode	oemdell_countrycode	Active Directory の国名。2 文字。
cfgRacSecCsrEmailAddr	oemdell_emailaddress	証明書署名要求に使用する電子メールアドレス。最大 254 バイトの文字列。
cfgRacSecCsrKeySize	oemdell_keysize	暗号化キーの長さ(512、1024、または 2048)。デフォルト:**1024**
cfgRacSecCsrLocalityName	oemdell_localityname	Active Directory の市町村名。最大 254 バイトの文字列。
cfgRacSecCsrOrganizationName	organizationname	Active Directory の組織名。最大 254 バイトの文字列。
cfgRacSecCsrOrganizationUnit	oemdell_organizationunit	Active Directory の組織部門名。最大 254 バイトの文字列。
cfgRacSecCsrStateName	oemdell_statename	Active Directory の州名。最大 254 バイトの文字列。
cfgIpmiSol		
cfgIpmiSolAccumulateInterval		シリアルオーバー LAN パケット一部送信前の最大待機時間(1 ～ 255 ミリ秒)。デフォルト:**10**
cfgIpmiSolBaudRate		シリアルオーバー LAN に使用するボーレート(19200、57600、115200)。デフォルト:**115200**
cfgIpmiSolEnable		シリアルオーバー LAN 機能を有効にするには 1 に設定します。デフォルト:**0**
cfgIpmiSolSendThreshold		SOL データ送信前に収集する最大文字数(1 ～ 255)。デフォルト:**255**
cfgIpmiSolMinPrivilege		SOL の使用に必要とされる最小特権。2(ユーザー)、3(オペレータ)、または 4(システム管理者)。デフォルト:**4**
cfgIpmiLan		
cfgIpmiEncryptionKey		0 ～ 40 の 16 進法の文字列。デフォルト:**0000000000000000000000000000000000000000**
cfgIpmiLanAlertEnable		IPMI LAN 警告を有効にするには 1 に設定します。デフォルト:**0**
cfgIpmiLanEnable		LAN インタフェース上で IPMI を有効にするには 1 に設定します。デフォルト:**0**
cfgIpmiPetCommunityName		最大 18 バイトの文字列。デフォルト:**public**
cfgIpmiPef		
cfgIpmiPefAction		イベントが検知された場合に取る処置。0(なし)、1(電源を切る)、2(リセット)、3(パワーサイクル)。デフォルト:**0**
cfgIpmiPefEnable		プラットフォームイベントフィルタを有効にするには 1 に設定します。デフォルト:**0**
cfgIpmiPefIndex		プラットフォームイベントフィルタのインデックス番号。 (1 ～ 17)
cfgIpmiPefName		プラットフォームイベント名、最大 254 バイトの文字列。編集不可。
cfgIpmiPet		

cfgIpmiPetAlertDestIpAddr		プラットフォームイベントトラップレシーバの IP アドレス。デフォルト:**0.0.0.0**
cfgIpmiPetAlertEnable		プラットフォームイベントトラップを有効にするには 1 に設定します。デフォルト:**1**
cfgIpmiPetIndex		プラットフォームイベントトラップのインデックス番号(1 ～ 4)。

目次ページに戻る

目次ページに戻る

iDRAC の概要

Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00
ユーザーズガイド

Integrated Dell™ Remote Access Controller(iDRAC)はシステム管理ハードウェアおよびソフトウェアのソリューションで、Dell PowerEdge™ システムのリモート管理機能、クラッシュしたシステムの回復機能、電源制御機能を提供します。

iDRAC は、リモート監視 / 制御システムに、内蔵システムオンチップのマイクロプロセッサを採用しています。iDRAC は、システム基板上に管理下 PowerEdge サーバーと共存します。Microsoft® Windows® または Linux オペレーティングシステムを対象とするサーバーオペレーティングシステムは、アプリケーションの実行に従事し、一方で iDRAC はオペレーティングシステム外のサーバーの環境と状態の監視および管理に従事します。

警告またはエラーの発生において、電子メールまたはシンプルネットワーク管理プロトコル(SNMP)によるトラップ警告を送信するよう iDRAC を設定することができます。システムクラッシュの考えられる原因を診断する手助けとして、iDRAC はシステムクラッシュを検知すると、イベントデータのログや、画面のイメージキャプチャを実行できます。

管理下サーバーは、モジュール電源、冷却ファン、Chassis Management Controller(CMC)とともに Dell M1000-e システムエンクロージャ(シャーシ)にインストールされています。CMC は、シャーシにインストールされているすべてのコンポーネントを監視および管理します。冗長 CMC は、一次 CMC に障害が生じた場合にホットフェールオーバーを提供するために追加できます。シャーシは、LCD 表示、ローカルコンソール接続、またウェブインタフェースを介して iDRAC へのアクセスを提供します。

iDRAC へのすべてのネットワーク接続は、CMC ネットワークインタフェース(「GB1」とラベル付けされる CMC RJ45 接続ポート)を介しています。CMC によるサーバー上の iDRAC へのトラフィックは、プライベートな内部ネットワークを経由しています。このプライベートな管理ネットワークは、サーバーのデータパス外およびオペレーティングシステムの制御域外、つまり 帯域外 にあります。管理下サーバーの 帯域内ネットワークインタフェースへは、シャーシにインストールされている I/O モジュール(IOM)を介してアクセスします。

iDRAC ネットワークインタフェースは、デフォルトで無効になっています。iDRAC がアクセス可能な状態になる前に設定する必要があります。iDRAC がネットワーク上で有効になり、設定されると、iDRAC ウェブインタフェース、Telnet または SSH、および Intelligent Platform Management Interface(IPMI)をはじめとする対応のネットワーク管理プロトコルによって、割り当てられた IP アドレスにてアクセスできるようになります。

---

iDRAC の管理機能

iDRAC は次の管理機能を提供しています。

- ダイナミックドメイン名システム(DDNS)の登録
- ウェブインタフェース、コンソールリダイレクト経由のローカル RACADM コマンドラインインタフェース、Telnet/SSH 接続による SM-CLP コマンドラインを使用し、リモートシステムを管理および監視
- Microsoft Active Directory® 認証に対するサポート — 標準スキーマまたは拡張スキーマを使用し、Active Directory での iDRAC のユーザー ID およびパスワードを集中化
- コンソールリダイレクト — リモートシステムのキーボード、ビデオ、マウスの機能を提供
- 仮想メディア — 管理下サーバーによる、管理ステーションのローカルメディアドライブまたはネットワーク共有上の ISO CD/DVD イメージへのアクセスを有効にする
- 監視 — システム情報へのアクセスおよびコンポーネント状態を提供
- 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)、iDRAC のログ、およびオペレーティングシステムの状態とは関係なくクラッシュしたシステムや応答しないシステムの前回クラッシュ画面へのアクセスを提供
- Dell OpenManage™ ソフトウェアの統合 — Dell OpenManage Server Administrator または IT Assistant からの iDRAC ウェブインタフェースの起動が可能
- iDRAC 警告 — 電子メールメッセージまたは SNMP トラップによって、考えられる管理下ノードの不具合を警告
- リモート電源管理 — シャットダウンやリセットなどのリモート電源管理の機能を管理コンソールから提供
- Intelligent Platform Management Interface(IPMI)サポート
- Secure Sockets Layer(SSL)暗号化 — ウェブインタフェースから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不正アクセスを防止
- 役割ベースの権限 — 各種システム管理タスク別に割り当て可能な権限を提供

---

iDRAC のセキュリティ機能

iDRAC は次のセキュリティ機能を提供しています。

- Microsoft Active Directory(オプション)またはハードウェアに保存されたユーザー ID とパスワードによるユーザー認証
- システム管理者が各ユーザーに特定の特権を設定できる役割ベースの権限
- ウェブインタフェースまたは SM-CLP を使用したユーザー ID とパスワードの設定
- 128 ビットの SSL 暗号化と 40 ビットの 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 SM-CLP とウェブインタフェース
- ウェブインターフェースまたは SM-CLP を使用したセッションタイムアウトの設定(秒単位)

- 設定可能な IP ポート(該当する場合)

  メモ: Telnet は SSL 暗号化に対応していません。

- 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制限により制限を越えた IP アドレスのログインを阻止
- iDRAC に接続するクライアントの IP アドレス範囲を限定

対応プラットフォーム

iDRAC は、Dell PowerEdge M1000-e システムエンクロージャ内の以下の PowerEdge システムに対応しています。

- PowerEdge M600
- PowerEdge M605

最新の対応プラットフォームに関しては、iDRAC の readme ファイルおよびデルのサポートウェブサイト **support.dell.com** の『Dell PowerEdge 互換性ガイド』を参照してください。

対応オペレーティングシステム

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

最新情報に関しては、デルのサポートウェブサイト **support.dell.com** の『Dell OpenManage Server Administrator 互換性ガイド』を参照してください。

表 1-1. 対応オペレーティングシステム

オペレーティングシステムファミリ	オペレーティングシステム
Microsoft Windows	Microsoft® Windows Server 2003 R2 Standard、Enterprise(32 ビット x86)Edition SP2 Microsoft Windows Server 2003 Web、Standard、Enterprise(32 ビット x86)Edition SP2 Microsoft Windows Server 2003 Standard、Enterprise(x64)Edition SP2 Microsoft Windows Storage Server 2003 R2 Express、Workgroup、Standard、Enterprise x64 Edition Microsoft Windows Vista® Gold Business、Enterprise Edition Microsoft Windows Server 2008 Web、Standard、Enterprise(32 ビット x86)Edition Microsoft Windows Server 2008 Web、Standard、Enterprise、Datacenter(x64)Edition **メモ:** Windows Server 2003 Service Pack 1 をインストールする場合は、DCOM セキュリティ設定に対する変更に注意してください。詳細は、Microsoft サポート Web サイト **support.microsoft.com/kb/903220** の記事 903220 を参照してください。
Red Hat® Linux®	Enterprise LinuxWS、ES、AS(バージョン 3)(x86 および x86_64) Enterprise LinuxWS、ES、AS(バージョン 4)(x86 および x86_64) Enterprise Linux 5(x86 および x86-64)
SUSE® Linux	Enterprise Server 9 アップデート 2 および 3(x86_64) Enterprise Server 10(Gold)(x86_64)

対応 Web ブラウザ

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

表 1-2 に、iDRAC のクライアントとしてサポートされているウェブブラウザをリストします。

最新情報に関しては、iDRAC の readme ファイルおよびデルのサポートウェブサイト **support.dell.com** の『Dell OpenManage Server Administrator 互換性ガイド』を参照してください。

表 1-2. 対応 Web ブラウザ

オペレーティングシステム	対応ウェブブラウザ
Windows	Internet Explorer 6.0(32 ビット)Service Pack 2(SP2)(Windows XP および Windows 2003 R2 SP2 のみ) Internet Explorer 7.0 Windows Vista、Windows XP および Windows 2003 R2 SP2 のみ
Linux	Mozilla Firefox 1.5(32 ビット)(SUSE Linux(バージョン 10)のみ) Mozilla Firefox 2.0(32 ビット)

対応リモートアクセス接続

表 1-3 に接続の機能をリストにします。

表 1-3. 対応リモートアクセス接続

接続	機能
iDRAC NIC	• 10Mbps/100Mbs/1Gbps Ethernet(CMC GB Ethernet ポート経由) • DHCP 対応 • SNMP トラップと電子メールイベント通知 • SM-CLP(Telnet または SSH)コマンドシェル、および iDRAC 設定、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操作に対するサポート • impitool および ipmishell などの IPMI ユーティリティに対するサポート

---

iDRAC のポート

表 1-4 に、iDRAC が接続において通信に使用するポートをリストします。表 1-5 に、iDRAC 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 iDRAC にリモートからアクセスする場合に必要です。

表 1-4. iDRAC サーバーの通信ポート

ポート番号	機能
22*	Secure Shell(SSH)
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
3668*、3669*	仮想メディアサービス
3770*、3771*	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 1-5. iDRAC のクライアントポート

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

その他の必要マニュアル

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

- iDRAC オンラインヘルプでは、ウェブインタフェースの使用方法について説明しています。
- 『Dell CMC ファームウェアバージョン 1.0 ユーザーズガイド』では、PowerEdge サーバーを含むシャーシ内のすべてのモジュールを管理するコントローラの使用方法について説明しています。
- 『Dell OpenManage IT Assistant ユーザーズガイド』と『Dell OpenManage IT Assistant リファレンスガイド』には、IT Assistant に関する情報が含まれています。
- 『Dell OpenManage Server Administrator ユーザーズガイド』では、Server Administrator のインストールと使用方法について説明しています。
- 『Dell Update Packages ユーザーズガイド』では、システムアップデート対策の一環として Dell Update Packages を入手して使用する方法を説明しています。

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

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

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

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

目次ページに戻る

iDRAC の設定

Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00
ユーザーズガイド

本項では、iDRAC へのアクセスの確立方法と、iDRAC の使用における管理環境の設定方法について説明します。

はじめに

iDRAC の設定には以下のアイテムが必要です。

- 『Dell Chassis Management Controller ユーザーズガイド』
- 『Dell PowerEdge Installation and Server Management CD』
- 『Dell Systems Management Consoles CD』
- 『Dell PowerEdge Service and Diagnostic Utilities CD』
- 『Dell PowerEdge Documentation CD』

---

iDRAC の設定に使用するインタフェース

iDRAC 設定ユーティリティ、iDRAC ウェブインタフェース、ローカル RACADM CLI または SM-CLP CLI を使用して iDRAC を設定できます。管理下サーバーにオペレーティングシステムおよび Dell PowerEdge サーバー管理ソフトウェアをインストールすると、ローカル RACADM CLI が使用可能になります。表 2-1 でこれらのインタフェースについて説明します。

注意: 複数の DRAC 設定インタフェースを同時に使用すると、不測の結果が生じることがあります。

表 2-1. 設定インタフェース

インタフェース	説明
iDRAC 設定ユーティリティ	起動時にアクセスできる設定ユーティリティは、新規 PowerEdge サーバーのインストール時に便利です。ネットワークや基本的なセキュリティ機能の設定、また他の機能を有効にする場合に使用します。
iDRAC ウェブインタフェース	iDRAC ウェブインタフェースは、インタラクティブな iDRAC の管理および管理下サーバーの監視に使用できるブラウザベースの管理アプリケーションです。システム正常性の監視、システムイベントログの表示、ローカル iDRAC ユーザーの管理、CMC ウェブインタフェースやコンソールリダイレクトセッションの起動をはじめとする日常タスクの一次インタフェースです。
CMC ウェブインタフェース	CMC ウェブインタフェースは、シャーシの監視および管理に加え、管理下サーバーの状態の表示、iDRAC のネットワーク設定、管理下サーバーの起動、停止、リセットに使用できます。
シャーシ LCD パネル	iDRAC を搭載したシャーシの LCD パネルは、シャーシ内のサーバーの高レベルな状態表示に使用できます。CMC の初期設定中、設定ウィザードを使用して iDRAC ネットワークの DHCP 設定を有効にできます。
ローカル RACADM	ローカル RACADM コマンドラインインタフェースは管理下サーバーで実行されます。iDRAC ウェブインタフェースで起動された iKVM またはコンソールリダイレクトセッションからアクセスします。RACADM は、Dell OpenManage Server Administrator インストール時に管理下サーバーにインストールされます。 RACADM コマンドは、ほぼすべての iDRAC 機能へのアクセスを提供します。センサーデータ、システムイベントログのレコード、また iDRAC で維持される現在の状態および設定値を調べることができます。さらに、iDRAC 設定値の変更、ローカルユーザーの管理、機能を有効 / 無効にする、管理下サーバーのシャットダウンや再起動などの電源機能の実行も可能です。
iVM-CLI	iDRAC 仮想メディアコマンドラインインタフェース(iVM-CLI)は、管理下サーバーに管理ステーションのメディアへのアクセスを与えます。複数の管理下サーバーにオペレーティングシステムをインストールするスクリプトの展開に便利です。
SM-CLP	SM-CLP は、iDRAC 内蔵のサーバー管理ワークグループサーバー管理-コマンドラインプロトコル(SM-CLP)実装です。SM-CLP コマンドラインには、Telnet または SSH を使用した iDRAC へのログインを使用してアクセスします。 SM-CLP コマンドは、ローカル RACADM コマンドの便利なサブセットを実装します。これらのコマンドは管理ステーションコマンドラインから実行可能なため、スクリプティングに便利です。XML をはじめとする特定のフォーマットで取得可能なコマンドの出力は、スクリプティングや、既存のレポートツールや管理ツールとの統合を容易にします。 RACADM および SM-CLP コマンドの比較については、RACADM と SM-CLP の比較 を参照してください。
IPMI	IPMI は、iDRAC などの内蔵管理システムによる他の内蔵システムや管理アプリケーションとの通信における標準の手法を定義します。 IPMI のプラットフォームイベントフィルタ(PEF)やプラットフォームイベントトラップ(PET)の設定には、iDRAC ウェブインタフェース、SM-CLP、または RACADM コマンドを使用できます。

	PEF は、ある状態を検知したときに選択可能な処置（例：管理下サーバーの再起動）の実行を促します。PET は、特定のイベントまたは状態を検知したときに電子メールまたは IPMI 警告を送信するよう iDRAC に指示します。 また iDRAC では、IPMI オーバー LAN を有効にしている場合に **ipmitool** や **ipmishell** などの標準 IPMI ツールを使用できます。

設定タスク

本項では、管理ステーション、iDRAC、管理下サーバーの設定タスクについての概要を説明します。実行可能なタスクには iDRAC のリモート使用を可能にする iDRAC の設定、使用する iDRAC 機能の設定、管理下サーバーへのオペレーティングシステムのインストール、管理ステーションおよび管理下サーバーへの管理ソフトウェアのインストールなどが含まれます。

各タスクの実行に使用可能な設定タスクは、タスク下にリストされています。

メモ: 本書の設定手順を実行する前に、CMC および I/O モジュールがシャーシにインストールされ、設定されている必要があります。また、PowerEdge サーバーはシャーシ内に物理的に設置されていなければなりません。

管理ステーションの設定

Dell OpenManage ソフトウェア、ウェブブラウザ、他のソフトウェアユーティリティをインストールして、管理ステーションを設定します。

- 管理ステーションの設定 を参照してください。

iDRAC ネットワークの設定

iDRAC ネットワークを有効にし、IP、ネットマスク、ゲートウェイ、DNS アドレスを設定します。

メモ: iDRAC ネットワーク設定の変更により、iDRAC に対する現在のネットワーク接続はすべて終了されます。

メモ: LCD パネルを使用したサーバーの設定オプションは、CMC の初期設定中のみに使用できます。シャーシ導入後、LCD パネルは iDRAC の再設定に使用できません。

メモ: LCD パネルは iDRAC ネットワークの設定において DHCP を有効にする際に使用できます。静的アドレスを割り当てるには、iDRAC 設定ユーティリティまたは CMC ウェブインタフェースを使用します。

- シャーシの LCD パネル — 『Dell Chassis Management Controller ユーザーズガイド』を参照してください。
- iDRAC 設定ユーティリティ — LAN を参照してください。
- CMC ウェブインタフェース — CMC ウェブインタフェースを使用したネットワーク設定 を参照してください。
- RACADM CLI — cfgLanNetworking を参照してください。

iDRAC ユーザーの設定

ローカル iDRAC ユーザーと権限を設定します。iDRAC では、ファームウェアに 16 のローカルユーザーをまとめた表があります。これらのユーザーに対しユーザー名、パスワード、役割を設定できます。

- iDRAC 設定ユーティリティ（システム管理ユーザーのみの設定）— LAN ユーザー設定 を参照してください。
- iDRAC ウェブインタフェース — iDRAC ユーザーの追加と設定 を参照してください。
- RACADM — iDRAC ユーザーの追加 を参照してください。

Active Directory の設定

ローカル iDRAC ユーザーに加え、iDRAC ユーザーログインの認証には Microsoft® Active Directory® を使用できます。

- Microsoft Active Directory との iDRAC の使用 を参照してください。

IP フィルタおよび IP ブロックの設定

ユーザー認証に加え、規定範囲外の IP アドレスからの接続を拒否したり、設定可能な時間枠内で複数回認証に失敗した IP アドレスからの接続を一時的にブロックすることにより、不正なアクセスを阻止できます。

- iDRAC ウェブインタフェース — IP フィルタおよび IP ブロックの設定 を参照してください。
- RACADM — IP フィルタ（IpRange）の設定、IP ブロックの設定 を参照してください。

プラットフォームイベントの設定

プラットフォームイベントは、iDRAC が管理下サーバーのセンサーから警告状態または重要状態を検知した場合に発生します。

プラットフォームイベントフィルタ(PEF)を設定して、あるイベントが検知された時に管理下サーバーを再起動するなど、検知するイベントを選択します。

- iDRAC ウェブインタフェース — プラットフォームイベントフィルタ(PEF)を参照してください。
- RACADM — PEF の設定 を参照してください。

プラットフォームイベントトラップ(PET)を設定して、IPMI ソフトウェアを搭載した管理ステーションなどの IP アドレスに警告通知を送信したり、指定の電子メールアドレスに電子メールを送信します。

- iDRAC ウェブインタフェース — プラットフォームイベントトラップ(PET)を参照してください。
- RACADM — PET の設定 を参照してください。

シリアルオーバー LAN の設定

シリアルオーバー LAN(SOL)は、管理下サーバーのネットワーク上のシリアルポート I/O をリダイレクトできる IPMI 機能です。SOL は、iDRAC のコンソールリダイレクト機能を有効にします。

- iDRAC ウェブインタフェース — シリアルオーバー LAN の設定 を参照してください。
- GUI コンソールリダイレクトの使用 も参照してください。

iDRAC サービスの設定

iDRAC ネットワークサービス(Telnet、SSH、Web Server インタフェースなど)を有効 / 無効にしたり、ポートや他のサービスパラメータを再設定します。

- iDRAC ウェブインタフェース — iDRAC サービスの設定 を参照してください。
- RACADM — ローカル RACADM を使用した iDRAC Telnet および SSH サービスの設定 を参照してください。

セキュアソケットレイヤ(SSL)の設定

iDRAC Web Server の SSL 設定

- iDRAC ウェブインタフェース — セキュアソケットレイヤ(SSL)を参照してください。
- RACADM — cfgRacSecurity、sslcsrgen、sslcertupload、sslcertdownload、sslcertview を参照してください。

仮想メディアの設定

PowerEdge サーバーにオペレーティングシステムをインストールできるよう、仮想メディア機能を設定します。仮想メディアを使用すると、管理下サーバーは管理ステーションのメディアデバイスやネットワーク共有上の ISO CD/DVD イメージにまるで管理下サーバーにあるデバイスであるようにアクセスできるようになります。

- iDRAC ウェブインタフェース — 仮想メディアの設定および使い方 を参照してください。
- iDRAC 設定ユーティリティ — 仮想メディア を参照してください。

管理下サーバーソフトウェアのインストール

仮想メディアを使用して PowerEdge サーバーに Microsoft Windows または Linux オペレーティングシステムをインストールし、管理下 PowerEdge サーバーに Dell OpenManage ソフトウェアをインストールして、前回クラッシュ画面機能を設定します。

- コンソールリダイレクト — 管理下サーバーのソフトウェアのインストール を参照してください。
- iVM-CLI — 仮想メディアコマンドラインインタフェースユーティリティの使用 を参照してください。

前回クラッシュ画面機能に対する管理下サーバーの設定

オペレーティングシステムのクラッシュや凍結後に iDRAC が画面イメージをキャプチャできるよう、管理下サーバーを設定します。

- 管理下サーバー — 管理下サーバーの前回クラッシュ画面キャプチャ設定、Windows 自動再起動オプションを無効にする を参照してください。

CMC ウェブインタフェースを使用したネットワーク設定

メモ: CMC から iDRAC ネットワークを設定するには、シャーシ設定システム管理者特権が必要です。

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

メモ: CMC の IP アドレスは、**システム**→ **リモートアクセス**→ **CMC** をクリックすると iDRAC ウェブインタフェースに表示されます。このページから CMC ウェブインタフェースを起動することもできます。

1. ウェブブラウザに https://<CMC-IP-アドレス> または https://<CMC-DNS-名> 形式の URL を入力して、CMC ウェブユーザーインタフェースにログインします。
2. CMC のユーザー名とパスワードを入力して、**OK** をクリックします。
3. 左の列の **シャーシ** の隣にあるプラス(+)をクリックし、**サーバー** をクリックします。
4. **設定**→ **導入** をクリックします。
5. **LAN を有効にする** の見出し下のサーバーの隣にあるチェックボックスを選択してサーバーの LAN を有効にします。
6. **IPMI オーバー LAN を有効にする** の見出し下のサーバーの隣にあるチェックボックスを選択 / 選択解除して、IPMI オーバー LAN を有効 / 無効にします。
7. **DHCP の有効** の見出し下のサーバーの隣にあるチェックボックスを選択 / 選択解除してサーバーの DHCP を有効 / 無効にします。
8. DHCP が無効にされている場合は、サーバーの静的 IP アドレス、ネットマスク、デフォルトゲートウェイを入力します。
9. ページ下にある **適用** をクリックします。

---

iDRAC ファームウェアのアップデート

iDRAC ファームウェアのアップデートによって、iDRAC のフラッシュメモリの新規ファームウェアイメージがインストールされます。次のいずれかの方法でファームウェアをアップデートできます。

- SM-CLP **load** コマンド
- iDRAC ウェブインタフェース
- Dell アップデートパッケージ(Linux または Microsoft Windows 用)
- DOS iDRAC ファームウェアアップデートユーティリティ
- CMC ウェブインタフェース(iDRAC ファームウェアが破壊されている場合のみ)

ファームウェアまたはアップデートパッケージのダウンロード

ファームウェアを **support.dell.com** からダウンロードします。ファームウェアイメージは、使用可能な各種アップデート方法に対応するいくつかのフォーマットで入手可能です。

iDRAC ウェブインタフェースまたは SM-CLP を使用した iDRAC ファームウェアのアップデート、または CMC ウェブインタフェースを使用した iDRAC の回復には、自己解凍式アーカイブとしてパッケージされるバイナリイメージをダウンロードします。

管理下サーバーからの iDRAC ファームウェアのアップデートには、アップデートする iDRAC のサーバーで実行しているオペレーティングシステム特有の Dell アップデートパッケージ(DUP)をダウンロードします。

DOS iDRAC ファームウェアアップデートユーティリティを使用した iDRAC ファームウェアのアップデートには、自己解凍式のアーカイブファイルにパッケージされたアップデートユーティリティおよびバイナリイメージの両方をダウンロードします。

ファームウェアアップデートの実行

メモ: iDRAC ファームウェアアップデートが開始されると、すべての既存 iDRAC セッションは切断され、アップデートプロセスが完了するまで新規セッションは許可されません。

メモ: シャーシファンは iDRAC ファームウェアアップデート中 100% で稼動します。アップデートが完了すると、正常なファン速度制御が再開されます。これは、センサー情報を CMC に送信できないときにサーバーをオーバーヒートから保護するよう設計されている、正常な動作です。

Linux または Microsoft Windows 用の Dell アップデートパッケージを使用するには、管理下サーバーでオペレーティングシステム特有の DUP を実行します。

SM-CLP **load** コマンドを使用する場合、トリビアルファイル転送プロトコル(TFTP)サーバーが iDRAC に配信可能なディレクトリにファームウェアのバイナリイメージを配置します。SM-CLP を使用した iDRAC ファームウェアのアップデート を参照してください。

iDRAC ウェブインタフェースまたは CMC ウェブインタフェースを使用する場合、ウェブインタフェースを実行している管理ステーションにアクセス可能なディスクにファームウェアのバイナリイメージを配置します。iDRAC ファームウェアのアップデート を参照してください。

メモ: iDRAC ウェブインタフェースを使用すると、iDRAC 設定を出荷時のデフォルト設定にリセットすることもできます。

CMC ウェブインタフェースは、iDRAC ファームウェアアップデートの進行が完了前に中断された場合など、CMC が iDRAC ファームウェアの破壊を検知したときにファームウェアのみをアップデートするのに使用できます。CMC を使用した iDRAC ファームウェアの回復 を参照してください。

DOS アップデートユーティリティの使用

DOS アップデートユーティリティを使用して iDRAC ファームウェアをアップデートするには、管理下サーバーを DOS に起動し、**idrac16d** コマンドを実行します。コマンドの構文は次の通りです。

```
idrac16d [-f] [-i=<ファイル名>] [-l=<ログファイル>]
```

オプションなしで実行すると、**idrac16d** コマンドは現在のディレクトリにあるファームウェアイメージファイル **firmimg.imc** を使って iDRAC をアップデートします。

オプションは次の通りです。

`-f` — アップデートの強制。`-f` オプションは、ファームウェアを以前のイメージにダウングレードする際に使用できます。

`-i=<ファイル名>` — ファームウェアイメージを含むファイル名イメージの指定。このオプションは、ファームウェアファイル名がデフォルト名 **firmimg.imc** から変更された場合に必要です。

`-l=<ログファイル>` — アップデートアクティブティからの出力ログ。このオプションは、デバッグに使用します。

注意:idrac16d コマンドに不正な引数を入力したり、`-h` オプションを与えると、使用方法の出力に追加オプション `-nopresconfig` が与えられます。このオプションは、設定情報を一切保存することなくファームウェアをアップデートするのに使用されます。IP アドレス、ユーザー、パスワードなどの既存の iDRAC 設定情報をすべて削除してしまうため、このオプションは使用 **しない** でください。

デジタル署名の検証

デジタル署名は、ファイル署名者の身元を認証したり、署名後ファイルのオリジナル内容が変更されていないことを証明するのに使用されます。

システムにまだインストールされていない場合は、デジタル署名の検証を行う Gnu Privacy Guard（GPG）をインストールしてください。標準の検証手順を使用するには、次の手順を実行してください。

1. まだ取得していない場合は、**lists.us.dell.com** に移動し、**Dell Public GPG キー** リンクをクリックして Dell Linux GnuPG 公開キーをダウンロードします。ファイルをローカルシステムに保存します。デフォルト名は、**linux-security- publickey.txt** です。

2. 次のコマンドを実行し、公開キーを `gpg` トラストデータベースにインポートします。

   ```
   gpg --import <公開キーファイル名>
   ```

   メモ: プロセスを完了するには、プライベートキーが必要です。

3. 不信なキー警告を回避するため、Dell Public GPG キーのトラストレベルを変更します。

   a. 次のコマンドを入力します。

      ```
      gpg --edit-key 23B66A9D
      ```

   b. GPG キーエディターに `fpr` と入力します。次のメッセージが表示されます。

      ```
      pub 1024D/23B66A9D 2001-04-16 Dell, Inc. （製品グループ）<linux-security@dell.com>
      一次キーフィンガープリント：4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D
      ```

      インポートしたキーのフィンガープリントが上記と一致していれば、キーの正確なコピーを入手したことになります。

   c. GPG キーエディターに `trust` と入力します。次のメニューが表示されます。

      ```
      Please decide how far you trust this user to correctly verify other users' keys (by looking at passports, checking fingerprints from
      different sources, etc.)
        1 = I don't know or won't say
        2 = I do NOT trust
        3 = I trust marginally
        4 = I trust fully
        5 = I trust ultimately
        m = back to the main menu

      Your decision?

