Integrated Dell™ Remote Access Controller ファームウェア バージョン 1.11 ユーザー ガイド

メモおよび注意

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

注意: 注意は、ハードウェアの損傷やデータの損失の可能性があることを示し、その危険を回避する方法を説明しています。

2008 年 6 月Rev.A02

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 1.11 ユーザー ガイド

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

---

help

表 A-1 に、**help** コマンドについて説明します。

表 A-1 Help コマンド

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

概要

```
racadm help

racadm help <サブコマンド>
```

説明

help サブコマンドは **racadm** コマンドで使用できるサブコマンドすべてをリストにし、各サブコマンドにつき一行ずつの説明を表示します。**help** の後にサブコマンドを入力して、そのサブコマンドの構文を表示することもできます。

出力

racadm help コマンドはすべてのサブコマンドのリストを表示します。

racadm help <サブコマンド> コマンドは、指定したコマンドだけの情報を表示します。

対応インタフェース

- ローカル RACADM

---

config

表 A-2 に、**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、または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 に、**config** サブコマンド 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。ファイルの内容は「設定ファイルの構文」で指定した形式のデータでなければなりません。
-p	パスワードオプションである **-p**は、設定が完了した後、**config** に config ファイル **-f** <ファイル名> に含まれているパスワードエントリを削除させます。
-g	**-g** <グループ名>(グループオプション)は、**-o** オプションと一緒に使用する必要があります。<グループ名> は、設定するオブジェクトを含むグループを指定します。
-o	**-o** <オブジェクト名> <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> で書き込まれるオブジェクト名を指定します。
-i	**-i** <インデックス>(インデックス)オプションは、インデックス付きのグループのみに有効で、一意のグループを指定できます。この場合、インデックスは「名前付き」の値ではなく、インデックス値で指定されます。
-c	**-c**(チェック)オプションは、**config** サブコマンドと一緒に使用し、**.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。エラーが検出されたら、その行番号とエラーの短い説明が表示されます。iDRAC には書き込まれません。このオプションはチェックのみです。

出力

このサブコマンドは、次の場合にエラー出力を生成します。

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

このサブコマンドは、**.cfg** ファイル内にあるオブジェクトの総数のうちいくつの設定オブジェクトが書き込まれたかを示す数値を返します。

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)の値を 10.35.10.110 に設定します。この IP アドレスオブジェクトは **cfgLanNetworking** グループにあります。

- `racadm config -f myrac.cfg`

  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。**myrac.cfg** ファイルは、構文解析ルールに従って手動で編集することもできます。

  メモ: **myrac.cfg** ファイルにはパスワード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、またはすべての iDRAC 設定グループを取得して 1 つのファイルに保存できます。

入力

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

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

表 A-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** オプションでは **cfgIpmiPet** と **cfgIpmiPef** グループ用のエントリは作成されません。 **cfgIpmiPet** グループをファイルに取り込むためのトラップ先を少なくとも 1 つ設定する必要があります。
-g	**-g** <グループ名>(グループ) オプションを使用すると、単一グループの設定を表示できます。グループ名 は、**racadm.cfg** ファイルで使用されているグループの名前です。グループがインデックスグループの場合は、**-i** オプションを使用してください。
-h	**-h**(ヘルプ)オプションは、使用可能な設定グループすべてを表示します。このオプションは、正確なグループ名を覚えていない場合に便利です。
-i	**-i** <インデックス>(インデックス) オプションは、インデックス付きのグループのみに有効で、固有のグループを指定できます。**-i** <インデックス>を指定しなければ、グループに 1 の値が想定されます。これは複数のエントリを含んだテーブルです。インデックスは、「名前付き」の値ではなく、インデックス値で指定されます。
-o	-o <オブジェクト名> (オブジェクト)オプションは、クエリで使用す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)オプションを使うと、指定したユーザーの設定を表示できます。<**ユーザー名** > オプションはユーザーのログインユーザー名です。
-v	**-v**(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
- RACADM CLI 転送エラー

エラーが発生しなければ、指定した設定の内容が表示されます。

例

- `racadm getconfig -g cfgLanNetworking`

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

- `racadm getconfig -f 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 という名前のユーザーの設定プロパティを表示します。

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

  インデックス 2 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 に、**getssninfo** サブコマンドについて説明します。

表 A-5 getssninfo サブコマンド

サブコマンド	定義
getssninfo	Session Manager のセッションテーブルから、1 つまたは複数の現在アクティブまたは保留中のセッションの情報を取得します。

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。概要情報では次の情報が表示されます。

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

対応インタフェース

- ローカル RACADM

入力

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

表 A-6 getssninfo サブコマンドオプション

オプション	説明
-A	**-A** オプションを指定するとデータヘッダは印刷されません。
-u	**-u** <ユーザー名> ユーザー名オプションは、そのユーザー名の詳細セッション記録のみを印刷出力します。ユーザー名としてアスタリスク(*)を入力すると、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、概要情報は印刷されません。

例

- `racadm getssninfo`

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

表 A-7 getssninfo サブコマンド出力例

User	IP Address	Type	Consoles
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 に、**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、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 に、**getsysinfo** サブコマンド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 / ラベルを印刷しません。

出力

getsysinfo サブコマンドは、iDRAC、管理下サーバー、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
Register 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" "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 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には空白または不正確な情報が表示されます。

---

getractime

表 A-10 に、**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	リモートアクセスコントローラから現在の時刻を表示します。

概要

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

説明

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

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

出力

getractime サブコマンドは出力を 1 行で表示します。

出力例

```
racadm getractime

Thu Dec 8 20:15:26 2005

racadm getractime -d

20071208201542.000000
```

対応インタフェース

- ローカル RACADM

---

setniccfg

表 A-11 に、**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 設定を指定します。

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

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

- **-o** オプションは、NIC を完全に無効にします。<IPアドレス>、<ネットマスク>、<ゲートウェイ> は文字列をドットで区切って入力する必要があります。

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

出力

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

対応インタフェース

- ローカル RACADM

---

getniccfg

表 A-12 に**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 サブコマンドは操作に失敗した場合にエラーメッセージを表示します。成功した場合は、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 に**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` と入力します。出力は次のように表示されます。

```
Y76TP0G
```

成功すると 0、エラーの場合はゼロ以外の値を返します。

対応インタフェース

- ローカル RACADM

---

racreset

表 A-14 **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き、iDRAC が使用可能な状態に戻るまでに最大 1 分間かかることがあります。

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 に、**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 設定全体を工場出荷時のデフォルト値に戻します。