      （パスポートを確認したり、他から入手したフィンガープリントの検査を行うことで、他のユーザーのキーを正確に検証することに関しての、このユーザーに対する信用度
      を決めてください。
        1 = 分からない、または何とも言えない
        2 = 信用しない
        3 = ある程度信用する
        4 = 完全に信用する
        5 = 絶対的に信用する
        m = メインメニューに戻る

      あなたの決定は？）
      ```

   d. `5 <Enter>` と入力します。次のプロンプトが表示されます。

      ```
      Do you really want to set this key to ultimate trust? （y/N）
      （本当にこのキーを絶対的に信用しますか？[y/N]）
      ```

   e. `y <Enter>` と入力して意思を確認します。

   f. `quit <Enter>` と入力して GPG キーエディターを終了します。

公開キーは、一度だけインポートおよび認証してください。

4. 必要なパッケージ（例、Linux DUP または自己解凍式アーカイブ）および関連の署名ファイルをデルのサポートウェブサイト **support.dell.com / support / downloads** から取得します。

   メモ: Linux アップデートパッケージにはそれぞれ、アップデートパッケージとして同じウェブページに表示される別個の署名ファイルがあります。検証には、アップデートパッケージと関連の署名ファイルが両方必要です。デフォルトで、署名ファイル名は DUP ファイル名と同じで、**.sign** 拡張子を含んでいます。例えば、Linux DUP は **PE1850-BIOS-LX-A02.BIN**、その署名ファイル名は **PE1850-BIOS-LX-A02.BIN.sign** です。iDRAC ファームウェアイメージにもファームウェアイメージとともに自己解凍式アーカイブに含まれる、関連の **.sign** ファイルが含まれます。ファイルをダウンロードするには、ダウンロードリンクを右クリックし、**名前を付けて保存...** ファイルオプションを使用します。

5. アップデートパッケージの検証:

   ```
   gpg --verify <Linux アップデートパッケージ署名ファイル名> <Linux アップデートパッケージファイル名>
   ```

次の例で 1425SC BIOS アップデートパッケージの検証手順を説明します。

1. **support.dell.com** から次の 2 つのファイルをダウンロードします。
   - PESC1425-BIOS-LX-A01.bin.sign
   - PESC1425-BIOS-LX-A01.bin

2. 次のコマンドラインを実行して公開キーをインポートします。

   ```
   gpg --import <linux-security-publickey.txt>
   ```

   次の出力メッセージが表示されます。

   ```
   gpg: key 23B66A9D: "Dell Computer Corporation (Linux Systems Group)<linux-security@dell.com> " not changed
   gpg: Total number processed: 1
   gpg: unchanged: 1
   ```

3. Dell 公開キーの GPG トラストレベルを設定します（まだ設定していない場合）。

   a. 次のコマンドを入力します

      ```
      gpg --edit-key 23B66A9D
      ```

   b. コマンドプロンプトで、次のコマンドを入力します。

      ```
      fpr
      trust
      ```

   c. 5 <Enter> と入力して、メニューから I trust ultimately （絶対的に信用する） を選択します。

   d. y <Enter> と入力して意思を確認します。

   e. quit <Enter> と入力して GPG キーエディターを終了します。

   Dell 公開キーの検証が完了しました。

4. 次のコマンドを実行して、PESC1425 BIOS パッケージのデジタル署名を検証します。

   ```
   gpg --verify PESC1425-BIOS-LX-A01.bin.sign PESC1425-BIOS-LX-A01.bin
   ```

   次の出力メッセージが表示されます。

   ```
   gpg: Signature made Thu 14 Apr 2005 04:25:37 AM IST using DSA key ID 23B66A9D
   gpg: Good signature from "Dell Computer Corporation (Linux Systems Group) <linux-security@dell.com>&
   ```

   メモ: ステップ 3 で説明しているキーの検証を行っていない場合、追加メッセージが表示されます。

   ```
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg: There is no indication that the signature belongs to owner.
   Primary key fingerprint: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D>
   ```

目次ページに戻る

目次ページに戻る

管理ステーションの設定

Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00
ユーザーズガイド

管理ステーションは、シャーシ内の PowerEdge サーバーとその他のモジュールを監視および管理するのに使用するコンピュータです。本項では、iDRAC と連動する管理ステーションを設定するソフトウェアのインストールと設定タスクについて説明します。iDRAC の設定を開始する前に、本項の手順に従い必要なツールがインストールおよび設定されているかを確認してください。

管理ステーションの設定手順

管理ステーションを設定するには、次の手順を実行してください。

1. 管理ステーションネットワークを設定します。
2. 対応ウェブブラウザをインストールして設定します。
3. Java Runtime Environment(JRE)をインストールします(Windows の場合はオプション)。
4. 必要に応じて Telnet または SSH クライアントをインストールします。
5. 必要に応じて TFTP サーバーをインストールします。
6. Dell OpenManage IT Assistant をインストールします(オプション)。

管理ステーションのネットワーク要件

iDRAC にアクセスするには、管理ステーションが「GB1」とラベル付けされた CMC RJ45 接続ポートと同じネットワーク上に存在する必要があります。管理ステーションが iDRAC に LAN アクセスできても管理下サーバーにはアクセスできないようにCMC ネットワークを管理下サーバーが存在するネットワークから切り離すことも可能です。

iDRAC コンソールリダイレクト機能を使用すると(GUI コンソールリダイレクトの使用)、サーバーのポートにネットワークアクセスしていない場合でも管理下サーバーのコンソールにアクセスできます。iDRAC 機能を使用すると、コンピュータの再起動など、管理下サーバーの一部の管理機能も実行できます。ただし、管理下サーバーでホストされるネットワークやアプリケーションサービスにアクセスするには、管理コンピュータに追加 NIC が必要な場合があります。

対応 Web ブラウザの設定

本項では、iDRAC ウェブインタフェースと併用する対応ウェブブラウザの設定手順について説明します。対応ウェブブラウザのリストについては、対応 Web ブラウザ を参照してください。

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

ウェブインタフェースに接続するウェブブラウザの設定

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

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

1. Web ブラウザのウィンドウを開きます。
2. **ツール** をクリックし、**インターネットオプション** をクリックします。
3. **インターネットオプション** ウィンドウで、**接続** タブをクリックします。

4. **ローカルエリアネットワーク(LAN)の設定** で **LAN の設定** をクリックします。
5. **プロキシサーバーを使用** ボックスが選択されている場合は、**ローカルアドレスにはプロキシサーバーを使用しない** ボックスを選択します。
6. **OK** を 2 度クリックします。

信用できるドメインリストへの iDRAC の追加

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

ローカライズされたウェブインタフェースバージョンの表示

iDRAC ウェブインタフェースは、次のオペレーティングシステム言語に対応しています。

- 英語
- フランス語
- ドイツ語
- スペイン語
- 日本語
-

Internet Explorer 6.0(Windows)

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

1. **ツール** メニューをクリックし、**インターネットオプション** を選択します。
2. **インターネットオプション** ウィンドウで **言語** をクリックします。
3. **言語の設定** ウィンドウで **追加** をクリックします。
4. **言語の追加** ウィンドウで、サポートされている言語から 1 つを選択します。

   複数の言語を選択するには、<Ctrl> を押します。
5. 使用する言語を選択し、**上へ移動** をクリックしてその言語をリストの一番上に移動します。
6. **言語の設定** ウィンドウで **OK** をクリックします。
7. **OK** をクリックします。

Firefox 1.5(Linux)

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

1. **編集→ 設定** をクリックし、**詳細設定** タブをクリックします。
2. **言語** セクションで **選択** をクリックします。
3. **追加する言語を選択...** をクリックします。
4. 対応言語を選択し、**追加** をクリックします。
5. 使用する言語を選択し、**上へ移動** をクリックしてその言語をリストの一番上に移動します。
6. 言語メニューで **OK** をクリックします。
7. **OK** をクリックします。

Linux のロケール設定

コンソールリダイレクトビューアで正しく表示するには、UTF-8 文字コードが必要です。文字化けしている場合は、ロケールを確認し、必要に応じて文字コードをリセットしてください。

次の手順は、簡体中国語 GUI の Red Hat® Enterprise Linux® クライアントで文字コードを設定する方法です。

1. コマンドターミナルを開きます。
2. locale と入力し、<Enter> キーを押します。次のような出力画面が表示されます。

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

3. 値に「zh_CN.UTF-8」が含まれる場合は、変更の必要はありません。値に「zh_CN.UTF-8」が含まれない場合は、ステップ 4 に進みます。
4. テキストエディターで **/etc/sysconfig/i18n** ファイルを編集します。
5. ファイルに、次の変更を適用します。

   現在のエントリ

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

   アップデートされたエントリ

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

6. ログアウトしてから、オペレーティングシステムにログインします。

他の言語から切り換える場合、この修正が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。

Firefox のホワイトリスト機能を無効にする

Firefox には、プラグインをホストする各サイトに対してプラグインをインストールするにあたりユーザーの許可を求める「ホワイトリスト」と呼ばれるセキュリティ機能があります。ホワイトリスト機能は、有効な場合、ビューアのバージョンは同一でも iDRAC にアクセスする度にコンソールリダイレクトビューアをインストールするよう要求します。

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

1. Firefox ウェブブラウザのウィンドウを開きます。
2. アドレスフィールドに about:config と入力し、<Enter> を押します。
3. **設定名** 行の **xpinstall.whitelist.required** を検索しダブルクリックします。

   設定名、**状態**、**型**、**値**の値が太字に変更されます。**状態**の値が**ユーザ設定**に変わり、**値** 値が **false**に変わります。
4. **設定名** の列で、**xpinstall.enabled** を検索します。

   値 が **true** になっていることを確認します。true になっていない場合は、**xpinstall.enabled** をダブルクリックし、**値** を **true** に設定します。

Java Runtime Environment（JRE）のインストール

メモ: Internet Explorer ブラウザを使用する場合、コンソールビューアに対し ActiveX コントロールが提供されます。JRE をインストールし、ビューア起動前に iDRAC ウェブインタフェースでコンソールビューアを設定すると、Internet Explorer で Java コンソールビューアも使用できます。詳細に関しては、iDRAC ウェブインタフェースでのコンソールリダイレクトの設定 を参照してください。

ビューアを起動する前に代わりに Java Viewer を使用するよう選択できます。

Firefox ブラウザを使用する場合、コンソールリダイレクト機能を使用するには JRE(または Java Development Kit [JDK])をインストールする必要があります。コンソールビューアは、iDRAC ウェブインタフェースから管理ステーションにダウンロードされ、管理ステーション上で Java Web Start によって起動されます。

java.sun.com へアクセスし、JRE または JDK をインストールします。バージョン 1.6(Java 6.0)以降が推奨されます。

Telnet または SSH クライアントのインストール

デフォルトで、iDRAC の Telnet サービスは無効に、SSH サービスは有効になっています。Telnet はセキュアでないプロトコルなため、SSH クライアントをインストールできない場合またはネットワーク接続がセキュアな場合のみに使用してください。

メモ: iDRAC に対して 1 度にアクティブ可能な接続は Telnet または SSH のいずれかのみです。アクティブな接続が存在する場合、他の接続を試行すると拒否されます。

iDRAC での Telnet

Telnet は、Microsoft® Windows® および Linux オペレーティングシステムに搭載され、コマンドシェルから実行できます。オペレーティングシステムに搭載されているスタンダードバージョンの他に、さらに便利な機能の付いた有料 / 無料 Telnet クライアントをインストールするよう選択することもできます。

管理ステーションで Windows XP または Windows 2003 を実行している場合は、iDRAC の Telnet セッションで文字の不具合が発生する可能性があります。リターンキーが応答しなかったり、パスワードプロンプトが表示されないなど、ログインの停止が発生することがあります。

この不具合を修正するには、Microsoft のサポートウェブサイト **support.microsoft.com** から修正プログラム 824810 をダウンロードしてください。詳細に関しては、Microsoft Knowledge Base の記事 824810 を参照してください。

Telnet セッションのバックスペースキーの設定

クライアントによっては、<Backspace> キーを使用すると、不測の結果が生じることがあります。たとえば、セッションが ^h をエコーする場合があります。ただし、ほとんどの Microsoft および Linux telnet クライアントでは <Backspace> キーを使えるように設定できます。

Microsoft telnet クライアントで <Backspace> キーを使えるように設定するには、次の手順を実行してください。

1. コマンドプロンプトウィンドウを開きます(必要な場合)。
2. telnet セッションを実行していない場合は、次のように入力します。

   ```
   Telnet
   ```

   telnet セッションを実行している場合は、<Ctrl><]> を押します。
3. プロンプトで次のように入力します。

   ```
   set bsasdel
   ```

   次のメッセージが表示されます。

   ```
   Backspace will be sent as delete.
   (Backspace が削除として送信されます。)
   ```

Linux の telnet セッションで <Backspace> キーを使えるように設定するには、次の手順を実行してください。

1. シェルを開き、次のように入力します。

   ```
   stty erase ^h
   ```
2. プロンプトで次のように入力します。

   ```
   Telnet
   ```

iDRAC での SSH

セキュアシェル(SSH)は、Telnet セッションと同じ機能を持つコマンドライン接続ですが、セキュリティ向上のためセッションのネゴシエーションと暗号化機能を備えています。iDRAC は、パスワード認証付きの SSH バージョン 2 に対応しています。SSH はデフォルトで、iDRAC で有効になっています。

管理下サーバーの iDRAC に接続するのに、管理ステーション上の PuTTY(Windows)または OpenSSH(Linux)を使用できます。ログイン手続中にエラーが発生すると、**ssh** クライアントからエラーメッセージが発行されます。メッセージのテキストはクライアントによって異なり、iDRAC ではコントロールできません。

メモ: OpenSSH はWindows の VT100 または ANSI ターミナルエミュレータから実行する必要があります。Windows のコマンドプロンプトで OpenSSH を実行すると、完全には機能しません(一部のキーが応答せず、グラフィックが表示されません)。

1 度にサポートされる Telnet または SSH セッションは 1 つだけです。セッションタイムアウトは、iDRAC 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 に記述されるように、

cfgSsnMgtSshIdleTimeout プロパティによって制御されます。

iDRAC の SSH の実装では、表 3-1 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。

メモ: SSHv1 はサポートされていません。

表 3-1. 暗号化スキーム

スキームの種類	スキーム
非対称暗号	Diffie-Hellman DSA/DSS 512-1024(ランダム)ビット(NIST 仕様当り)
対称暗号	• 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

TFTP サーバーのインストール

メモ: SSL 証明書の転送および新規 iDRAC ファームウェアのアップロードに iDRAC ウェブインタフェースのみを使用する場合、TFTP サーバーは不要です。

トリビアルファイル転送プロトコル(TFTP)は、ファイル転送プロトコル(FTP)が簡素化されたものです。iDRAC へ / からのファイル転送に SM-CLP や RACADM コマンドラインインタフェースと併用されます。

iDRAC へ / からのファイルのコピーが必要になるのは、iDRAC ファームウェアをアップデートする場合または iDRAC に証明書をインストールする場合のみです。これらのタスクを実行する際に SM-CLP または RACADM を使用する場合、iDRAC が IP 番号または DNS 名でアクセスできるコンピュータで TFTP サーバーを実行している必要があります。

TFTP サーバーがすでに通信しているかどうかを調べるには、Windows または Linux オペレーティングシステムの **netstat -a** コマンドを使用できます。TFTP のデフォルトポートは、ポート 69 です。サーバーが実行されていない場合、次のオプションがあります。

- TFTP サービスを実行しているネットワーク上で別のコンピュータを検索する
- Linux を使用している場合、配線から TFTP サーバーをインストールする
- Windows を使用している場合、有料 / 無料の TFTP サーバーをインストールする

Dell OpenManage IT Assistant のインストール

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

- 『Dell Systems Management Consoles CD』— Dell OpenManage IT Assistant をはじめとする最新 Dell システム管理コンソール製品のすべてが含まれています。
- 『Dell PowerEdge Service and Diagnostic Utilities CD』— システムの設定に必要なツールを提供し、システムの最新の BIOS、ファームウェア、診断、Dell 用に最適化したドライバを配布します。
- 『Dell PowerEdge Documentation CD』— システム、システム管理ソフトウェア製品、周辺機器、RAID コントローラなどの最新マニュアルを提供します。
- デルのサポートウェブサイトおよび readme ファイル — Dell 製品についての最新情報に関しては、readme ファイルおよびデルのサポートウェブサイト **support.dell.com** を確認してください。

Dell OpenManage IT Assistant を含む管理コンソールソフトウェアを管理ステーションにインストールするには、『Dell System Management Consoles CD』を使用します。このソフトウェアのインストール手順は、『クイックインストールガイド』を参照してください。

目次ページに戻る

目次ページに戻る

管理下サーバーの設定

Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00
ユーザーズガイド

本項では、リモート管理機能を強化する管理下サーバーの設定タスクについて説明します。これらのタスクには、Dell Open Manage Server Administrator ソフトウェアのインストールおよび管理下サーバーの前回クラッシュ画面キャプチャ設定が含まれます。

管理下サーバーのソフトウェアのインストール

Dell 管理ソフトウェアには、次の機能が含まれます。

- ローカル RACADM CLI — 管理下システムから iDRAC の設定および管理を可能にします。設定タスクおよび管理タスクのスクリプティングをサポートする強力なツールです。
- iDRAC の前回クラッシュ画面機能を使用するには Server Administrator が必要です。
- Server Administrator — ネットワーク上のリモートホストからリモートシステムを管理できるウェブインタフェース。
- Server Administrator Instrumentation Service — 業界標準のシステム管理エージェントによって収集される詳細なエラー情報およびパフォーマンス情報へのアクセスを提供し、シャットダウン、起動、セキュリティを含む監視下システムのリモート管理を可能にします。
- Server Administration Storage Management Service — 内蔵グラフィカル表示でストレージ管理情報を提供します。
- Server Administrator ログ — システム、監視下ハードウェアイベント、POST イベント、システム警告に対して / よって発行されるコマンドのログを表示します。ホームページでのログの表示、レポートとしての印刷または保存、指定サービス連絡先への電子メールの送信が可能です。

Server Administrator をインストールするには、『Dell PowerEdge Installation and Server Management CD』を使用します。このソフトウェアのインストール手順は、『クイックインストールガイド』を参照してください。

管理下サーバーの前回クラッシュ画面キャプチャ設定

iDRAC は、管理下システムのクラッシュ原因についてトラブルシューティングをサポートするよう前回クラッシュ画面をキャプチャし、ウェブインタフェースに表示できます。前回クラッシュ画面機能を有効にするには、次の手順を実行します。

1. 管理下サーバーソフトウェアのインストール管理下サーバーソフトウェアのインストールについての詳細に関しては、『Server Administrator ユーザーズガイド』を参照してください。
2. Microsoft® Windows® オペレーティングシステムを実行している場合、**Windows 起動と回復** で自動再起動機能が選択解除されていることを確認してください。Windows 自動再起動オプションを無効にする を参照してください。
3. iDRAC ウェブインタフェースで前回クラッシュ画面（デフォルトでは無効）を有効にします。

   iDRAC ウェブインタフェースで前回クラッシュ画面機能を有効にするには、**システム**→ **リモートアクセス**→ **iDRAC**→ **ネットワーク / セキュリティ**→ **サービス** をクリックし、自動システム回復エージェント設定の見出し下にある **有効** チェックボックスを選択します。

   ローカル RACADM を使用して前回クラッシュ画面機能を有効にするには、管理下システムでコマンドプロンプトを開き、次のコマンドを入力します。

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

4. Server Administrator ウェブインタフェースで、**自動回復** タイマーを有効にし、**自動回復** 処置を **リセット**、**電源オフ**、または **パワーサイクル** に設定します。

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

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

Windows 自動再起動オプションを無効にする

iDRAC が前回クラッシュ画面をキャプチャできるようにするには、Microsoft Windows Server® または Windows Vista® を実行している管理下サーバーの **自動再起動** オプションを無効にします。

1. Windows の **コントロールパネル** を開いて、**システム** アイコンをダブルクリックします。
2. **詳細** タブをクリックします。
3. **起動と回復** で、**設定** をクリックします。

4. **自動的に再起動する** 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。

目次ページに戻る

目次ページに戻る

ウェブインタフェースを使用した iDRAC の設定

Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00
ユーザーズガイド

iDRAC は、iDRAC プロパティとユーザーの設定、リモート管理タスクの実行、リモート(管理下)システムの不具合におけるトラブルシューティングが可能なウェブインタフェースを提供します。日常のシステム管理では、iDRAC のウェブインタフェースを使用します。本章では、iDRAC のウェブインタフェースを使って一般的なシステム管理タスクを実行する方法について説明し、関連情報へのリンクも掲載します。

ほとんどのウェブインタフェース設定タスクは、ローカル RACADM コマンドまたは SM-CLP コマンドでも実行できます。

ローカル RACADM コマンドは、管理下サーバーから実行できます。ローカル RACADM の詳細に関しては、ローカル RACADM コマンドラインインタフェースの使用 を参照してください。

SM-CLP コマンドは、Telnet または SSH 接続によってリモートでアクセス可能なシェルにて実行できます。SM-CLP の詳細に関しては、iDRAC SM-CLP コマンドラインインタフェースの使用 を参照してください。

ウェブインタフェースへのアクセス

iDRAC ウェブインタフェースにアクセスするには、次の手順を実行してください。

1. サポートされている Web ブラウザのウィンドウを開きます。

   詳細については、対応 Web ブラウザ を参照してください。

2. **アドレス** フィールドに、`https://<iDRAC IP アドレス>` を入力し、<Enter> を押します。

   デフォルトの HTTPS ポート番号(ポート 443)が変更されていたら、次のように入力します。

   `https://<iDRAC IP アドレス>:<ポート番号>`

   「iDRAC IP アドレス」は iDRAC 用の IPアドレスで、「ポート番号」は HTTPS ポート番号です。

   iDRAC の **ログイン** ウィンドウが表示されます。

ログイン

iDRAC ユーザーまたは Microsoft® Active Directory® ユーザーとしてログインできます。デフォルトのユーザー名は **root**、デフォルトのパスワードは **calvin** です。

iDRAC にログインするには、システム管理者から **iDRAC へのログイン** 特権が与えられている必要があります。

ログインするには、次の手順を実行してください。

1. **ユーザー名** フィールドに、次のいずれかを入力します。
   - iDRAC ユーザー名。

     ローカルユーザーのユーザー名は大文字と小文字が区別されます。例えば、`root`、`it_user`、`john_doe` などです。

   - Active Directory ユーザー名。

     Active Directory 名は、<ドメイン>\<ユーザー名>、<ドメイン>/<ユーザー名>、<ユーザー>@<ドメイン> のいずれかの形式で入力できます。大文字と小文字の区別はありません。例えば、`dell.com\john_doe`、`JOHN_DOE@DELL.COM` などです。

2. **パスワード** フィールドに、iDRAC のユーザーパスワードまたは Active Directory のユーザーパスワードを入力します。パスワードは大文字と小文字が区別されます。

3. **OK** をクリックするか <Enter> を押します。

ログアウト

1. セッションを閉じるには、メインウィンドウの右上にある **ログアウト** をクリックします。

2. ブラウザのウィンドウを閉じます。

メモ: ログインするまで **ログアウト** ボタンは表示されません。

メモ: 正常にログアウトせずにブラウザを閉じると、セッションはタイムアウトになるまで開いたままになることがあります。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。この手順でログアウトしない場合、タイムアウトになるまでセッションが開いたままになることがあります。

メモ: Microsoft Internet Explorer で、ウィンドウの右上端の閉じるボタン("x")を使用して iDRAC ウェブインタフェースを閉じると、アプリケーションエラーが発生する可能性があります。この不具合を修正するには、Microsoft サポートウェブサイト support.microsoft.com から、最新の Internet Explorer 用累積セキュリティアップデートをダウンロードして下さい。

---

iDRAC NIC の設定

本項では、iDRAC がすでに設定され、ネットワーク上でアクセス可能である状態を想定しています。初期 iDRAC ネットワーク設定のヘルプに関しては、iDRAC ネットワークの設定 を参照してください。

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、**iDRAC の設定** 特権が必要です。

メモ: ほとんどの DHCP サーバーでは、クライアント識別トークンをその予約テーブルに保存する必要があります。このトークンはクライアント(例、iDRAC)が DHCP ネゴシエーション中に提供します。iDRAC は、6 バイトの MAC アドレスに続いて 1 バイトのインタフェース 番号(0)を使用してクライアント識別オプションを提供します。

1. **システム**→ **リモートアクセス**→ **iDRAC** をクリックします。
2. **ネットワーク / セキュリティ** タブをクリックして **ネットワーク設定** ページを開きます。

   表 5-1 と 表 5-2 で、**ネットワーク設定** ページの **ネットワーク設定** と **IPMI LAN 設定** について説明します。
3. 必要な設定を入力したら、**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。表 5-3 を参照してください。

表 5-1. ネットワーク設定

設定	説明
NIC を有効にする	選択すると、NIC が有効で、このグループの残りのコントロールがアクティブになることを示します。NIC が無効になっている場合、ネットワーク経由の iDRAC とのすべての通信はブロックされます。 デフォルトは **オフ** です。
メディアアクセス制御(MAC)アドレス	ネットワークの各ノードを一意に識別するメディアアクセスコントロール(MAC)アドレスを表示します。MAC アドレスは変更できません。
DHCP を使用する(NIC IP アドレス用)	iDRAC に動的ホスト構成プロトコル(DHCP)サーバーから NIC の IP アドレスを取得するように 要求します。また、**静的 IP アドレス**、**静的サブネットマスク**、**静的ゲートウェイ** コントロールを無効にします。 デフォルトは **オフ** です。
静的 IP アドレス	iDRAC NIC の静的 IP アドレスを入力または編集できます。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選択解除します。
静的サブネットマスク	iDRAC NIC のサブネットマスクを入力または編集できます。この設定を変更するには、まず **DHCP を使用(NIC IP アドレス用)**チェックボックスを選択解除します。
静的ゲートウェイ	iDRAC NIC の静的ゲートウェイを入力または編集できます。この設定を変更するには、まず **DHCP を使用(NIC IP アドレス用)**チェックボックスを選択解除します。
DHCP を使用して DNS サーバーアドレスを取得する	**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選択し、DHCP を有効にして DNS サーバーアドレスを取得します。DNS サーバーアドレスの取得に DHCP を使用しない場合は、**静的優先 DNS サーバー** および **静的代替 DNS サーバー** フィールドに IP アドレスを入力します。 デフォルトは **オフ** です。 **メモ:** **DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスが選択されている場合、IP アドレスを **静的優先 DNS サーバー** および **静的代替 DNS サーバー** フィールドに入力することはできません。
静的優先 DNS サーバー	iDRAC NIC の 優先 DNS サーバーの静的 IP アドレスを 入力または編集できます。この設定を変更するには、まず**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選択解除します。
静的代替 DNS サーバー	**DHCP を使用して DNS サーバーアドレスを取得する** が選択されていない場合は、二次 DNS サーバーの IP アドレスを使用します。代替 DNS サーバーが存在しない場合は、IP アドレスとして「0.0.0.0」を入力します。
DNS 上の iDRAC を登録	DNS サーバーに iDRAC 名を登録 します。 デフォルトは **無効** です。
DNS iDRAC 名	**DNS 上の DRAC を登録** が選択されている場合にのみ DRAC 名を表示します。デフォルト名は idrac-<u>サービスタグ</u>で、<u>サービスタグ</u>は Dell サーバーのサービスタグ番号を示します。例:idrac-00002
DNS ドメイン名の DHCP を	デフォルトの DNS ドメイン名を使用します。このチェックボックスが選択されておらず、**DNS 上の iDRAC を登録** オプションが選択されている場合は、**DNS ド**

使用	**メイン名** フィールドで DNS ドメイン名を変更します。 デフォルトは **無効** です。 **メモ:** **DNS ドメイン名の DHCP を使用** チェックボックスを選択するには、**DHCP の使用(NIC IP アドレス用)**チェックボックスも選択されている必要があります。
DNS ドメイン名	デフォルトの **DNS ドメイン名**は空白です。**DNS ドメイン名の DHCP を使用** チェックボックスが選択されている場合はこのオプションがグレー表示になり、フィールドは変更できません。
コミュニティ文字列	iDRAC から送信される**シンプルネットワーク管理プロトコル(SNMP)**の警告トラップで使用するコミュニティ文字列を示します。SNMP 警告トラップは、プラットフォームイベント発生時に送信されます。デフォルトは **public** です。
SMTP サーバーアドレス	プラットフォームイベント発生時に電子メール警告を送信するために iDRAC が通信する**Simple Mail Transfer Protocol(SMTP)**サーバーの IP アドレス。デフォルトは **127.0.0.1** です。

表 5-2. IPMI LAN の設定

設定	**説明**
IPMI オーバー LAN を有効にする	選択されている場合、IPMI LAN チャネルが有効であることを示します。デフォルトは **オフ** です。
チャネル特権レベルの制限	LAN チャネルで受け入れられるユーザーの最大特権レベルを設定します。**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。デフォルトは **システム管理者** です。
暗号化キー	暗号化キーの文字形式の設定では、0 から 20 の 16進法の文字を使用します(空白は使用できません)。デフォルトは空白です。

表 5-3. ネットワーク設定ページのボタン

ボタン	**説明**
詳細設定	**ネットワークセキュリティ** ページを開いて、IP 範囲と IP ブロックの属性を入力できます。
印刷	画面に表示中の **ネットワーク設定** ページのデータを印刷します。
更新	**ネットワーク設定** ページを再ロードします。
適用	ネットワーク設定ページに追加された新規設定を保存します。 **メモ:** NIC の IP アドレス設定を変更すると、すべてのユーザーセッションが終了します。ユーザーは、更新後の IP アドレス設定を使って iDRAC ウェブインタフェースに再接続する必要があります。その他を変更するには、NIC をリセットする必要があります。その場合、接続が短時間中断することがあります。

IP フィルタおよび IP ブロックの設定

メモ: 次の手順を実行するには、**iDRAC の設定** 権限が必要です。

1. **システム**→ **リモートアクセス**→ **iDRAC** をクリックし、**ネットワーク / セキュリティ** タブをクリックして **ネットワーク設定** ページを開きます。
2. **詳細設定** をクリックして、ネットワークセキュリティ設定を行います。

   表 5-4で、**ネットワークセキュリティ** ページの設定について説明します。
3. 設定が終了したら、**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。表 5-5 を参照してください。

表 5-4. ネットワークセキュリティページの設定

設定	**説明**
IP 範囲有効	IP 範囲のチェック機能を有効します。これにより、iDRAC にアクセスできる IP アドレスの範囲を定義できます。デフォルトは **オフ** です。
IP 範囲のアドレス	受け入れる IP サブネットアドレスを決定します。デフォルトは **192.168.1.0** です。
IP 範囲のサブネットマスク	IP アドレスの有効ビット位置 を定義します。サブネットマスクは、下位ビットのすべての「1」が 1 度の移行ですべて「0」になるネットマスクの形式にします。デフォルトは **255.255.255.0** です。

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。デフォルトは **オフ** です。
IP ブロックのエラーカウント	IP アドレスからのログイン失敗回数を設定します。この数を超えると、そのアドレスからのログイン試行が拒否されます。デフォルトは **10** です。
IP ブロックのエラーウィンドウ	IP ブロックのペナルティ時間をトリガするために、IP ブロックのログイン失敗回数を数える時間枠を秒で指定します。デフォルトは **3600** です。
IP ブロックのペナルティ時間	ログイン失敗回数が制限を越えた IP アドレスからのログインを拒否する時間を秒で指定します。デフォルトは **3600** です。

表 5-5. ネットワークセキュリティページのボタン

ボタン	説明
印刷	画面に表示中の **ネットワークセキュリティ** ページのデータを印刷します。
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。
適用	**ネットワークセキュリティ** ページに追加された新規設定を保存します。
ネットワークページに戻る	**ネットワーク** ページに戻ります。

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は、iDRAC が特定のイベントメッセージについて、選択した処置を実行するように設定するためのメカニズムを提供します。処置には、処置の必要なし、システムの再起動、システムの電源を入れなおす、システムの電源を切る、警告の生成（プラットフォームイベントトラップ [PET] および / または電子メール）が含まれます。

表 5-6 は、フィルタ可能なプラットフォームを示したものです。

インデックス	プラットフォームイベント
1	バッテリ警告アサート
2	バッテリ重要アサート
3	低電圧重要アサート
4	温度警告アサート
5	温度重要アサート
6	冗長性低下
7	冗長性喪失
8	プロセッサ警告アサート
9	プロセッサ重要アサート
10	プロセッサ不在アサート
11	イベントログ重要アサート
12	ウォッチドッグ重要アサート

プラットフォームイベント（例、バッテリ警告アサート）が発生すると、システムイベントが生成され、システムイベントログ（SEL）に記録されます。このイベントが有効にされているプラットフォームイベントフィルタ（PEF）と一致し、警告（PET または電子メール）を生成するようフィルタを設定している場合、1 つまたは複数の設定されている送信先に PET または電子メール警告が送信されます。

同じプラットフォームフィルタが処置（システムの再起動など）も実行するように設定してある場合は、その処置が実行されます。

プラットフォームイベントフィルタ（PEF）の設定

メモ: プラットフォームイベントトラップや電子メール警告設定を指定する前に、プラットフォームイベントフィルタを設定します。

1. iDRAC ウェブインタフェースにログインします。ウェブインタフェースへのアクセス を参照してください。
2. **システム** をクリックし、**警告管理** タブをクリックします。
3. プラットフォームイベントページで、当該イベントに対し相当する **警告の生成** チェックボックスをクリックしてイベントに対し **警告の生成** を有効にします。

メモ: [警告の生成] 列の見出しの横にあるチェックボックスをクリックすると、すべてイベントに対して [警告の生成] を有効 / 無効にできます。

4. 各イベントに対し、有効にする処置の下にあるラジオボタンをクリックします。各イベントに対し 1 つの処理のみ設定できます。

5. **適用** をクリックします。

メモ: 設定済みの有効な宛先（PET または電子メール）に警告が送信されるためは、**警告の生成** を有効にする必要があります。

プラットフォームイベントトラップ（PET）の設定

メモ: SNMP 警告を追加したり有効 / 無効にするには、**iDRAC の設定** 権限が必要です。**iDRAC の設定** 権限がない場合、次のオプションは使用できません。

1. 対応ウェブブラウザを使用してリモートシステムにログインします。ウェブインタフェースへのアクセス を参照してください。
2. プラットフォームイベントフィルタ（PEF）の設定 で説明されている手順に従ってください。
3. PET の送信先 IP アドレスを設定します。
   a. 有効にする **送信先番号** の横にある **有効** チェックボックスをクリックします。
   b. **送信先の IP アドレス** ボックスに IP アドレスを入力します。

   メモ: 送信先コミュニティ文字列は iDRAC コミュニティと同じ文字列であることが必要です。

   c. **適用** をクリックします。

   メモ: トラップを確実に<u>送信</u>するには、**ネットワーク設定** ページの **コミュニティ文字列** の値を設定します。**コミュニティ文字列** の値は、iDRAC から送信されるシンプルネットワーク管理プロトコル（SNMP）の警告トラップで使用するコミュニティ文字列を示します。SNMP 警告トラップは、プラットフォームイベント発生時に送信されます。**コミュニティ文字列** のデフォルト設定は、**Public** です。

   d. 必要に応じて **送信** をクリックして、設定した警告をテストします。
   e. 残りの送信先番号にもステップ a ～ d を繰り返します。

電子メール警告の設定

1. 対応ウェブブラウザを使用してリモートシステムにログインします。
2. プラットフォームイベントフィルタ（PEF）の設定 で説明されている手順に従ってください。
3. 電子メール警告設定を指定します。
   a. **警告管理** タブで、**電子メール警告設定** をクリックします。
4. 電子メール警告の送信先を指定します。
   a. **電子メール警告番号** 列で、送信先番号をクリックします。4 つの電子メール送信先に警告を受信できます。
   b. **有効** 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. **送信先電子メールアドレス** フィールドに有効な電子メールアドレスを入力します。
   d. **適用** をクリックします。

   メモ: テストメールを確実に送信するには、**ネットワーク設定** ページで **SMTP サーバーアドレス** を設定する必要があります。**SMTP サーバー** の IP アドレスは、プラットフォームイベントが発生すると、iDRAC と通信して電子メール警告を送信します。

   e. 必要に応じて **送信** をクリックして、設定した電子メール警告をテストします。
   f. 残りの電子メール警告設定にも a ～ e の手順を繰り返します。

IPMI の設定

1. 対応ウェブブラウザを使用してリモートシステムにログインします。
2. IPMI オーバー LAN を設定します。
   a. **システム**→ **リモートアクセス**→ iDRAC をクリックして、**ネットワーク / セキュリティ** をクリックします。
   b. **IPMI LAN 設定** の **ネットワーク設定** ページで、**IPMI オーバー LAN を有効にする** を選択します。
   c. 必要に応じて、IPMI LAN チャネルの特権を更新します。

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

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

d. 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: iDRAC IPMI は RMCP+ プロトコルに対応しています。

メモ: 暗号化キーは、最大 20 文字の偶数の 16 進数文字で構成する必要があります。

IPMI LAN 設定 の **暗号化キー** フィールドに暗号化キーを入力します。

e. **適用** をクリックします。

3. IPMI シリアルオーバー LAN(SOL)を設定します。

a. **システム**→ **リモートアクセス**→ **iDRAC** をクリックします。

b. **ネットワークセキュリティ** タブをクリックして、**シリアルオーバー LAN** をクリックします。

c. **シリアルオーバー LAN 設定** ページで、**シリアルオーバー LAN を有効にする** チェックボックスをクリックしてシリアルオーバー LAN を有効にします。

d. IPMI SOL のボーレートを更新します。

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

ボーレート ドロップダウンメニューをクリックして 19.2 kbps、57.6 kbps、115.2 kbps からデータ速度を選択します。

e. **適用** をクリックします。

---

iDRAC ユーザーの追加と設定

iDRAC を使用してシステムを管理し、システムのセキュリティを確保するには、特定の管理者権限(役割ベースの権限)を持つ固有のユーザーを作成します。

iDRAC のユーザーを追加して設定するには、次の手順を実行してください。

メモ: 次の手順を実行するには、**iDRAC の設定** 権限が必要です。

1. **システム**→ **リモートアクセス**→ **iDRAC** をクリックして、**ネットワーク / セキュリティ** タブをクリックします。

2. **ユーザー** ページを開き、ユーザーを設定します。

   ユーザー ページには、各ユーザーの **ユーザー ID**、**状態**、**ユーザー名**、**IPMI LAN 特権**、**iDRAC 特権**、および **シリアルオーバー LAN** が表示されます。

   メモ: ユーザー 1 は IPMI の任意ユーザー用に予約されており、設定不可です。

3. **ユーザー ID** 列のユーザー ID 番号をクリックします。

4. **ユーザー設定** ページで、ユーザーのプロパティと特権を設定します。

   表 5-7 では、iDRAC ユーザー名とパスワードを設定するための **一般** 設定について説明します。

   表 5-8 では、ユーザーの LAN 特権を設定するための **IPMI LAN 特権** について説明します。

   表 5-9 では、**IPMI LAN 特権** および **iDRAC ユーザー権限** 設定の **ユーザー グループ**権限について説明します。

   表 5-10 では、**iDRAC グループ** 権限について説明します。**iDRAC ユーザー権限** を **システム管理者**、**パワーユーザー**、**ゲストユーザー** に追加すると、**iDRAC グループ** が **カスタム** グループに変わります。

5. 設定が完了したら、**適用** をクリックします。

6. 適切なボタンをクリックして続行します。表 5-11 を参照してください。

表 5-7. 一般プロパティ

プロパティ	説明
ユーザー ID	16 プリセットユーザー ID 番号の 1 つを含みます。このフィールドは、編集できません。
ユーザーを有効にする	選択されている場合、iDRAC へのユーザーのアクセスが有効であることを示します。選択解除されている場合、ユーザーアクセスは無効であることを示します。
ユーザ名	iDRAC ユーザー名は最大 16 文字で指定します。各ユーザーに固有のユーザー名が必要です。

	メモ: iDRAC のユーザー名に **/**（フォワードスラッシュ）または **.**（ピリオド）を含めることはできません。 **メモ:** ユーザー名を変更した場合は、ユーザーが次回ログインするまで新しい名前は表示されません。
パスワードの変更	**新しいパスワード** および **新しいパスワードの確認** フィールドを有効にします。チェックボックスを選択解除すると、ユーザーの **パスワード** を変更できません。
新しいパスワード	iDRAC ユーザーのパスワードの編集を有効にします。最大 20 文字の **パスワード** を入力します。文字は表示されません。
新しいパスワードの確認	確認のため、iDRAC ユーザーのパスワードを再入力します。

表 5-8. IPMI LAN ユーザー特権

プロパティ	**説明**
LAN ユーザー最大特権許可	IPMI LAN チャネルでのユーザーの最大特権を、**なし**、**システム管理者**、**オペレータ**、**ユーザー** の中から指定します。
シリアルオーバー LAN を有効にする	IPMI シリアルオーバー LAN を使用できます。このチェックボックスをオンにすると、この特権が有効になります。

表 5-9. iDRAC ユーザー権限

プロパティ	**説明**
iDRAC グループ	ユーザーの最大の iDRAC ユーザー権限を **システム管理者**、**パワーユーザー**、**ゲストユーザー**、**カスタム**、**なし** の中から指定します。 **iDRAC グループ** 権限については、表 5-10 を参照してください。
iDRAC へのログイン	iDRAC にログインできます。
iDRAC の設定	iDRAC を設定できます。
ユーザーの設定	特定のユーザーにシステムへのアクセスを許可できます。
ログのクリア	iDRAC のログをクリアできます。
サーバー制御コマンドの実行	RACADM コマンドを実行できます。
コンソールリダイレクトへのアクセス	コンソールリダイレクトを実行できます。
仮想メディアへのアクセス	仮想メディアを実行して使用できます。
テスト警告	テスト警告（電子メールと PET）を特定のユーザーに送信できます。
診断コマンドの実行	診断コマンドを実行できます。

表 5-10. iDRAC グループ権限

ユーザーグループ	**与えられる許可**
システム管理者	**iDRAC へのログイン**、**iDRAC の設定**、**ユーザー設定**、**ログのクリア**、**サーバー制御コマンドの実行**、**コンソールリダイレクトへのアクセス**、**仮想メディアへのアクセス**、**テスト警告**、**診断コマンドの実行**。
パワーユーザー	**iDRAC 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	**iDRAC へのログイン**
カスタム	次の権限を組み合わせて選択します。**iDRAC へのログイン**、**iDRAC の設定**、**ユーザーの設定**、**ログのクリア**、**サーバー処置コマンドの実行**、**コンソールリダイレクトへのアクセス**、**仮想メディアへのアクセス**、**テスト警告**、**診断コマンドの実行**。
なし	権限の割り当てなし

表 5-11. ユーザー設定ページのボタン

ボタン	**処置**
印刷	画面に表示中の **ユーザー設定** ページのデータを印刷します。
更新	**ユーザー設定** ページを再ロードします。
適用	ユーザー設定に追加された新規設定を保存します。
ユーザーページに戻る	**ユーザーページ** に戻ります。

SSL とデジタル証明書を使用した iDRAC 通信のセキュリティ

本項では、iDRAC に組み込まれているデータセキュリティの機能について説明します。

- セキュアソケットレイヤ（SSL）
- 証明書署名要求（CSR）
- SSL メインメニューへのアクセス
- 新しい CSR の生成
- サーバー証明書のアップロード
- サーバー証明書の表示

セキュアソケットレイヤ（SSL）

iDRAC には、業界標準の SSL セキュリティプロトコルを使用してネットワーク上で暗号化データを送信するように設定された Web Server が含まれています。公開キーと秘密キーの暗号化技術を基盤とする SSL は、ネットワークでの盗聴を防ぐためにクライアントとサーバー間に認証された暗号化通信を提供する技術として広く普及しています。

SSL 有効システムは、次のタスクを実行できます。

- SSL が有効のクライアントへの認証
- クライアントのサーバーへの認証の許可
- 両システムの暗号化接続の確立許可

暗号化プロセスは高度なデータ保護を提供します。iDRAC では、北米のインターネットブラウザで使用できる暗号化の最も安全な方式である 128 ビットの SSL 暗号化標準を導入しています。

iDRAC の Web Server は、Dell の署名入り SSL デジタル証明書（サーバー ID）を提供します。インターネット上で高セキュリティを確保するには、有名な認証局によって署名された証明書による Web Server の SSL 証明書と交換します。署名された証明書の取得プロセスを開始するには、iDRAC ウェブインタフェースを使用して貴社の企業情報を掲載した証明書署名要求（CSR）を生成できます。生成した CSR を VeriSign または Thawte などの CA に送信します。

証明書署名要求（CSR）

CSR とは、認証局（CA）に安全なサーバー証明書のデジタル要求を送ることです。セキュアなサーバー証明書によって、サーバーのクライアントは接続しているサーバーの身元を信用できるほか、サーバーとの暗号化セッションを交渉できます。

認証局は、IT 業界で認められたビジネス組織で、高水準で信頼できる審査、身元確認、その他の重要なセキュリティ要件を満たしています。CA には、Thawte や VeriSign があります。CA は CSR を受信すると、その情報の確認と検証を行います。申請者が CA のセキュリティ基準を満たしていれば、ネットワークおよびインターネットでトランザクションを固有に識別するデジタル署名済みの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、それを iDRAC ファームウェアにアップロードする必要があります。iDRAC ファームウェアに保管されている CSR 情報は、証明書に記載さ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**→ **リモートアクセス**→ **iDRAC** をクリックして、**ネットワーク / セキュリティ** タブをクリックします。
2. **SSL** をクリックして **SSL メインメニュー** ページを開きます。

SSL メインメニュー ページを使用して CSR を生成し、CA に送信します。CSR 情報は iDRAC ファームウェアに保管されています。

表 5-12 では、CSR の生成時に使用可能なオプションについて説明します。

表 5-13 では、**SSL メインメニュー** ページで使用可能なボタンについて説明します。

表 5-12. SSL メインメニューのオプション

フィールド	説明
新規証明書署名要求の生成（CSR）	オプションを選択し、**次へ** をクリックして **証明書署名要求（CSR）の生成** ページを開きます。 **メモ:** 新しい CSR はファームウェアの以前の CSR を上書きします。CA が CSR を受け入れるには、CA から返される証明書とファームウェアの CSR が一致する必要があります。
サーバー証明書のアップロード	オプションを選択し、**次へ** をクリックして **証明書のアップロード** ページを開き、CA から送信された証明書をアップロードします。

	メモ: iDRAC で受け入れられるのは、X509、Base 64 エンコードの証明書のみです。DER でエンコードされた 証明書は受け入れられません。
サーバー証明書の表示	オプションを選択し、**次へ** をクリックして **サーバー証明書の表示** ページを開き、既存のサーバー証明書を表示します。

表 5-13. SSL メインメニューのボタン

ボタン	説明
印刷	画面に表示中の **SSL メインメニュー** ページのデータを印刷します。
更新	**SSL メインメニュー** ページを再ロードします。
次へ	**SSL メインメニュー** ページの情報を処理し、次のステップに進みます。

新しい証明書署名要求の生成

メモ: 新しい CSR はファームウェアに保存されている前の CSR データを上書きします。ファームウェアの CSR は、CAから返された証明書と一致している必要があります。一致しない場合、iDRAC は証明書を受け入れません。

1. **SSL メインメニュー** ページで、**新規証明書署名要求(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 5-14 では、**証明書署名要求(CSR)の生成** ページのオプションについて説明します。
3. CSR を作成するには、**生成** をクリックします。
4. CSR ファイルをローカルコンピュータに保存するには、**ダウンロード** をクリックします。
5. 適切なボタンをクリックして続行します。表 5-15 を参照してください。

表 5-14. 証明書署名要求(CSR)の生成

フィールド	説明
コモンネーム (CN)	認証されている名前(通常は **www.xyzcompany. com** のような Web Server のドメイン名)。使用できるのは、英数字、ハイフン、下線、ピリオドのみです。スペースは使用できません。
組織名	この組織に付ける名前(例、XYZ Corporation)。使用できるのは、英数字、ハイフン、下線、ピリオド、スペースのみです。
部門名	部門など組織単位に関連付ける名前(例、Information Technology)。使用できるのは、英数字、ハイフン、下線、ピリオド、スペースのみです。
地域	認証する組織の都市その他の場所(例、Round Rock)。使用できるのは、英数字とスペースのみです。下線や他の文字で単語を区切らないでください。
都道府県名	証明書を申請している組織のある都道府県(例、Texas)。使用できるのは、英数字とスペースのみです。略語は使用しないでください。
国番号	証明書を申請している事業体の所在国。
電子メール	CSR に関連付ける電子メールアドレス。組織の電子メールアドレスまたは CSR に関連付ける電子メールアドレスを入力します。このフィールドはオプションです。

表 5-15. 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	画面に表示中の **証明書署名要求の生成** ページのデータを印刷します。
更新	**証明書署名要求の生成** ページを再ロードします。
生成	CSR を生成し、指定のディレクトリに保存するようユーザーにプロンプトします。
ダウンロード	証明書をローカルコンピュータにダウンロードします。
SSL メインメニューに戻る	**SSL メインメニュー** ページに戻ります。

サーバー証明書のアップロード

1. **SSL メインメニュー** ページで、**サーバー証明書のアップロード** を選択して **次へ** をクリックします。

証明書のアップロード ページが表示されます。

2. **ファイルパス** フィールドで証明書へ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へナビゲートします。

メモ: アップロードする証明書の相対パスが **ファイルパス** の値に表示されます。フルパスと完全なファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

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。表 5-16 を参照してください。

表 5-16. 証明書管理ページのボタン

ボタン	説明
印刷	画面に表示中の **証明書のアップロード** ページのデータを印刷します。
更新	**証明書のアップロード** ページを再ロードします。
適用	証明書を iDRAC ファームウェアに適用します。
SSL メインメニューに戻る	**SSL メインメニュー** ページに戻ります。

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 5-17 に、**証明書** ウィンドウに表示されるフィールドとその説明を示します。

2. 適切なボタンをクリックして続行します。表 5-18 を参照してください。

表 5-17. 証明書情報

フィールド	説明
シリアルナンバー	証明書のシリアル番号
対象者情報	対象者が入力した証明書の属性
発行者情報	発行者から返された証明書の属性
発効日	証明書の発効日
失効日	証明書の有効期日

表 5-18. サーバー証明書の表示ページのボタン

ボタン	説明
印刷	画面に表示中の **サーバー証明書の表示** ページのデータを印刷します。
更新	**サーバー証明書の 表示** ページを再ロードします。
SSL メインメニューに戻る	**SSL メインメニュー** ページに戻ります。

Active Directory 証明書の設定と管理

メモ: Active Directory を設定して Active Directory 証明書をアップロード、ダウンロード、表示するには、**iDRAC の設定** 権限が必要です。

メモ: Active Directory 設定および、Active Directory を標準スキーマまたは拡張スキーマで設定する方法の詳細に関しては、Microsoft Active Directory との iDRAC の使用 を参照してください。

Active Directory メインメニュー にアクセスするには、次の手順を実行してください。

1. **システム→ リモートアクセス→iDRAC** をクリックして、**ネットワーク / セキュリティ** タブをクリックします。

2. **Active Directory** をクリックして **Active Directory メインメニュー** ページを開きます。

   表 5-19 に、**Active Directory メインメニュー** ページのオプションを一覧にします。

3. 適切なボタンをクリックして続行します。表 5-20 を参照してください。

表 5-19. 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 を設定する	Active Directory の **ルートドメイン名**、**Active Directory 認証タイムアウト**、**Active Directory スキーマの選択**、**iDRAC 名**、**iDRAC ドメイン名**、**役割グループ**、**グループ名**、**グループのドメイン** 設定を設定します。
Active Directory CA 証明書をアップロードする	iDRAC に Active Directory 証明書をアップロードします。
iDRAC サーバー証明書をダウンロードする	**Windows Download Manager** は iDRAC サーバー証明書をシステムにダウンロードします。
Active Directory の CA 証明書を表示する	iDRAC にアップロードされた Active Directory 証明書を表示します。

表 5-20. Active Directory メインメニューページのボタン

ボタン	定義
印刷	画面に表示中の **Active Directory メインメニュー** ページのデータを印刷します。
更新	**Active Directory メインメニュー** ページを再ロードします。
次へ	**Active Directory メインメニュー** ページの情報を処理し、次のステップに進みます。

Active Directory（標準スキーマと拡張スキーマ）の設定

1. **Active Directory メインメニュー** ページで、**Active Directory の設定** を選択して **次へ** をクリックします。

2. **Active Directory 設定** ページで、Active Directory 設定を入力します。

   表 5-21 で、**Active Directory の設定と管理** ページの設定について説明します。

3. **適用** をクリックして設定を保存します。

4. 適切なボタンをクリックして続行します。表 5-22 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 5-23 と 表 5-24 を参照してください。

   メモ: **Active Directory 設定** 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 5-21. Active Directory 設定ページの設定

設定	説明
Active Directory を有効にする	選択されている場合、Active Directory は有効です。デフォルトは **無効** です。
ルートドメイン名	Active Directory のルートドメイン名。このデフォルトは空白です。 名前は *x.y* から成る有効なドメイン名にします。*x* は文字間に空白スペースのない 1 ～ 254 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。デフォルトは空白です。
タイムアウト	Active Directory のクエリが完了するのを待つ時間（秒）。最小値は 15 秒以上です。デフォルト値は **120** です。
標準スキーマの使用	Active Directory に標準スキーマを使用します。
拡張スキーマの使用	Active Directory に拡張スキーマを使用します。
iDRAC 名	Active Directory で iDRAC を一意に識別する名前。このデフォルトは空白です。 名前には 1 ～ 254 文字の ASCII 文字列を使用し、空白スペースは使用できません。
iDRAC ドメイン名	Active Directory iDRAC オブジェクトが属するドメインの DNS 名。このデフォルトは空白です。 名前は *x.y* から成る有効なドメイン名にします。*x* は文字間に空白スペースのない 1 ～ 254 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	iDRAC に関連付けられた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の役割グループ番号をクリックします。
グループ名	iDRAC に関連付けられた Active Directory で役割グループを識別する名前。このデフォルトは空白です。
グループドメイン	役割グループの属するドメインタイプ。

表 5-22. Active Directory 設定ページのボタン

ボタン	説明
印刷	画面に表示中の **Active Directory 設定** ページのデータを印刷します。
更新	**Active Directory 設定** ページを再ロードします。
適用	**Active Directory 設定** ページに追加された新規設定を保存します。
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 5-23. 役割グループの特権

設定	説明
役割グループの特権レベル	ユーザーの最大の iDRAC ユーザー権限を **システム管理者**、**パワーユーザー**、**ゲストユーザー**、**カスタム**、**なし** から指定します。 **役割グループ権限** については、表 5-24 を参照してください。
iDRAC へのログイン	グループに iDRAC へのログインアクセスを許可します。
iDRAC の設定	iDRAC を設定するグループ権限を許可します。
ユーザーの設定	ユーザーを設定するグループ権限を許可します。
ログのクリア	ログをクリアするグループ権限を許可します。
サーバー制御コマンドの実行	サーバー制御コマンドを実行するグループ権限を許可します。
コンソールリダイレクトへのアクセス	コンソールリダイレクトへのグループアクセスを許可します。
仮想メディアへのアクセス	仮想メディアへのグループアクセスを許可します。
テスト警告	グループがテスト警告(電子メールおよび PET)を特定のユーザーに送信できます。
診断コマンドの実行	診断コマンドを実行するグループ権限を許可します。

表 5-24. 役割グループの権限

プロパティ	説明
システム管理者	**iDRAC へのログイン**、**iDRAC の設定**、**ユーザー設定**、**ログのクリア**、**サーバー制御コマンドの実行**、**コンソールリダイレクトへのアクセス**、**仮想メディアへのアクセス**、**テスト警告**、**診断コマンドの実行**。
パワーユーザー	**iDRAC 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	**iDRAC へのログイン**
カスタム	次の権限を組み合わせて選択します。**iDRAC へのログイン**、**iDRAC の設定**、**ユーザーの設定**、**ログのクリア**、**サーバー処置コマンドの実行**、**コンソールリダイレクトへのアクセス**、**仮想メディアへのアクセス**、**テスト警告**、**診断コマンドの実行**。
なし	権限の割り当てなし

Active Directory CA 証明書のアップロード

1. **Active Directory メインメニュー** ページで、**Active Directory CA 証明書をアップロードする** を選択して **次へ** をクリックします。
2. **証明書のアップロード ページで、ファイルパス** フィールドに証明書のファイルパスを入力するか、**参照** をクリックして証明書ファイルまで移動します。

   メモ: アップロードする証明書の相対パスが **ファイルパス** の値に表示されます。フルパスと完全なファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

ドメインコントローラの SSL 証明書が同じ認証局によって署名されており、この証明書が iDRAC にアクセスする管理ステーション上で使用可能であることを確認します。

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。表 5-25 を参照してください。

表 5-25. 証明書管理ページのボタン

ボタン	説明
印刷	画面に表示中の **証明書のアップロード** ページのデータを印刷します。
更新	**証明書のアップロード** ページを再ロードします。
適用	証明書を iDRAC ファームウェアに適用します。
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。

iDRAC サーバー証明書のダウンロード

1. **Active Directory メインメニュー** ページで、**Active Directory iDRAC サーバー証明書をダウンロードする** を選択して **次へ** をクリックします。
2. ファイルをシステムのディレクトリに保存します。
3. **ダウンロードの完了** ウィンドウで、**閉じる**をクリックします。

Active Directory CA 証明書の表示

Active Directory メインメニュー ページを使用して、iDRAC 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 の CA 証明書を表示する** を選択して **次へ** をクリックします。

   表 5-26 に、**証明書** ウィンドウに表示されるフィールドとその説明を示します。

2. 適切なボタンをクリックして続行します。表 5-27 を参照してください。

表 5-26. Active Directory CA 証明書の情報

フィールド	説明
シリアルナンバー	証明書のシリアル番号
対象者情報	対象者が入力した証明書の属性
発行者情報	発行者から返された証明書の属性
発効日	証明書の発行日
失効日	証明書の有効期日

表 5-27. Active Directory の CA 証明書の表示ページのボタン

ボタン	説明
印刷	画面に表示中の **Active Directory の CA 証明書** ページのデータを印刷します。
更新	**Active Directory の CA 証明書の表示 ページ** を再ロードします。
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。

シリアルオーバー LAN の設定

1. **システム**→ **リモートアクセス**→ **iDRAC**→ **ネットワーク / セキュリティ** をクリックします。
2. **シリアルオーバー LAN** をクリックして **シリアルオーバー LAN 設定** ページを開きます。

   表 5-28 で、**シリアルオーバー LAN 設定** ページの設定について説明します。

3. **適用** をクリックします。

4. 必要に応じて詳細設定を指定します。指定しない場合は、適切なボタンをクリックして続行します。表 5-29 を参照してください。

   詳細設定を指定するには、次の手順を実行してください。

   a. **詳細設定** をクリックします。

   b. **シリアルオーバー LAN 詳細設定** ページで、必要に応じて詳細を指定します。表 5-30 を参照してください。

   c. **適用** をクリックします。

   d. 適切なボタンをクリックして続行します。表 5-31 を参照してください。

表 5-28. シリアルオーバー LAN 設定ページの設定

設定	説明
シリアルオーバー LAN を有効にする	チェックボックスが選択されている場合、シリアルオーバー LAN が有効であることを示します。
ボーレート	IPMI のデータ速度を示します。データ速度を **19.2 kbps**、**57.6 kbps**、**115.2 kbps** の中から選択します。

表 5-29. シリアルオーバー LAN 設定ページのボタン

ボタン	説明
印刷	画面に表示中の **シリアルオーバー LAN 設定** ページのデータを印刷します。
更新	**シリアルオーバー LAN 設定** ページを再ロードします。
詳細設定	**シリアルオーバー LAN 詳細設定** ページを開きます。
適用	**シリアルオーバー LAN 設定** ページ表示中に行った新しい設定を保存します。

表 5-30. シリアルオーバー LAN 詳細設定 ページの設定

設定	説明
文字累積間隔	SQL 文字データパッケージの一部を 送信する前に iDRAC が待つ時間。時間は秒で測定されます。
文字送信しきい値	iDRAC は、この文字数（またはそれ以上）が受け入れられ次第に、文字を格納した SOL 文字のデータパッケージを送信します。しきい値は文字で測定されます。

表 5-31. シリアルオーバー LAN 詳細設定ページのボタン

ボタン	説明
印刷	画面に表示中の **シリアルオーバー LAN 詳細設定** ページのデータを印刷します。
更新	**シリアル オーバー LAN 詳細設定** ページを再ロードします。
適用	**シリアルオーバー LAN 詳細設定** ページ表示中に行った新しい設定を保存します。
シリアルオーバー LAN 設定ページに戻る	**シリアルオーバー LAN 設定** ページに 戻ります。

---

iDRAC サービスの設定

メモ: これらの設定を変更するには、**iDRAC の設定** 権限が必要です。

メモ: サービスに変更を適用する場合、変更は即時発効します。既存の接続は、警告なしで終了されることがあります。

1. **システム**→ **リモートアクセス**→ **iDRAC** をクリックして、**ネットワーク / セキュリティ** タブをクリックします。

2. **サービス** をクリックして **サービス** 設定ページを開きます。

3. 必要に応じて、次のサービスを設定します。

- Web Server — Web Server の設定については、表 5-32 を参照してください。
- SSH — SSH の設定については、表 5-33 を参照してください。
- Telnet — Telnet の設定については、表 5-34 を参照してください。
- 自動システム回復エージェント — 自動システム回復エージェントの設定については、表 5-35 を参照してください。

4. **適用** をクリックします。
5. 適切なボタンをクリックして続行します。表 5-36 を参照してください。

表 5-32. Web Server の設定

設定	説明
有効	iDRAC の Web Server を有効または無効にします。チェックボックスが選択されている場合、Web Server が有効であることを示します。デフォルトは **有効** です。
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。このフィールドは編集できません。同時セッションは 4 セッションまで可能です。
現在の セッション	システムの現在のセッション数(**最大セッション数** かそれ以下)。このフィールドは編集できません。
タイムアウト	接続がアイドル状態でいられる秒数。タイムアウトになると、セッションはキャンセルされます。タイムアウト設定の変更はすぐに有効になり、Web Server はリセットされます。タイムアウト範囲は 60 ～ 1920 秒です。デフォルトは **300** 秒です。
HTTP ポート番号	ブラウザ接続で iDRAC が通信するポート。デフォルトは **80** です。
HTTPS ポート番号	セキュアなブラウザ接続で iDRAC が通信するポート。デフォルトは **443** です。

表 5-33. SSH の設定

設定	説明
有効	SSH を有効または無効にします。チェックボックスが選択されている場合、SSH は有効であることを示します。
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。1 セッションのみサポートされています。
アクティブセッション	システムの現在のセッション数。
タイムアウト	セキュアシェルのアイドルタイムアウト(秒)。タイムアウト範囲は 60 ～ 1920 秒です。タイムアウト機能を無効にするには、0 秒を入力します。デフォルトは **300** です。
ポート番号	SSH 接続で iDRAC が通信するポート。デフォルトは **22** です。

表 5-34. Telnet の設定

設定	説明
有効	Telnet を有効または無効にします。選択されている場合、Telnet は有効です。
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。1 セッションのみサポートされています。
アクティブセッション	システムの現在のセッション数。
タイムアウト	telnet のアイドルタイムアウト(秒)。タイムアウト範囲は 60 ～ 1920 秒です。タイムアウト機能を無効にするには、0 秒を入力します。デフォルトは **0** です。
ポート番号	Telnet 接続で iDRAC が通信するポート。デフォルトは **23** です。

表 5-35. 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 5-36. 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。

---

iDRAC ファームウェアのアップデート

注意: iDRAC ファームウェアのアップデートが完了前に中断されるなどで、iDRAC ファームウェアが破壊された場合、CMC を使って iDRAC を回復できます。手順については、『CMC ファームウェアユーザーズガイド』を参照してください。

メモ: ファームウェアアップデートは、デフォルトで現在の iDRAC 設定を保持します。アップデートプロセス中、iDRAC 設定を出荷時のデフォルト設定にリセットできるオプションがあります。設定を出荷時のデフォルト設定にすると、アップデート完了時に外部ネットワークアクセスが無効になります。iDRAC 設定ユーティリティまたは CMC ウェブインタフェースを使ってネットワークを有効にし、設定する必要があります。

1. iDRAC ウェブインタフェースを起動します。
2. **システム→ リモートアクセス→iDRAC** をクリックして、**アップデート** タブをクリックします。

   メモ: ファームウェア をアップデートするには、iDRAC がアップデートモードになっている必要があります。このモードでは、アップデートプロセスをキャンセルした場合でも iDRAC は自動的にリセットされます。
3. **ファームウェアアップデート** ページで、**次へ** をクリックしてアップデートプロセスを開始します。
4. **ファームウェアアップデート - アップロード(1 / 4 ページ)** ウィンドウで、**参照** をクリックするか、ダウンロードしたファームウェアイメージへのファイルパスを入力します。

   例:

   `C:\Updates\V1.0\<イメージ名>.`

   デフォルトのファームウェアイメージ名は **firmimg.imc** です。
5. **次へ** をクリックします。
   - ファイルは iDRAC にアップロード されます。この処理の完了には数分かかります。

     または
   - ファームウェアアップグレードのプロセスを終了する場合は、この時点で **キャンセル** をクリックします。**キャンセル** を クリックすると、iDRAC は正常な動作モードにリセットされます。
6. **ファームウェアアップデート - 検証 (2 / 4 ページ)** ウィンドウには、アップロードしたイメージファイルで実行された検証の結果が表示されます。
   - イメージファイルが 確実にアップロードされ、すべての検証チェックに合格した場合、ファームウェアイメージが 確認されたことを示すメッセージが表示されます。

     または
   - イメージが無事アップロードされなかったり、検証チェックに合格しない場合、ファームウェアアップデートは **ファームウェアアップデート - アップロード(1 / 4 ページ)** ウィンドウに戻ります。iDRAC のアップグレードを再試行するか、**キャンセル** をクリックして iDRAC を正常な動作モードにリセットします。

   メモ: 設定の保存 チェックボックスを選択解除する場合、iDRAC はデフォルト設定にリセットされます。デフォルト設定では LAN は無効になっています。iDRAC ウェブインタフェースにログインできません。BIOS POST 中に iDRAC 設定ユーティリティを使用して CMC ウェブインタフェースまたは iKVM で LAN 設定を再設定する必要があります。
7. デフォルトでは、アップグレード後も iDRAC で現在の設定を保存するための**設定の保存** チェックボックスがチェックされています。設定を保存しない場合は、**設定の保存** チェックボックスを選択解除します。
8. **アップデートの開始** をクリックして、アップグレードプロセスを開始します。アップグレードプロセスには割り込まないでください。
9. **ファームウェアアップデート - アップデート(3 / 4 ステップ)** ウィンドウには、アップグレードの状態が表示されます。ファームウェア アップグレード操作の進行状況は、**進行状況** 列にパーセントで 表示されます。
10. ファームアップデートが完了すると、**ファームウェアアップデート - アップデート結果 (4 / 4 ステップ)** ウィンドウが表示され、iDRAC は自動的にリセットされます。現在のブラウザウィンドウを閉じ、新しいブラウザウィンドウを使って iDRAC に再接続する 必要があります。

CMC を使用した iDRAC ファームウェアの回復

通常、iDRAC ファームウェアは iDRAC ウェブインタフェース、SM-CLP コマンドラインインタフェース、もしくは **support.dell.com** よりダウンロード可能なオペレーティングシステム特有のアップデートパッケージなどの iDRAC アイテムを使用してアップデートします。

iDRAC ファームウェアのアップデートが完了前に中断されるなどでiDRAC ファームウェアが破壊された場合、CMC ウェブインタフェースを使ってファームウェアをアップデートできます。

CMC が iDRAC ファームウェアの破壊を検知した場合、iDRAC は CMC ウェブインタフェースの **アップデート可能なコンポーネント** ページにリストされます。

メモ: CMC ウェブインタフェースの使用に関する手順については、『CMC ファームウェアユーザーズガイド』を参照してください。

iDRAC ファームウェアをアップデートするには、次の手順を実行してください。

1. **support.dell.com** から管理コンピュータに最新の iDRAC ファームウェアをダウンロードします。
2. CMC ウェブインタフェースにログインします。
3. **システムツリーでシャーシ** をクリックします。
4. **アップデート** タブをクリックします。**アップデート可能なコンポーネント** ページが表示されます。CMC から回復可能な iDRAC であれば、これを搭載したサーバーがリストに含まれます。
5. **サーバー-*n***（***n*** は回復する iDRAC のサーバー番号）をクリックします。
6. **参照** をクリックしてダウンロードした iDRAC ファームウェアイメージを検索し、**開く** をクリックします。
7. **ファームウェアアップデートを開始する** をクリックします。

ファームウェアイメージファイルが CMC にアップロードされると、iDRAC はイメージを自動的にアップデートします。

目次ページに戻る

目次ページに戻る

Microsoft Active Directory との iDRAC の使用

Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00
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、他のデバイスを制御するのに必要な全情報に共通のデータベースを維持します。会社が Microsoft® Active Directory® サービスソフトウェアを使用している場合は、iDRAC にアクセスできるように設定して、Active Directory ソフトウェアで iDRAC のユーザー特権を既存のユーザーに追加して制御できます。

メモ: Microsoft Windows® 2000 および Windows Server® 2003 オペレーティングシステムでは Active Directory を使用して iDRAC のユーザーを認識できます。

Active Directory を使用すると、iDRAC でのユーザーアクセスを次の 2 つの方法で定義することができます。拡張スキーマソリューションを使うと、Dell が定義した Active Directory オブジェクトを使用することができ、標準スキーマソリューションを使うと、Active Directory グループオブジェクトのみを使用することができます。

拡張スキーマと標準スキーマの利点と欠点

Active Directory を使用して iDRAC へのアクセスを設定する場合は、拡張スキーマまたは標準スキーマソリューションのどちらかを選択する必要があります。

拡張スキーマソリューションを使用する上での利点は次のとおりです。

- すべてのアクセス制御オブジェクトを Active Directory に保持可能。
- 特権レベルがそれぞれ異なる iDRAC 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。

標準スキーマソリューションを使用する上での利点は次のとおりです。

- 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は不要。
- Active Directory 側での設定が簡単。

拡張スキーマの Active Directory の概要

拡張スキーマで Active Directory を有効にするには 3 つの方法があります。

- iDRAC ウェブインタフェースを使用します。ウェブインタフェースを使用して拡張スキーマ Active Directory で iDRAC を設定する を参照してください。
- RACADM CLI ツールを使用します。RACADM を使用して拡張スキーマ Active Directory で iDRAC を設定する を参照してください。
- SM-CLP コマンドラインを使用します。SM-CLP を使用して拡張スキーマ Active Directory で iDRAC を設定する を参照してください。

Active Directory スキーマ拡張

Active Directory データは、属性とクラスのデータベースに分散されます。The Active Directory スキーマには、データベースに追加または挿入するデータタイプを決定する規則があります。ユーザークラスは、データベースに保存されるクラスの一例です。ユーザークラスの属性の例としては、ユーザーの名、姓、電話番号、などがあります。企業は独自の一意な属性とクラスを環境に特有のニーズを満たすのに追加することで、Active Directory データベースを拡張できます。デルでは、このスキーマにリモート管理の認証と許可をサポートするための「属性」および「クラス」を加えて、機能を拡張しました。

既存の Active Directory スキーマに追加した各属性やクラスは、固有の ID で定義する必要があります。業界全体で固有の ID を維持するために、Microsoft では Active Directory オブジェクト識別子（OID）が入ったデータベースを保持しています。その結果、企業がスキーマに拡張を追加する場合、相互の競合や重複がないことが保証されます。Microsoft Active Directory のスキーマを拡張するにあたり、デルは、表 6-1 に示すように、ディレクトリサービスに追加した属性およびクラスに対して、固有の OID、固有の名前のエクステンション、固有にリンク付けられた属性 ID を受け取りました。

表 6-1. Dell Active Directory のオブジェクト識別子

Active Directory サービスクラス	Active Directory OID
Dell の拡張子	dell
Dell のベース OID	1.2.840.113556.1.8000.1280
RAC LinkID 範囲	12070 ～ 12079

RAC スキーマ拡張の概要

多くの顧客環境においても柔軟に対応するため、デルではユーザーが希望する成果に応じた設定が行えるプロパティグループを提供しています。デルでは、関連、デバイス、および特権のプロパティを加えて、このスキーマを拡張しました。関連プロパティは、特定の特権セットを持つユーザーまたはグループを 1 台以上の RAC デバイスにリンクするために使用します。このモデルを使用すると、管理者は簡単に、ユーザー、RAC 特権、およびネットワーク上の RAC デバイスを柔軟に組み合わせることができます。

Active Directory オブジェクトの概要

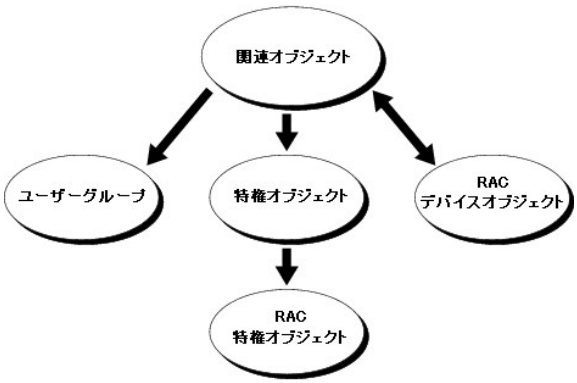
認証と許可の目的で Active Directory に統合するネットワーク上の物理的な RAC 1 台につき、少なくとも 1 個ずつ関連オブジェクトと RAC デバイスオブジェクトを作成しておきます。関連オブジェクトは複数作成することができ、それぞれにリンクできるユーザー、ユーザーグループ、RAC デバイスオブジェクトの数に制限はありません。ユーザーと RAC デバイスオブジェクトは、企業内のどのドメインのメンバでもかまいません。

ただし、各関連オブジェクトは 1 つの特権オブジェクトにしか関連付けられません。また、ユーザー、ユーザーグループ、RAC デバイスオブジェクトを 1 つの特権オブジェクトにしか関連付けられません。この例では、システム管理者が特定の RAC で各ユーザーの特権を制御できます。

RAC デバイスオブジェクトは、Active Directory に認証と認可を照会するための RAC ファームウェアへのリンクです。RAC がネットワークに追加されると、システム管理者は Active Directory 名を使って RAC とそのデバイスオブジェクトを設定する必要があります。その結果、ユーザーは Active Directory を使って認証と承認を実行できます。システム管理者はユーザーが認証できるように、RAC を少なくとも 1 つの関連オブジェクトに追加する必要があります。

図 6-1 は、すべての認証と認可に必要な接続を関連オブジェクトが提供する仕組みを示しています。

図 6-1. Active Directory オブジェクトの標準的な設定



メモ: RAC 特権オブジェクトは DRAC 4 と iDRAC の両方に適用されます。

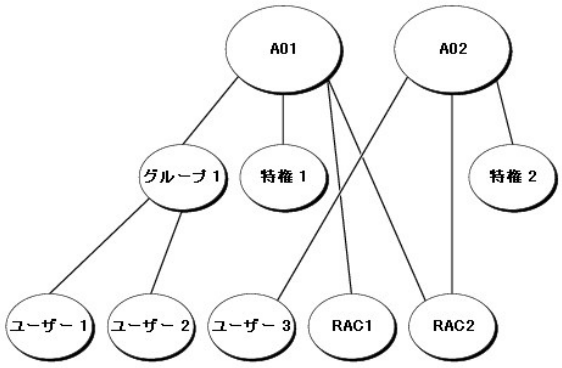
作成する関連オブジェクトの数に制限はありませんが、ただし、RAC(iDRAC)を使って認証と承認用に Active Directory と統合するネットワーク上の各 RAC(iDRAC)において、関連オブジェクトと RAC デバイスオブジェクトを最低 1 つずつ作成する必要があります。

関連オブジェクトには、RAC デバイスオブジェクトのほか、含めるユーザーとグループの数にも制限がありません。ただし、関連オブジェクトに含まれる特権オブジェクトは、関連オブジェクト 1 つにつき 1 つだけです。関連オブジェクトは RACで「特権」を持つ「ユーザー」を接続します。

Active Directory オブジェクトは、単一ドメインにでも複数ドメインにでも設定できます。例えば、iDRAC が 2 つ(RAC1 と RAC2)、既存の Active Directory ユーザーが 3 台(ユーザー 1、ユーザー 2、ユーザー 3)あるとします。ユーザー 1 と ユーザー 2 に 両方の iDRAC へのシステム管理者権限を与え、ユーザー 3 に RAC2 カードへのログイン特権を与えることにします。図 6-2 に、このシナリオで Active Directory オブジェクトを設定する方法を示します。

別のドメインからユニバーサルグループを追加する場合は、ユニバーサルスコープの関連オブジェクトを作成します。Dell Schema Extender ユーティリティを使って作成したデフォルト関連オブジェクトは、ドメインのローカルグループであるため、他のドメインのユニバーサルグループと相互作用できません。

図 6-2. 単一ドメインで Active Directory オブジェクトを設定する方法



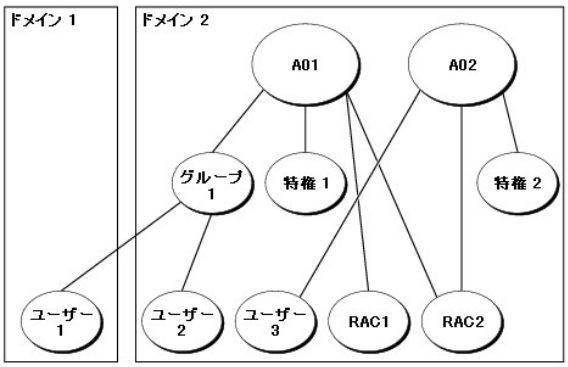
単一ドメインでオブジェクトを設定するシナリオでは、次のタスクを実行します。

1. 関連オブジェクトを 2 つ作成します。
2. 2 つの iDRAC を表す 2 つの RAC デバイスオブジェクト(RAC1 と RAC2)を作成します。
3. 2 つの特権オブジェクト特権 1 と特権 2 を作成し、特権 1 にはすべての特権(システム管理者)、特権 2 にはログイン特権を与えます。
4. ユーザー 1 と ユーザー 2 を グループ 1 に入れます。
5. グループ 1 を関連オブジェクト 1(AO1)のメンバに、特権 1 を特権オブジェクトとして AO1 に、RAC1、 RAC2 を RAC デバイスとして AO1 にそれぞれ追加します。
6. ユーザー 3 をメンバとして関連オブジェクト 2(AO2)に、特権 2 を特権オブジェクトとして AO2 に、RAC2 を RAC デバイスとして AO2 に追加します。