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、データベースプロパティのすべてのユーザー設定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、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** にシャーシ内の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 に、**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電源の投入 / 切断 / 入れ直しを実行します。

概要

```
racadm serveraction <動作>
```

説明

serveraction サブコマンドを使うと、ホストシステムの電源管理を行うことができます。表 A-17 に、**serveraction** 電源管理オプションについて説明します。

表 A-17 serveraction サブコマンドオプション

文字列	定義
<動作**>**	動作を指定します。<動作> 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** - 管理下サーバーの電源の入れ直しを行います。この動作は、システムのフロントパネルの電源ボタンを押すことでシステムの電源を切ってから入れ直すのと同様です。 • **powerstatus** - サーバーの現在の電源状態（**オン** または **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、要求された動作が実行できなかった場合はエラーメッセージを表示し、要求された動作が正常に完了した場合は成功したことを知らせる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 count] [-s start-record] [-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: オプションを何も指定しないと、ログ全体が表示されます。

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

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	返されるエントリの最大数を表示します。
-m	一度に 1 画面ずつの情報を表示して、ユーザーに続行するように指示します(UNIX の **more** コマンドに類似)。
-o	出力を 1 行で表示します。
-s	表示を開始するレコードを指定します。

出力

デフォルトの出力には、レコード番号、タイムスタンプ、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分されます。管理下サーバーの起動後、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

- ローカル RACADM

---

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 に、**getsel** 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 サブコマンドは SEL 内のエントリ数を表示します。

以下の **getsel** オプション(**-i** オプションなし)はエントリの読み込みに使います。

メモ: 引数を何も指定しないと、ログ全体が表示されます。

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	返されるエントリの最大数を表示します。
-o	出力を 1 行で表示します。
-s	表示を開始する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 画面ずつの情報を表示して、ユーザーに続行するように指示します(UNIX の **more** コマンドに類似)。

出力

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

出力例:

```
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 に、**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）コマンドはエントリを読み込みます。以下の **gettracelog** エントリを使ってエントリを読み込みます。

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 画面ずつの情報を表示して、ユーザーに続行するように指示します（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	表示を開始する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

デフォルトの出力には、レコード番号、タイムスタンプ、重要度、説明が表示されます。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。管理下サーバーの起動後、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 08:21:30

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 に、**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	RAC から SSL 証明書署名要求 (CSR) を生成して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 サブコマンドを使って、CSR を生成し、クライアントのローカルファイルシステムにダウンロードできます。CSR は、RAC 上での SSL トランザクションに使用できるカスタム SSL 証明書の作成に使用できます。

オプション

表 A-25 に、**sslcsrgen** サブコマンド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 生成プロセスの状態を返します（生成進行中、アクティブ、なし）。
-f	CSR をダウンロードする先の場所の <ファイル名> を指定します。

メモ: **-f** オプションを指定しないと、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。

オプションを何も指定しないと、生成された CSR はデフォルトでローカルファイルシステムに **sslcsr** としてダウンロードされます。 **-g** オプション は **-s** オプションと一緒には使用できず、**-f** オプションは **-g** オプションと一緒にしか使用できません。

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

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

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

例

```
racadm sslcsrgen -s
```

または

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

対応インタフェース

- ローカル RACADM

---

sslcertupload

表 A-26 に、**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 <type> [-f <ファイル名>]
```

オプション

表 A-27 に、**sslccertupload** サブコマンド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	アップロードする証明書の種類が CA 証明書かサーバー証明書かを指定します。 1 = サーバー証明書 2 = CA 証明書
-f	アップロードする証明書のファイル名を指定します。ファイルを指定しないと、現在のディレクトリ内の **sslcert** ファイルが選択されます。

sslcertupload コマンドはアップロードに成功すると 0 を返し、成功しないと非ゼロ値を返します。

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 に、**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 <種類> [-f <ファイル名>]
```

オプション

表 A-29 に、**sslccertdownload** サブコマンド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	ダウンロードする証明書の種類が Microsoft® Active Directory® 証明書かサーバー証明書かを指定します。 1 = サーバー証明書 2 = Microsoft Active Directory 証明書
-f	ダウンロードする証明書のファイル名を指定します。**-f** オプションまたはファイル名が指定されていないと、現在のディレクトリ内の **sslcert** ファイルが選択されます。

sslcertdownload コマンドはダウンロードに成功すると 0 を返し、成功しないと非ゼロ値を返します。

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 に、**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 <種類> [-A]
```

オプション

表 A-31 に、**sslccertview** サブコマンド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	表示する証明書の種類が Microsoft Active Directory 証明書かサーバ証明書かを指定します。 1 = サーバー証明書 2 = Microsoft Active Directory 証明書
-A	ヘッダー / ラベルを印刷しません。

出力例

```
racadm sslcertview -t 1

Serial Number             : 00

Subject Information:
Country Code (CC)         : US
State (S)                 : Texas
Locality (L)              : Round Rock
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 に、**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。

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 **cfgEmailAlert** グループのコマンド例を示します。

表 A-33 testemail の設定

動作	コマンド
警告を有効にします。	racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
宛先の電子メールアドレスを設定します。	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します。	racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "This is a test!"
SNMP の IP アドレスが正しく設定されていることを確認します。	racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr -i 192.168.0.152
現在の電子メール警告設定を表示します。	racadm getconfig -g cfgEmailAlert -i <インデックス> ここで、<インデックス> は 1～4 の数値です。

オプション

表 A-34 に、**testemail** サブコマンド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 に、**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**グループに関するコマンドを示します。

表 A-36 cfg 電子メール警告コマンド

動作	コマンド
警告を有効にします。	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
宛先の電子メールの IP アドレスを設定します。	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します。	racadm getconfig -g cfgIpmiPet -i <インデックス> ここで、<インデックス> は 1～4 の数値です。

入力

表 A-37 に、**testtrapI** サブコマンド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	テストに使う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 に、**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 サブコマンドを使うと、他のユーザーの仮想メディアセッションを切断できます。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のグループと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 1.11 ユーザー ガイド

iDRAC プロパティデータベースには iDRAC の設定情報が格納されています。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ています。ここには、プロパティデータベースでサポートされているグループとオブジェクトの ID のリストが掲載されています。

RACADM ユーティリティでこれらのグループとオブジェクト ID を使って iDRAC を設定します。以下の各項で、それぞれのオブジェクトについて説明し、オブジェクトが読み取り可能か、書き込み可能か、またはその両方が可能であるかを示します。

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

表示可能文字

表示可能文字には以下の文字セットが含まれます。

```
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格納されています。

このグループでは 1 つのインスタンスが使用できます。以下の各項で、このグループの各オブジェクトについて説明します。

idRacProductInfo（読み取り専用）

有効値

最大 63 文字の ASCII 文字列。

デフォルト

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）

有効値

最大 255 文字の ASCII 文字列。

デフォルト

このシステムコンポーネントは Dell PowerEdge サーバー用のリモート管理機能一式をすべて提供します。

説明

RAC の種類を説明するテキスト。

idRacVersionInfo（読み取り専用）

有効値

最大 63 文字の ASCII 文字列。

デフォルト

1.0

説明

現在の製品ファームウェアバージョンを示す文字列。

idRacBuildInfo（読み取り専用）

有効値

最大 16 文字の ASCII 文字列。

デフォルト

現在の RAC ファームウェアビルドバージョン。例：05.12.06

説明

現在の製品ビルドバージョンを示す文字列。

idRacName（読み取り専用）

有効値

最大 15 文字の ASCII 文字列。

デフォルト

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 として識別します。

---

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格納されています。

このグループでは 1 つのインスタンスが使用できます。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)

有効値

1 (TRUE = 真)

0 (FALSE = 偽)

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)

有効値

最大 254 文字の 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、「-」 および 「.」に制限されています。

メモ: Microsoft™ Active Directory™ は、64 バイト以下の完全修飾ドメイン名 (FQDN) しかサポートしていません。

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 = 偽) に設定されているときにのみ有効です。

cfgDNSRacName (読み取り / 書き込み)

有効値

最大 63 文字の 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。

メモ: 一部の DNS サーバーは 31 文字以内の名前しか登録しません。

デフォルト

rac-サービスタグ

説明

デフォルトの RAC 名 rac-サービスタグ が表示されます。このパラメータは、**cfgDNSRegisterRac** が 1 (TRUE = 真) に設定されているときにのみ有効です。

cfgDNSRegisterRac (読み取り / 書き込み)

有効値

1 (TRUE = 真)

0 (FALSE = 偽)

デフォルト

0

説明

DNS サーバーに iDRAC 名を登録します。

cfgTrapsSnmpFromDHCP（読み取り / 書き込み）

有効値

1 (TRUE = 真)

0 (FALSE = 偽)

デフォルト

0

説明

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

cfgDNSServer1（読み取り / 書き込み）

有効値

有効な IP アドレスを表す文字列。例：192.168.0.20

説明

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

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

cfgDNSServer2（読み取り / 書き込み）

有効値

有効な IP アドレスを表す文字列。例：192.168.0.20

デフォルト

0.0.0.0

説明

DNS サーバー 2 の IP アドレスを取得します。このパラメータは、**cfgDNSServersFromDHCP** が 0 (FALSE = 偽) に設定されているときにのみ有効です。

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

cfgNicEnable（読み取り / 書き込み）

有効値

1 (TRUE = 真)

0 (FALSE = 偽)

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 = 偽) に設定されているときにのみ設定できます。

有効値

有効な IP アドレスを表す文字列。例：192.168.0.20

デフォルト

192.168.0.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 = 偽) 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 = 偽) に設定されているときにのみ設定できます。

有効値

有効な IP アドレスを表す文字列。例：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 = 偽) 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 = 偽) に設定されているときにのみ設定できます。

有効値

有効なゲートウェイ IP アドレスを表す文字列。例：192.168.0.1

デフォルト

192.168.0.1

説明

RAC IP アドレスの静的割り当てに使うゲートウェイ IP アドレス。このプロパティは、**cfgNicUseDhcp** が **0** (FALSE = 偽) 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）

有効値

1 (TRUE = 真)

0 (FALSE = 偽)

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 = 真 ）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 = 偽) に設定すると、静的 IP アドレス、サブネットマスク、ゲートウェイは**cfgNicIpAddress**、**cfgNicNetmask**、**cfgNicGateway** プロパティから割り当てられます。

cfgNicMacAddress（読み取り専用）

有効値

RAC NIC MAC アドレスを表す文字列

デフォルト

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

このグループには、使用可能なリモートインタフェース経由での RAC へのアクセスが許可されているユーザーについての設定情報が格納されています。

最大 16 のユーザーグループのインスタンスを使用できます。各インスタンスは各ユーザーの設定を表します。

cfgUserAdminIpmiLanPrivilege（読み取り / 書き込み）

有効値

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 チャネル上での最大権限。

cfgUserAdminPrivilege（読み取り / 書き込み）

有効値

0x00000000～0x000001ff

デフォルト

0x00000000

説明

このプロパティは、ユーザーのロールベースの権限を指定します。値は、権限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 に、組み合わせてビットマスクを作成できるユーザー権限ビット値について説明します。

表 B-1 ユーザー権限を表すビットマスク

ユーザー権限	権限ビットマスク
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-21 つまたは複数の権限を表す権限ビットマスクの例を示します。

表 B-2 ユーザー権限ビットマスクの例

ユーザー権限	権限ビットマスク
ユーザーは 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、仮想メディアにアクセスして、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）

有効値

文字列。最大 16 文字。

デフォルト

""

説明

このインデックスのユーザーの名前。インデックスに何も入っていない場合は、文字列をこの名前フィールドに書き込むとユーザーインデックスが作成されます。二重引用符（""）の文字列を書き込むと、そのインデックスのユーザーが削除されます。この名前は変更できません。削除してから再作成する必要があります。文字列に / （フォワードスラッシュ）、\ （バックスラッシュ）、.（ピリオド）、@（アットマーク）および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）

有効値

最大 20 文字の ASCII 文字列。

デフォルト

""

説明

このユーザーのパスワード。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

有効値

1 (TRUE = 真)

0 (FALSE = 偽)

デフォルト

0

説明

ユーザーを個別に有効または無効にします。

cfgUserAdminSolEnable

有効値

1 (TRUE = 真)

0 (FALSE = 偽)

デフォルト

0

説明

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

---

cfgEmailAlert

このグループには、RAC 電子メール警告機能を設定するためのパラメータが入っています。

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

cfgEmailAlertIndex（読み取り専用）

有効値

1～4

デフォルト

このパラメータは既存のインスタンスに基づいて設定されます。

説明

警告インスタンスの一意インデックス。

cfgEmailAlertEnable（読み取り / 書き込み）

有効値

1 (TRUE = 真)

0 (FALSE = 偽)

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

有効値

電子メールアドレス形式、最大 64 文字の ASCII 文字。

デフォルト

""