詳細手順に関しては、Active Directory への iDRAC ユーザーと特権の追加 を参照してください。

図 6-3 に、複数ドメインの Active Directory オブジェクトの例を示します。このシナリオでは、iDRAC 2 つ(RAC1 および RAC2)、既存の Active Directory ユーザーが 3 つ(ユーザー 1、ユーザー 2、およびユーザー 3)あるとします。ユーザー 1 はドメイン 1 に、ユーザー 2 とユーザー 3 はドメイン 2 にあります。このシナリオでは、両方の iDRAC のシステム管理者特権を持つユーザー 1 とユーザー 2 を設定し、RAC2 カードへのログイン特権を持つユーザー 3 を設定します。

図 6-3. 複数のドメインで Active Directory オブジェクトを設定する方法



複数ドメインでオブジェクトを設定するシナリオでは、次のタスクを実行します。

1. ドメインのフォレスト機能がネイティブまたは Windows 2003 モードにあることを確認します。
2. 2 つの関連オブジェクトである(ユニバーサルスコープの)AO1 と AO2 を任意のドメインに作成します。

   図 6-3 に、ドメイン 2 のオブジェクトを示します。
3. 2 つの iDRAC を表す 2 つの RAC デバイスオブジェクト(RAC1 と RAC2)を作成します。
4. 2 つの特権オブジェクト特権 1 と特権 2 を作成し、特権 1 にはすべての特権(システム管理者)、特権 2 にはログイン特権を与えます。
5. ユーザー 1 とユーザー 2 をグループ 1 に入れます。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 を関連オブジェクト 1（AO1）のメンバに、特権 1 を特権オブジェクトとして AO1 に、RAC1、RAC2 を RAC デバイスとして AO1 にそれぞれ追加します。

7. ユーザー 3 をメンバとして関連オブジェクト 2（AO2）に、特権 2 を特権オブジェクトとして AO2 に、RAC2 を RAC デバイスとして AO2 に追加します。

iDRAC 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 iDRAC 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 iDRAC 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 参照）。

2. Active Directory ユーザーとコンピュータスナップインを拡張します（Active Directory ユーザーとコンピュータスナップインへの Dell 拡張のインストール 参照）。

3. iDRAC ユーザーとその特権を Active Directory に追加します（Active Directory への iDRAC ユーザーと特権の追加 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上で SSL を有効にする 参照）。

5. iDRAC Active Directory プロパティを、iDRAC ウェブインタフェースまたは RACADM を使用して設定します（ウェブインタフェースを使用して拡張スキーマ Active Directory で iDRAC を設定する または RACADM を使用して拡張スキーマ Active Directory で iDRAC を設定する 参照）。

Active Directory スキーマの拡張

Active Directory スキーマを拡張すると、Dell の組織ユニット、スキーマクラスと属性、およびサンプル特権と関連オブジェクトが Active Directory スキーマに追加されます。スキーマを拡張する前に、ドメインフォレストのスキーママスター Flexible Single Master Operation（FSMO）の役割所有者に対するスキーマ管理者特権が必要です。

次の方法を使用してスキーマを拡張できます。

- Dell スキーマ拡張ユーティリティ
- 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、デルの組織ユニットは追加されません。

LDIF ファイルと Dell の Schema Extender は、それぞれ『Dell Systems Management Consoles CD』の次のディレクトリにあります。

- CD ドライブ:**\support\OMActiveDirectory Tools\RAC4-5\LDIF_Files**
- CD ドライブ:**\support\OMActiveDirectory Tools\RAC4-5\Schema_Extender**

LDIF ファイルを使用するときは、LDIF ファイルディレクトリにある readme の説明を参照してください。Dell Schema Extender を使用して Active Directory スキーマを拡張するには、Dell Schema Extender の使用 を参照してください。

スキーマ拡張または LDIF ファイルはどの場所からでもコピーと実行ができます。

Dell Schema Extender の使用方法

注意: Dell Schema Extender は **SchemaExtenderOem.ini** ファイル を使用します。Dell のスキーマ拡張ユーティリティ機能が正しく機能するように、このファイルの名前は変更しないでください。

1. ようこそ画面で **次へ** をクリックします。

2. 警告を読み、把握してから、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を使用** を選択するか、スキーマ管理者権限を使ってユーザー名とパスワードを入力します。

4. **次へ** をクリックして、Dell スキーマ拡張を実行します。

5. **終了** をクリックします。

   スキーマが拡張されます。スキーマ拡張子を確認するには、Microsoft 管理コンソール (MMC) と Active Directory スキーマスナップインを使用して、次のものが存在することを確認してください。

   - クラス（表 6-2 から 表 6-7 を参照）
   - 属性（表 6-8 ）

   MMC における Active Directory のスキーマスナップインを有効にし、使用する方法の詳細については、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	割り当てられるオブジェクト識別番号(OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

表 6-3. 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。この設定を使って、iDRAC は Lightweight Directory Access Protocol(LDAP)クエリを Active Directory に送信できます。
クラスの種類	構造体クラス
SuperClass	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。関連オブジェクトはユーザーとデバイスを関連付けます。
クラスの種類	構造体クラス
SuperClass	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	iDRAC デバイスの特権(承認権限)を定義します。
クラスの種類	補助クラス
SuperClass	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	Dell の特権（承認権限）のコンテナクラスとして使用します。
クラスの種類	構造体クラス
SuperClass	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	これはメインのクラスで、このクラスからすべての Dell 製品が派生しています。
クラスの種類	構造体クラス
SuperClass	コンピュータ
属性	dellAssociationMembers

表 6-8. Active Directory スキーマに追加される属性のリスト

属性名 / 説明	割り当てられる OID / 構文オブジェクト識別子	単一値
dellPrivilegeMember この属性に属する dellPrivilege オブジェクトのリスト。	1.2.840.113556.1.8000.1280.1.1.2.1 識別名（LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12）	FALSE
dellProductMembers この役割に属する dellRacDevices オブジェクトのリスト。この属性は dellAssociationMembers 後方リンクへの前方リンクです。 リンク ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 識別名（LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12）	FALSE
dellIsLoginUser ユーザーがデバイスでログイン権限を持っている場合には TRUE。	1.2.840.113556.1.8000.1280.1.1.2.3 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsCardConfigAdmin ユーザーがデバイスでカード設定権限を持っている場合には TRUE。	1.2.840.113556.1.8000.1280.1.1.2.4 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsUserConfigAdmin ユーザーがデバイスでユーザー設定権限を持っている場合は TRUE。	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 ユーザーがデバイスにログのクリア権限を持っている場合には 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 ユーザーがデバイスにサーバーリセット権限を持っている場合には TRUE。	1.2.840.113556.1.8000.1280.1.1.2.7 ブーリアン（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsConsoleRedirectUser ユーザーがデバイスにコンソールリダイレクト権限を持っている場合には 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 ユーザーがデバイスに仮想メディア権限を持っている場合には 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 ユーザーがデバイスにテスト警告ユーザー権限を持っている場合には 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 ユーザーがデバイスにデバッグコマンド管理者権限を持っている場合には 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 現在のスキーマバージョンを使って、スキーマをアップデートします。	1.2.840.113556.1.8000.1280.1.1.2.12 ケース無視文字列（LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905）	TRUE

dellRacType この属性は、dellRacDevice オブジェクトの現在の Rac の種類で、dellAssociationObjectMembers 前方リンクへの後方リンクです。	1.2.840.113556.1.8000.1280.1.1.2.13 ケース無視文字列 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers この製品に属する dellAssociationObjectMembers のリスト。この属性は dellProductMembers リンク属性への後方リンクです。 リンク ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 識別名(LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Active Directory ユーザーとコンピュータスナップインへの Dell 拡張のインストール

Active Directory でスキーマを拡張する場合は、RAC(iDRAC)デバイス、ユーザーとユーザーグループ、RAC の関連、RAC の特権などを管理できるように、Active Directory ユーザーとコンピュータスナップインも拡張する必要があります。

『Dell Systems Management Consoles CD』を使用してシステム管理ソフトウェアをインストールした場合、インストール手順中に **Active Directory ユーザーおよびコンピュータスナップインへの Dell 拡張** オプションを選択して、スナップインを拡張することができます。Systems Management Software のインストールの詳細については、『Dell OpenManage ソフトウェアクイックインストールガイド』を参照してください。

Active Directory ユーザーとコンピュータスナップインの詳細については、Microsoft のマニュアルを参照してください。

Administrator Pack のインストール

Active Directory iDRAC オブジェクトを管理している各システム上で、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。

詳細に関しては、Active Directory ユーザーとコンピュータスナップインを開く を参照してください。

Active Directory ユーザーとコンピュータスナップインを開く

Active Directory ユーザーとコンピュータスナップインを開くには、次の手順を実行してください。

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 ユーザーおよびコンピュータ** をクリックします。

   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** をクリックし、MMC と入力してから **Enter** を押します。

   Microsoft 管理コンソール(MMC)が表示されます。

2. **コンソール 1** ウィンドウで **ファイル**(または Windows 2000 を実行しているシステムでは **コンソール**)をクリックします。

3. **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、**追加** クリックします。

5. **閉じる** をクリックして、**OK** をクリックします。

Active Directory への iDRAC ユーザーと特権の追加

Dell の拡張 Active Directory ユーザーとコンピュータスナップインを使用して、RAC、関連、および特権オブジェクトを作成すると、iDRAC ユーザーと特権を追加できます。各オブジェクトタイプを追加するには、次の手順を実行します。

- RAC デバイスオブジェクトを作成する
- 特権オブジェクトを作成する
- 関連オブジェクトを作成する
- 関連オブジェクトにオブジェクトを追加する

RAC デバイスオブジェクトの作成

1. MMC **コンソールルート** ウィンドウで、コンテナを右クリックします。

2. **新規作成→ Dell RAC オブジェクト** を選択します。

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、ウェブインタフェースを使用して拡張スキーマ Active Directory で iDRAC を設定する のステップ a で入力する名前と同一でなければなりません。
4. **RAC デバイスオブジェクト** を選択します。
5. **OK** をクリックします。

特権オブジェクトの作成

メモ: 特権オブジェクトは、関係する関連オブジェクトと同じドメインに作成する必要があります。

1. **コンソールルート**(MMC)ウィンドウで、コンテナを右クリックします。
2. **新規作成**→ **Dell RAC オブジェクト** を選択します。

   新規オブジェクト 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. **特権オブジェクト** を選択します。
5. **OK** をクリックします。
6. 作成した特権オブジェクトを右クリックして、**プロパティ** を選択します。
7. **RAC 特権** タブをクリックして、ユーザーに与える特権を選択します(詳細に関しては iDRAC ユーザー権限 を参照)。

関連オブジェクトの作成

関連オブジェクトはグループから派生し、グループタイプが含まれている必要があります。関連スコープで、関連オブジェクトのセキュリティグループタイプを指定します。関連オブジェクトを作成する場合は、追加するオブジェクトの種類に適用される関連のスコープを選択します。

たとえば、**ユニバーサル** を選択すると、関連オブジェクトは Active Directory ドメインがネイティブモード以上で機能するときにのみ使用可能になります。

1. **コンソールルート**(MMC)ウィンドウで、コンテナを右クリックします。
2. **新規作成**→ **Dell RAC オブジェクト** を選択します。

   新規オブジェクト ウィンドウが開きます。
3. 新しいオブジェクトの名前を入力します。
4. **関連オブジェクト** を選択します。
5. **関連オブジェクト** のスコープを選択します。
6. **OK** をクリックします。

関連オブジェクトへのオブジェクトの追加

関連オブジェクトプロパティ ウィンドウを使用すると、ユーザーやユーザーグループ、特権オブジェクト、RAC デバイスや RAC デバイスグループを関連付けることができます。Windows 2000 モード以上のシステムを使用している場合は、ユニバーサルグループを使ってユーザーまたは RAC オブジェクトでドメインを拡張する必要があります。

ユーザーと RAC デバイスのグループを追加できます。Dell 関連グループと Dell に関連しないグループを作成する手順は同じです。

ユーザーまたはユーザーグループの追加

1. **関連オブジェクト** を右クリックして、**プロパティ** を選択します。
2. **ユーザー** タブを選択して、**追加** をクリックします。

3. ユーザーまたはユーザーグループ名を入力して、**OK** をクリックします。

ユーザーの特権やユーザーグループの特権を定義する特権オブジェクトを関連に追加するには、RC デバイスに認証するときに **特権オブジェクト** タブをクリックします。関連オブジェクトに追加できる特権オブジェクトは 1 つだけです。

特権の追加

1. **特権オブジェクト** タブを選択し、**追加** をクリックします。
2. 特権オブジェクト名を入力し、**OK** をクリックします。

製品 タブをクリックして、1 つまたは複数の RAC デバイスを関連に追加します。関連デバイスは、ネットワークに接続している RAC デバイスのうち、定義したユーザーまたはユーザーグループが使用できるものを指定します。関連オブジェクトには複数の RAC デバイスを追加できます。

RAC デバイスまたは RAC デバイスグループの追加

RAC デバイスまたは RAC デバイスグループを追加するには、次の操作を実行します。

1. **製品** タブを選択して、**追加** をクリックします。
2. RAC デバイスまたは RAC デバイスグループ名を入力して、**OK** をクリックします。
3. **プロパティ** ウィンドウで、**適用**、**OK** の順にクリックします。

ウェブインタフェースを使用した拡張スキーマ Active Directory での iDRAC の設定

1. サポートされている Web ブラウザのウィンドウを開きます。
2. iDRAC ウェブインタフェースにログインします。
3. **システム→ 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** を選択して **次へ** をクリックします。
6. 全般設定セクションでは以下の処理を行います。
   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** はフォレストの完全修飾ルートドメイン名です。
   c. **タイムアウト** の時間を秒で入力します。
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は以下の処理を行います。
   a. **DRAC 名** を入力します。この名前は、ドメインコントローラに作成した新規 RAC オブジェクトのコモンネームと同一でなければなりません（RAC デバイスオブジェクトの作成 の ステップ 3 参照）。
   b. **DRAC ドメイン名** を入力します（例、iDRAC.com）。NetBIOS 名は使用しないでください。**DRAC ドメイン名** は RAC デバイスオブジェクトがあるサブドメインの完全修飾ドメイン名です。
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. ドメインフォレストのルート CA 証明書を iDRAC にアップロードします。
    a. **Active Directory CA 証明書をアップロードする** ラジオボタンを選択して、**次へ** をクリックします。
    b. **証明書のアップロード** ページで、証明書のファイルパスを入力するか、証明書ファイルまで参照します。

メモ: アップロードする証明書の相対パスが **ファイルパス** の値に表示されます。フルパスと完全なファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

ドメインコントローラの 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。iDRAC にアクセスする管理ステーション上でルート CA 証明書を使用可能な状態にします（ドメインコントローラルート CA 証明書のエクスポート 参照）。

c. **適用** をクリックします。

iDRAC のウェブサーバーは、**適用** をクリックすると自動的に再起動します。

12. iDRAC Active Directory 機能の設定を完了するには、ログアウトしてから iDRAC にログインします。
13. **システム→ リモートアクセス** をクリックします。
14. **設定** タブをクリックして、**ネットワーク** をクリックします。
15. **ネットワーク設定** で **DHCP を使用（NIC IP アドレス用）を**選択している場合は、**DNS サーバーアドレスの取得に DHCP を使用** を選択します。

DNS サーバー IP アドレスを手動で入力する場合は、**DNS サーバーアドレスの取得に DHCP を使用** をオフにし、一次および代替 DNS サーバー IP アドレスを入力します。

16. **変更の適用** をクリックします。

iDRAC 拡張スキーマ Active Directory 機能の設定が完了しました。

RACADM を使用した拡張スキーマ Active Directory での iDRAC の設定

ウェブインタフェースでなく RACADM CLI を使用して、拡張スキーマで iDRAC 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 <RAC FQDN>

racadm config -g cfgActiveDirectory -o cfgADRootDomain <ルート FQDN>

racadm config -g cfgActiveDirectory -o cfgADRacName <RAC コモンネーム>

racadm sslcertupload -t 0x2 -f <ルート CA 証明書-TFTP-URI>

racadm sslcertdownload -t 0x1 -f <RAC SSL 証明書>
```

2. iDRAC で DHCP が有効で、DHCP サーバーが提供する DNS を使用する場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
```

3. iDRAC で DHCP が無効な場合、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 <一次 DNS IP アドレス>

racadm config -g cfgLanNetworking -o cfgDNSServer2 <二次 DNS IP アドレス
```

4. <**Enter**> を押して、iDRAC Active Directory 機能の設定を完了します。

SM-CLP を使用した拡張スキーマ Active Directory での iDRAC の設定

メモ: ルート CA 証明書を取得でき、iDRAC サーバー証明書を保存できる TFTP サーバーを実行している必要があります。

SM-CLP を使用して拡張スキーマで iDRAC の Active Directory 機能を設定するには、次のコマンドを使用します。

1. Telnet または SSH を使用して iDRAC にログインし、次の SM-CLP コマンドを入力します。

```
cd /system/sp1/oemdell_adservice1

set enablestate=1

set oemdell_schematype=1

set oemdell_adracdomain=<RAC FQDN>

set oemdell_adrootdomain=<ルート FQDN>
```

```
set oemdell_adracname=<RAC コモンネーム>

set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD

load -source <ルート CA 証明書 TFTP-URI>

set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL
dump -destination <DRAC サーバー証明書 TFTP-URI> /system1/sp1/oemdell_ssl1
```

2. iDRAC で DHCP が有効で、DHCP サーバーが提供する DNS を使用する場合は、次の SM-CLP コマンドを入力します。

```
set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1 oemdell_serversfromdhcp=1
```

3. iDRAC で DHCP が無効な場合、または手動で DNS IP アドレスを入力する場合は、次の SM-CLP コマンドを入力します。

```
set /system1/sp1/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oemdell_serversfromdhcp=0

set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<一次 DNS IP アドレス>

set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<二次 DNS IP アドレス>
```

Active Directory 標準スキーマの概要

図 6-4 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 iDRAC の両方で設定が必要となります。Active Directory では、標準グループオブジェクトは役割グループとして使用します。iDRAC 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となります。このユーザーに指定の iDRAC へのアクセスを与えるには、役割グループ名とそのドメイン名を指定の iDRAC 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、役割と特権レベルは Active Directory でなく、各 iDRAC で定義されます。各 iDRAC について、5 つまでの役割グループを設定および定義できます。表 5-10 は役割グループの特権レベルを、表 6-9 はデフォルトの役割グループの設定を示したものです。

図 6-4. Microsoft Active Directory および標準スキーマを使った iDRAC の設定

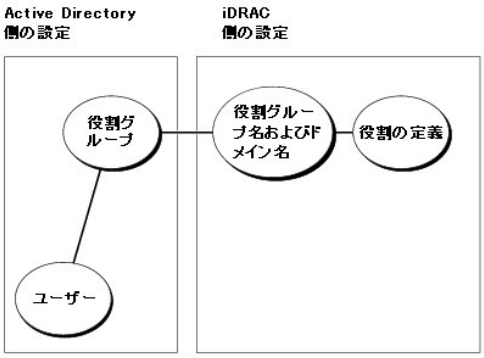


表 6-9. デフォルトの役割グループの特権

デフォルトの特権レベル	与えられる許可	ビットマスク
システム管理者	iDRAC へのログイン、iDRAC の設定、ユーザー設定、ログのクリア、サーバー制御コマンドの実行、コンソールリダイレクトへのアクセス、仮想メディアへのアクセス、テスト警告、診断コマンドの実行。	0x000001ff
パワーユーザー	iDRAC 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
ゲストユーザー	iDRAC へのログイン	0x00000001
なし	権限の割り当てなし	0x00000000
なし	権限の割り当てなし	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。

Active Directory で標準スキーマを有効にするには、次の 2 つの方法があります。

- iDRAC ウェブユーザーインタフェースを使用します。標準スキーマ Active Directory およびウェブインタフェースで iDRAC を設定する を参照してください。

- RACADM CLI ツールを使用します。標準スキーマ Active Directory および RACADM で iDRAC を設定する を参照してください。

iDRAC 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 iDRAC にアクセスできるようにするには、まず次のステップを実行し、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。グループ名およびこのドメイン名は、ウェブインタフェース、RACADM、SM-CLP のいずれかを使用して iDRAC で設定しなければなりません(標準スキーマ Active Directory およびウェブインタフェースで iDRAC を設定する または 標準スキーマ Active Directory および RACADM で iDRAC を設定する 参照)。
3. Active Directory ユーザーを、iDRAC にアクセスする Active Directory グループのメンバーとして追加します。

標準スキーマ Active Directory およびウェブインタフェースでの iDRAC の設定

1. サポートされている Web ブラウザのウィンドウを開きます。
2. iDRAC ウェブインタフェースにログインします。
3. **システム**→ **リモートアクセス**→ **iDRAC** をクリックして、**設定** タブをクリックします。
4. **Active Directory** を選択して **Active Directory メインメニュー** ページを開きます。
5. **Active Directory メインメニュー** ページで、**Active Directory の設定** を選択して **次へ** をクリックします。
6. 全般設定セクションでは以下の処理を行います。
   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** はフォレストの完全修飾ルートドメイン名です。
   c. **タイムアウト** の時間を秒で入力します。
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**、**役割グループの特権** が含まれています。
10. **グループ名** を入力します。iDRAC に関連付けられた Active Directory で役割グループを識別するグループ名。
11. **グループドメイン** を入力します。**グループドメイン** はフォレストの完全修飾ルートドメイン名です。
12. **役割グループの特権** ページでグループの特権を設定します。

    5-10 では **役割グループの特権** について説明します。

    権限を変更すると、既存の **役割グループの特権**(**システム管理者**、**パワーユーザー**、**ゲストユーザー**)は変更した権限に基づいてカスタムグループまたは適切な**役割グループの特権**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. ドメインフォレストのルート CA 証明書を iDRAC にアップロードします。
    a. **Active Directory CA 証明書をアップロードする** ラジオボタンを選択して、**次へ** をクリックします。
    b. **証明書のアップロード** ページで、証明書のファイルパスを入力するか、証明書ファイルまで参照します。

    メモ: アップロードする証明書の相対パスが **ファイルパス** の値に表示されます。フルパスと完全なファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

    ドメインコントローラの 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。iDRAC にアクセスする管理ステーション上でルート CA 証明書を使用可能な状態にします(ドメインコントローラルート CA 証明書のエクスポート 参照)。

c. **適用** をクリックします。

iDRAC のウェブサーバーは、**適用** をクリックすると自動的に再起動します。

17. iDRAC Active Directory 機能の設定を完了するには、ログアウトしてから iDRAC にログインします。
18. **システム→ リモートアクセス** をクリックします。
19. **設定** タブをクリックして、**ネットワーク** をクリックします。
20. **ネットワーク設定** で **DHCP を使用（NIC IP アドレス用）** を選択している場合は、 **DNS サーバーアドレスの取得に DHCP を使用** を選択します。

    DNS サーバー IP アドレスを手動で入力する場合は、**DNS サーバーアドレスの取得に DHCP を使用** をオフにし、一次および代替 DNS サーバー IP アドレスを入力します。
21. **変更の適用** をクリックします。

    iDRAC 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 および RACADM での iDRAC の設定

ウェブインタフェースでなく RACADM CLI を使用して、標準スキーマで iDRAC 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 <ルート FQDN>

   racadm config -g cfgStandardSchema -i <インデックス> -o cfgSSADRoleGroupName <役割グループのコモンネーム>

   racadm config -g cfgStandardSchema -i <インデックス> -o cfgSSADRoleGroupDomain <RAC FQDN>

   racadm config -g cfgStandardSchema -i <インデックス> -o cfgSSADRoleGroupPrivilege <権限ビットマスク>

   racadm sslcertupload -t 0x2 -f <ルート CA 証明書 TFTP-URI>

   racadm sslcertdownload -t 0x1 -f <RAC SSL 証明書 TFTP-URI>
   ```

   メモ: ビットマスク値については、表 B-1 を参照してください。
2. iDRAC で DHCP が有効で、DHCP サーバーが提供する DNS を使用する場合は、次の RACADM コマンドを入力します。

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 1
   ```
3. iDRAC で DHCP が無効な場合、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 <一次 DNS IP アドレス>

   racadm config -g cfgLanNetworking -o cfgDNSServer2 <<二次 DNS IP アドレス>
   ```

標準スキーマ Active Directory および SM-CLP での iDRAC の設定

メモ: 証明書は SM-CLP を使用してアップロードできません。iDRAC ウェブインタフェースまたはローカル RACADM コマンドを使用します。

SM-CLP を使用して標準スキーマで iDRAC の Active Directory 機能を設定するには、次のコマンドを使用します。

1. Telnet または SSH を使用して iDRAC にログインし、次の SM-CLP コマンドを入力します。

   ```
   cd /system/sp1/oemdell_adservice1

   set enablestate=1

   set oemdell_schematype=2

   set oemdell_adracdomain=<RAC FQDN>
   ```

2. 次の 5 つの Active Directory 役割グループそれぞれに対して次のコマンドを入力します。

```
set /system1/sp1/groupN oemdell_groupname=<役割グループ N コモンネーム>

set /system1/sp1/groupN oemdell_groupdomain=<RAC FQDN>

set /system1/sp1/groupN oemdell_groupprivilege=<ユーザー権限ビットマスク>
```

N は 1 ～ 5 の数字です。

3. Active Directory SSL 証明書を設定するには、次のコマンドを入力します。

```
set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD
load -source <ルート CA 証明書 TFTP-URI>

set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL

dump -destination <iDRAC サーバー証明書 TFTP URI> /system1/sp1/oemdell_ssl1
```

4. iDRAC で DHCP が有効で、DHCP サーバーが提供する DNS を使用する場合は、次の SM-CLP コマンドを入力します。

```
set /system1/sp1/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oemdell_serversfromdhcp=1
```

5. iDRAC で DHCP が無効な場合、または手動で DNS IP アドレスを入力する場合は、次の SM-CLP コマンドを入力します。

```
set /system1/sp1/enetport1/lanendpt1/\
ipendpt1/dnsendpt1 oemdell_serversfromdhcp=0

set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<一次 DNS IP アドレス>

set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<二次 DNS IP アドレス>
```

ドメインコントローラの SSL の有効化

Microsoft Enterprise ルート CA を使ってすべてのドメインコントローラを SSL 証明書に自動的に割り当てる場合は、次の手順を実行して各ドメインコントローラで SSL を有効にする必要があります。

1. Microsoft Enterprise ルート CA をドメインコントローラにインストールします。
   a. **スタート**→ **コントロールパネル**→ **プログラムの追加 / 削除** を選択します
   b. **Windows コンポーネントの追加 / 削除** を選択します。
   c. **Windows コンポーネンウィザード** で、**証明書サービス** チェックボックスをオンにします。
   d. **CA の種類** として **Enterprise ルート CA** を選択し、**次へ** をクリックします。
   e. **この CA の共通名 (CN)** を入力し、**次へ** をクリックしてから、**終了** をクリックします。
2. 各コントローラに SSL 証明書をインストールして、それぞれのドメインコントローラで SSL を有効にします。
   a. **スタート**→ **管理ツール**→ **ドメインセキュリティポリシー** をクリックします。
   b. **公開キーポリシー** フォルダを展開し、**自動証明書要求設定** を右クリックして、**自動証明書要求** をクリックします。
   c. **自動証明書要求セットアップウィザード** で、**次へ** をクリックし、**ドメインコントローラ** を選択します。
   d. **次へ** をクリックして、**終了** をクリックします。

ドメインコントローラルート CA 証明書のエクスポート

メモ: Windows 2000 を実行しているシステムでは、次の手順が異なる場合があります。

1. Microsoft Enterprise CA サービスを実行しているドメインコントローラを見つけます。
2. **スタート**→ **実行** をクリックします。
3. **ファイル名を指定して実行** のフィールドに「mmc」と入力し、**OK** をクリックします。

4. **コンソール 1**(MMC)ウィンドウで、**ファイル**(Windows 2000 システムでは **コンソール**)をクリックし、**スナップインの追加 / 削除** を選択します。
5. **スナップインの追加 / 削除** ウィンドウで、**追加** をクリックします。
6. **スタンドアロンスナップイン** ウィンドウで、**証明書** を選択し、**追加** をクリックします。
7. **コンピュータ** アカウントを選択し、**次へ** をクリックします。
8. **ローカルコンピュータ** を選択し、**終了** をクリックします。
9. **OK** をクリックします。
10. **コンソール 1** ウィンドウで、**証明書** フォルダを展開し、**個人** フォルダを展開してから、**証明書** フォルダをクリックします。
11. ルート CA 証明書を見つけて右クリックし、**すべてのタスク** を選択して、**エクスポート...** をクリックします。
12. **証明書のエクスポートウィザード** で、**次へ** をクリックし、**プライベートキーをエクスポートしない** を選択します。
13. **次へ** をクリックして、フォーマットとして **Base-64 エンコード X.509(.cer)**を選択します。
14. **次へ** をクリックしてシステムのディレクトリに証明書を保存します。
15. ステップ 14 で iDRAC に保存した証明書をアップロードします。

    RACADM を使用して証明書をアップロードするには、ウェブインタフェースを使用して拡張スキーマ Active Directory で iDRAC を設定する を参照してください。

    ウェブインタフェースを使って証明書をアップロードするには、次の手順を実行します。

    a. サポートされている Web ブラウザのウィンドウを開きます。
    b. iDRAC ウェブインタフェースにログインします。
    c. **システム**→ **リモートアクセス** をクリックし、**設定** タブをクリックします。
    d. **セキュリティ** をクリックして **セキュリティ証明書メインメニュー** ページを開きます。
    e. **セキュリティ証明書のメインメニュー** ページの **サーバー証明書のアップロード** を選択して、**適用** をクリックします。
    f. **証明書のアップロード** 画面で、次の手順の 1 つを実行します。
        - **参照** をクリックして証明書を選択します。
        - **値** フィールドに証明書のパスを入力します。
    g. **適用** をクリックします。

iDRAC ファームウェア SSL 証明書のインポート

次の手順を使って、すべてのドメインコントローラの信頼された証明書のリストに iDRAC ファームウェア SSL 証明書をインポートします。

メモ: Windows 2000 を実行しているシステムでは、次の手順が異なる場合があります。

メモ: iDRAC ファームウェア SSL 証明書が既知の CA によって署名されている場合は、この手順を実行する必要はありません。

iDRAC の SSL 証明書は、iDRAC のウェブサーバーで使用される証明書と同じです。すべての iDRAC は、デフォルトの自己署名済み証明書付きで出荷されます。

iDRAC 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**→ **iDRAC サーバー証明書をダウンロードする** を選択します。

1. ドメインコントローラ上で、**MMC コンソール** ウィンドウを開き、**証明書**→ **信用できるルート認証局** を選択します。
2. **証明書** を右クリックし、**すべてのタスク** を選択して、**インポート** をクリックします。
3. **次へ** をクリックして、SSL 証明書ファイルを参照します。
4. 各ドメインコントローラの **信頼されたルート認証局** に RAC SSL 証明書をインストールします。

   ユーザー独自の証明書をインストールしている場合は、証明書に署名をしている CA が **信頼されたルート認証局** リストにあることを確認します。認証局がリストにない場合は、それをすべてのドメインコントローラにインストールする必要があります。
5. **次へ** をクリックし、証明書の種類に基づいて Windows に自動的に証明書ストアを選択させるか、指定するストアまで参照します。
6. **終了** をクリックして、**OK** をクリックします。

Active Directory を使用した iDRAC へのログイン

ウェブインタフェースを使用して iDRAC にログインするのに、Active Directory を使用できます。次のフォーマットのいずれかを使ってユーザー名を入力します。

<ユーザー名@ドメイン>

または

<ドメイン>\<ユーザー名>

または

<ドメイン>/<ユーザー名>

「ユーザー名」は、1 ～ 256 バイトの ASCII 文字列です。

ユーザー名とドメイン名に、空白スペースや特殊文字(\、/、または @ など)は使用できません。

メモ: "America" などの NetBIOS ドメイン名は名前解決できないため、指定できません。

よくあるお問い合わせ(FAQ)

表 6-10 に、よくあるお問い合わせ(FAQ)とその回答を示します。

表 6-10. Active Directory との iDRAC の使用:よくあるお問い合わせ(FAQ)

質問	回答
複数のツリー全体で Active Directory を使って iDRAC にログインできますか?	はい。iDRAC の Active Directory クエリアルゴリズムでは、1 つのフォレストで複数のツリーをサポートします。
異種機混合モードでは Active Directory を使って iDRAC にログインできますか(フォレストのドメインコントローラが、Microsoft Windows NT® 4.0、Windows 2000、または Windows Server 2003 など、異なるオペレーティングシステムを実行する場合)?	はい。混合モードでは、iDRAC クエリプロセスが使用するすべてのオブジェクト(ユーザー、RAC デバイスオブジェクト、関連オブジェクト)は、同一のドメインになければなりません。 デル拡張 Active Directory ユーザーとコンピュータスナップインはモードをチェックし、混合モードであれば、ドメイン間でオブジェクトを作成するためにユーザーを制限します。
Active Directory との iDRAC の使用は複数のドメイン環境をサポートしていますか?	はい。ドメインフォレスト機能のレベルがネイティブまたは Windows 2003 モードでなければなりません。さらに、関連オブジェクト、RAC ユーザーオブジェクト、および RAC デバイスオブジェクト(関連オブジェクトを含む)間のグループがユニバーサルグループでなければなりません。
これらのデル拡張オブジェクト(デル関連オブジェクト、Dell RAC デバイス、およびデル特権オブジェクト)が別のドメインにあってもかまいませんか?	関連オブジェクトと特権オブジェクトは、同じドメインになければなりません。Dell 拡張 Active Directory ユーザーとコンピュータスナップインを使用すると、同じドメインにこれら 2 つのオブジェクトを作成するように強制されます。その他のオブジェクトは別のドメインに作成できます。
ドメインコントローラ SSL 設定に制限はありますか?	はい。フォレストにある Active Directory サーバーの SSL 証明書は、すべて同じルートによって署名される必要があります。これは、iDRAC でアップロード可能な信用できる CA SSL 証明書は 1 つのみであるためです。
新しい RAC 証明書を作成しアップロードしましたが、ウェブインタフェースが起動しません。	Microsoft 証明書サービスを使用して RAC 証明書を生成した場合、証明書の作成時に **Web 証明書** でなく **ユーザー証明書** を誤って選択した可能性があります。 回復するには、CSR を生成してから新しいウェブ証明書を Microsoft Certificate Services を使って作成し、管理下サーバーの RACADM CLI を用いてロードするには、次の RACADM コマンドを使用します。 racadm sslcsrgen [-g] [-u] [-f {ファイル名}] racadm sslcertupload -t 1 -f {web_sslcert}
Active Directory 認証を使って iDRAC にログインできない場合、どうすればよいですか? トラブルシューティングの方法を教えてください。	1. ログイン中、NetBIOS 名ではなく、正しいユーザードメイン名を使用していることを確認します。 2. ローカル iDRAC ユーザーアカウントがある場合は、ローカルの資格情報を使用して iDRAC にログインします。 ログインし後、次の手順を実行してください。 a. iDRAC **Active Directory 設定** ページにある **Active Directory を有効にする** ボックスが選択されているのを確認します。 b. iDRAC **ネットワーク設定** ページの DNS 設定が正しいことを確認します。 c. Active Directory ルート CA から iDRAC に Active Directory 証明書をアップロードしたことを確認します。 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 ドメイン名** が Active Directory の環境設定と一致することを確認します。 f. iDRAC のパスワードが 127 文字以下であることを確認します。iDRAC は最大 256文字のパスワードをサポートしていますが、Active Directory がサポートしているパスワードは最大 127 文字です。

目次ページに戻る

GUI コンソールリダイレクトの使用

Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00
ユーザーズガイド

本項では、iDRAC コンソールリダイレクト機能の使用法について説明します。

概要

iDRAC コンソールリダイレクト機能を使用すると、グラフィックまたはテキストモードでローカルサーバーコンソールにリモートでアクセスできます。この機能を使用すると、1 つの場所から単一または複数の iDRAC システムを制御できます。