説明

警告ソースの電子メールアドレス。

cfgEmailAlertCustomMsg

有効値

文字列。最大 32 文字。

デフォルト

""

説明

警告と一緒に送信するカスタムメッセージを指定します。

---

cfgSessionManagement

このグループには、iDRAC に接続できるセッション数を設定するパラメータが格納されています。

このグループでは 1 つのインスタンスが使用できます。以下の各項では、このグループの各オブジェクトについて説明します。

cfgSsnMgtConsRedirMaxSessions（読み取り / 書き込み）

有効値

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）

有効値

60～1920

デフォルト

300

説明

ウェブサーバーのタイムアウトを定義します。このプロパティでは、接続が無動作（ユーザー入力なし）状態が何秒続くとタイムアウトするかを指定します。このプロパティで設定した制限時間が過ぎたら、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）。

時間切れになったウェブサーバーのセッションは、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）

有効値

0 (タイムアウトなし)

60～1920

デフォルト

300

説明

セキュアシェル（SSH）のアイドルタイムアウトを定義します。このプロパティでは、接続が無動作（ユーザー入力なし）状態が何秒続くとタイムアウトするかを指定します。このプロパティで設定した制限時間が過ぎたら、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 キーを押した後にのみ、次のエラーメッセージが表示されます。

警告：セッションは有効でなくなりました。タイムアウトしたようです。

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）

有効値

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。このプロパティでは、接続が無動作（ユーザー入力なし）状態が何秒続くとタイムアウトするかを指定します。このプロパティで設定した制限時間が過ぎたら、セッションはキャンセルされます。この設定を変更しても、現在のセッションには影響しません（新しい設定を有効にするには、ログアウトしてログインすることが必要です）。

時間切れになった Telnet セッションでは、Enter キーを押した後にのみ、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：セッションは有効でなくなりました。タイムアウトしたようです。)

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できます。以下の各項では、このグループの各オブジェクトについて説明します。

cfgSerialSshEnable（読み取り / 書き込み）

有効値

1 (TRUE = 真)

0 (FALSE = 偽)

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）

有効値

1 (TRUE = 真)

0 (FALSE = 偽)

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）

有効値

10～65535

デフォルト

80

説明

RAC との HTTP ネットワーク通信に使うポート番号を指定します。

cfgRacTuneHttpsPort（読み取り / 書き込み）

有効値

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

有効値

1 (TRUE = 真)

0 (FALSE = 偽)

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

有効値

文字列、フォーマットされた 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 (**cfgRacTuneIpRangeMask**). 1 で決定される IP アドレスビットパターンの可能な位置を指定します。

cfgRacTuneIpRangeMask

有効値

左寄せビットを使用した標準的な IP マスク値

デフォルト

255.255.255.0

説明

IP アドレス形式の文字列。例：255.255.255.0

cfgRacTuneIpBlkEnable

有効値

1 (TRUE = 真)

0 (FALSE = 偽)

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

有効値

2～16

デフォルト

5

説明

ウィンドウ（cfgRacTuneIpBlkFailWindow）内で何回ログインに失敗したら、この IP アドレスからのログイン試行が拒否されるかを指定します。

cfgRacTuneIpBlkFailWindow

有効値

10～65535

デフォルト

60

説明

ログインの失敗回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、失敗回数カウントはゼロにリセットされます。

cfgRacTuneIpBlkPenaltyTime

有効値

10～65535

デフォルト

300

説明

失敗回数が制限値を超えた IP アドレスからのセッション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）

有効値

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）

有効値

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）

有効値

1 (TRUE = 真)

0 (FALSE = 偽)

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）

有効値

1～65535

デフォルト

5900

説明

iDRAC のコンソールリダイレクト時に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）

有効値

1～65535

デフォルト

5901

説明

iDRAC のコンソールリダイレクト時に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）

有効値

0 (FALSE = 偽)

1 (TRUE = 真)

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）

有効値

0 (FALSE = 偽)

1 (TRUE = 真)

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）

有効値

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を記述するプロパティが格納されています。

このグループでは 1 つのインスタンスが使用できます。以下の各項では、このグループの各オブジェクトについて説明します。

ifcRacMnOsHostname (読み取り / 書き込み)

有効値

文字列。最大 255 文字。

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)

有効値

文字列。最大 255 文字。

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します。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）

有効値

文字列。最大 254 文字。

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）

有効値

文字列。最大 254 文字。

デフォルト

「」

説明

CSR 組織名（O）を指定します。

cfgSecCsrOrganizationUnit（読み取り / 書き込み）

有効値

文字列。最大 254 文字。

デフォルト

""

説明

CSR 部門名（OU）を指定します。

cfgSecCsrLocalityName（読み取り / 書き込み）

有効値

文字列。最大 254 文字。

デフォルト

""

説明

CSR 地域（L）を指定します。

cfgSecCsrStateName（読み取り / 書き込み）

有効値

文字列。最大 254 文字。

デフォルト

""

説明

CSR 地域（L）を指定します。

cfgSecCsrCountryCode（読み取り / 書き込み）

有効値

文字列。最大 2 文字。

デフォルト

""

説明

CSR 国番号（CC）を指定します。

cfgSecCsrEmailAddr（読み取り / 書き込み）

有効値

文字列。最大 254 文字。

デフォルト

""

説明

CSR の電子メールアドレスを指定します。

cfgSecCsrKeySize（読み取り / 書き込み）

有効値

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できます。以下の各項では、このグループの各オブジェクトについて説明します。

cfgVirMediaAttached（読み取り / 書き込み）

有効値

1 (TRUE = 真)

0 (FALSE = 偽)

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接続するために使用されます。デバイスを接続すると、サーバーはこれらのデバイスをシステムに接続された有効な USB 大量ストレージデバイスとして認識します。これは、ローカル USB CD-ROM/ フロッピードライブをシステムの USB ポートに接続する場合と同じです。デバイスが接続されると、iDRAC の ウェブインタフェースまたは CLI を使用してこれらの仮想デバイスにリモート接続できるようになります。このオブジェクトを **0** に設定すると、デバイスは USB バスから切断されます。

メモ: 変更を有効にするには、システムを再起動する必要があります。

cfgVirAtapiSrvPort（読み取り / 書き込み）

有効値

1～65535

デフォルト

3668

説明

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

cfgVirAtapiSrvPortSsl（読み取り / 書き込み）

有効値

未使用のポート番号 0～65535 (10 進数)。

デフォルト

3670

説明

SSL 仮想メディアの接続に使用するポートを設定します。

cfgVirMediaBootOnce（読み取り / 書き込み）

有効値

1（有効）

0（無効）

デフォルト

0

説明

iDRAC の仮想メディアのブートワンス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）

有効値

1 (TRUE = 真)