すべてのルーチンメンテナンスを実行するのに各サーバーの前に座って行う必要はありません。デスクトップまたはラップトップコンピュータを使ってリモートからサーバーを管理できます。また、リモートからすぐに他のユーザーと情報を共有することもできます。

コンソールリダイレクトの使用

メモ: コンソールリダイレクトのセッションを開くと、管理下サーバーにはそのコンソールがリダイレクトされていることが表示されません。

コンソールリダイレクト ページでは、ローカルの管理ステーションのキーボード、ビデオ、およびマウスを使って、リモートシステムを管理し、リモート管理下サーバーで対応するデバイスを制御できます。この機能を仮想メディア機能と併用すると、リモートソフトウェアのインストールを実行することもできます。

コンソールリダイレクトセッションには次の規則が適用されます。

- 同時にサポートされているコンソールリダイレクトセッションは最大 2 つです。両セッションで、同じ管理下サーバーコンソールを同時に表示します。
- コンソールリダイレクトセッションは、管理下システムのウェブブラウザから起動できません。
- 1 MB/sec 以上の使用可能ネットワーク帯域幅が必要です。

対応画面解像度およびリフレッシュレート

表 7-1 は、管理下サーバーで起動しているコンソールリダイレクトセッションの対応画面解像度および対応リフレッシュレートをリストにしたものです。

表 7-1. 対応画面解像度およびリフレッシュレート

画面解像度	リフレッシュレート（Hz）
720x400	70
640x480	60、72、75、85
800x600	60、70、72、75、85
1024x768	60、70、72、75、85
1280x1024	60

管理ステーションの設定

管理ステーションでコンソールリダイレクトを使用するには、次の手順を実行してください。

1. 対応ウェブブラウザをインストールして設定します。詳細については、以下の項を参照してください。
   - 対応 Web ブラウザ

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

   - 対応 Web ブラウザの設定

2. Firefox を使用している場合、または Internet Explorer で Java Viewer を使用する場合、Java Runtime Environment(JRE)をインストールします。Java Runtime Environment (JRE)のインストール を参照してください。

3. 画面解像度は、1280x1024 ピクセル以上に設定することをお勧めします。

注意:アクティブなコンソールリダイレクトセッションがあり、推奨解像度以下の画面で iKVM に接続している場合、サーバーがローカルコンソールで選択されているとサーバーのコンソール解像度はリセットされることがあります。サーバーが Linux オペレーティングシステムを実行している場合、X11 コンソールはローカル画面で表示不可能なことがあります。iKVM で <Ctrl><Alt><F1> を選択すると、Linux からテキストコンソールに切り替わります。

iDRAC ウェブインタフェースでのコンソールリダイレクトの設定

iDRAC ウェブインタフェースで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. **システム** をクリックし、**コンソール** タブをクリックしします。

2. **設定** をクリックして **コンソールリダイレクトの設定** ページを開きます。

3. コンソールリダイレクトのプロパティを設定します。表 7-2 はコンソールリダイレクトの設定について説明したものです。

4. 設定が完了したら、**適用** をクリックします。

5. 適切なボタンをクリックして続行します。表 7-3 を参照してください。

表 7-2 コンソールリダイレクトの設定プロパティ

プロパティ	説明
有効	クリックして、コンソールリダイレクト を有効または無効にします。 **チェックボックスが選択されている場合**、コンソールリダイレクトは有効です。 **チェックボックスが選択されていない場合**、コンソールリダイレクトは無効です。 デフォルトは **有効** です。
最大セッション数	コンソールリダイレクトの可能な最大セッション数(**1** または **2**)が表示されます。ドロップダウンメニュー を使って、コンソールリダイレクト の 可能な最大セッション数を変更します。デフォルトは **2** です。
アクティブセッション	アクティブなコンソール セッション数を表示します。このフィールドは読み取り専用です。
キーボードとマウスポート番号	コンソール リダイレクト のキーボード / マウスオプションへの接続に 使用されるネットワークポート番号です。トラフィックは常に暗号化されます。別のプログラムでデフォルトのポートが使用されている場合、この番号を変更しなければならない可能性があります。デフォルトは **5900** です。
ビデオポート番号	コンソールリダイレクトの画面サービスへの接続に使用されるネットワークポート番号。別のプログラムでデフォルトのポートが使用されている場合、この設定を変更しなければならない可能性があります。デフォルトは **5901** です。
ビデオ暗号化の有効	**チェックボックスが選択されている場合**、ビデオ暗号化は有効です。ビデオポートを経由するすべてのトラフィックは 暗号化されます。 **チェックボックスが選択されていない場合**、ビデオ暗号化は無効です。ビデオポートを経由するトラフィックは暗号化されません。 デフォルトは **暗号化** されています。**暗号化を無効にすると、低速なネットワークのパフォーマンスを改善できます**。
マウス モード	管理下サーバーが、Windows オペレーティングシステム環境で実行している場合は、**Windows** を選択します。 サーバーが Linux 環境で実行されている場合は、**Linux** を選択します。 サーバーが Windows または Linux オペレーティングシステム環境で実行していない場合は、**なし** を選択します。 デフォルトは **Windows** です。
IE 用 コンソールプラグインタイプ	Windows オペレーティングシステム環境で Internet Explorer を使用している場合は、次の viewer から 選択します。 ActiveX - ActiveX コンソールリダイレクト Viewer Java - Java コンソールリダイレクト Viewer **メモ:** Java Viewer を使用するには、クライアントシステムに Java Runtime Environment がインストールされている必要があります。
ローカルコンソールを 無効にする	チェックボックスが選択されている場合、コンソールリダイレクト中 iKVM モニターへの出力は無効です。その結果、**コンソールリダイレクト** を使って実行したタスクは、管理下サーバーのローカルモニターに表示されなくなります。

メモ:コンソールリダイレクトでの仮想メディアの使用に関する詳細は、仮想メディアの設定および使い方 を参照してください。

コンソールリダイレクトの設定 ページでは、表 7-5 に示したボタンを使用できます。

表 7-3. コンソールリダイレクトの設定ページのボタン

ボタン	定義
印刷	**コンソールリダイレクト** ページを印刷します。
更新	**コンソールリダイレクト** ページを印刷します。
適用	コンソールリダイレクトに追加された新規設定を保存します。

SM-CLP コマンドラインインタフェースでのコンソールダイレクトの設定

コンソールリダイレクトセッションの開始

コンソールリダイレクトのセッションを開くと、Dell Virtual KVM Viewer アプリケーションが起動し、リモートシステムのデスクトップがビューアに表示されます。この仮想 KVM アプリケーションを使用すると、ローカル管理ステーションからシステムのマウスとキーボードの機能を制御できます。

ウェブインタフェースでコンソールリダイレクトセッションを開くには、次の手順を実行してください。

1. **システム** をクリックし、**コンソール** タブをクリックしします。
2. **コンソールリダイレクト** ページで、表 7-4 の情報を使用してコンソールリダイレクトセッションが利用可能であることを確認します。

   表示されるプロパティ値を再設定するには、iDRAC ウェブインタフェースでのコンソールリダイレクトの設定 を参照してください。

表 7-4. 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の有効	はい / いいえ
ビデオ暗号化の有効	はい / いいえ
最大セッション数	サポートされているコンソールリダイレクトの最大数セッションを表示します。
現在の セッション	現在アクティブなコンソールリダイレクトセッション数を表示します。
マウス モード	現在有効な マウスアクセラレータを表示します。**マウスアクセラレータ** モードは、管理下サーバーにインストールされている オペレーティングシステムの種類に応じて選択する必要があります。
コンソールのプラグインタイプ	現在 設定されているプラグインタイプを表示します。 **ActiveX** — Active-X Viewer が起動します。Active-X Viewer は、Windows オペレーティングシステム環境の Internet Exlorer でのみ機能します。 **Java** — Java Viewer が起動します。Java viewer は、Internet Explorer を含め、どのブラウザでも使用できます。クライアントが Windows 以外のオペレーティングシステムを実行している場合は、Java viewer を使用する必要があります。Windows オペレーティングシステム環境で、Internet Explorer を使って iDRAC にアクセスする場合は、プラグインタイプとして Active-X または Java を 選択できます。
ローカルコンソール	チェックボックスが選択されていない場合、ローカルコンソールは無効にされていません。チェックボックスが選択されている場合、シャーシ上で iKVM 接続を使用しているユーザーがコンソールを使用できません。

メモ: コンソールリダイレクトでの仮想メディアの使用に関する詳細は、仮想メディアの設定および使い方 を参照してください。

コンソールリダイレクト ページでは、表 7-5 に示したボタンを使用できます。

表 7-5. コンソールリダイレクトページのボタン

ボタン	定義
更新	**コンソールリダイレクト** ページを印刷します。
ビューアの起動	目的のリモートシステムのコンソールリダイレクトセッションを開きます。
印刷	**コンソールリダイレクト** ページを印刷します。

3. コンソールリダイレクトセッションが使用可能であれば、**ビューアの起動** をクリックします。

   メモ: アプリケーションが起動した後、複数のメッセージボックスが表示される場合があります。アプリケーションへの不正なアクセスを防ぐため、これらのメッセージボックスは 3 分内に参照してください。それができない場合、アプリケーションの再起動プロンプトが表示されます。

   メモ: 以降の手順の途中で 1 つ、または複数の **セキュリティ警告** ウィンドウが表示された場合は、その内容を読んでから、**はい** をクリックして続行します。

管理ステーションが iDRAC に接続し、リモートシステムのデスクトップに Dell Digital KVM Viewer アプリケーションが表示されます。

4. 2 つのマウスポインタ(1 つはリモートシステム用、もう 1 つはローカルシステム用)が Viwer ウィンドウに表示されます。リモートのマウスポインタがローカルのマウスポインタに従うよう 2 つのマウスポインタを同期化する必要があります。マウスポインタの同期 を参照してください。

Video Viewer の使用

Video Viewer は管理ステーションと管理下サーバーの間のユーザーインタフェースを提供するので、管理ステーション側から管理下サーバーのデスクトップを表示して、そのマウスやキーボード機能を制御できます。リモートシステムに接続すると、別のウィンドウで Video Viewer が開始します。

Video Viewer は、カラーモード、マウスの同期、スナップショット、キーボードマクロ、仮想メディアへのアクセスなど、各種コントロール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、Video Viewer が表示されたら、カラーモードの調整やマウスポインタの同期を行わなければならない場合があります。

表 7-6 は、Viewer で使用可能なメニューオプションについて説明したものです。

表 7-6. Viewer メニューバーの選択

メニューアイテム	アイテム	説明
ビデオ	一時停止	コンソールリダイレクトを一時停止します。
	再開	コンソールリダイレクトを再開します。
	更新	Viewer の画面イメージを更新します。
	現在の画面を取り込む	現在のリモートシステム画面を Windows 上の **.bmp** ファイルまたは Linux 上の **.png** ファイルにキャプチャします。ダイアログボックスが表示されたら、ファイルを指定の場所に保存できます。
	全画面表示	Video Viewer を全画面表示モードに拡大するには、**ビデオ** メニューから **全画面表示** を選択します。
	終了	コンソールの使用を終了し、(リモートシステムのログアウト手順に従って)ログアウトしたら、**ビデオ** メニューから **終了** を選択して **Video Viewer** ウィンドウを閉じます。
キーボード	右 Alt キーを押し続ける	右 <Alt> キーと組み合わせるキーを入力する前にこのアイテムを選択します。
	左 Alt キーを押し続ける	左 <Alt> キーと組み合わせるキーを入力する前にこのアイテムを選択します。
	左 Windows キー	左 Windows キーと組み合わせる文字を入力する前に **押し続ける** を選択します。左 Windows キーのキーストロークを送信するには、**押してリリースする** を選択します。
	右 Windows キー	右 Windows キーと組み合わせる文字を入力する前に **押し続ける** を選択します。右 Windows キーのキーストロークを送信するには、**押してリリースする** を選択します。
	マクロ	マクロを選択したり、またはマクロ用に指定されたホットキーを入力すると、その処置がリモートシステムで実行されます。Video Viewer は以下のマクロを提供しています。 • Ctrl-Alt-Del • Alt-Tab • Alt-Esc • Ctrl-Esc • Alt-Space • Alt-Enter • Alt-ハイフン • Alt-F4 • PrtScn • Alt-PrtScn • F1 • Pause • Alt+m
	キーボードのパススルー	キーボードのパススルーモードでは、クライアント上のすべてのキーボード機能をサーバーにリダイレクトできます。
マウス	カーソルの同期	**マウス** メニューでは、カーソルを同期化できるため、クライアント上のマウスをサーバー上のマウスにリダイレクトできます。
オプション	カラーモード	ネットワーク上でパフォーマンスを向上させるための色彩度を選択できます。例えば、仮想メディアからソフトウェアをインストールする場合、コンソールビューアが使用するネットワーク帯域幅を軽減し、メディアからのデータ転送に使用する帯域幅を増大させるよう、最も彩度の低い色(3 ビットグレー)を選択できます。 カラーモードは、15 ビットカラー、7 ビットカラー、4 ビットカラー、4 ビットグレー、3 ビットグレーに設定できます。
メディア	仮想メディアウィザード	**メディア** メニューでは、仮想メディアウィザードへのアクセスが提供され、以下のようなデバイスまたはイメージにリダイレクトできます。 • フロッピードライブ • CD • DVD • ISO フォーマットのイメージ • USB フラッシュドライブ 仮想メディア機能に関する詳細については、仮想メディアの設定および使い方 を参照してください。 仮想メディアを使用するには、コンソールビューアウィンドウをアクティブにしている必要があります。
ヘルプ	なし	**ヘルプ** メニューをアクティブにします。

マウスポインタの同期

リモート PowerEdge システムにコンソールリダイレクトを使用して接続する場合、リモートシステム上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せず、Video Viewer ウィンドウに 2 つのマウスポインタが表示されることがあります。

マウスポインタを同期するには、**マウス→ カーソルの同 期** をクリックするか、<Alt><M> を押します。

[カーソルの同期] メニューアイテムはトグル式です。メニューでアイテムの横にチェックマークがあり、マウスの同期がアクティブであることを確認してください。

Red Hat® Linux® または Novell® SUSE® Linux を使用している場合、Viewer を起動する前に必ず Linux 用のマウスモードに設定してください。設定に関するヘルプは、iDRAC ウェブインタフェースでのコンソールリダイレクトの設定 を参照してください。オペレーティングシステムのデフォルトマウス設定は、iDRAC コンソールリダイレクト画面でマウス矢印のコントロールに使用されます。

ローカルコンソールを無効 / 有効にする

iDRAC ウェブインタフェースを使用して iKVM 接続を無効にするよう iDRAC を設定できます。ローカルコンソールが無効な場合、黄色の状態ドットがサーバーリスト(OSCAR)に表示され、コンソールが iDRAC でロックされていることを示します。ローカルコンソールが有効な場合、状態ドットは緑色で表示されます。

管理下サーバーのコンソールへの専用アクセスを確保する場合、ローカルコンソールを無効にし、また **コンソールリダイレクトページ** で **最大セッション数** を 1 に再設定する必要があります。

メモ: ローカルコンソール機能は、PowerEdge SC1435 および 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: サーバー上のローカルビデオを無効にする(オフにする)と、iKVM に接続されたモニター、キーボード、マウスが無効になります。

ローカルコンソールを無効または有効にするには、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 iDRAC にログインします。詳細に関しては、ウェブインタフェースへのアクセス を参照してください。
2. **システム** をクリックし、**コンソール** タブをクリックして、**設 定** をクリックします。
3. サーバー上のローカルビデオを無効にする(オフにする)場合は、**コンソールリダイレクト** ページで、**ローカルコンソールを無効にする** チェックボックスを選択し、**適 用** をクリックします。デフォルト値は **オフ** です。
4. サーバー上のローカルビデオを有効にする(オンにする)場合は、**コンソールリダイレクト** ページで、**ローカルコンソールを無効にする** チェックボックスを選択解除し、**適 用** をクリックします。

コンソールリダイレクト ページには、ローカルサーバービデオの状態が表示されます。

よくあるお問い合わせ(FAQ)

表 7-7 に、よくあるお問い合わせ(FAQ)とその回答を示します。

表 7-7. コンソールリダイレクトの使用:よくあるお問い合わせ(FAQ)

質問	回答
サーバー上のローカルビデオがオフになっている場合に、新しいリモートコンソールビデオセッションを起動できますか ?	はい。
ローカルビデオをオフにするように要求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 秒かかるのはなぜですか ?	ビデオがオフに切り替わる前に、ローカルユーザーが必要であれば別の操作を行うことができるように配慮しているためです。
ローカルビデオをオンにする場合に、遅延時間は発生しますか ?	発生しません。iDRAC によりローカルビデオを **オン** にする要求を受信すると、ビデオは瞬時にオンになります。
ローカルユーザーはビデオをオフにすることもできますか ?	はい、できます。ローカルユーザーは ローカル RACADM CLI 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 ?	いいえ。ローカルコンソールを無効にすると、ローカルユーザーのキーボードおよびマウスは無効にされるため、設定を変更することはできません。
ローカルビデオをオフに切り替えると、ローカルキーボードとマウスもオフに切り替わりますか ?	はい。
ローカルコンソールをオフにすると、リモートコンソールセッションのビデオはオフになりますか ?	いいえ、ローカルビデオをオン / オフに切り替えても、リモートコンソールセッションには影響しません。
iDRAC ユーザーがローカルサーバービデオをオン / オフにするのに必要な権限とは何ですか ?	iDRAC を設定権限を持ったユーザーであればローカルコンソールをオン / オフにできます。
ローカルサーバービデオの現在の状態はどのように取得できますか ?	状態は iDRAC のウェブインタフェースの **コンソールリダイレクト** ページに表示されます。

	RACADM CLI コマンド **racadm getconfig –g cfgRacTuning** は、オブジェクト **cfgRacTuneLocalServerVideo** 内の状態を表示します。 状態は、iKVM OSCAR モニターにも表示されます。ローカルコンソールが有効な場合、サーバー名の横に緑色のドットで表示されます。無効な場合は、ローカルコンソールが iDRAC によってロックされていることを示す黄色のドットが表示されます。
コンソールリダイレクトウィンドウで、システム画面の底部が見えません。	管理ステーションのモニター解像度が 1280x1024 に設定されているか確認します。
コンソールウィンドウが文字化けします。	Linux のコンソールビューアには UTF-8 文字コードが必要です。ロケールを確認し、必要に応じて文字コードをリセットしてください。詳細に関しては、Linux のロケール設定 を参照してください。
Windows 2000 オペレーティングシステムをロードする場合に、管理下サーバーの画面に何も表示されないのはなぜですか ?	管理下サーバーに正しい ATI ビデオドライバがありません。『Dell PowerEdge Installation and Server Management CD』を使用してビデオドライバをアップデートしてください。
コンソールリダイレクトの実行時に DOS でマウスが同期しないのはなぜですか ?	Dell BIOS はマウスドライバを PS/2 マウスとしてエミュレートしています。設計によって、PS/2 マウスはマウスポインタに対する相関位置を使用しているため、同期に遅延が生じます。iDRAC には USB マウスドライバが搭載されているため、絶対位置を使用した、より密接なマウスポインタのトラッキングが可能となります。iDRAC が USB の絶対的なマウスの位置を Dell BIOS にパスしても、BIOS エミュレーションによって相対的な位置に戻されるため、動作は変わりません。この問題を修正するには、[コンソールリダイレクト] 設定でマウスモードを **なし** に設定します。
Linux テキストコンソールでマウスは同期しないのはなぜですか ?	仮想 KVM には USB マウスドライバが必要ですが、USB マウスドライバは X-Windows オペレーティングシステムでしか使用できません。
まだマウスの同期に不具合があります。	コンソールリダイレクトセッションの起動前に、オペレーティングシステムに対して正しいマウスが選択されていることを確認します。 **マウス** メニューで、**マウスの同期** が選択されていることを確認します。マウスの同期をトグルするには、**マウス** → **マウスの同期** を選択するか、<Alt><M> を押します。同期が有効になっている場合、**マウス** メニューで選択項目の横にチェックマークが表示されます。
iDRAC のコンソールリダイレクトを使って Microsoft® オペレーティングシステムをリモートでインストールする間、キーボードやマウスを使用できないのはなぜですか ?	BIOS でコンソールリダイレクトが有効になっているシステムで、Microsoft の対応オペレーティングシステムをリモートかでインストールするとき、EMS 接続メッセージが表示され、続行する前に **OK** を選択するように要求されます。リモートでマウスを使って **OK** を選択することはできません。ローカルシステムで **OK** を選択するか、リモートで管理下サーバーを再起動し、再インストールしてから、BIOS のコンソールリダイレクトをオフにする必要があります。 このメッセージは Microsoft によって生成され、コンソールリダイレクトが有効であることをユーザーに警告します。このメッセージが表示されないようにするには、常に BIOS でコンソールリダイレクトをオフにしてから、オペレーティングシステムをリモートでインストールしてください。
管理ステーションの Num Lock インジケータがリモートサーバーの Num Lock 状態を反映しないのはなぜですか ?	iDRAC からアクセスした場合、管理ステーションの Num Lock インジケータは必ずしもリモートサーバーの Num Lock 状態と一致するとは限りません。Num Lock の状態は、リモートセッションが接続するときのリモートサーバーの設定によって決まり、管理ステーションの Num Lock の状態とは関係ありません。
ローカルホストからコンソールリダイレクトセッションを確立すると、複数の Session Viewer ウィンドウが表示されるのはなぜですか ?	コンソールリダイレクトセッションをローカルシステムから設定しています。この操作は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を実行中、ローカルユーザーがリモートシステムにアクセスする場合、警告メッセージを受信しますか ?	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は、両方のユーザーがシステムをコントロールできます。
コンソールリダイレクトセッションを実行するのに必要な帯域幅はどのくらいですか?	良いパフォーマンスを得るには、5 MB/sec の接続をお勧めします。最小限のパフォーマンスは、1 MB/sec の接続で実現可能です。
コンソールリダイレクトを実行する管理ステーションのシステム最小要件は何ですか?	管理ステーションには、256 MB 以上の RAM を搭載した Intel Pentium III 500 MHz プロセッサが必要です。

目次ページに戻る

目次ページに戻る

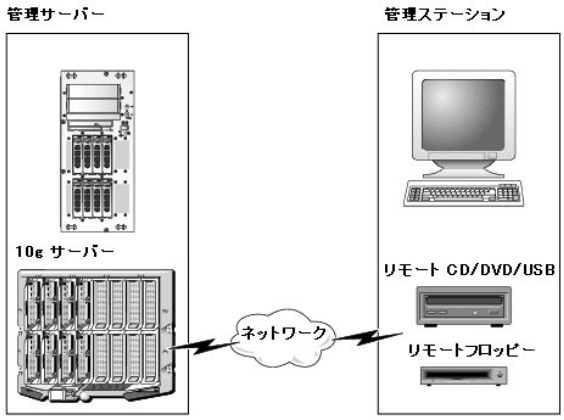
仮想メディアの設定および使い方

Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00
ユーザーズガイド

概要

コンソールリダイレクトビューア経由でアクセスする **仮想メディア** 機能は、管理下サーバーに対しネットワーク上でリモートシステムに接続されるメディアへのアクセスを提供します。図 8-1 **は、仮想メディア** のアーキテクチャの概要を示したものです。

図 8-1. 仮想メディアのアーキテクチャの概要



仮想メディア を使用すると、管理下サーバーの起動から、アプリケーションのインストール、ドライバのアップデート、新しいオペレーティングシステムのインストールまで、CD/DVD やディスケットドライブからリモートで実行することができます。

メモ: **仮想メディア** には、128 Kbps 以上のネットワーク帯域幅が必要です。

仮想メディア は、管理下サーバーのオペレーティングシステムと BIOS に対し 2 つのデバイス（フロッピーディスクデバイスおよびオプティカルディスクデバイス）を定義します。

管理ステーションは、物理メディアやイメージファイルをネットワーク経由で提供します。**仮想メディア** が接続されていると、管理下サーバーからのすべての仮想 CD/フロッピードライブアクセス要求がネットワーク間の管理ステーションに向けられます。**仮想メディア** への接続は、物理デバイスへのメディアの挿入と同じ様に表示されます。仮想メディアが接続していないとき、管理下サーバーの仮想デバイスは、ドライブにメディアがインストールされていない 2 台のドライブに見えます。

表 8-1 に、仮想フロッピーと仮想オプティカルドライブでサポートされているドライブ接続を示します。

メモ: 接続中に **仮想メディア** を変更すると、システム起動シーケンスが停止する場合があります。

表 8-1. サポートされているドライブ接続

サポートされている仮想フロッピードライブ接続	サポートされている仮想オプティカルドライブ接続
1. 44 フロッピーディスケット使用のレガシー 1.44 フロッピードライブ	CD-ROM メディアのある CD-ROM、DVD、CDRW、コンビネーションドライブ
1. 44 フロッピー ディスケットを使用の UBC フロッピードライブ	ISO9660 フォーマットの CD-ROM/DVD イメージファイル
1.44 フロッピーイメージ	CD-ROM メディアのある USB CD-ROMドライブ
USB リムーバブルディスク	

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、対応しているバージョンの Internet Explorer と ActiveX コントロールプラグインをインストールします。ブラウザのセキュリティを **中** またはそれ以下に設定し、Internet Explorer が ActiveX コントロールをダウンロードしてインストールできるようにします。

詳細については、対応 Web ブラウザ を参照してください。

ActiveX をインストールするには、システム管理権限が必要です。ActiveX コントロールをインストールする前に、Internet Explorer でセキュリティ警告が表示される場合があります。ActiveX コントロールのインストール手順を完了するには、Internet Explorer でセキュリティ警告が表示されたときに ActiveX コントロールを受け入れる必要があります。

Linux ベースの管理ステーション

Linux オペレーティングシステムを実行している管理ステーションで仮想メディア機能を実行するには、Firefox のサポートされているバージョンをインストールします。詳細については、対応 Web ブラウザ を参照してください。

コンソールリダイレクトプラグインを実行するには、Java Runtime Environment (JRE) が必要です。JRE は、**java.sun.com** からダウンロードできます。JRE バージョン 1.6 以降が推奨されます。

仮想メディアの設定

1. iDRAC ウェブインタフェースにログインします。
2. ナビゲーションツリーで **システム** を選択し、**コンソール** タブをクリックします。
3. **設定→ 仮想メディア** をクリックして仮想メディアを設定します。

   表 8-2 は、**仮想メディア** の設定値について説明したものです。
4. 設定が終了したら、**適用** をクリックします。
5. 適切なボタンをクリックして続行します。表 8-3 を参照してください。

表 8-2. 仮想メディアの設定値

属性	値
仮想メディアの連結	**連結** - 直ちに **仮想メディア** をサーバーに連結します。 **分離** - 直ちに **仮想メディア** からサーバーを分離します。 **自動連結** - 仮想メディアセッションが起動されている場合のみ、**仮想メディア** をサーバーに連結します。
最大セッション	可能な **仮想メディア** の最大セッション数を 表示します。これは常に 1 です。
アクティブセッション	仮想メディアの現在のセッション数を表示します。
仮想 メディアの暗号化の有効	チェックボックスを クリックして、**仮想メディア** 接続の暗号化を有効 または無効にします。チェックボックスが選択されている場合、暗号化は有効、チェックボックスが選択されていない場合、暗号化は無効です。
仮想メディアポート番号	**仮想メディア** サービスへの暗号化なしの接続に使用されるネットワークポート番号。**仮想メディア** サービスへの接続には、指定したポート番号から始まる 2 つの連続ポートが使用されます。指定ポートに続くポート番号は、その他の iDRAC サービスに対して設定できません。デフォルトは **3668** です。
仮想メディア SSL ポート番号	**仮想 メディア** サービスへの暗号化接続に 使用されるネットワークポート番号。**仮想メディア** サービスへの接続には、指定したポート番号から始まる 2 つの連続ポートが 使用されます。指定ポートに続くポート番号は、その他の iDRAC サービスに対して設定できません。デフォルトは **3670** です。
フロッピーの エミュレーション	**仮想メディア** がサーバーにフロッピードライブとして表示されるか USB キーとして表示されるかを示します。**フロッピーのエミュレーション** のチェックボックスがオンの場合、**仮想メディア** デバイスはサーバーでフロッピーデバイスとして表示されます。チェック ボックスがオフの場合は、USB キードライブとして表示されます。
起動を 1 度有効にする	このボックスを チェックして、起動を 1 度有効にするオプションを有効にします。このオプションは、サーバーが 1 度起動した後で **仮想メディア** セッションを終了します。このオプションは、自動展開の際に 便利です。

表 8-3. 仮想メディア設定ページのボタン

ボタン	説明
印刷	画面に表示中の **コンソール設定** ページのデータを印刷します。
更新	**コンソール設定** ページを再ロードします。
適用	**コンソール設定** ページに追加された新規設定を保存します。

仮想メディアの実行

注意:仮想メディア のセッションを実行している間は、**racreset** コマンドを使用しないでください。使用すると、データ損失などの不測の結果が生じます。

注意:仮想メディアアクセス中、[コンソールビューア] のウィンドウアプリケーションはアクティブでなくてはなりません。

1. 管理ステーションで対応 Web ブラウザを開きます。対応 Web ブラウザ を参照してください。

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

2. iDRAC ウェブインタフェースを起動します。ウェブインタフェースへのアクセス を参照してください。

3. ナビゲーションツリーで **システム** を選択し、**コンソール** タブをクリックします。

   コンソールリダイレクト ページが表示されます。表示されている属性値を変更する場合は、仮想メディアの設定 を参照してください。

   メモ:フロッピードライブ(該当する場合)の **フロッピーイメージファイル** が表示される場合は、このデバイスを仮想フロッピーとして仮想化できます。オプティカルドライブ 1 つとフロッピー 1 つを同時に選択するか、単一ドライブを選択できます。

   メモ: 管理下サーバーの仮想デバイスドライブ文字と、管理ステーションの物理ドライブ文字とは一致しません。

   メモ: Internet Explorer 拡張セキュリティを設定した Windows オペレーティングシステムでは、**仮想メディア** が正しく機能しない可能性があります。この不具合を解決するには、Microsoft オペレーティングシステムマニュアルを参照するか、またはシステム管理者に問い合わせてください。

4. **ビューアの起動** をクリックします。

   メモ: Linux では、ファイル **jviewer.jnlp** がデスクトップにダウンロードされ、ファイルの処置について尋ねるダイアログボックスが表示されます。**プログラムを指定して開く** オプションを選択し、JRE インストールディレクトリの **bin** サブディレクトリにある **javaws** アプリケーションを選択します。

   iDRACView アプリケーションが別のウィンドウに起動します。

5. **メディア→ 仮想メディアウィザード...** をクリックします。

   [メディアリダイレクト] ウィザードが開きます。

6. [状態] ウィンドウが表示されます。メディアが接続されている場合は、別のメディアソースに接続する前に接続解除してください。接続解除するメディアの右にある **接続解除** ボタンをクリックします。

7. 接続するメディアタイプの隣にあるラジオボタンを選択します。

   フロッピー / USB ドライブ セクションのラジオボタン 1 つ、**CD / DVD ドライブ** セクションのラジオボタンを 1 つ選択できます。

   フロッピーイメージまたは ISO イメージを接続する場合、(ローカルコンピュータに)イメージまでのパスを入力するか、**検索** ボタンでイメージを検索します。

8. **選択した各メディアタイプの隣にある接続ボタン** をクリックします。

   メディアは接続され、[状態] ウィンドウがアップデートされます。

9. **閉じる** ボタンをクリックします。

仮想メディアの接続解除

1. **メディア→ 仮想メディアウィザード...** をクリックします。

2. 接続解除するメディアの隣にある **接続解除** をクリックします。

   メディアは接続解除され、[状態] ウィンドウがアップデートされます。

3. **閉じる** をクリックします。

仮想メディアからの起動

システム BIOS によって、仮想オプティカルドライブまたは仮想フロッピードライブから起動できるようになります。POST 中に、BIOS 設定ウィンドウで仮想メディアが有効になり、正しい順序でリストに表示されていることを確認します。

BIOS 設定を変更するには、次の手順を実行してください。

1. 管理下サーバーを起動します。

2. <F2> を押して BIOS 設定ウィンドウに進みます。

3. 起動順序にスクロールして <Enter> を押します。

   ポップアップウィンドウに、仮想オプティカルドライブと仮想フロッピードライブが、標準的な起動デバイスと一緒にリストに表示されます。

4. 仮想ドライブが有効になり、ブータブルメディアの最初のデバイスとして表示されていることを確認します。必要に応じて、画面の説明に従って起動順番を変更します。

5. 変更を保存して終了します。

   管理下サーバーが再起動します。

   管理下サーバーは起動順序に基づいて、ブータブルデバイスから起動しようとします。仮想デバイスが接続済みでブータブルメディアが存在している場合、システムはこの仮想デバイスで起動します。ここからブートできない場合、ブータブルメディアのない物理デバイスと同様に、このデバイスは無視されます。

仮想メディアを使用したオペレーティングシステムのインストール

本項では、オペレーティングシステムをインタラクティブな方法で管理ステーションに手動でインストールする方法を説明します。完了に数時間かかる可能性があります。**仮想メディア** を使用する場合、スクリプト記述されたオペレーティングシステムのインストール手順では 15 分以内で完了します。詳細に関しては、オペレーティングシステムの導入 を参照してください。

1. 以下を確認します。
   - オペレーティングシステムのインストール CD が管理ステーションの CD ドライブに挿入されている。
   - ローカル CD ドライブが選択されている。
   - 仮想ドライブに接続している。
2. 仮想メディアから起動するには、仮想メディアからの起動 の項のステップに従い、BIOS がインストール元の CD ドライブ から確実に起動するようにしてください。
3. 画面の説明に従ってインストールを完了します。

サーバーのオペレーティングシステムが実行中の仮想メディアの使用

Windows ベースのシステム

Windows システムでは、仮想メディアドライブは連結されると自動的にマウントされ、ドライブ文字が設定されます。

Windows 内から仮想ドライブを使用する操作は、物理ドライブを使用する場合と似ています。仮想メディアウィザードを使用してメディアに接続し、ドライブをクリックしてその内容を参照すると、そのシステムでメディアが使用できるようになります。

Linux ベースのシステム

システムのソフトウェア設定によっては、仮想メディアドライブが自動的にマウントされない場合もあります。ドライブが自動的にマウントされない場合、Linux の **mount** コマンドを使ってドライブを手動でマウントします。

よくあるお問い合わせ（FAQ）

表 8-4 は、よくあるお問い合わせ（FAQ）とその回答を示したものです。

表 8-4. 仮想メディアの使い方：よくあるお問い合わせ（FAQ）

質問	回答
仮想メディアのクライアントの接続が時々切断されます。なぜですか？	ネットワークタイムアウトが発生した場合、iDRAC ファームウェアはサーバーと仮想ドライブ間のリンクを切断し、接続を中断します。 仮想メディア設定が iDRAC ウェブインタフェースまたはローカル RACADM コマンドで変更された場合、設定変更が適用されると接続されているすべてのメディアが接続解除されます。 仮想ドライブに再接続するには、仮想メディアウィザードを使用します。
どのオペレーティングシステムが iDRAC をサポートしていますか？	対応オペレーティングシステムのリストについては、対応オペレーティングシステム を参照してください。
どのウェブブラウザが iDRAC をサポートしていますか？	対応ウェブブラウザのリストについては、対応 Web ブラウザ を参照してください。
時々クライアントの接続が切断されるのはなぜですか？	• ネットワークが遅い場合や、クライアントシステムの CD ドライブの CD を交換した場合に、クライアントの接続を損失する場合が