0 (FALSE = 偽)

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格納されています。

cfgADRacDomain（読み取り / 書き込み）

有効値

空白文字を含まない印刷可能なテキスト文字列。最大 254 文字。

デフォルト

""

説明

DRAC が置かれている Active Directory ドメイン。

cfgADRacName（読み取り / 書き込み）

有効値

空白文字を含まない印刷可能なテキスト文字列。最大 254 文字。

デフォルト

""

説明

Active Directory フォレストに記録された iDRAC 名。

cfgADEnable（読み取り / 書き込み）

有効値

1 (TRUE = 真)

0 (FALSE = 偽)

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の設定**権限が必要です。

有効値

15～300

デフォルト

120

説明

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

cfgADRootDomain（読み取り / 書き込み）

有効値

空白文字を含まない印刷可能なテキスト文字列。最大 254 文字。

デフォルト

""

説明

ドメインフォレストのルートドメイン。

cfgADSpecifyServerEnable（読み取り / 書き込み）

有効値

1 または 0 (TRUE または FALSE)

デフォルト

0

説明

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

cfgADDomainController（読み取り / 書き込み）

有効な IP アドレスまたは完全修飾ドメイン名（FQDN）

デフォルト

デフォルト値なし

説明

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）

有効値

有効な IP アドレスまたは完全修飾ドメイン名（FQDN）

デフォルト

デフォルト値なし

説明

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）

有効値

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指定します。

---

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格納されています。

cfgSSADRoleGroupIndex（読み取り専用）

有効値

1～5 の整数。

説明

Active Directory で記録したロールグループのインデックス。

cfgSSADRoleGroupName（読み取り / 書き込み）

有効値

空白文字を含まない印刷可能なテキスト文字列。最大 254 文字。

デフォルト

（空白）

説明

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

cfgSSADRoleGroupDomain（読み取り / 書き込み）

有効値

空白文字を含まない印刷可能なテキスト文字列。最大 254 文字。

デフォルト

（空白）

説明

ロールグループが置かれている Active Directory ドメイン。

cfgSSADRoleGroupPrivilege（読み取り / 書き込み）

有効値

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、ロールグループのロールベースの権限を設定します。

表 B-3 ロールグループの特権のビットマスク

ロールグループの権限	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）

有効値

0 (FALSE = 偽)

1 (TRUE = 真)

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）

有効値

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）

有効値

2 (ユーザー)

3 (オペレータ)

4 (管理者)

デフォルト

4

説明

SOL アクセスに必要な最小権限を指定します。

cfgIpmiSolAccumulateInterval（読み取り / 書き込み）

有効値

1～255

デフォルト

10

説明

SOL 文字データパケットの一部を送信する前に通常 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）

有効値

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）

有効値

0 (FALSE = 偽)

1 (TRUE = 真)

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）

有効値

2 (ユーザー)

3 (オペレータ)

4 (管理者)

デフォルト

4

説明

IPMI オーバー LAN アクセスに許可される最大権限レベルを指定します。

cfgIpmiLanAlertEnable（読み取り / 書き込み）

有効値

0 (FALSE = 偽)

1 (TRUE = 真)

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 / 無効プロパティすべてに優先されます。

cfgIpmiEncryptionKey（読み取り / 書き込み）

有効値

空白文字を含まない 0～20 文字の16 進数文字列。

デフォルト

00000000000000000000

説明

IPMI 暗号化キー。

cfgIpmiPetCommunityName（読み取り / 書き込み）

有効値

最大 18 バイトの文字列。

デフォルト

public

説明

トラップの SNMP コミュニティ名。

---

cfgIpmiPef

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

イベントフィルタは、管理下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）

有効値

文字列。最大 255 文字。

デフォルト

インデックスフィルタの名前。

説明

プラットフォームイベントフィルタの名前を指定します。

cfgIpmiPefIndex（読み取り専用）

有効値

1～17

デフォルト

プラットフォームイベントフィルタオブジェクトのインデックス値。

説明

特定のプラットフォームイベントフィルタのインデックスを指定します。

cfgIpmiPefAction（読み取り / 書き込み）

有効値

0 (なし)

1 (電源を切る)

2 (リセット)

3 (電源を入れ直す)

デフォルト

0

説明

警告がトリガされたときに管理下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）

有効値

0 (FALSE = 偽)

1 (TRUE = 真)

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します。

cfgIpmiPetIndex（読み取り / 書き込み）

有効値

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）

有効値

有効な IP アドレスを表す文字列。例：192.168.0.67

デフォルト

0.0.0.0

説明

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

有効値

0 (FALSE = 偽)

1 (TRUE = 真)

デフォルト

1

説明

個々のトラップを有効または無効にします。

目次ページに戻る

目次ページに戻る

RACADM と SM-CLP との対応付け

Integrated Dell™ Remote Access Controller ファームウェア バージョン 1.11 ユーザー ガイド

表 C-1 に、RACADM グループとオブジェクト、および SM-CLP MAP 上での対応する SM-CLP の場所（存在する場合）を示します。

表 C-1 RACADM グループ / オブジェクトと SM-CLP との対応付け

RACADM グループ / オブジェクト	SM-CLP	説明
idRacInfo		
idRacName		最大 15 文字の ASCII 文字列。デフォルト: **iDRAC**
idRacProductInfo		最大 63 文字の ASCII 文字列。デフォルト: **Integrated Dell Remote Access Controller**
idRacDescriptionInfo		最大 255 文字の ASCII 文字列。デフォルト: **このシステムコンポーネントは Dell PowerEdge サーバーのリモート管理機能一式をすべて提供しています。**
idRacVersionInfo		最大 63 文字の ASCII 文字列。デフォルト: **1**
idRacBuildInfo		最大 16 文字の 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 文字の文字列。
cfgADRacDomain	oemdell_adracdomain	最大 254 文字の文字列。
cfgADRootDomain	oemdell_adrootdomain	最大 254 文字の文字列。
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**
cfgADSpecifyServerEnable	oemdell_adspecifyserverenable	有効になっている場合、LDAP またはグローバルカタログサーバーを指定します。 無効にするには 0、有効にするには 1。デフォルト: **0**
cfgADDomainController	oemdell_addomaincontroller	LDAP 検索に使用するドメインコントローラの DNS 名または IP アドレス。
cfgADGlobalCatalog	oemdell_adglobalcatalog	LDAP 検索に使用するグローバルカタログサーバーの DNS 名または IP アドレス。
cfgStandardSchema		
cfgSSADRoleGroupIndex	**/system1/sp1/group1 ～ /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 文字の文字列。
cfgSSADRoleGroupDomain	oemdell_groupdomain	最大 254 文字の文字列。
cfgSSADRoleGroupPrivilege	oemdell_groupprivilege	0x00000000 ～ 0x000001ff のビットマスク値。
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 文字の 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。