	あります。たとえば、クライアントシステムの CD ドライブの CD を交換すると、新しい CD に自動スタート機能があるかもしれません。このような場合、ファームウェアタイムアウトになり、CD の読み取りを開始するまでに時間がかかると、接続が失われることがあります。接続が失われた場合は、GUI から再接続して前の操作を続行してください。 • ネットワークタイムアウトが発生した場合、iDRAC ファームウェアはサーバーと仮想ドライブ間のリンクを切断し、接続を中断します。また、ウェブインタフェースまたは RADACM コマンドの入力による仮想メディアの設定を変更できます。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 オペレーティングシステムのインストールに非常に時間がかかるように思います。なぜですか？	『Dell PowerEdge Installation and Server Management CD』と低速ネットワーク接続を使用して Windows オペレーティングシステムをインストールする場合、ネットワークレイテンシによって iDRAC ウェブインタフェースへのアクセスにかかる時間が長くなることがあります。インストールウィンドウにインストール進行状況が表示されない場合でも、インストール作業は進行しています。
フロッピードライブまたは USB メモリキーの内容を表示しています。同じドライブを使用して仮想メディア接続を確立しようとすると、接続エラーメッセージが表示され、再試行を要求されます。なぜですか?	仮想フロッピードライブへの同時アクセスは許可されません。ドライブを仮想化する前に、ドライブの内容表示に使用しているアプリケーションを閉じてください。
どのようにして仮想デバイスを起動デバイスとして設定するのですか？	管理下サーバーの [BIOS 設定] にアクセスし、起動メニューに進みます。仮想 CD、仮想フロッピー、または仮想フラッシュを探し、必要に応じてデバイスの起動順序を変更します。たとえば、CD ドライブから起動するには、CD ドライブを起動順序の最初に設定する必要があります。
どのようなメディアで起動できますか？	iDRAC では、以下のブータブルメディアで起動することができます。 • 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 • オペレーティングシステムによりリムーバブルディスクと認識された USB キー • USB キーイメージ
USB キーを起動可能にするにはどうしますか？	**support.dell.com** で Dell USB キーを起動可能にするのに使用できる Windows プログラム、Dell 起動ユーティリティを検索します。 Windows 98 起動ディスクでの起動、および起動ディスクから USB キーへのシステムファイルのコピーも可能です。例えば、DOS プロンプトから、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。 また、デルの起動ユーティリティを使って、起動可能な 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デル製の USB キーに対してのみ対応しています。ユーティリティをダウンロードするには、ウェブブラウザを開き、デルのサポートウェブサイト **support.dell.com** から「R122672.exe」を検索します。
Red Hat® Enterprise Linux® または SUSE® Linux オペレーティングシステムを起動しているシステム上では、仮想フロッピーを検索できません。仮想メディアを取り付け、リモートフロッピーに接続しています。どうすべきですか？	Linux のバージョンによってはフロッピードライブと仮想 CD ドライブを同じようにオートマウントしません。仮想フロッピードライブをマウントするには、Linux が仮想フロッピーに割り当てたデバイスノードを検索します。次の手順を実行して仮想フロッピードライブを検索し、マウントします。 1. Linux コマンドプロンプトを開き、次のコマンドを実行します。 `grep "仮想フロッピー" /var/log/messages` 2. そのメッセージに対する最後のエントリを検索し、時間を記録します。 3. Linux 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* はステップ 1 の grep で返されたメッセージのタイムスタンプです。 4. ステップ 3 で、grep コマンドの結果を読み、"DELL 仮想フロッピー" に付けられたデバイス名を検索します。 5. 仮想フロッピードライブが取り付けられ、接続されていることを確認します。 6. Linux プロンプトで、次のコマンドを実行する。 `mount /dev/sdx /mnt/floppy` ここで、 */dev/sdx* はステップ 4 で検出したデバイス名です。 /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サポートされているファイルシステムの種類は何ですか？	仮想フロッピードライブは、FAT16 または FAT32 ファイルシステムをサポートしています。
iDRAC ウェブインタフェースを使用して、ファームウェアのアップデートをリモートで実行した時に、サーバーの仮想ドライブが削除されました。なぜですか？	ファームウェアのアップデートにより iDRAC がリセットされ、リモート接続が切断して仮想ドライブがアンマウントされます。iDRAC リセットが完了すると、ドライブは再表示されます。

目次ページに戻る

目次ページに戻る

ローカル RACADM コマンドラインインタフェースの使用

Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00
ユーザーズガイド

ローカル RACADM コマンドラインインタフェース(CLI)は、管理下サーバーからの iDRAC 管理機能へのアクセスを提供します。RACADM は、iDRAC ウェブインタフェースと同じ機能へのアクセスを提供します。ただし、RACADM は複数のサーバーおよび iDRAC の設定を簡易化するスクリプトで使用できる一方、ウェブインタフェースはインタラクティブな管理に便利です。

ローカル RACADM コマンドは、管理下サーバーから iDRAC へのアクセスにネットワーク接続を使用しません。従って、最初の iDRAC ネットワーク設定にローカル RACADM コマンドを使用できます。

複数の iDRAC の設定に関する詳細については、複数の iDRAC の設定 を参照してください。

本項では次の情報を提供します。

- コマンドプロンプトからの RACADM の使用
- **racadm** コマンドを使用した iDRAC の設定
- `racadm` 設定ファイルを使用した複数の iDRAC の設定

RACADM コマンドの使用

コマンドプロンプトまたはシェルプロンプトからローカル(管理下サーバー上)で RACADM コマンドを実行します。

管理下サーバーにログインし、コマンドシェルを起動して、ローカル RACADM コマンドを次のフォーマットで入力します。

```
racadm <サブコマンド> -g <グループ> -o <オブジェクト> <値>
```

RACADM コマンドには、オプションなしの一般的な使用情報が表示されます。RACADM サブコマンドリストを表示するには、次のように入力します。

```
racadm help
```

サブコマンドのリストには、iDRAC でサポートされるコマンドがすべて含まれています。

サブコマンドのヘルプを取得するには、次のように入力します。

```
racadm help <サブコマンド>
```

このコマンドによって、サブコマンドの構文およびコマンドラインオプションが表示されます。

RACADM サブコマンド

表 9-1 では、RACADM で実行できる各 RACADM サブコマンドについて説明します。構文や有効なエントリなど、RACADM サブコマンドの詳細なリストは、RACADM サブコマンド概要 を参照してください。

表 9-1. RACADM サブコマンド

コマンド	説明
clrraclog	iDRAC のログをクリアします。クリアすると、ログがクリアされたときのユーザーと時刻を示すエントリが 1 つ作成されます。
clrsel	管理下サーバーの [システムイベントログ] エントリをクリアします。
config	iDRAC を設定します。
getconfig	現在の iDRAC 設定のプロパティを表示します。
getniccfg	コントローラの現在の IP 設定を表示します。
getraclog	iDRAC のログを表示します。
getractime	iDRAC の時間を表示します。
getssninfo	アクティブセッションに関する情報を表示します。
getsvctag	サービスタグを表示します。
getsysinfo	iDRAC および管理下サーバーに関する情報を表示します。

gettracelog	iDRAC のトレースログを表示します。-i コマンドを使用すると、iDRAC のトレースログ内のエントリ数を表示します。
help	iDRAC サブコマンドをリストします。
help <サブコマンド>	指定したサブコマンドの使用法ステートメントをリストにします。
racreset	iDRAC をリセットします。
racresetcfg	iDRAC をデフォルト設定にリセットします。
serveraction	管理下サーバーの電源管理操作を実行します。
setniccfg	コントローラの IP 設定を行います。
sslcertdownload	CA 証明書をダウンロードします。
sslcertupload	CA 証明書またはサーバー証明書を iDRAC にアップロードします。
sslcertview	iDRAC に CA 証明書またはサーバー証明書を表示します。
sslcsrgen	SSL CSR を生成してダウンロードします。
testemail	iDRAC NIC 経由で iDRAC に電子メールを送信させます。
testtrap	iDRAC NIC 経由で iDRAC に SNMP 警告を送信させます。
vmdisconnect	仮想メディア接続を終了させます。

RACADM ユーティリティを使用した iDRAC の設定

本項では、RACADM を使用して各種 iDRAC 設定タスクを実行する方法について説明します。

現在の iDRAC 設定の表示

RACADM **getconfig** サブコマンドは、iDRAC からの現在の設定を取得します。設定値は、1 つまたは複数の オブジェクト を含む グループ に組織化され、オブジェクトには 値 が含まれます。

グループおよびオブジェクトについての詳細に関しては、iDRAC プロパティデータベースのグループおよびオブジェクトの定義 を参照してください。

すべての iDRAC グループのリストを表示するには、次のコマンドを入力します。

```
racadm getconfig -h
```

特定のグループのオブジェクトおよび値を表示するには、次のコマンドを入力します。

```
racadm getconfig -g <グループ>
```

例えば、**cfgLanNetworking** 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 cfgLanNetworking
```

RACADM を使用した iDRAC ユーザーの管理

注意: **racresetcfg** コマンドを使用する際、すべての設定パラメータが元のデフォルトにリセットされるため、注意してください。前の変更は失われます。

メモ: 新しい iDRAC を設定している場合や、**racadm racresetcfg** コマンドを実行した場合、現在のユーザーは、パスワードが **calvin** の **root** のみです。

メモ: ユーザーは後日、有効 / 無効にできます。その結果、ユーザーは各 iDRAC に異なるインデックス番号を持つことになります。

iDRAC のプロパティデータベースには 15 のユーザーを設定できます。(16 番目のユーザーは、IPMI LAN ユーザー用に予約されています。) iDRAC ユーザーを手動で有効にする前に、現在のユーザーが存在するか確認します。

コマンドプロンプトで、次のコマンドを入力すると、ユーザーが存在するかどうかを確認できます。

```
racadm getconfig -u <ユーザー名>
```

または

1 ～ 16 の各インデックスに 1 回ずつ次のコマンドを入力できます。

```
racadm getconfig -g cfgUserAdmin -i <インデックス>
```

メモ: また、racadm getconfig -f <ファイル名> と入力し、生成した <ファイル名> ファイルを表示することもできます。このファイルにはすべてのユーザーおよびその他の iDRAC 設定パラメータが含まれます。

複数のパラメータとオブジェクト ID が現在の値と一緒に表示されます。オブジェクトは次の 2 つです。

```
# cfgUserAdminIndex=nn

cfgUserAdminUserName=
```

cfgUserAdminUserName オブジェクトに値がない場合は、**cfgUserAdminIndex** オブジェクトで示されるインデックス番号を使用できます。「=」の後に名前が表示されたら、そのインデックス

はそのユーザー名が使用しています。

iDRAC ユーザーの追加

新規ユーザーを iDRAC に追加するには、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. ログインを iDRAC ユーザー権限に設定します。
4. ユーザーを有効にします。

例

次の例は、パスワードが「123456」で iDRAC へのログイン特権を持つ「John」という新しいユーザーを追加する方法を示しています。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456

racadm config -g cfgUserAdmin -o cfgUserPrivilege -i 2 0x00000001

racadm config -g cfgUserAdmin -o cfgUserAdminEnable -i 2 1
```

新規ユーザーを検証するには、次のコマンドのいずれかを使用します。

```
racadm getconfig -u john

racadm getconfig -g cfgUserAdmin -i 2
```

権限付きの iDRAC ユーザーを有効にする

ユーザーに特定のシステム管理者（役割ベース）権限を与えるには、**cfgUserAdminPrivilege** プロパティを 表 9-2 に示す値で構成されたビットマスクに設定します。

表 9-2. ユーザー特権に応じたビットマスク

ユーザー特権	特権ビットマスク
iDRAC へのログイン	0x0000001
iDRAC の設定	0x0000002
ユーザーの設定	0x0000004
ログのクリア	0x0000008
サーバーコントロールコマンドの実行	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

例えば、ユーザーに **iDRAC の設定**、**ユーザーの設定**、**ログのクリア**、**コンソールリダイレクトへのアクセス** 権限を与えるには、値 0x00000002、0x00000004、0x00000008、0x00000010 を追加してビットマップ 0x0000002E を構成します。続いて次のコマンドを入力して権限を設定します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i2 0x00000001E
```

iDRAC ユーザーの削除

RACADM を使用するとき、ユーザーは手動で個別に無効にする必要があります。設定ファイルを使ってユーザーを削除することはできません。

次の例は、RAC ユーザーを削除するときに使用できるコマンド構文です。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <インデックス> ""
```

二重引用符の（""）のヌル文字列は、指定したインデックスのユーザー設定を削除して、出荷時のデフォルトにリセットするように iDRAC に指示します。

電子メール警告のテスト

iDRAC 電子メール警告機能により、ユーザーは管理下サーバーで重要なイベントが発生したときに電子メール警告を受信することができます。次の例は、電子メール警告機能をテストして、iDRAC が電子メール警告をネットワーク全域に正しく送信できることを確認する方法を示しています。

```
racadm testemail -i 2
```

メモ: 電子メール警告機能をテストする前に、[SMTP] および [電子メール警告設定] が設定されていることを確認してください。詳細に関しては、電子メール警告の設定 を参照してください。

iDRAC SNMP トラップ警告機能のテスト

iDRAC SNMP トラップ警告機能を使用すると、管理下サーバーで発生したシステムイベントを受信するための SNMP トラップリスナーを設定できます。

次の例は、SNMP トラップ警告機能をユーザーがテストする方法を示しています。

```
racadm testtrap -i 2
```

メモ: iDRAC SNMP トラップ警告機能をテストする前に、SNMP とトラップの設定が正しいことを確認します。これらの設定を行うには、**testtrap** および **testemail** サブコマンドの説明を参照してください。

iDRAC ネットワークプロパティの設定

使用可能なネットワークプロパティのリストを生成するには、次のように入力します。

```
racadm getconfig -g cfgLanNetworking
```

DHCP を使用して IP アドレスを取得するには、このコマンドでオブジェクト **cfgNicUseDhcp** を書き込んで、この機能を有効にします。

```
racadm config -g cfgLanNetworking -o cfgNicUseDhcp 1
```

コマンドは、起動時に <Ctrl><E> の入力を求められたときの iDRAC 設定ユーティリティと同じ設定機能を提供します。iDRAC 設定ユーティリティを使用したネットワークプロパティ設定についての詳細に関しては、LAN を参照してください。

次の例に、特定の LAN ネットワークプロパティを設定するときに使用できるコマンドの使い方を示します。

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1

racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicUseDhcp 0

racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o ccfgDNSServer1 192.168.0.5

racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6

racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1

racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002

racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

メモ: **cfgNicEnable** を **0** に設定すると、DHCP が有効になっていても iDRAC LAN は無効になります。

IPMI の設定

1. 次のコマンドを入力して、IPMI オーバー LAN を設定します。

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

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

   a. 次のコマンドを入力して、IPMI チャネル特権をアップデートします。

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

<レベル> は次のいずれかになります。

- 2(**ユーザー**)
- 3(**オペレータ**)
- 4(**システム管理者**)

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

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

b. 必要に応じて、次のようなコマンドを使用して IPMI LAN チャネルの暗号化キーを設定します。

メモ: iDRAC IPMI は RMCP+ プロトコルに対応しています。詳細に関しては、IPMI 2.0 の仕様を参照してください。

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

<キー> は有効な 16 進フォーマットの 20 文字の暗号化キーです。

2. 次のコマンドを使用して、IPMI シリアルオーバー LAN(SOL)を設定します。

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

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

a. 次のコマンドを使用して IPMI SOL の最小特権レベルをアップデートします。

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

<レベル> は次のいずれかになります。

- 2(**ユーザー**)
- 3(**オペレータ**)
- 4(**システム管理者**)

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

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

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

b. 次のコマンドを使用して IPMI SOL のボーレートをアップデートします。

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

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

例:

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

c. コマンドプロンプトで次のコマンドを入力して SOL を有効にします。

注: SOL はユーザーごとに有効または無効にできます。

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

<*id*> はユーザーの固有の ID です。

PEF の設定

各プラットフォーム警告に対して iDRAC が講じる処置を設定できます。表 9-3 は、RACADM で識別できる可能な処置と値をリストにしたものです。

表 9-3. プラットフォームイベントの処置

処置	値
処置の必要なし	0
電源オフ	1

再起動	2
パワーサイクル	3

1. 次のコマンドを使用して PEF 処置を設定します。

   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i <インデックス> <処置値>

   <インデックス> は PEF インデックス(表 5-6 参照)で、<処置値> は 表 9-3 からの値です。

   例えば、プロセッサの重要イベントが検知された場合にシステムを再起動し、IPMI 警告を送信するように PEF を有効にするには、次のコマンドを入力します。

   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i 9 2

PET の設定

1. 次のコマンドを使用してグローバル警告を有効にします。

   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1

2. 次のコマンドを使用して PET を有効にします。

   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i <インデックス> <0|1>

   <インデックス> は PET の送信先インデックスで、0 は PET を無効に、1 は PET を有効にします。

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

   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 1

3. 次のコマンドを使用して PET ポリシーを設定します。

   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i <インデックス><IP アドレス>

   <インデックス> は PET の送信先インデックスで、<IP アドレス> は、プラットフォームイベント警告を受け取るシステムの宛先 IP アドレスです。

4. コミュニティ文字列を設定します。

   コマンドプロンプトで次のように入力します。

   racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName <名前>

   <名前> は PET コミュニティ名です。

電子メール警告の設定

1. 次のコマンドを入力してグローバル警告を有効にします。

   racadm config -g cfgIpmiLan -o cfgIpmiLanAlertEnable 1

2. 次のコマンドを入力して電子メール警告を有効にします。

   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i <インデックス> <0|1>

   <インデックス> は電子メール送信先インデックスで、0 は電子メール警告を無効に、1 は電子メール警告を有効にします。電子メール送信先インデックスは 1 ～ 4 の値になります。

   たとえば、インデックス 4 の電子メールを有効にするには、次のコマンドを入力します。

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

3. 次のコマンドを使用して電子メール設定を行います。

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

   1 は電子メール送信先のインデックスで、<電子メールアドレス> は、プラットフォームイベント警告を受け取る宛先電子メールアドレスです。

4. カスタムメッセージを設定するには、次のコマンドを入力します。

   racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i <インデックス> <カスタムメッセージ>

   <インデックス> は電子メール送信先インデックスで、<カスタムメッセージ> はカスタムメッセージです。

5. 必要に応じて、次のコマンドを使用して設定した電子メール警告をテストします。

   ```
   racadm testemail -i <インデックス>
   ```

   <インデックス> は、テストする電子メール送信先インデックスです。

IP フィルタ(IpRange)の設定

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 iDRAC へのアクセスを許可できます。その他のすべてのログイン要求は拒否されます。

IP フィルタは着信ログインの IP アドレスを、次の **cfgRacTuning** プロパティで指定する IP アドレス範囲と比べます。

- 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。結果が同一の場合、着信ログイン要求の iDRAC 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はエラーを受け取ります。

次の式がゼロと等しい場合に、ログインが続行します。

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

& は数量のビットワイズの AND で、^ はビットワイズの exclusive-OR です。

cfgRacTuning プロパティの完全リストについては、cfgRacTuning を参照してください。

表 9-4. 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を決定します。 このプロパティはビットワイズの anded と **cfgRacTuneIpRangeMask** で、許可する IP アドレスの上位部分を決定します。上位部分のビットパターンを含むすべての IP アドレスがログイン許可されます。この範囲外の IP アドレスからのログインは失敗します。各プロパティのデフォルト値は、ログインできるアドレス範囲を 192.168.1.0 ～ 192.168.1.255 で許可しています。
cfgRacTuneIpRangeMask	IP アドレスの有効ビット位置 を定義します。マスクは、下位ビットのすべての「1」が 1 度の移行ですべて「0」になるネットマスクの形式にします。

IP フィルタの設定

ウェブインタフェースで IP フィルタを設定するには次の手順を実行してください。

1. **システム**→ **リモートアクセス**→ **iDRAC**→ **ネットワーク / セキュリティ** をクリックします。
2. **ネットワーク設定** ページで、**詳細設定** をクリックします。
3. **IP 範囲有効** チェックボックスを選択し、**IP 範囲のアドレス** および **IP 範囲のサブネットマスク** を入力します。
4. **適用** をクリックします。

次の例では、ローカル RACADM を使用して IP フィルタを設定しています。

メモ: RACADM および RACADM コマンドについての詳細に関しては、ローカル RACADM コマンドラインインタフェースの使用 を参照してください。

1. 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。

   ```
   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
   ```

2. ログインを 4 つの連続する IP アドレスに限定するには(192.168.0.212 ～ 192.168.0.215)、次のようにマスクの最下位の 2 ビットを除くすべてを選択します。

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

```
racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 255.255.255.252
```

範囲マスクの最後のバイトは 252 に設定されています。10 進数にして 11111100 バイトです。

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** がネットマスクの形態で設定されるようにします。最重要ビットがすべて 1 で(これがマスクのサブネットを定義)、下位のビットではすべてゼロに遷移します。
- 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のすべてでゼロになる必要があります。

IP ブロックの設定

IP ブロックは、事前に選択した時間内に特定の IP アドレスからのログイン失敗回数が過剰になる時を動的に決定し、そのアドレスが iDRAC にログインするのをブロック(防止)します。

IP ブロックには次の機能が含まれます。

- 許可されるログインの失敗の回数(**cfgRacTuneIpBlkFailcount**)
- これらの失敗が発生できる時間枠(秒)(**cfgRacTuneIpBlkFailWindow**)
- 許可される失敗の回数の合計を超えてから、ブロックされた IP アドレスがセッションを確立することが妨げられるときの秒数の合計(**cfgRacTuneIpBlkPenaltyTime**)

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登録されます。ユーザーがログインに成功すると、失敗履歴はクリアされ、内部カウンタがリセットされます。

メモ: クライアント IP アドレスからのログイン試行が拒否されると、SSH に「ssh exchange identification: Connection closed by remote host」のようなメッセージが表示される場合があります。

cfgRacTune プロパティの完全なリストは、iDRAC 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。

ログイン試行制限のプロパティ は、ユーザー定義のパラメータをリストしています。

表 9-5. ログイン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(**cfgRacTuneIpBlkFailWindow**)1 つの IP アドレスからの失敗が連続すると(**cfgRacTuneIpBlkFailCount**)、以降そのアドレスからのセッション確立試行がすべて一定の時間(**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	失敗した試行がカウントされる時間枠(秒)。失敗がこの制限を越えると、カウンタからドロップされます。
cfgRacTuneIpBlkPenaltyTime	ログイン失敗回数が制限を越えた IP アドレスからのログインを拒否する時間を秒で指定します。

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 cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 300
```

次の例は、1 分以内に失敗が 3 回を超えた場合に、1 時間ログイン試行を防止します。

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

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60

racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime 360
```

ローカル RACADM を使用した iDRAC Telnet および SSH サービスの設定

Telnet/SSH コンソールは、RACADM コマンドを使用してローカル（管理下サーバー上）で設定できます。

メモ: 本項のコマンドを実行するには、**iDRAC の設定** 権限が必要です。

メモ: iDRAC で Telnet または SSH 設定を再設定する場合、いずれの現行セッションも警告なしで終了されます。

ローカル RACADM から Telnet/SSH コンソールを有効にするには、管理下サーバーにログインし、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 cfgSerialTelnetEnable 1
```

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

Telnet または SSH サービスを無効にするには、値を 1 から 0 に変更します。

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

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

iDRAC 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>
```

例えば、Telnet ポートをデフォルトの 22 から 8022 に変更するには、次のコマンドを入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort 8022
```

使用可能な RACADM CLI コマンドの完全リストについては、ローカル RACADM コマンドラインインタフェースの使用 を参照してください。

---

iDRAC 設定ファイルの使用

iDRAC 設定ファイルは、iDRAC データベースの代表値を含むテキストファイルです。RACADM **getconfig** サブコマンドを使用して iDRAC からの現在の値を含む設定ファイルを生成できます。次にファイルを編集し、RACADM **config -f** サブコマンドを使用してファイルを iDRAC にロードし直すか、設定を他の iDRAC にコピーできます。

iDRAC 設定ファイルの作成

設定ファイルは、フォーマットされていないテキストファイルです。有効なファイル名はすべて使用できますが、推奨される拡張子は **.cfg** です。

設定ファイルの特徴は以下の通りです。

- テキストエディターで作成可能
- RACADM **getconfig** サブコマンドで iDRAC から取得可能
- RACADM **getconfig** サブコマンドで iDRAC から取得および編集可能

RACADM **getconfig** コマンドで設定ファイルを取得するには、管理下サーバーのコマンドプロンプトで次のコマンドを入力します。

```
racadm getconfig -f myconfig.cfg
```

このコマンドは、現在のディレクトリにファイル **myconfig.cfg** を作成します。

設定ファイルの構文

注意: Windows の **Notepad** や Linux の **vi** など、プレーンなテキストエディターで設定ファイルを編集してください。**racadm** ユーティリティは ASCII テキストのみパースします。フォーマットするとパーサが混乱して、iDRAC データベースが破壊される可能性があります。

本項では設定ファイルのフォーマットについて説明します。

- # で始まる行はコメントです。

  コメントは、行の一列目にあります。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。

  例:

  ```
  #
  # これはコメントです。
  [cfgUserAdmin]
  cfgUserAdminPrivilege=4
  ```

- すべてのグループエントリは、**[** と**]** の文字で囲む必要があります。

  グループ名を示すときの開始の **[** は一列目になければなりません。グループ名はそのグループ内のどのオブジェクトよりも前に指定する必要があります。オブジェクトに関係するグループ名がない場合、エラーが発生します。設定データは、iDRAC プロパティデータベースのグループおよびオブジェクトの定義 に定義されるようにグループ分けされています。

  次に、グループ名、オブジェクト、およびオブジェクトのプロパティ値の使用例を示します。

  例:

  ```
  [cfgLanNetworking] （グループ名）
  ```

  ```
  cfgNicIpAddress=143.154.133.121 （オブジェクト名）
  ```

- パラメータは、object、=、value の間に空白を入れずに「object=value」のペアとして指定されます。

  値の後の空白スペースは無視されます。値の文字列内にあるスペースはそのままにされます。「=」の右側の文字はそのまま使用されます（例、2 番目の「=」、または「#」、「[」、「]」など）。

- パーサは、インデックスオブジェクトエントリを無視します。

  使用されるインデックスは指定できません。インデックスがすでに存在している場合は、それが使用されます。インデックスがない場合は、そのグループで最初に使用可能なインデックスに新たなエントリが作成されます。

  `racadm getconfig -f <ファイル名>` コマンドは、インデックスオブジェクトの前にコメントを配置するため、ここでコメントを確認できます。

メモ: 次のコマンドを使用して手動でインデックス付きグループを作成できます。
`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><固有のアンカー名>`

- インデックス付きグループの行は設定ファイルから削除できません。

  次のコマンドを使用して、インデックス付きオブジェクトを手動で削除する必要があります。

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

メモ: NULL 文字列（2 つの"" 文字）は、iDRAC 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>
  ```

- インデックス付きグループの場合、オブジェクトアンカーは [ ] の組の後にくる最初のオブジェクトでなければなりません。次に、現在のインデックス付きグループの例を示します。

  ```
  [cfgUserAdmin]
  ```

  ```
  cfgUserAdminUserName=<ユーザー名>
  ```

- インデックス付きグループが検出された場合、これはさまざまなインデックスを区別するアンカー付きオブジェクトの値です。

  パーサーは、iDRAC からそのグループのすべてのインデックスを読み取ります。グループ内のオブジェクトはすべて iDRAC が設定されたときに若干修正されたものです。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 iDRAC のインデックスが作成されます。

- 設定ファイルで所望のインデックスを指定することはできません。

  インデックスは作成や削除ができるため、グループは次第に使用中のインデックスと未使用のインデックスで断片化される可能性があります。インデックスが存在する場合は、変更されます。インデックスが存在しない場合は、最初に使用できるインデックスが使用されます。この方法では、管理しているすべての RAC 間で同じインデックスを作成する必要がないので、インデックスエントリを柔軟に追加できます。新しいユーザーは最初に使用できるインデックスに追加されます。1 つの DRAC 5 で正しくパースおよび実行される設定ファイルは、すべてのインデックスが一杯で新しいユーザーを追加しなければならない場合に、別の iDRAC で正しく実行されない場合があります。

設定ファイルの iDRAC IP アドレスの変更

設定ファイルの iDRAC IP アドレスを変更するには、不要な **<変数>**=<値> のエントリをすべて削除します。IP アドレス変更に関連する 2 つの **<変数>**=<値> エントリを含む [と] が付いた実際の変数グループのラベルのみが残ります。

例:

```
#
```

```
# オブジェクトグループ "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。

```
#
```

```
# オブジェクトグループ "cfgLanNetworking"
```

```
#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# コメント、この行の残りの部分は無視されます

cfgNicGateway=10.35.9.1
```

iDRAC への設定ファイルのロード

コマンド `racadm config -f <ファイル名>` は、有効なグループおよびオブジェクトが存在し、構文ルールに従っていることを検証するよう設定ファイルをパースします。ファイルにエラーがなければ、コマンドはファイルの内容で iDRAC データベースをアップデートします。

メモ: 構文のみを検証し、iDRAC データベースをアップデートしない場合は、**config** サブコマンドに **-c** オプションを追加します。

設定ファイルのエラーには、検出された行番号のフラグと、その問題を説明した簡単なメッセージが付きます。設定ファイルで iDRAC をアップデートする前にすべてのエラーを修正する必要があります。

注意: **racresetcfg** サブコマンドを使用すると、データベースと iDRAC NIC は元のデフォルトの設定にリセットされ、ユーザーおよびユーザー設定はすべて削除されます。`root` ユーザーは使用可能ですが、その他のユーザーの設定もデフォルトにリセットされます。

`racadm config -f <ファイル名>` コマンドを実行する前に、**racreset** サブコマンドを使用して iDRAC をデフォルト設定にリセットすることができます。ロードする設定ファイルに所望のオブジェクト、ユーザー、インデックス、他のパラメータがすべて含まれていることを確認してください。

設定ファイルで iDRAC をアップデートするには、管理下サーバーのコマンドプロンプトで次のコマンドを実行します。

```
racadm config -f <ファイル名>
```

コマンドが完了したら、RACADM **getconfig** サブコマンドを実行してアップデートが正常に終了したことを確認できます。

複数の iDRAC の設定

設定ファイルを使用して、同一のプロパティで他の IDRAC を設定できます。複数の iDRAC を設定するには、次の手順を実行してください。

1. 他の iDRAC に複写したい設定を所有する iDRAC から設定ファイルを作成します。管理下サーバーのコマンドプロンプトで次のコマンドを入力します。

   ```
   racadm getconfig -f <ファイル名>
   ```

   ここで、<ファイル名> は **myconfig.cfg** など、iDRAC プロパティを保存するファイルの名前です。

   詳細については、iDRAC 設定ファイルの作成 を参照してください。

   メモ: 一部の設定ファイルには、他の iDRAC にファイルをエクスポートする前に変更しなければならない固有の iDRAC 情報（静的 IP アドレスなど）が含まれています。

2. 前のステップで作成した設定ファイルを編集し、複写しない設定を削除またはコメントアウトします。
3. 設定する iDRAC が存在する各管理下サーバーにアクセス可能なネットワークドライブに編集した設定ファイルをコピーします。
4. 各 iDRAC に対して、次の設定を行うものとします。
   a. 管理下サーバーへのログインおよびコマンドプロンプトの開始
   b. デフォルト設定から iDRAC を再設定するには、次のコマンドを入力します。

      ```
      racadm racreset
      ```

   c. 次のコマンドを使用して設定ファイルを iDRAC にロードします。

      ```
      racadm config -f <ファイル名>
      ```

      ここで、<ファイル名> は、作成した設定ファイルの名前です。ファイルが機能中のディレクトリにない場合は完全パスを入力してください。

   d. 次のコマンドを入力して設定した iDRAC をリセットします。

      ```
      racadm reset
      ```

目次ページに戻る

目次ページに戻る

iDRAC SM-CLP コマンドラインインタフェースの使用

Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00
ユーザーズガイド

本項では、iDRAC に内蔵されている Workgroup(SMWG)Server Management Command Line Protocol(SM-CLP)について説明します。

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

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

SM-CLP は、ローカル RACADM コマンドラインインタフェースが提供する機能のサブセットを別のアクセスパスで提供します。SM-CLP は iDRAC 内で実行されますが、RACADM は管理下サーバーで実行されます。また、RACADM は Dell 専用インタフェースであるのに対し、SM-CLP は業界標準インタフェースです。RACADM および SM-CLP コマンドのマッピングについては、RACADM と SM-CLP の比較 を参照してください。

SM-CLP によるシステム管理

iDRAC SM-CLP によって、コマンドラインまたはスクリプトから次のシステム機能を管理できます。

- 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)の管理 — SEL レコードの表示やクリア
- iDRAC ユーザーのアカウント管理
- Active Directory 設定
- iDRAC LAN 設定
- SSL 証明書署名要求(CSR)の生成
- 仮想メディア設定
- Telnet または SSH でのシリアルオーバー LAN(SOL)リダイレクト

---

iDRAC SM-CLP サポート

SM-CLP は iDRAC ファームウェアからホストされ、Telnet および SSH 接続をサポートしています。iDRAC 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、iDRAC からホストされる SM-CLP 機能の概要を提供します。

SM-CLP の機能

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

SM-CLP はバーブとターゲットの概念を奨励して、CLI を経由したシステム設定機能を提供します。バーブは実行する処理を指し、ターゲットはその処理を実行するエンティティ(またはオブジェクト)を決定します。

以下は SM-CLP コマンドラインの構文です。

<バーブ> [<オプション>] [<ターゲット>] [<プロパティ>]

表 10-1 は、iDRAC CLI がサポートするバーブのリスト、各コマンドの構文、バーブがサポートするオプションのリストを示したものです。

表 10-1. サポートされている SM-CLP CLI バーブ

バーブ	説明	オプション
CD	シェルを使用して管理下システムアドレス領域経由でナビゲートします。 構文: cd [オプション] [ターゲット]	−default, −examine, −help, −output, −version
delete	オブジェクトのインスタンスを削除します。 構文: delete [オプション] [ターゲット]	−examine, −help, −output, −version
dump	バイナリイメージを MAP から URI に移動します。 dump -destination <URI> [オプション] [ターゲット]	−destination, −examine, −help, −output, −version
exit	SM-CLP シェルのセッションを終了します。 構文: exit [オプション]	−help, −output, −version
help	SM-CLP コマンドのヘルプを表示します。 help	-examine, -help, -output, -version
load	バイナリイメージを URI から MAP に移動します。 構文: load -source <URI> [オプション] [ターゲット]	−examine, −help, −output, −source, −version
reset	ターゲットをリセットします。 構文: reset [オプション] [ターゲット]	−examine, −help, −output, −version
set	ターゲットのプロパティをセットします。 構文: set [オプション] [ターゲット] <プロパティ名>=<値>	−examine, −help, −output, −version
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。 構文: show [オプション] [ターゲット] <プロパティ名>=<値>	-all, -default, −display, −examine, −help, −level, −output, −version
start	ターゲットを開始します。 構文: start [オプション] [ターゲット]	−examine, −force, −help, −output, −version
stop	ターゲットをシャットダウンします。 構文: stop [オプション] [ターゲット]	−examine, −force, −help, −output, −state, −version, −wait
version	ターゲットのバージョン属性を表示します。 構文: version [オプション]	−examine, −help, −output, −version

表 10-2 で、SM-CLP オプションについて説明します。一部のオプションは、表に示すように省略形です。

表 10-2. 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, −a	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。
-destination	dump コマンドのイメージを保存する場所を指定します。 構文: -destination <URI>
-display, -d	コマンド出力をフィルタします。 構文: -display <プロパティ | ターゲット | バーブ>[, <プロパティ | ターゲット | バーブ>]*

-examine, -x	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, –h	バーブのヘルプを表示します。
–level, -l	指定ターゲット下の追加レベルでターゲットで動作するようバーブに指示します。 構文: -level <*n* | すべて>
–output, –o	出力のフォーマットを指定します。 構文: -output <テキスト | clpcsv | clpxml>
-source	load コマンドのイメージ場所を指定します。 構文: -source <URI>
–version, –v	SMASH-CLP バージョン番号を表示します。

MAP アドレス領域のナビゲーション

メモ: SM-CLP アドレスパスにおいてスラッシュ(/)およびバックスラッシュ(\)は交換可能です。ただし、コマンドラインの最後のバックスラッシュは次の行のコマンドに続き、コマンドが解析されると無視されます。

SM-CLP で管理できるオブジェクトは Manageability Access Point(MAP)アドレス領域と呼ばれる階層スペースに整理されるターゲットによって代表されます。アドレスパスは、アドレス領域のルートからアドレス領域のオブジェクトへのパスを指定します。

ルートターゲットは、スラッシュ(/)またはバックスラッシュ(\)によって表されます。iDRAC にログインするときのデフォルトの開始ポイントです。cd バーブを使用してルートからナビゲートします。例えば、システムイベントログ(SEL)で 3 番目のレコードへナビゲートするには、次のコマンドを入力します。