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 文字の 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。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**
	/system1/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。
	/system1/sp1/enetport1/lanendpt1/ ipendpt1/dnsendpt1/remotesap2	
cfgDNSServer2	dnsserveraddresses2	DNS サーバーの IP アドレスを表す文字列。
	/system1/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	**/system1/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	メディアを接続するには、(RACADM)/ VMEDIA_ATTACH (SM-CLP) を 1 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**
	/system1/sp1/oemdell_vmservice1/ tcpendpt1	
	oemdell_sslenabled	最初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 に設定します。編集不可。
cfgVirAtapiSvrPort	portnumber	最初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**
	/system1/sp1/oemdell_vmservice1/ tcpendpt2	
	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 に設定します。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	**/system1/sp1/account1 ～ /system1/sp1/account16**	
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	パスワード	最大 20 文字の 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 文字の文字列。
cfgEmailAlert		
cfgEmailAlertAddress		電子メール送信先アドレス、最大 64 文字。
cfgEmailAlertCustomMsg		電子メールで送信するメッセージ、最大 32 文字。
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するまでのアイドル時間(秒)。0(タイムアウトを無効にする)、または 60 ～ 1920 秒。デフォルト: **300**
cfgSsnMgtTelnetIdleTimeout		Telnet セッションタイムアウトするまでのアイドル時間(秒)。0(タイムアウトを無効にする)、または 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がタイムアウトするまでのアイドル時間(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 範囲フィルタを有効にするには 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 文字の文字列。
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 文字の文字列。
cfgRacSecurity	**/system1/sp1/oemdell_racsecurity1**	
cfgRacSecCsrCommonName	commonname	Active Directory のコモンネーム(CN)。最大 254 文字の文字列。
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 文字の文字列。
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 の市区町村名。最大 254 文字の文字列。
cfgRacSecCsrOrganizationName	organizationname	Active Directory の組織名。最大 254 文字の文字列。
cfgRacSecCsrOrganizationUnit	oemdell_organizationunit	Active Directory の組織部門名。最大 254 文字の文字列。
cfgRacSecCsrStateName	oemdell_statename	Active Directory の州名。最大 254 文字の文字列。
cfgIpmiSol		
cfgIpmiSolAccumulateInterval		シリアルオーバー LAN パケットの一部を送信するまでの最大待機時間(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権限。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: **00000000000000000000000000000000000000000000**
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 文字の文字列。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(電源を入れ直す)。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 文字の文字列。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)。

表 C-2 RACADM サブコマンドと SM-CLP の比較

RACADM サブコマンド	SM-CLP	説明
sslcsrgen -g	set /system1/sp1/oemdell_ssl1 oemdell_certtype=CSR set /system1/sp1/oemdell_ssl1 generate=1 dump -destination <iDRAC サーバー証明書 TFTP URI> /system1/sp1/oemdell_ssl1	SSL 証明書署名要求 (CSR) を生成してダウンロードします。
sslcsrgen -s	show /system1/sp1/oemdell_ssl1 oemdell_status	CSR 生成プロセスのステータスを表示します。
sslcertupload -t 1	set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL load -source <iDRAC サーバー証明書 TFTP-URI> /system1/sp1/oemdell_ssl1	iDRAC サーバー証明書を iDRAC にアップロードします。
sslcertupload -t 2	set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD load -source <ActiveDirectory 証明書 TFTP-URI> /system1/sp1/oemdell_ssl1	iDRAC に Active Directory 証明書をアップロードします。
sslcertdownload -t 1	set /system1/sp1/oemdell_ssl1 oemdell_certtype=SSL load -source <iDRAC サーバー証明書 TFTP-URI> /system1/sp1/oemdell_ssl1	iDRAC から iDRAC サーバー証明書をダウンロードします。
sslcertdownload -t 2	set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD load -source <ActiveDirectory 証明書 TFTP-URI> /system1/sp1/oemdell_ssl1	iDRAC から Active Directory 証明書をダウンロードします。

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 1.11 ユーザー 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、電源制御機能などを提供します。

iDRAC は、リモート監視 / 制御システムに、システムオンチップの内蔵マイクロプロセッサを採用しています。iDRAC は、管理する PowerEdge サーバーとシステム基板上で共存します。サーバーのオペレーティングシステム(Microsoft® Windows® または Linux)は、アプリケーションの実行に集中し、iDRAC はオペレーティングシステム以外のサーバーの環境や状態の監視と管理を行います。

警告やエラーが発生したときに、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)のトラップ警告を送信するように iDRAC を設定できます システムクラッシュの原因を診断する際の手助けとして、iDRAC はシステムクラッシュを検出すると、イベントデータをログに記録し、画面イメージをキャプチャできます。

管理下サーバーは、モジュール電源、冷却ファン、Chassis Management Controller(CMC) と共に Dell M1000-e システムエンクロージャ(シャーシ)に設置されています。CMC は、シャーシに搭載されているすべてのコンポーネントの監視と管理を行います。冗長 CMC を追加すると、プライマリ CMC に障害が発生した場合にホットフェールオーバーを提供することもできます。シャーシは、LCD ディスプレイ、ローカルコンソール接続、および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 へのネットワーク接続はすべて、CMC ネットワークインタフェース(「GB1」というラベルの CMC RJ45 接続ポート)を経由します。CMC は、サーバー上の iDRAC へのトラフィックを専用の内部ネットワークにルーティングします。この専用の管理ネットワークは、サーバーのデータパス外で、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、シャーシに搭載されている I/O モジュール(IOM)からアクセスします。

iDRAC ネットワークインタフェースは、デフォルトでは無効になっています。これを設定しなければ、iDRAC にアクセスできません。iDRAC をネットワーク上で有効にして設定すると、iDRAC ウェブインタフェース、Telnet、SSH や、Intelligent Platform Management Interface(IPMI)などの対応するネットワーク管理プロトコルを使用して、割り当てられた IP アドレスにアクセスできるようになります。