```
->cd /system1/sp1/logs1/record3
```

ターゲットなしで cd バーブを入力し、アドレス領域の現在の場所を検索します。. . および . の省略形は Windows や Linux で機能するのと同様に機能します。. . は親レベル、. は現在のレベルを示します。

ターゲット

表 10-3 は、SM-CLP 経由で使用可能なターゲットのリストを示したものです。

表 10-3. 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/sp1	サービスのプロセッサ。
/system1/sol1	シリアルオーバー LAN のターゲット。
/system1/sp1/account1 through /system1/sp1/account16	16 のローカル iDRAC ユーザーアカウント。account1 はルートアカウントです。
/system1/sp1/enetport1	iDRAC NIC の MAC アドレス。
/system1/sp1/enetport1/lanendpt1/ipendpt1	iDRAC IP、ゲートウェイ、ネットマスクの設定。
/system1/sp1/enetport1/lanendpt1/ipendpt1/dnsendpt1	iDRAC DNS サーバーの設定。
/system1/sp1/group1 through /system1/sp1/group5	Active Directory 標準スキーマのグループ。
/system1/sp1/logs1	ログ収集ターゲット。
/system1/sp1/logs1/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/sp1/logs1/records	管理下システムの SEL ターゲット。
/system1/sp1/oemdell_racsecurity1	証明書署名要求の生成に使用するパラメータのストレージ。
/system1/sp1/oemdell_ssl1	SSL 証明書要求の状態。
/system1/sp1/oemdell_vmservice1	仮想メディアの設定および状態。

---

show バーブの使用

ターゲットについての詳細を把握するには、show バーブを使用します。このバーブは、その場所で許可されているターゲットのプロパティ、サブターゲット、SM-CLP バーブのリストを表示します。

-display オプションの使用

show –display オプションで、コマンドの出力を 1 つまたは複数のプロパティ、ターゲット、バーブに限定できます。例えば、現在の場所のプロパティとターゲットのみを表示する場合は、次のコマンドを使用します。

```
show -d properties,targets /system1/sp1/account1
```

特定のプロパティのみをリストし、認定する場合は、次のコマンドを使用します。

```
show -d properties=(userid,username) /system1/sp1/account1
```

1 つのプロパティのみを表示する場合、括弧は省略できます。

-level オプションの使用

show -level オプションは、指定ターゲット下の追加レベル上で **show** を実行します。例えば、**account1** の **username** および **userid** プロパティを、**/system1/sp1** 下の **account16** ターゲットから表示する場合、次のコマンドを入力できます。

```
show -l 1 -d properties=(userid,username) /system1/sp1/account*
```

アドレス領域のすべてのターゲットとプロパティを表示するには、次のコマンドのように **-l all** オプションを使用します。

```
show -l all -d properties /
```

-output オプションの使用

-output オプションは、SM-CLP バーブの出力の 4 つのフォーマット（**テキスト**、**clpcsv**、**キーワード**、**clpxml**）の 1 つを指定します。

デフォルトのフォーマットは **テキスト** で、最も読み取り可能な出力です。**clpcsv** フォーマットはカンマで区切られる値のフォーマットで、表計算プログラムへのロードに適切です。**キーワード** フォーマットは、行当たりの [キーワード=値] 組のリストとして情報を出力します。**clpxml** フォーマットは、**応答** XML 要素を含む XML ドキュメントです。DMTF は **clpcsbv** および **clpxml** フォーマットを指定しており、これらの仕様は DMTF ウェブサイト（**www.dmtf.org**）で参照できます。

次の例では、XML における SEL の内容の出力方法を説明しています。

```
show -l all -output format=clpxml /system1/sp1/logs1
```

---

iDRAC 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例を提供します。

- 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
- システムのプロパティの表示
- iDRAC IP アドレス、サブネットマスク、ゲートウェイアドレスの設定

サーバーの電源管理

表 10-4 に、SM-CLP を使用して管理下サーバーの電源管理操作を実行する例を示します。

表 10-4. サーバーの電源管理操作

操作	構文
SSH インタフェースを使用して iDRAC にログインする	>ssh 192.168.0.120 >login: root >password:
サーバーの電源を切る	->stop /system1 system1 has been stopped successfully
電源オフの状態からサーバーの電源を入れる	-->start /system1 system1 has been started successfully
サーバーを再起動する	->reset /system1 system1 has been reset successfully

SEL の管理

表 10-5 に、SM-CLP を使用して管理下システムに SEL 関連の操作を実行する例を示します。

表 10-5. SEL の管理操作

操作	構文
SEL を表示する	->show /system1/sp1/logs1 Targets: record1 record2 record3 record4 record5 Properties: Description=IPMI SEL MaxNumberOfRecords=512 CurrentNumberOfRecords=5 Verbs: cd delete exit help show version
SEL のレコードを表示する	->show /system1/sp1/logs1/record4 ufip=/system1/sp1/logs1/log1/record4 Properties: Caption=Not defined Description=Backplane Drive 0: drive slot sensor for Backplane, drive presence was asserted ElementName=Not Supported LogCreationClassName=CIM_RecordLog LogName=IPMI SEL CreationClassName=CIM_LogRecord RecordID=4 MessageTimeStamp=16:37:10,January 13,2007 Verbs: cd exit help show version
SEL をクリアする	->delete /system1/sp1/logs1 All records deleted successfully

MAP ターゲットのナビゲーション

表 10-6 に **cd** バーブを使用して MAP をナビゲートする例を示します。すべての例で、最初のデフォルトターゲットは / であると想定されます。

表 10-6. Map ターゲットのナビゲーション操作

操作	構文
システムターゲットまでナビゲートして再起動する	->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 sp1 ->cd logs1 ->show
	->cd system1/sp1/logs1 ->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

iDRAC IP アドレス、サブネットマスク、ゲートウェイアドレスの設定

SM-CLP を使用して iDRAC ネットワークプロパティをアップデートするには 2 段階のプロセスがあります。

1. **/system1/sp1/enetport1/lanendpt1/ipendpt1:** で NIC プロパティの新しい値を設定します。
   - **oemdell_nicenable** — iDRAC ネットワークを有効にするには 1 に、無効にするには 0 に設定します。
   - **ipaddress** — IP アドレス
   - **subnetmask** — サブネットマスク
   - **oemdell_usedhcp** — DHCP の使用を有効にして **ipaddress** および **subnetmask** プロパティを設定するには 1 に、静的な値を設定するには 0 に設定します。
2. **committed** プロパティを 1 に設定して新しい値を確認します。

commit プロパティの値が 1 の場合、プロパティの現在の設定はアクティブです。いずれかのプロパティの変更すると、**commit** プロパティが 0 にリセットされ、その値が確認されていないことを示します。

メモ: **commit** プロパティは、**/system1/sp1/enetport1/lanendpt1/ipendpt1** MAP 場所のプロパティのみに影響します。その他の SM-CLP コマンドはすべてすぐに有効になります。

メモ: ローカル RACADM を使用して iDRAC ネットワークプロパティを設定する場合、ローカル RACADM はネットワーク接続に依存しないため、変更事項は即時発効します。

変更事項を確認すると、新しいネットワーク設定が発効し、Telnet または SSH セッションが終了されます。この確認手順を導入すると、SM-CLP コマンドをすべて完了するまでセッションの終了を延長できます。

表 10-7 は、SM-CLP を使用した iDRAC プロパティの設定例を示したものです。

表 10-7. SM-CLP による iDRAC ネットワークプロパティの設定

操作	構文
iDRAC NIC プロパティ場所へナビゲートします。	->cd /system1/sp1/enetport1/lanendpt1/ipendpt1
新しい IP アドレスを設定します。	->set ipaddress=10.10.10.10
サブネットマスクを設定します。	->set subnetmask=255.255.255.255
DHCP フラグをオンにします。	->set oemdell_usedhcp=1
NIC を有効にします。	->set oemdell_nicenable=1
変更事項を確認します。	->set committed=1

SM-CLP を使用した iDRAC ファームウェアのアップデート

SM-CLP を使用して iDRAC をアップデートするには、Dell アップデートパッケージの TFTP URI を把握している必要があります。

SM-CLP を使用してファームウェアをアップデートするには、次の手順を実行してください。

1. Telnet または SSH を使用して iDRAC にログインします。
2. 次のコマンドを入力して、現在のファームウェアバージョンを確認します。

   ```
   version
   ```

3. 次のコマンドを入力します。

   ```
   load -source tftp://<TFTP サーバー>/<アップデートパス> /system1/sp1
   ```

   ここで、<TFTP サーバー> は、TFTP サーバーの DNS 名または IP アドレス、<アップデートパス> は TFTP サーバー上のアップデートパッケージまでのパスです。

   開いている Telnet または SSH セッションは終了されます。ファームウェアアップデートが完了するまでには数分かかることがあります。

4. 新しいファームウェアが書き込まれたことを検証するには、新しい Telnet または SSH セッションを起動し、version コマンドをもう一度入力します。

Telnet または SSH によるシリアルオーバー LAN（SOL）の使用

管理ステーションの Telnet または SSH コンソールを使用して iDRAC に接続詞、管理下サーバーのシリアルポートをコンソールにリダイレクトします。これは IPMI SOL の代替機能で、シリアルストリームをネットワークパケットへ / から翻訳する **solproxy** などのユーティリティが必要です。iDRAC SOL の実装によって、シリアルとネットワーク間の翻訳は iDRAC 内で行われるため、追加ユーティリティは不要になります。

使用する Telnet または SSH コンソールには、管理下サーバーのシリアルポートから到着するデータを解釈し、これに対応する能力が必要です。通常、シリアルポートは ANSI- または VT100- ターミナルにエミュレートするシェルに連結しています。

Telnet を使用すると、IPMI LAN SOL ポートーポート 2100 に接続します。シリアルコンソールは自動的に Telnet コンソールにリダイレクトされます。

SSH または Telnet を使用すると、SM-CLP に接続するのと同様に iDRAC に接続します。続いて、SOL リダイレクトは **/system1/sol1** ターゲットから起動できます。

iDRAC での Telnet および SSH クライアントの使用についての詳細に関しては、Telnet または SSH クライアントのインストール を参照してください。

Microsoft Windows のハイパーターミナルでの SOL オーバー Telnet の使用

1. **スタート**→ **すべてのプログラム**→ **アクセサリ**→ **通信**→ **ハイパーターミナル** を選択します。
2. 接続用の名前を入力し、アイコンを選択して **OK** をクリックします。
3. **接続方法** フィールドのリストから **TCP/IP（Winsock）** を選択します。
4. **ホストアドレス** フィールドに iDRAC の DNS 名または IP アドレスを入力します。
5. **ポート番号** フィールドに Telnet ポート番号を入力します。
6. **OK** をクリックします。

SOL セッションを終了するには、ハイパーターミナルの接続解除アイコンをクリックします。

Linux での SOL オーバー Telnet の使用

Linux 管理ステーションで Telnet から SOL を起動するには、次の手順を実行してください。

1. シェルを起動します。
2. 次のコマンドで iDRAC に接続します。

   ```
   telnet <iDRAC IP アドレス>
   ```

   メモ: Telnet サービスのポート番号をデフォルトのポート 23 から変更した場合は、**telnet** コマンドの末尾にポート番号を追加します。

3. 次のコマンドを入力して SOL を起動します。

   ```
   start /system1/sol1
   ```

   これで、管理下サーバーのシリアルポートに接続します。

SOL を終了する準備ができたら、<Ctrl>+] と入力します（[Ctrl] キーを押したまま「]」を入力し、放します）。Telnet のプロンプトが表示されます。quit と入力して Telnet を終了します。

SOL オーバー SSH の使用

/system1/sol1 ターゲットによって、管理下サーバーのシリアルポートを SSH コンソールにリダイレクトできます。

1. OpenSSH または PuTTY を使用して iDRAC に接続します。
2. 次のコマンドを入力して SOL を起動します。

   ```
   start /system1/sol1
   ```

これで、管理下サーバーのシリアルポートに接続します。SM-CLP コマンドは現在使用できなくなりました。

SOL リダイレクトを終了する準備ができたら、<Ctrl>+. と入力します（[Ctrl] キーを押したまま「.」を入力して放します）。SSH セッションが閉じます。

一度 SOL を起動すると、SM-CLP に戻ることはできません。SSH セッションを終了し、新しいセッションを起動して SM-CLP を使用する必要があります。

目次ページに戻る

目次ページに戻る

iVM-CLI を使用したオペレーティングシステムの導入

Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00
ユーザーズガイド

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

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

はじめに

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

リモートシステムの要件

- 各リモートシステムで iDRAC が設定されていること。

ネットワークの要件

ネットワーク共有に以下のコンポーネントが含まれている必要があります。

- 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ブートイメージファイル

  イメージファイルは、業界標準のブータブルフォーマットのオペレーティングシステム CD か CD/DVD ISO イメージであることが必要です。

ブータブルイメージファイルの作成

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

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

Linux システム用イメージファイルの作成

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

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

```
dd if=<入力-デバイス> of=<出力-ファイル>
```

例:

```
dd if=/dev/sdc0 of=mycd.img
```

Windows システム用イメージファイルの作成

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

導入の準備

リモートシステムの設定

1. 管理ステーションでアクセスできるネットワーク共有を作成します。
2. オペレーティングシステムファイルをネットワーク共有にコピーします。
3. リモートシステムにオペレーティングシステムを導入するために、事前に設定済みのブータブルな導入イメージファイルがある場合は、このステップをとばします。

   設定済みのブータブルな導入イメージファイルがない場合は、ファイルを作成します。オペレーティングシステムの導入手順に使用されるプログラムやスクリプトをすべて含めます。

   例えば、Microsoft® Windows® を導入するには、Microsoft Systems Management Server(SMS)が使用する導入方式に似たプログラムをイメージファイルに含めます。

   イメージファイルを作成するときは、以下の操作を行ってください。

   - ネットワークベースのインストール手順に従う
   - ターゲットシステムのそれぞれが同じ導入手順を起動して実行するように導入イメージを「読み取り専用」とマークする

4. 次のいずれかの処理を実行してください。

   - **ipmitool** と仮想メディアコマンドラインインタフェース(iVM-CLI)を既存のオペレーティングシステム導入アプリケーションに統合します。ユーティリティの使用におけるガイドとして **ivmdeploy** サンプルスクリプトを使用します。
   - オペレーティングシステムの導入には、既存の **ivmdeploy** スクリプトを使用します。

オペレーティングシステムの導入

リモートシステムにオペレーティングシステムを導入するには、iVM-CLI と **ivmdeploy** スクリプトを使用します。

始める前に、iVM-CLI ユーティリティに含まれている**vmdeploy** サンプルスクリプトを確認してください。このスクリプトは、ネットワーク内のリモートシステムにオペレーティングシステムを導入するために必要な詳しい手順を説明しています。

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

1. **ip.txt** テキストファイルに、導入するリモートシステムの iDRAC IP アドレスを、1 行に 1 つの IP アドレスを入力してリストします。
2. ブータブルオペレーティングシステム CD または DVD をクライアントメディアドライブに挿入します。
3. コマンドラインで **ivmdeploy** を実行します。

ivmdeploy スクリプトを実行するには、コマンドプロンプトで次のコマンドを入力します。

```
ivmdeploy -r ip.txt -u <iDRAC ユーザー> -p <iDRAC パスワード> -c {<iso9660-img> | <パス>}
```

ここで、

- <iDRAC ユーザー> は、iDRAC ユーザー名です(例、**root**)。
- <iDRAC パスワード> は、iDRAC ユーザーのパスワードです(例、**calvin**)。
- <iso9660-img> は、オペレーティングシステムインストール CD またはDVD の ISO9660 イメージまでのパスです。
- <パス> は、オペレーティングシステムインストール CD またはDVD に含まれるデバイスまでのパスです。

ivmdeploy スクリプトは、コマンドラインオプションを **ivmcli** ユーティリティに渡します。これらのオプションについての詳細に関しては、コマンドラインオプション を参照してください。スクリプトによる **-r** オプションのプロセスは **ivmcli -r** オプションのプロセスと若干異なります。**-r** オプションに対する引数が既存のファイル名である場合、スクリプトは指定されたファイルから iDRAC IP アドレスを読み取り、各行に対して **ivmcli** ユーティリティを一度実行します。**-r** オプションに対する引数が既存のファイル名でない場合は単独の iDRAC のアドレスです。この場合、**-r** は **ivmcli** ユーティリティの説明と同様に機能します。

ivmdeploy スクリプトは、CD/DVD または CD/DVD ISO9660 イメージからのみインストールをサポートします。フロッピーディスクまたはフロッピーディスクイメージからのインストールが必要な場合は、スクリプトを変更して **ivmcli -f** オプションを使用できます。

仮想メディアコマンドラインインタフェースユーティリティの使用

仮想メディアコマンドラインインタフェース(iVM-CLI)ユーティリティは、管理ステーションから iDRAC に仮想メディアの機能を提供するスクリプト可能なコマンドラインインタフェースです。

iVM-CLI ユーティリティは次の機能を提供します。

メモ: 読み取り専用のイメージファイルを仮想化する場合は、複数のセッションが同じイメージメディアを共有します。物理ドライブを仮想化する場合は、一度に 1 セッションだけが特定の物理ドライブにアクセスできます。

- リムーバブルメディアデバイスまたはイメージファイルは、仮想メディアプラグインと一貫性があります。

- iDRAC ファームウェアのブートワンス機能が有効の場合、自動終了オプションが有効になります。
- セキュアソケットレイヤ(SSL)を使用して iDRAC の通信をセキュリティ保護します。

ユーティリティを実行する前に、iDRAC に対し仮想メディアの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システム管理者特権、オペレーティングシステムに固有の特権またはグループメンバーシップをサポートしている場合は、iVM-CLI コマンドを実行するためにもシステム管理者特権が必要です。

クライアントシステムのシステム管理者はユーザーグループと特権を制御するので、ユーティリティを実行できるユーザーを制御します。

Windows システムの場合は、iVM-CLI ユーティリティのパワーユーザー特権が必要です。

Linux システムでは、システム管理者の特権がなくても、**sudo** コマンドを使って iVM-CLI ユーティリティにアクセスできます。このコマンドは、システム管理者以外のアクセスを集中管理する方法で、すべてのユーザーコマンドをログに記録します。iVM-CLI グループのユーザーを追加または編集するには、システム管理者が **visudo** コマンドを使用します。システム管理者特権のないユーザーは、**sudo** コマンドを iVM-CLI コマンドライン(または iVM-CLI スクリプト)の接頭辞として追加すると、リモートシステムの iDRAC にアクセスしてユーティリティを実行できます。

iVM-CLI ユーティリティのインストール

iVM-CLI ユーティリティは『Dell OpenManage™ Systems Management Consoles CD』にあります。この CD は Dell OpenManage System Management Software キットに含まれています。ユーティリティをインストールするには、『Systems Management Consoles CD』をシステムの CD ドライブに挿入し、画面上の手順に従ってください。

『Systems Management Consoles CD』には、診断、Storage Management、Remote Access Service、および RACADM ユーティリティをはじめとする最新の Systems Management Software 製品が含まれています。また、Systems Management Software 製品に関する最新情報を記載した readme ファイルも含まれています。

さらに、『Systems Management Consoles CD』には、**vmdeploy**(iVM-CLI および RACADM ユーティリティを使用して、複数のリモートシステムにソフトウェアを導入する方法を説明するサンプルスクリプト)が含まれます。

メモ: ivmdeploy スクリプトは、インストール時にそのディレクトリに存在する他のファイルに依存しています。他のディレクトリからスクリプトを使用する場合、一緒にすべてのファイルをコピーしなければなりません。

コマンドラインオプション

iVM-CLI インタフェースは、Windows と Linux システムで共通しています。このユーティリティは、RACADM ユーティリティオプションと同じオプションを使用しています。例えば、iDRAC IP アドレスを指定するオプションでは、RACADM でも iVM-CLI ユーティリティでも同じ構文が必要です。

iVM-CLI コマンドのフォーマットは以下の通りです。

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

コマンドライン構文には大文字と小文字の区別があります。詳細に関しては、iVM-CLI パラメータ を参照してください。

リモートシステムのコマンドが受け入れられ、iDRAC が接続を許可した場合は、次のどちらかが発生するまでコマンドの実行が続行します。

- 理由に関わらず iVM-CLI 接続は終了します。
- プロセスは、オペレーティングシステムのコントロールを使用して手動で終了します。たとえば、Windows ではタスクマネージャを使用してプロセスを終了します。

iVM-CLI パラメータ

iDRAC の IP アドレス

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

このパラメータは、iDRAC の IP アドレスと SSL ポートを提供します。これらは、ユーティリティによって、ターゲット iDRAC による仮想メディア接続の確立に必要となります。無効な IP アドレスまたは DDNS 名を入力した場合は、エラーメッセージが表示され、コマンドは終了します。

<iRAC IP アドレス> は有効な固有の IPアドレスまたは iDRAC ダイナミックドメインネームシステム(DDNS)名です(サポートしている場合)。<iDRAC SSL ポート> を省くと、ポート 443(デフォルトポート)が使用されます。iDRAC のデフォルト SSL ポートを変更していない限り、オプションの SSL ポートは不要です。

iDRAC ユーザー名

```
-u <iDRAC ユーザー名>
```

このパラメータは仮想メディアを実行する iDRAC ユーザー名を提供します。

<iDRAC ユーザー名> には次の属性が必要です。

- 有効なユーザー名
- iDRAC 仮想メディアユーザー権限

iDRAC の認証に失敗した場合は、エラーメッセージが表示され、コマンドが終了します。

iDRAC ユーザーパスワード

```
-p <iDRAC ユーザーパスワード>
```

このパラメータは、指定した iDRAC ユーザーのパスワードを提供します。

iDRAC の認証に失敗した場合は、エラーメッセージが表示され、コマンドが終了します。

フロッピー / ディスクデバイスまたはイメージファイル

```
-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)またはマウント可能なファイルシステムのパーティション数(Linux システム)を含む有効なデバイスファイル名です。<イメージファイル> は、有効なイメージファイルのファイル名とパスです。

このパラメータは、仮想フロッピー / ディスクメディアを供給するデバイスまたはファイルを指定します。

たとえば、以下のようにイメージファイルを指定します。

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

```
-f /tmp/myfloppy.img(Linux システム)
```

ファイルが書き込み禁止でない場合は、仮想メディアがイメージファイルに書き込む可能性があります。オペレーションシステムを設定して、上書きしてはいけないフロッピーイメージを書き込み禁止にしてください。

たとえば、次のようにデバイスを指定します。

```
-f a:\(Windows システム)
```

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

デバイスに書込み保護の機能がある場合は、その機能を使って、仮想メディアからそのメディアへの書き込みを禁止してください。

フロッピーメディアを仮想化しない場合は、コマンドラインからこのパラメータを省きます。無効な値が検出された場合は、エラーメッセージが表示され、コマンドが終了します。

CD / DVD デバイスまたはイメージファイル

```
-c {デバイス名 | イメージファイル>
```

ここで、<デバイス名> は、有効な CD/DVD(Windows システム)または CD/DVD デバイスファイル名(Linux システム)で、<イメージファイル> は、有効な ISO-9660 のファイル名とパスです。

このパラメータは、仮想 CD/DVD-ROM メディアを供給するデバイスまたはファイルを指定します。

たとえば、以下のようにイメージファイルを指定します。

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

```
-c /tmp/mydvd.img(Linux システム)
```

たとえば、次のようにデバイスを指定します。

```
-c d:\(Windows システム)
```

```
-c /dev/cdrom(Linux システム)
```

CD/DVD メディアを仮想化しない場合は、コマンドラインからこのパラメータを省きます。無効な値が検出された場合は、エラーメッセージが表示され、コマンドが終了します。

スイッチオプションだけが提供されている場合を除き、メディアの種類を少なくとも 1 つコマンドで指定します(フロッピーまたは CD/DVD ドライブ)。そうしないと、エラーメッセージが表示され、コマンドがエラーを生成して終了します。

バージョン表示

```
-v
```

このパラメータは iVM-CLI ユーティリティのバージョンを表示するために使用します。スイッチ以外の他のオプションが提供されていない場合は、エラーメッセージなしにコマンドが終了します。

ヘルプ表示

```
-h
```

このパラメータは iVM-CLI ユーティリティのパラメータの概要を表示します。スイッチ以外の他のオプションが提供されていない場合は、エラーなしにコマンドが終了します。

手動表示

```
-m
```

このパラメータは、可能なすべてのオプションに関する説明を含む iVKM ユーティリティの詳細ページを表示します。

暗号化されたデータ

```
-e
```

このパラメータがコマンドラインに含まれていると、iVM-CLI は SSL-暗号化チャネルを使用して、管理ステーションとリモートシステムの iDRAC の間でデータを転送します。このパラメータがコマンドラインにない場合、データ転送は暗号化されません。

iVM-CLI オペレーティングシステムのシェルオプション

iVM-CLI のコマンドラインでは次のオペレーティングシステムの機能を使用できます。

- stderr/stdout リダイレクト — ファイルへ印刷されたユーティリティの出力をリダイレクトします。

  例えば、大なり記号(>)の後にファイル名を入力すると、指定したファイルが iVM-CLI ユーティリティの印刷出力で上書きに使用されます。

  メモ: iVM-CLI ユーティリティは、スタンダード入力(**stdin**)から読み取りしません。この結果、**stdin** リダイレクトは不要です。

- バックグラウンド実行 — iVM-CLI ユーティリティはデフォルトではフォアグラウンドで実行します。ユーティリティ機能をバックグラウンドで実行させるには、オペレーティングシステムのコマンドシェルのバックグラウンド文字を使用します。 たとえば、Linux オペレーティングシステムでは、アンパサンド文字(&)の後にコマンドを入力すると、プログラムが新しいバックグラウンドプロセスとして始動します。

後者の方法はスクリプトプログラムの場合に便利です。iVM-CLI コマンドの新しいプロセスが開始した後、スクリプトが継続できます(そうでない場合は、iVM-CLI プログラムが終了するまでスクリプトがブロックされます)。iVM-CLI の複数のインスタンスがこの方法で開始し、コマンドインスタンスの 1 つまたは複数を手動で終了しなければならない場合は、オペレーティングシステムに固有の機能を使ってプロセスをリストにして終了します。

iVM-CLI の戻りコード

0 = エラーなし

1 = 接続不能

2 = iVM-CLI コマンドラインエラー

3 = RAC ファームウェア接続喪失

テキストメッセージ(英語のみ)も、エラーが発生するたびに標準的なエラー出力として発行されます。

目次ページに戻る

目次ページに戻る

iDRAC 設定ユーティリティの使用

Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00
ユーザーズガイド

概要

iDRAC 設定ユーティリティは、iDRAC および管理下サーバーのパラメータを表示および設定できる起動前の設定環境です。厳密には、以下のことが可能です。

- iDRAC および一次バックプレーンのファームウェアバージョン番号を表示する
- iDRAC ローカルエリアネットワーク設定、設定を有効 / 無効にする
- IPMI オーバー LAN を有効 / 無効にする
- LAN プラットフォームイベントトラップ(PET)送信先を有効にする
- 仮想メディアデバイスを連結 / 分離する
- システム管理者のユーザー名およびパスワードを変更する
- iDRAC 設定を出荷時のデフォルトにリセットする
- システムイベントログ(SEL)メッセージを表示する、またはログからのメッセージをクリアする

iDRAC 設定ユーティリティを使用して実行できるタスクは、iDRAC または OpenManage ソフトウェアが提供する他のユーティリティ(ウェブインタフェース、SM-CLP コマンドラインインタフェース、ローカル RACADM コマンドラインインタフェース)を使用しても実行できるほか、基本的なネットワーク設定は最初の CMC 設定時に CMC LCD でも実行できます。

---

iDRAC 設定ユーティリティの起動

最初、または iDRAC をデフォルト設定にリセット後は、iDRAC 設定ユーティリティにアクセスするのに iKVM に接続したコンソールを使用する必要があります。

1. iKVM コンソールに接続したキーボードで、<画面印刷> キーを押して iKVM の On Screen Configuration and Reporting(OSCAR)メニューを表示します。<上矢印> キーおよび <下矢印> キーを使用してサーバーが含まれるスロットをハイライトし、<Enter> キーを押します。
2. サーバーの前にある電源ボタンを押してサーバーの電源を入れるか、再起動します。
3. **リモートアクセス設定は 5 秒以内に <Ctrl-E> キーを押してください.....** メッセージが表示されたらすぐに <Ctrl><E> を押します。

メモ: <Ctrl><E> を押す前にオペレーティングシステムがロードを開始した場合は、起動が完了するのを待ってからシステムを再起動して、もう一度実行します。

iDRAC 設定ユーティリティが表示されます。最初の 2 行に、iDRAC ファームウェアと一次バックプレーンファームウェアのリビジョンに関する情報が表示されます。リビジョンレベルは、ファームウェアアップグレードが必要かどうかを決定するのに役立ちます。

iDRAC ファームウェアは、ウェブインタフェース、SM-CLP など、外部インタフェースに関連するファームウェアの一部です。一次バックプレーンファームのファームウェアは、サーバーのハードウェア環境とインタフェースし、それを監視するファームウェアの一部です。

---

iDRAC 設定ユーティリティの使用

ファームウェアのリビジョンメッセージの下の iDRAC 設定ユーティリティの残りの部分は、<上矢印> キーおよび <下矢印> キーを使用してアクセスできるメニューアイテムです。

- メニューアイテムによってサブメニューまたは編集可能なテキストフィールドが表示されたら、<Enter> キーを押してアイテムにアクセスし、設定が終了したら <Esc> キーで終了します。
- アイテムに [はい / いいえ]、[有効 / 無効] など選択可能な値がある場合は、<左矢印> キーまたは <右矢印> キー、<スペース> キーを押して値を選択します。
- 編集不可能なアイテムは青色で表示されます。アイテムによっては、他の選択事項によって編集可能になります。
- 画面下には現在のアイテムの手順が表示されます。<F1> キーを押すと現在のアイテムに対するヘルプを表示できます。
- iDRAC 設定ユーティリティの使用を終了したら、<Esc> キーを押して Exit(終了)メニューを表示します。ここから、変更事項を保存または無視できるほか、ユーティリティに戻ることもできます。

次項では、iDRAC 設定ユーティリティのメニューアイテムについて説明します。

LAN

<左矢印>、<右矢印>、スペースキーを使用し **有効** か **無効** を選択します。

iDRAC LAN は、デフォルト設定では無効になっています。LAN は、ウェブインタフェース、SM-CLP コマンドラインインタフェースへの Telnet/SSH アクセス、コンソールリダイレクト、仮想メディアなど iDRAC アイテムの使用を許可するのに有効でなくてはなりません。

LAN を無効にすると、次の警告が表示されます。

```
iDRAC Out-of-Band interface will be disabled if the LAN Channel is OFF.
（LAN チャネルがオフの場合、iDRAC 帯域外インタフェースは無効になります。）
```

いずれかのキーを押してメッセージをクリアし、続行します。

LAN が無効になっていると、iDRAC HTTP、HTTPS、Telnet または SSH ポートに直接接続してアクセスするアイテムに加え、管理ステーションから iDRAC に送信される IPMI メッセージなどの帯域外管理ネットワークトラフィックも受信できないことが通知されます。ただしローカル RACADM インタフェースは使用可能で、iDRAC LAN の再設定にも使用できます。

IPMI オーバー LAN（オン / オフ）

<左矢印>、<右矢印>、スペースキーを押して **オン** か **オフ** を選択します。**オフ** を選択すると、iDRAC は LAN インタフェース上に到着する IPMI メッセージを受け入れません。

オフ を選択すると、次の警告が表示されます。

```
iDRAC Out-of-Band interface will be disabled if the LAN Channel is OFF.
（LAN チャネルがオフの場合、iDRAC 帯域外インタフェースは無効になります。）
```

いずれかのキーを押してメッセージをクリアし、続行します。メッセージの説明に関しては、LAN を参照してください。

LAN パラメータ

LAN パラメータのサブメニューを表示するには、<Enter> キーを押します。LAN パラメータの設定が終了し、<Esc> キーを押すと前のメニューに戻ります。

表 12-1. LAN パラメータ

アイテム	説明
RMCP+ 暗号化キー	<Enter> キーを押して値を編集し、終了したら <Esc> キーを押します。RMCP+ 暗号化キーは、40 文字の 16 進法の文字列（文字 0 ～ 9、a ～ f、A ～ F）です。RMCP+ は認証および暗号化を IPMI に追加する IPMI エクステンションです。デフォルト値は、40 文字列です。
IP アドレスソース	**DHCP** か **静的** を選択します。DHCP を選択すると、DHCP サーバーから **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** フィールドが取得されます。ネットワーク上に DHCP が見つからない場合、フィールドはゼロに設定されます。 **静的** を選択すると、**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** アイテムは編集可能になります。
Ethernet IP アドレス	**IP アドレスソース** を **DHCP** に設定すると、このフィールドには DHCP から取得された IP アドレスが表示されます。 **IP アドレスソース** を **静的** に設定する場合、iDRAC に割り当てる IP アドレスを入力します。 デフォルトは、**192.168.0.120** に、サーバーに含まれるスロット番号を加えた値です。
MAC アドレス	これは、iDRAC ネットワークインタフェースの編集不可能な MAC アドレスです。
サブネットマスク	**IP アドレスソース** を **DHCP** に設定すると、このフィールドには DHCP から取得されたサブネットマスクアドレスが表示されます。 **IP アドレスソース** を **静的** に設定している場合は、iDRAC のサブネットマスクを入力します。 デフォルトは **255.255.255.0** です。
デフォルトゲートウェイ	**IP アドレスソース** を **DHCP** に設定すると、このフィールドには DHCP から取得された デフォルトゲートウェイのアドレスが表示されます。 **IP アドレスソース** を **静的** に設定する場合は、デフォルトゲートウェイの IP アドレスを入力します。 デフォルトは **192.168.0.1** です。
LAN 警告有効	**オン** を選択するとプラットフォームイベントトラップ（PET）LAN 警告が有効になります。
警告ポリシーエントリ 1	[有効] または [無効] を選択すると、1 番目の送信先がアクティブになります。
警告送信先 1	PET LAN 警告の送信先の IP アドレスを入力します。
ホスト名文字列	<Enter> キーを押して編集します。PET 警告のホスト名を入力します。
DHCP からの DNS サーバー	**オン** を選択するとネットワーク上の DHCP サービスから DNS サーバーアドレスが取得されます。**オフ** を選択すると以下の DNS サーバーアドレスを指定できます。
DNS サーバー 1	**DHCP からの DNS サーバー** が **オフ** の場合、1 番目の DNS サーバーの IP アドレスを入力します。
DNS サーバー 2	**DHCP からの DNS サーバー** が **オフ** の場合、2 番目の DNS サーバーの IP アドレスを入力します。
iDRAC 名の登録	**オン** を選択すると DNS サービスに iDRAC 名を登録できます。DNS でユーザーが iDRAC を見つけられないようにするには、**オフ** を選択します。
iDRAC 名	**iDRAC 名の登録** を **オン** に設定する場合、<Enter> キーを押すと **現在の DNS iDRAC 名** テキストフィールドを編集できます。iDRAC 名の編集が終了したら <Enter> キーを押します。前のメニューに戻るには <Esc> キーを押します。iDRAC 名は有効な DNS ホスト名でなければなりません。
DHCP からのドメイ	ネットワーク上の DHCP サービスからドメイン名を取得するには、**オン** を選択します。ドメイン名を指定するには、**オフ** を選択します。

ン名	
ドメイン名	**DHCP からのドメイン名** が **オフ** の場合、<Enter> キーを押すと **現在のドメイン名** テキストフィールドを編集できます。編集が終了したら <Enter> キーを押します。前のメニューに戻るには <Esc> キーを押します。ドメイン名は、有効な DNS ドメイン（例、mycompany.com）でなければなりません。

仮想メディア

<左矢印> と <右矢印> を使用して **連結** または **分離** を選択します。**連結** を選択すると、仮想メディアデバイスが USB バスに連結され、**コンソールリダイレクト** セッション中に使用可能になります。

分離 を選択すると、ユーザーは **コンソールリダイレクト** セッション中に仮想メディアデバイスにアクセスできません。

メモ: **仮想メディア** 機能で USB フラッシュドライブを使用するには、BIOS 設定ユーティリティで **USB フラッシュドライブのエミュレーションタイプ** を **ハードディスク** に設定してください。BIOS 設定ユーティリティへは、サーバー起動中に <F2> キーを押すとアクセスできます。**USB フラッシュドライブのエミュレーションタイプ** が **自動** に設定されていると、フラッシュドライブはシステムに対しフロッピードライブとして表示されます。

LAN ユーザー設定

LAN ユーザーは iDRAC のシステム管理者アカウント（デフォルトで **root**）です。LAN ユーザー設定のサブメニューを表示するには、<Enter> キーを押します。LAN ユーザーの設定が終了し、<Esc> キーを押すと前のメニューに戻ります。

表 12-2. LAN ユーザー設定ページ

アイテム	説明
アカウントアクセス	**有効** を選択するとシステム管理者アカウントが有効になります。**無効** を選択するとシステム管理者アカウントが無効になります。
アカウント特権	**システム管理者**、**ユーザー**、**オペレータ**、**アクセスなし** のいずれかを選択します。
アカウントユーザー名	<Enter> キーを押してユーザー名を編集し、終了したら <Esc> キーを押します。デフォルトのユーザー名は **root** です。
パスワードを入力する	システム管理者アカウントの新しいパスワードを入力します。入力時に、文字は表示されません。
パスワードを確認する	システム管理者アカウントの新しいパスワードを再入力します。入力した文字が **パスワードを入力する** フィールドに入力した文字と一致しない場合はメッセージが表示されますので、パスワードを再度入力する必要があります。

デフォルトにリセット

デフォルトにリセット メニューアイテムを使用すると、iDRAC 設定アイテムがすべて出荷時のデフォルトにリセットされます。これは、システム管理者のユーザーパスワードを忘れた場合や iDRAC をデフォルト設定から再設定する場合に必要になる可能性があります。

メモ: デフォルト設定で iDRAC ネットワークは無効になっています。iDRAC 設定ユーティリティで iDRAC ネットワークを有効にするまでネットワーク上で iDRAC を再設定することはできません。

<Enter> キーを押してアイテムを選択します。次の警告メッセージが表示されます。

```
Resetting to factory defaults will restore remote Non-Volatile user settings. Continue?

< NO (Cancel) >

< YES (Continue) >
```

（出荷時のデフォルト設定にリセットするとリモートの非揮発性ユーザー設定が復元されます。続行しますか ？

<いいえ（キャンセル）>

<はい（続行）> ）

はい を選択し、<Enter> キーを押すと iDRAC はデフォルト設定にリセットされます。

システムイベントログメニュー

システムイベントログ メニューでは、システムイベントログ（SEL）メッセージを表示したり、ログメッセージをクリアできます。<Enter> キーを押すと **システムイベントログメニュー** が表示されます。システムはログエントリをカウントし、レコード総数と最新のメッセージを表示します。SEL は、最大 512 のメッセージを保持します。

SEL メッセージを表示するには、**システムイベントログの表示** を選択して <Enter> キーを押します。<左矢印> キーを使用すると前の（古い）メッセージに移動し、<右矢印> を押すと次の（新しい）メッセージに移動します。レコード番号を入力すると当該のレコードに移動します。SEL メッセージの表示を終了する場合は <Esc> キーを押します。

メモ: iDRAC 設定ユーティリティまたは iDRAC ウェブインタフェース内の SEL のみクリアできます。

SEL メッセージをクリアするには、**システムイベントログのクリア** を選択して <Enter> キーを押します。

SEL メニューの使用を終了したら、<Esc> キーを押すと前のメニューに戻ります。

iDRAC 設定ユーティリティの終了

iDRAC 設定の変更が終了し、<Esc> キーを押すと Exit(終了)メニューが表示されます。

変更を保存して終了 を選択して <Enter> キーを押すと変更が保存されます。

変更を保存せずに終了 を選択して <Enter> キーを押すと変更は保存されません。

設定に戻る を選択して <Enter> キーを押すと iDRAC 設定ユーティリティに戻ります。

目次ページに戻る

目次ページに戻る

管理下サーバーの回復とトラブルシューティング

Integrated Dell™ Remote Access Controller ファームウェアバージョン 1.00
ユーザーズガイド

本項では、iDRAC アイテムを使用したリモート管理下サーバーの診断とトラブルシューティングに関連するタスクの実行方法について説明します。本項には以下のサブセクションが含まれます。

- トラブル指標 — 問題の診断に導くメッセージやその他のシステム指標を見つけるのに役立ちます。
- 不具合解決ツール — システムのトラブルシューティングに使用できる iDRAC ツールについて説明します。
- トラブルシューティングとよくあるお問い合わせ(FAQ)— 遭遇する可能性のある一般的な状況に対する回答を提供します。

安全第一 – ユーザーとシステム

本項の特定の手順を実行するには、シャーシ、PowerEdge サーバー、または他のハードウェアモジュールとの連動が必要です。本書およびシステムマニュアルで説明されている以外のシステムハードウェアの補修は行わないでください。

警告:修理の多くは、認定を受けたサービス技術者のみが行うことができます。製品マニュアルで認可されている、もしくはオンライン / 電話によるサービスおよびサポートチームによって指示されるトラブルシューティングと簡単な修理のみを実行してください。デルの認可していない補修作業によって生じた損傷は、保証対象外となります。製品に同梱されている安全にお使いいただくための注意を通読し、従ってください。

トラブルインジケータ

本項では、システムに不具合が生じている可能性がある兆候について説明します。

LED インジケータ

システムトラブルの最初の指標は、シャーシまたはシャーシにインストールされているコンポーネントの LED に示される可能性があります。次のコンポーネントおよびモジュールには状態 LED があります。

- シャーシ LCD モニター
- サーバー
- ファン
- CMC
- I/O モジュール
- 電源装置

シャーシ LCD の単独 LED は、システム内のコンポーネントすべての状態を要約します。LCD で青色の LED が点灯している場合、システム内で検知されているエラー状態がないことを示します。LCD で点滅中の黄色の LED は、1 つまたは複数のエラー状態が検知されたことを示します。

シャーシ LCD に点滅中の黄色の LED がある場合、LCD メニューを使用してエラーのあるコンポーネントを究明できます。LCD の使用についてのヘルプに関しては、『Dell CMC ファームウェアバージョン 1.0 ユーザーズガイド』を参照してください。

表 13-1 は、PowerEdge サーバー上の LED の意味を説明したものです。

表 13-1. サーバーの LED インジケータ

LED インジケータ	意味
緑色に点灯	サーバーの電源が入っている状態です。緑色の LED が不在の場合、サーバーの電源は入っていないことを示します。
青色に点灯	iDRAC は正常に動作しています。
黄色に点滅	iDRAC がエラー状態を検知したか、ファームウェアのアップデートを進行中である可能性があります。
青色に点滅	ユーザーがこのサーバーのロケータ ID をアクティブにした状態です。

ハードウェアのトラブルインジケータ

モジュールにハードウェアの不具合がある場合の兆候には、以下が含まれます。

- 電源投入エラー
- ファンのノイズ
- ネットワーク接続の喪失
- バッテリ、温度、電圧、電源モニタのセンサー警告
- ハードドライブエラー
- USB メディアエラー
- 落下、浸水、他の外部要因による物理的損傷

上記のような不具合が発生した場合、次の方法を使用して不具合を修正するよう試行できます。

- モジュールを抜き差し、再起動する
- モジュールをシャーシ内の別のベイに挿入する
- ハードドライブまたは USB キーを交換する
- 電源およびネットワークケーブルを再接続 / 交換する

これらの手順で不具合が修正されない場合、『ハードウェアオーナーズマニュアル』でハードウェアデバイス専用のトラブルシューティング情報を参照してください。

その他のトラブルインジケータ

表 13-2. トラブルインジケータ

注目すべき点:	処置:
Systems Management Software からの警告メッセージ	Systems Management Software のマニュアルを参照してください。
システムイベントログのメッセージ	システムイベントログ(SEL)の確認 を参照してください。
スタートアップ POST コードのメッセージ	POST コードの確認 を参照してください。
前回クラッシュ画面のメッセージ	システムの前回クラッシュ画面の表示 を参照してください。
iDRAC ログのメッセージ	iDRAC ログの表示 を参照してください。

不具合解決ツール

本項では、特にリモートで不具合の解決を試みる場合、システムの不具合を診断するのに使用できる iDRAC アイテムについて説明します。

- システム正常性の確認
- エラーメッセージに対するシステムイベントログの確認
- POST コードの確認
- 前回クラッシュ画面の表示
- iDRAC ログの表示
- システム情報へのアクセス
- シャーシ内の管理下サーバーの識別
- 診断コンソールの使用
- リモートシステムの電源管理

システム正常性の確認

iDRAC ウェブインタフェースにログインする際、最初に表示されるページにはシステムコンポーネントの正常性が説明されています。表 13-3 は、システム正常性インジケータの意味を説明したものです。

表 13-3. システム正常性インジケータ

インジケータ	説明

	緑のチェックマークは、正常な(平常)状態を示します。
	感嘆符の入った黄色の三角形は、警告(非重要)状態を示します。
	赤い X は、重大な(エラー)状態を示します。
	疑問符のアイコンは、不明な状態を示します。

正常性 ページのコンポーネントのいずれかをクリックすると、コンポーネントに関する情報が表示されます。バッテリ、温度、電圧、電源モニタに対してはセンサーの読み取り値が表示されますので、不具合の種類の診断に役立ちます。iDRAC および CMC 情報ページには、便利な現在の状態と設定情報が表示されます。

システムイベントログ(SEL)の確認

SEL ログ ページには、管理下サーバーで発生するイベントに対しメッセージが表示されます。

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** をクリックし、**ログ** タブをクリックします。
2. **システムイベントログ** をクリックして **システムイベントログ** ページを表示します。

   システムイベントログ ページには、システム正常性インジケータ(表 13-3 を参照)、タイムスタンプ、イベントの説明が表示されます。
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 13-4 を参照)。

表 13-4. SEL ページのボタン

ボタン	処置
印刷	**ウィンドウに表示されるソート順で SEL** を印刷します。
ログのクリア	**SEL** をクリアします。 **メモ:** **ログのクリア** ボタンは、**ログのクリア**権限がある場合にのみ表示されます。
名前を付けて保存	ポップアップウィンドウが開き、**SEL** を選択したディレクトリに保存できます。 **メモ:** Internet Explorer で保存中に不具合が発生した場合、Microsoft® Support ウェブサイト(support.microsoft.com)から Internet Explorer 用の Cumulative Security Update をダウンロードします。
更新	**SEL** ページを再ロードします。

POST コードの確認

POST コード ページには、オペレーティングシステムの起動前の最後のシステム POST コードが表示されます。POST コードはシステム BIOS からの進行状況インジケータで、電源オンリセットからの起動順序のさまざまな段階を示すので、システムの起動に関連する不具合を診断できます。

メモ: LCD モニターまたは『ハードウェアオーナーズマニュアル』の POST コードメッセージ番号のテキストを表示します。

POST コードを表示するには、次の手順を実行してください。

1. **システム**、**ログ** タブ、**POST コード** の順にクリックします。

   POST コード ページには、システム正常性インジケータ(表 13-3 を参照)、16 進コード、コードの説明が表示されます。
2. **POST コード** ページの適切なボタンをクリックして続行します(表 13-5 を参照)。

表 13-5. POST コードのボタン

ボタン	処置
印刷	**POST コード ページを** 印刷します。
更新	**POST コード** ページを再ロードします。

システムの前回クラッシュ画面の表示

注意: Server Administrator および iDRAC ウェブインタフェースで前回クラッシュ画面機能が設定されている必要があります。この機能の設定手順に関しては、管理下サーバーの前回クラッシュ画面キャプチャ設定 を参照してください。

前回クラッシュ画面 ページには、システムクラッシュ前に発生したイベントに関する情報を含む一番新しいクラッシュ画面が表示されます。最後にシステムがクラッシュしたときのイメージが、iDRAC の持続ストアに保存され、リモートでアクセスできます。

前回クラッシュ画面 ページを表示するには、次の手順を実行してください。

- **システム**、**ログ** タブ、**前回クラッシュ** の順にクリックします。

前回クラッシュ画面 ページには 表 13-6 に示すボタンが表示されます。

メモ: 保存されているクラッシュ画面が存在しない場合、**保存** および **削除** ボタンは表示されません。

表 13-6. 前回クラッシュ画面ページのボタン

ボタン	処置
印刷	**前回クラッシュ画面** ページを印刷します。
保存	ポップアップウィンドウが開き、選択したディレクトリに **前回クラッシュ画面** ページを保存できます。
削除	**前回クラッシュ画面** ページを削除します。
更新	**前回クラッシュ画面** ページを再ロードします。

メモ: 自動回復タイマーの変動により、システムリセットタイマーの値が高すぎる値で設定されている場合は、**前回クラッシュ画面** をキャプチャできない可能性があります。デフォルト設定は 480 秒です。Server Administrator と IT Assistant でシステムリセットタイマーを 60 秒に設定して、**前回クラッシュ画面** が正しく機能することを確認します。追加情報に関しては、管理下サーバーの前回クラッシュ画面キャプチャ設定 を参照してください。

iDRAC ログの表示

iDRAC ログ は持続的なログで、iDRAC ファームウェアに保管されています。ログにはユーザーの処置（ログイン、ログアウト、セキュリティポリシーの変更など）と iDRAC が発行する警告のリストが含まれています。ログが一杯になると、古いエントリから順に上書きされます。

システムイベントログ（SEL）は管理下サーバーで発生するイベントのレコードが含まれる一方、**iDRAC ログ** は iDRAC で発生するイベントのレコードが含まれます。

iDRAC ログにアクセスするには、次の手順を実行してください。

- **システム**→ **リモートアクセス**→ **iDRAC** をクリックし、**iDRAC ログ** をクリックします。

iDRAC ログ には、表 13-7 に示す情報が含まれています。

表 13-7. iDRAC ログページの情報

フィールド	説明
日付 / 時刻	日付と時刻（例：Dec 19 16:55:47）。 iDRAC のクロックは、管理下サーバーのクロックから設定されます。iDRAC を最初に起動する際に管理下サーバーと通信できない場合は、システムブートとして時刻が表示されます。
ソース	イベントを発生させたインタフェース。
説明	イベントの要約と iDRAC にログインしたユーザー名。

iDRAC ログページボタンの使用

iDRAC ログ ページには、次のボタンが含まれています（表 13-8 を参照）。

表 13-8. iDRAC ログのボタン

ボタン	処置
印刷	**iDRAC ログ** ページを印刷します。

ログのクリア	**iDRAC ログ** のエントリを表示します。 **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、**iDRAC ログ** を選択したディレクトリに保存できます。 **メモ:** Internet Explorer で保存中に問題が発生した場合、Microsoft Support ウェブサイト(**support.microsoft.com**)から Internet Explorer 用の Cumulative Security Update をダウンロードします。
更新	**iDRAC ログ** ページを再ロードします。

システム情報の表示

システム概要 ページに次のシステムコンポーネントが表示されます。

- メインシステムエンクロージャ
- iDRAC(Integrated Dell Remote Access Controller)

システム情報にアクセスするには、**システム→ プロパティ** をクリックします。

メインシステムエンクロージャ

表 13-9 と 表 13-10 で、メインシステムシャーシのプロパティについて説明します。

表 13-9. 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 説明を 表示します。
BIOS バージョン	システムの BIOS バージョンを表示します。
サービスタグ	システムのサービスタグ番号を表示します。
ホスト名	ホストシステムの名前を表示します。
OS 名	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表示します。

表 13-10. 自動回復のフィールド

フィールド	説明
回復処置	システムハング が検知されたときに、iDRAC が**処置の必要なし**、**ハードリセット**、**電源を切る**、**パワーサイクル** のいずれかの処置を実行するように設定できます。
初期カウントダウン	システムハング が検知されてから iDRACが回復処置を実行するまでの秒数。
現在のカウントダウン	カウントダウンタイマーの現在の値(秒)。

iDRAC(Integrated Dell Remote Access Controller)

表 13-11 は、iDRAC プロパティについて説明したものです。

表 13-11. iDRAC の情報フィールド

フィールド	説明
日付 / 時刻	iDRAC の現在の日時を GMT で表示します。
ファームウェアバージョン	iDRAC ファームウェアの バージョンを表示します。
ファームウェアアップデート	ファームウェアが 最後にアップデートされた日付 を表示します。日付は UTC フォーマットで表示されます(例:Tue, 8 May 2007, 22:18:21 UTC)。
IP アドレス	ネットワーク インタフェースを識別する 32 ビットのアドレス。値は、143.166.154.127 のようなドット区切りのフォーマットで表示されます。
ゲートウェイ	他のネットワークへのブリッジの役割を果たすゲートウェイの IP アドレス。値は、143.166.150.5 のようなドット区切りのフォーマットです。
サブネットマスク	サブネットマスクは、拡張ネットワークプレフィックスとホスト番号を構成する IP アドレスの一部を示します。値は、255.255.0.0 のようなドット区切りのフォーマットで表

	示されます。
MAC アドレス	ネットワークで各 NIC を固有に識別するメディアアクセスコントロール(MAC)アドレス(例、00-00-0c-ac-08)。これは、デルが割り当てる ID で、編集できません。
DHCP 有効	**有効** は、動的ホスト構成プロトコル(DHCP)が有効であることを示します。 **無効** は、DHCP が有効でないことを示します。

シャーシ内の管理下サーバーの識別

PowerEdge M1000-e シャーシは、最大 16 のサーバーを収容できます。シャーシ内の特定のサーバーを検索するには、iDRAC ウェブインタフェースを使用してサーバー上で青色の点滅 LED をオンにできます。LED をオンにする際、LED が点滅している間にシャーシに到達できるように LED を点滅させる秒数を指定できます。0 を入力すると、LED は無効にされるまで点滅し続けます。

サーバーを識別するには、次の手順を実行してください。

1. **システム**→ **リモートアクセス**→ **iDRAC**→ **トラブルシューティング** をクリックします。
2. **識別** ページで **サーバーの識別** の横の値ボックスを選択します。
3. **サーバータイムアウトの識別** フィールドに、LED を点滅させる秒数を入力します。無効にするまで点滅させる場合は 0 を入力します。
4. **適用** をクリックします。

サーバー上の青色の LED が指定した秒間点滅します。

0 を入力して LED を点滅させ続けている場合、次の手順を実行してこれを無効にします。

1. **システム**→ **リモートアクセス**→ **iDRAC**→ **トラブルシューティング** をクリックします。
2. **識別** ページで **サーバーの識別** の横の値ボックスを選択解除します。
3. **適用** をクリックします。

診断コンソールの使用

iDRAC は、Microsoft® Windows® システムや Linux システムのツールに似た標準的なネットワーク診断ツール(表 13-12 を参照)一式を提供します。iDRAC ウェブインタフェースを使用して、ネットワークのデバッグツールにアクセスできます。

診断コンソール ページにアクセスするには、次の手順を実行してください。

1. **システム**→ **iDRAC**→ **トラブルシューティング** をクリックします。
2. **診断** タブをクリックします。

表 13-12 は、**診断コンソール** ページに入力できるコマンドを説明したものです。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。

クリア ボタンをクリックして、前のコマンドで表示した結果をクリアします。

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。

表 13-12. 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表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。
Ping <u><IP アドレス></u>	送信先の IP アドレスが現在のルーティングテーブルの内容で iDRAC から到達可能かどうかを確認します。送信先の IP アドレスは、このオプションの右側のフィールドに入力する必要があります。現在のルーティングテーブルの内容に基づい、インターネットコントロールメッセージプロトコル(ICMP)のエコーパケットが送信先の IP アドレスに送信されます。
gettracelog	DRAC トレースログ を表示します。詳細に関しては、gettracelog を参照してください。

リモートシステムの電源管理

iDRAC では、管理下サーバーの電源管理操作をリモートで実行できます。再起動時と電源の投入および切断時に、オペレーティングシステムから通常のシャットダウンを実行するには、[電源管理] ページを使用します。

メモ: 電源管理処置を実行するには、**サーバー処置コマンドの実行** 権限が必要です。ユーザー権限の設定ヘルプに関しては、iDRAC ユーザーの追加と設定 を参照してください。

1. **システム** をクリックし、**電源管理** タブをクリックします。
2. **電源制御処置** を選択します(例、**システムをリセットする(ウォームブート)**)。
   表 13-13 は、電源制御処置についての情報を記載したものです。
3. 選択した処置を実行するには、**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。表 13-14 を参照してください。

表 13-13. 電源制御処置

システムの電源を入れる	システムの電源をオンにします(システムの電源がオフのときに電源ボタンを押すのと同じ)。
システムの電源を切る	システムの電源をオフにします(システムの電源がオンのときに電源ボタンを押すのと同じ)。
NMI(Non-Masking Interrupt)	オペレーティングシステムに高レベルの割り込みを送信し、重要な診断またはトラブルシューティング動作を可能にするためにシステム動作を一時停止させます。
正常なシャットダウン	オペレーティングシステムをクリーンにシャットダウンし、システムの電源を切ります。これには、システムの指示による電源管理が可能な詳細設定と、電源インタフェース(ACPI)対応のオペレーティングシステムが必要です。
システムをリセットする(ウォームブート)	電源を切らずに システムを 再起動します(ウォームリブート)。
システムの電源を入れなおす	電源を切って システムを再起動します(コールドリブート)。

表 13-14. 電源管理ページのボタン

ボタン	処置
印刷	画面に表示中の **電源管理** ページのデータを印刷します。
更新	**電源管理** ページを再ロードします。
適用	電源管理 ページで行った新しい設定を保存します。

トラブルシューティングとよくあるお問い合わせ(FAQ)

表 13-15 は、不具合のトラブルシューティングについてよくあるお問い合わせ(FAQ)について示したものです。

表 13-15. トラブルシューティングとよくあるお問い合わせ(FAQ)

質問	回答
サーバー上の LED が黄色で点滅中です。	SEL でメッセージを確認し、SEL をクリアして LED の点滅を停止します。 iDRAC ウェブインタフェースを使用する場合: • システムイベントログ(SEL)の確認 を参照してください。 SM-CLP を使用する場合: • SEL の管理 を参照してください。 iDRAC 設定ユーティリティを使用する場合: • システムイベントログメニュー を参照してください。
サーバー上で青色の LED が点滅しています。	ユーザーがサーバーのロケータ ID をアクティブにした状態です。シャーシ内のサーバーを識別するのに役立つ信号です。この機能についての情報に関しては、シャーシ内の管理下サーバーの識別 を参照してください。
iDRAC の IP アドレスの検索方法は ?	CMC ウェブインタフェースを使用する場合: 1. **シャーシ→ サーバー** をクリックし、**設定** タブをクリックします。 2. **導入** をクリックします。 3. 表示される表からサーバーの IP アドレスを読み取ります。 iKVM を使用する場合: • サーバーを再起動し、<Ctrl><E> キーを押して iDRAC 設定ユーティリティに入ります。 または

	• BIOS POST 中に表示される IP アドレスに注目します。 または • OSCAR の「Dell CMC」コンソールを選択してローカルシリアル接続経由で CMC にログインします。 CMC RACADM コマンドはこの接続から発行できます。CMC RACADM サブコマンドの完全リストについては、『CMC ファームウェアバージョン 1.0 ユーザーズガイド』を参照してください。
iDRAC の IP アドレスの検索方法は ?（続き）	例: $ racadm getniccfg -m server-1 DHCP Enabled = 1 IP Address = 192.168.0.1 Subnet Mask = 255.255.255.0 Gateway = 192.168.0.1 ローカル RACADM を使用する場合: 1. コマンドプロンプトで次のコマンドを入力します。 racadm getsysinfo LCD を使用する場合: 1. メインメニューで **サーバー** をハイライトし、チェックボタンを押します。 2. 検索する IP アドレスを選択し、チェックボタンを押します。
CMC の IP アドレスの検索方法は ?	iDRAC ウェブインタフェースを使用する場合: • **システム→リモートアクセス→ CMC** をクリックします。 **概要** ページに CMC の IP アドレスが表示されます。 または • OSCAR の「Dell CMC」コンソールを選択してローカルシリアル接続経由で CMC にログインします。CMC RACADM コマンドはこの接続から発行できます。CMC RACADM サブコマンドの完全リストについては、『CMC ファームウェアバージョン 1.0 ユーザーズガイド』を参照してください。 $ racadm getniccfg -m chassis NIC Enabled = 1 DHCP Elabled = 1 Static IP Address = 192.168.0.120 Static Subnet Mask = 255.255.255.0 Static Gateway = 192.168.0.1 Current IP Address = 10.35.155.151 Gurrent Subnet Mask = 255.255.255.0 Current Gateway = 10.35.155.1 Speed = Autonegotiate Duplex = Autonegotiate
iDRAC ネットワーク接続が機能しません。	• LAN ケーブルが CMC に接続されていることを確認してください。 • iDRAC の LAN が有効になっていることを確認してください。
サーバーをシャーシに挿入し、電源ボタンを押したのですが、何も起こりません。	• サーバーの電源が入るまでに、iDRAC は初期化に約 30 秒かかります。30 秒待ってから電源ボタンをもう一度押してください。 • CMC の電力バジェットを確認してください。シャーシの電力バジェットを超えている可能性があります。
iDRAC のシステム管理者ユーザー名とパスワードを忘れてしまいました。	iDRAC をデフォルト設定に復元する必要があります。 1. サーバーを再起動し、<Ctrl><E> キーを押して iDRAC 設定ユーティリティに切り替えます。 2. 設定ユーティリティメニューで、**デフォルトにリセットする** をハイライトして <Enter> キーを押します。 詳細に関しては、デフォルトにリセットする を参照してください。
サーバースロット名の変更方法は ?	1. CMC ウェブインタフェースにログインします。 2. **シャーシ** ツリーを開き、**サーバー** をクリックします。 3. **設定** タブをクリックします。 4. 当該サーバーの行に、新しいスロット名を入力します。 5. **適用** をクリックします。
iDRAC ウェブインタフェースからコンソールリダイレクトセッションを起動すると ActiveX セキュリティポップアップ画面が表示されます。	iDRAC がクライアントのブラウザで信頼済みサイトでない可能性があります。 コンソールリダイレクトセッションを開始するたびにセキュリティポップアップ画面が表示されるのを回避するには、iDRAC を信頼済みサイトリストに追加してください。 1. **ツール→ インターネットオプション...→ セキュリティ→ 信頼済みサイト** をクリックします。 2. **サイト** をクリックして iDRAC の IP アドレスまたは DNS 名を入力します。 3. **追加** をクリックします。
コンソールリダイレクトセッションを開始すると、ビューアの画面が空白です。	**仮想メディア** 特権があるが、**コンソールリダイレクト** 特権がない場合、仮想メディア機能にアクセスできるようビューアを起動できますが、管理下サーバーのコンソールは表示されません。
iDRAC が起動しません。	サーバーを取外し、挿入し直してください。

	iDRAC がアップグレード可能なコンポーネントとして表示されているかどうか CMC ウェブインタフェースを確認します。アップグレード可能なコンポーネントとして表示されている場合は、CMC を使用した iDRAC ファームウェアの回復 の手順に従ってください。 依然問題が修正されない場合は、テクニカルサポートにお問い合わせください。
管理下サーバーの起動を試行すると、電源インジケータは緑色ですが POST またはビデオが表示されません。	これは、次の状態である場合に発生します。 • メモリがインストールされていない、またはアクセス不可能である。 • CPU がインストールされていない、またはアクセス不可能である。 • ビデオライザーカードが不在、または接続が不適切である。 また、iDRAC ウェブインタフェースまたは LCD で iDRAC ログのエラーメッセージも確認してください。

目次ページに戻る

目次ページに戻る

用語集

Active Directory

Active Directory はユーザーデータ、セキュリティ、分散されたリソースのネットワーク管理を自動化し、他のディレクトリとの相互動作を可能にした一元管理型の標準化システムです。Active Directory は特に、分散ネットワーク環境用に設計されています。

AGP

Accelerated Graphics Port の略語。AGPは、グラフィックカードによるメインシステムメモリへの高速なインタフェースを提供するバス仕様です。

ARP

Address Resolution Protocol(アドレス解決プロトコル)の頭字語。インターネットアドレスからホストの Ethernet アドレスを求める手法。

ASCII

American Standard Code for Information Interchange(情報交換用アメリカ標準コード)の頭字語。文字、数字、その他の記号の表示と印刷に使用されるコード表現体系。

BIOS

Basic Input/Output System の頭字語。周辺デバイスに最も低位レベルのインタフェースを提供し、オペレーティングシステムのメモリへのロードなど、システム起動処理の第一段階を制御するシステムソフトウェアの一部。

CA

認証局は、高水準で信頼できる審査、身元確認、その他の重要なセキュリティ要件を満たすことで IT 業界で認められているビジネス組織です。CA には、Thawte や VeriSign があります。CA は CSR を受信すると、その情報の確認と検証を行います。申請者が CA のセキュリティ水準を満たしている場合は、申請者に証明書を発行します。この証明書によって、ネットワークまたはインターネット上で行ったトランザクションに対して、申請者を一意に識別できます。

CD

Compact Disc(コンパクトディスク)の略語。

CHAP

Challenge-Handshake Authentication Protocol の頭字語。接続の発信元 ID を確認するために PPP サーバが使用する認証方法。

CIM

Common Information Model の頭字語。ネットワーク上でシステムを管理するためのプロトコル。

CLI

Command Line Interface の略語。

CLP

Command Line Interface の略語。

CMC

Enclosure Management Controller(エンクロージャ管理コントローラ)の略語。iDRAC と管理下システムの CMC 間のコントローラインタフェースです。

CSR

Certificate Signing Request(証明書署名要求)の略語。

DDNS

Dynamic Domain Naming System(ダイナミックドメインネーミングシステム)の略語。

DHCP

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

DLL

Dynamic Link Library の略語。小さいプログラムで構成されたライブラリ。システムで実行中の大きいプログラムが必要時にメモリに呼び出すことができます。この小さいプログラムは、大きいプログラムがプリンタやスキャナなど特定のデバイスと通信できるように、一般に DLL プログラム(または、DLL ファイル)としてパッケージ化されています。

DMTF

Distributed Management Task Force(分散管理タスクフォース)の略語。

DNS

Domain Name System(ドメイン名システム)の略語。

DSU

Disk Storage Unit(ディスクストレージユニット)の略語。

FQDN

Fully Qualified Domain Names(完全修飾ドメイン名)の頭字語。Microsoft® Active Directory® は 64 バイト以下の FQDN のみをサポートしています。

FSMO

Flexible Single Master Operation の頭字語。Microsoft の拡張操作で単独性を保証する方法。

GMT

Greenwich Mean Time(グリニッジ標準時)の略語。世界各地に共通する標準時刻。GMT はイギリスのロンドン郊外にあるグリニッジ天文台跡を通過する本初子午線(経度 0°)に基づく平均太陽時を反映しています。

GPIO

General Purpose Input/Output(汎用入力/出力)の略語。

GRUB

GRand Unified Bootloader の略語。一般的に使用されている新しい Linux ローダー。

GUI

Graphical User Interface(グラフィカルユーザーインタフェース)の略語。ユーザーとの対話がすべてテキストによって表示または入力されるコマンド表示メッセージインタフェースとは対照的に、ウィンドウ、ダイアログボックス、ボタンなどの要素を使用するコンピュータ表示インタフェースを指します。

iAMT

Intel® Active Management Technology(アクティブマネジメントテクノロジ)— コンピュータの電源が入っている / いない、またオペレーティングシステムの応答不在に関わらず、よりセキュアなシステム管理機能を実現します。

ICMB

Intelligent Enclosure Management Bus(インテリジェントエンクロージャ管理バス)の略語。

ICMP

Internet Control Message Protocol(インターネットコントロールメッセージプロトコル)の略語。

ID

identifier(識別子)の略語。一般に、ユーザー識別子(ユーザー ID)またはオブジェクト識別子(オブジェクト ID)を参照するときに使用されます。

iDRAC

Dell Remote Access Controller 5 の略語。

iDRAC

integrated Dell Remote Access Controller の略語。Dell 10G PowerEdge サーバー用の内蔵システムオンチップ監視 / 制御システム。

IP

Internet Protocol(インターネットプロトコル)の略語。TCP/IP のネットワーク層。IP はパケットの経路指定、断片化、再構成などを提供します。

IPMB

Intelligent Platform Management Bus(インテリジェントプラットフォーム管理バス)の略語。システム管理テクノロジで使用されるバス。

IPMI

Intelligent Platform Management Interface(インテリジェントプラットフォーム管理インタフェース)の略語。システム管理テクノロジの一部。

Kbps

kilobits per second(キロビット/秒)の略語で、データ転送速度を表す単位。

LAN

Local Area Network(ローカルエリアネットワーク)の略語。

LDAP

Lightweight Directory Access Protocol の略語。

LED

Light-Emitting Diode(発光ダイオード)の略語。

LOM

Local area network On Motherboard の略語。

MAC

Media Access Control（メディアアクセスコントロール）の頭字語。ネットワークノードとネットワーク物理層の間のネットワークサブレイヤ。

MAC アドレス

Media Access Control アドレス。NIC の物理コンポーネントに組み込まれる固有アドレス。

MAP

Manageability Access Point の略語。

Mbps

megabits per second（メガビット/秒）の略語で、データ転送速度の単位。

MIB

Management Information Base（管理情報ベース）の略語。

MII

Media Independent Interface の略語。

NAS

Network Attached Storage の略語。

NIC

Network Interface Card（ネットワークインタフェースカード）の略語。アダプタ回路基板。コンピュータに搭載されて、ネットワークへの物理的な接続を提供します。

OID

Object Identifiers（オブジェクト識別子）の略語。

OSCAR

On Screen Configuration and Reporting の略語。<画面印刷> キーを押すと Avocent iKVM が表示するメニュー。CMC にインストールされるサーバーの CMC コンソールまたは iDRAC コンソールを選択できます。

PCI

Peripheral Component Interconnect（周辺機器コンポーネント相互接続）の略語。周辺機器をシステムに接続し、それらの周辺機器と通信するための標準インタフェースおよびバス技術。

POST

Power-On Self-Test（電源投入セルフテスト）の頭字語。コンピュータの電源を入れると、システムで自動的に診断テストが実行されます。

PPP

Point-to-Point Protocol の略語。シリアルポイントツーポイントリンクを介してネットワークレイヤデータグラム（IP パケットなど）を転送するためのインターネット標準プロトコル。

RAC

Remote Access Controller の略語。

RAM

Random-Access Memory（ランダムアクセスメモリ）の頭字語。システムおよび iDRAC の読み書き可能な汎用メモリ。

RAM ディスク

ハードディスクをエミュレートするメモリ常駐プログラム。iDRAC はメモリに RAM ディスクを保持しています。

ROM

Read-Only Memory（読み取り専用メモリ）の頭字語。データの読み取りはできますが、書き込みはできません。

RPM

Red Hat® Package Manager の略語。Red Hat Enterprise Linux® オペレーティングシステム用のパッケージ管理システムで、ソフトウェアパッケージのインストールに使用します。インストールプログラムに似ています。

SAC

Microsoft の Special Administration Console の頭字語。

SAP

Manageability Access Point の略語。

SEL

System Event Log の頭字語。

SMI

Systems Management Interrupt（システム管理割り込み）の略語。

SMTP

Simple Mail Transfer Protocol の略語。システム間の電子メール転送に使用されるプロトコルで、通常はイーサネットで使用されます。

SMWG

Systems Management Working Group の略語。

SNMP トラップ

iDRAC または CMC によって生成される通知（イベント）。管理下サーバーの状況変化やハードウェアの問題の可能性に関する情報が含まれています。

SSH

セキュア SHell（Secure Shell）の略語。

SSL

Secure Sockets Layer（セキュアソケットレイヤ）の略語。

TAP

Telelocator Alphanumeric Protocol の略語。ポケベルサービスに要求を送信するときに使用されるプロトコル。

TCP/IP

Transmission Control Protocol/Internet Protocol の略語。ネットワーク層とトランスポート層を含む標準イーサネットプロトコルのセットを表します。

TFTP

Trivial File Transfer Protocol の略語。ディスケットデバイスやシステムに起動コードをダウンロードするために使用されるシンプルファイル転送プロトコルの一種。

UPS

無停電電源装置(Uninterruptible power supply)の略語。

USB

ユニバーサルシリアルバス(Universal Serial Bus)の略語。

UTC

Universal Coordinated Time(協定世界時)の略語。「GMT」を参照してください。

VLAN

Virtual Local Area Network(仮想ローカルエリアネットワーク)の略語。

VNC

Virtual Network Computing(仮想ネットワークコンピューティング)の略語。

VT-100

Video Terminal 100 の略語。多くの共通端末エミュレーションプログラムで使用されています。

WAN

Wide Area Network(広域ネットワーク)の略語。

拡張スキーマ

Active Directory と併用されるソリューションで iDRAC へのユーザーアクセスを特定します。デル定義の Active Directory オブジェクトを使用します。

管理下サーバー

iDRAC が組み込まれているシステム。

管理ステーション

リモートで iDRAC にアクセスするシステム。

コンソールリダイレクト

コンソール転送とは、管理サーバーのディスプレイ画面、マウス機能、およびキーボード機能の宛先を管理ステーションの対応デバイスへ指示する機能のこと。これを利用して管理ステーションのシステムコンソールから管理下サーバーを制御することができます。

ハードウェアログ

iDRAC と CMC が生成するレコートイベント。

バス

コンピュータ内の各種の機能単位を接続する伝導体のセット。バスは、それが運ぶデータの種別ごとに、データバス、アドレスバス、または PCI バス、などと命名されます。

標準スキーマ

Active Directory と併用されるソリューションで iDRAC へのユーザーアクセスを特定します。Active Directory グループオブジェクトのみを使用します。

目次ページに戻る