---

iDRAC の管理機能

iDRAC には次の管理機能があります。

- 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たリモートシステムの管理と監視
- Microsoft Active Directory® 認証のサポート - 標準スキーマまたは拡張スキーマを使用して iDRAC のユーザー ID とパスワードを Active Directory で集中化
- コンソールリダイレクト - リモートシステムにキーボード、ビデオ、マウスの機能を提供
- 仮想メディア - 管理下サーバーが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フォルダの ISO CD/DVD イメージにアクセス可能
- 監視 - システム情報やコンポーネントの状態にアクセス可能
- 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にアクセス可能
- Dell OpenManage™ ソフトウェアの統合 - Dell OpenManage Server Administrator または IT Assistant から 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機能を管理コンソールから提供
- Intelligent Platform Management Interface(IPMI)のサポート
- 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 - さまざまなシステム管理タスクに応じて割り当て可能な権限

---

iDRAC のセキュリティ機能

iDRAC には次のセキュリティ機能があります。

- Microsoft Active Directory(オプション)またはハードウェアに保存されているユーザー ID とパスワードによるユーザー認証
- システム管理者が各ユーザーに特定の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 暗号化をサポートしていません。

- 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 アドレス範囲を制限

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ついては、iDRAC の Readme ファイルと、デルのサポートウェブサイト **support.dell.com** にある『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 は、iDRAC でサポートされているオペレーティングシステムのリストです。

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

表 1-1 対応 OS

オペレーティングシステムファミリー	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)エディション SP2 Microsoft Windows Server 2003 Web、Standard、および Enterprise(32 ビット x86)エディション SP2 Microsoft Windows Server 2003 Standard/Enterprise(x64)エディション SP2 Microsoft Windows Storage Server 2003 R2 Express、Workgroup、Standard、および Enterprise x64 エディション Microsoft Windows Vista® Gold Business および Enterprise エディション Microsoft Windows Server 2008 Web、Standard、および Enterprise(32 ビット x86)エディション Microsoft Windows Server 2008 Web、Standard、Enterprise、および Datacenter(x64)エディション **メモ:** Windows Server 2003 SP1 をインストールする場合は、DCOM のセキュリティ設定に注意してください。詳細については、Microsoft のサポートウェブサイト **support.microsoft.com/kb/903220** で記事番号 903220 を参照してください。
Red Hat® Linux®	Enterprise Linux WS、ES、および AS(バージョン 3)(x86 および x86_64) Enterprise Linux WS、ES、および 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 Update 2 および Update 3(x86_64) Enterprise Server 10(Gold)(x86_64)

対応ウェブブラウザ

注意: コンソールリダイレクトと仮想メディアは 32 ビットのウェブブラウザのみをサポートしています。64 ビットのウェブブラウザを使用すると、予期しない結果や不具合が生じます。

表 1-2 は、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のリストです。

最新情報については、iDRAC の Readme ファイルと、デルのサポートウェブサイト **support.dell.com** にある『Dell OpenManage Server Administrator 互換性ガイド』を参照してください。

表 1-2 対応ウェブブラウザ

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 は接続機能のリストです。

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 のサポート • SNMP トラップと電子メールによるイベント通知 • 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使用する SM-CLP (Telnet または SSH)コマンドシェルのサポート • impitool や ipmishell などの IPMI ユーティリティのサポート

---

iDRAC のポート

表 1-4 は、iDRAC が接続を待ち受けるポートのリストです。表 1-5 は、iDRAC がクライアントとして使用するポートです。この情報は、ファイアウォールのポートを開いて iDRAC へのリモートアクセスを許可する場合に必要です。

表 1-4 iDRAC サーバーリスニングポート

ポート番号	機能
22*	セキュアシェル (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 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

その他のマニュアル

この『ユーザーズガイド』のほかに、次の文書にもシステム内の 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全モジュールを管理するコントローラの使用法について説明しています。
- 『Dell OpenManage IT Assistant ユーザーズガイド』は、IT Assistant の使用法について説明しています。
- 『Dell OpenManage Server Administrator ユーザーズガイド』は、Server Administrator のインストールと使用法について説明しています。
- 『Dell Update Packages ユーザーズガイド』は、システムアップデート対策としての Dell Update Packages の入手とその使用法について説明しています。

次のシステム文書にも、iDRAC をインストールする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、安全と規制に関する説明が記載されています。保証情報については、この文書に含まれている場合と、別の文書が付属する場合があります。
- 『ラック取り付けガイド』および『ラック取り付け手順』では、システムをラックに取り付ける方法を説明しています。
- 『スタートアップガイド』では、システムの機能、システムのセットアップ、および技術仕様の概要を説明しています。
- 『ハードウェアオーナーズマニュアル』では、システムの機能、トラブルシューティングの方法、およびコンポーネントの取り付け方や交換方法について説明しています。
- システム管理ソフトウェアのマニュアルでは、ソフトウェアの機能、動作条件、インストール、および基本操作について説明しています。
- オペレーティングシステム のマニュアルには、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方法（必要な場合）、設定方法、および操作方法が記載されています。
- 別途購入したコンポーネントのマニュアルでは、これらのオプション装置の取り付けや設定について説明しています。
- システム、ソフトウェア、またはマニュアルの変更について記載されたアップデート情報がシステムに付属していることがあります。

  メモ: アップデート情報には他の文書より優先される情報が含まれていることがあるので、必ず最初にお読みください。

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

目次ページに戻る

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 1.11 ユーザー ガイド

この項では、iDRAC へのアクセスの確立方法と、iDRAC を使える管理環境に設定する方法を説明します。

始める前に

iDRAC を設定する前に、次のマニュアルを用意します。

- 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 を設定するには、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 を使用できます。管理下サーバーにオペレーティングシステムと 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 は、これらのインタフェースについて説明しています。

注意: 複数の設定インタフェースを同時に使用すると、予想外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、新しい PowerEdge サーバーをインストールする場合に便利です。ネットワークや基本的なセキュリティ機能の設定や、その他の機能を有効にするときに使用してください。
iDRAC ウェブインタフェース	iDRAC ウェブインタフェースは、iDRAC をインタラクティブに管理しながら、管理下サーバーを監視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開始などの日常的なタスクに使用する主要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、シャーシの監視と管理のほかに、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、リセットなどにも使用できます。
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大まかな状態を表示するために使用できます。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。このインタフェースには、iKVM または iDRAC ウェブインタフェースから開始した 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 の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、iDRAC のほぼすべての機能にアクセスを提供します。センサーデータや、システムイベントログのレコード、iDRAC で管理される現在の状態や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、機能の有効 / 無効、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上のメディアへのアクセスを提供します。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作成に便利です。
SM-CLP	SM-CLP は、iDRAC に組み込まれた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)の実装です。SM-CLP コマンドラインには、Telnet や SSH を使用して iDRAC にログインするとアクセスできます。 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ています。これらのコマンドは管理ステーションのコマンドラインから実行できるため、スクリプトの記述に便利です。コマンドの出力は、XML などの明確なフォーマットで取得でき、スクリプトの記述や、既存のレポートツールや管理ツールとの統合を円滑にします。 RACADM コマンドと SM-CLP コマンドの比較については、「RACADM と SM-CLP との対応付け」を参照してください。
IPMI	IPMI は、iDRAC などの組み込み管理サブシステムが他の組み込みシステムや管理アプリケーションと通信するための標準的な方法を定義しています。 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、ある状態を検出したときに、選択可能な処置(たとえば管理下サーバーの再起動)を iDRAC に実行させます。PET は、特定のイベントまたは状態を検出したときに電子メールまたは IPMI 警告を送信するよう iDRAC に命令します。 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** などの標準的な IPMI ツールも使用できます。

設定タスク

この項では、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概説します。実行するタスクには、iDRAC をリモートで使用するための設定、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あります。

タスクの下に、各タスクの実行に使用可能な設定タスクが一覧になっています。

メモ: このガイドの設定手順を実行する前に、CMC および I/O モジュールをシャーシに取り付けて設定する必要があります。また、PowerEdge サーバーもシャーシ内に物理的に設置する必要があります。

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、その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 ネットワーク設定を変更すると、iDRAC との現在のネットワーク接続がすべて終了します。

メモ: LCD パネルを使用してサーバーを設定するオプションは、CMC の初期設定中のみに使用できます。いったんシャーシを導入すると、LCD パネルを使用して iDRAC を再設定することはできません。

メモ: LCD パネルは、iDRAC ネットワークを設定するために DHCP を有効にする際にも使用できます。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の設定」を参照してください。
- RACADM - 「cfgLanNetworking」を参照してください。

iDRAC ユーザーの設定

ローカル iDRAC の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表示するテーブルがあります。これらのユーザーにユーザー名、パスワード、および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® も使用できます。

- 「Microsoft Active Directory での 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、定義した範囲外の IP アドレスからの接続を拒否したり、設定した時間枠内に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して、不正なアクセスを防止できます。

- iDRAC Web 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、検出するイベントを選択します(たとえば、あるイベントが検出されたときに管理下サーバーを再起動する)。

- 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) の設定」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)の設定」を参照してください。
- RACADM - PET の設定

シリアルオーバー LAN の設定

シリアルオーバー LAN(SOL)は、管理下サーバーのシリアルポート I/O をネットワーク上に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 の設定

- iDRAC ウェブインタフェース - 「SSL (Secure Sockets Layer)」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に、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上のメディアデバイスや、ネットワーク共有フォルダ内の ISO CD/DVD イメージに、それらが管理下サーバーにあるかのようにアクセスできます。

- iDRAC ウェブインタフェース - 「仮想メディアの設定と使用法」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、PowerEdge 管理下サーバーに 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 - 「管理下サーバーへ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。

管理下サーバーへの前回クラッシュ画面機能の設定

オペレーティングシステムのクラッシュまたはフリーズ後に iDRAC が画面イメージをキャプチャできるように管理下サーバーを設定します。

- 管理下サーバー - 「管理下サーバーを使用して前回クラッシュ画面をキャプチャする設定」、「Windows の 自動再起動オプションを無効にする」を参照してください。

CMC ウェブインタフェースを使用したネットワークの設定

メモ: CMC から iDRAC ネットワーク設定をセットアップするには、シャーシ設定管理者の権限が必要です。

メモ: デフォルトの CMC ユーザーは **root** で、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** の順にクリックすると 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. 左列の **シャーシ** の横にあるプラス(+)記号をクリックし、**サーバー** をクリックします。
4. **セットアップ** → **導入** の順にクリックします。
5. **LAN を有効にする** 見出しの下のサーバーの横にあるチェックボックスをオンにしてサーバーの LAN を有効にします。
6. **IPMI over LAN を有効にする** 見出しの下にあるサーバーの横のチェックボックスをオンかオフにして、IPMI over LAN を有効または無効にします。
7. **DHCP を有効にする** 見出しの下のサーバーの横にあるチェックボックスをオンかオフにしてサーバーの DHCP を有効または無効にします。
8. DHCP が無効になっている場合は、サーバーの静的 IP アドレス、ネットマスク、およびデフォルトのゲートウェイを入力します。
9. ページ下の **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 ファームウェアをアップデートすると、iDRAC フラッシュメモリの新しい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損している場合のみ)

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、さまざまなアップデート方法に対応するように複数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 を使用して iDRAC ファームウェアをアップデートする場合や、CMC ウェブインタフェースを使用して iDRAC を復旧する場合には、自己解凍式アーカイブとしてパッケージ化されてい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 iDRAC ファームウェアをアップデートするには、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専用の 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て iDRAC ファームウェアをアップデートするには、自己解凍式のアーカイブファイルにパッケージ化されたアップデートユーティリティと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すると、既存の iDRAC セッションがすべて切断され、アップデートプロセスが完了するまで新しいセッションは実行できません。

メモ: シャーシのファンは 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。これは正常な動作で、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に設計されています。

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専用の DUP を実行してください。

SM-CLP **load** コマンドを使用する場合は、簡易ファイル転送プロトコル(TFTP)サーバーが iDRAC に配信できるディレクトリにファームウェアのバイナリイメージを保存してください。「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は、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できるディスクにファームウェアのバイナリイメージを格納してください。「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 の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。

iDRAC ファームウェアアップデートの完了前に進行が中断した場合など、CMC が iDRAC ファームウェアの破損を検出した場合にのみ、CMC ウェブインタフェースを使用してファームウェアをアップデートできます。「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 で起動し、**idrac16d** コマンドを実行してください。コマンドの構文は次のとおりです。

```
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。

オプションは次のとおりです。

`-f` - アップデートを強制します。`-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場合に使用できます。

`-i=<ファイル名>` - ファームウェアのイメージが含まれているファイル名イメージを指定します。このオプションは、ファームウェアのファイル名をデフォルト名 **firmimg.imc** から変更した場合に必要です。

-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をログします。このオプションはデバッグに使用します。

注意: **idrac16d** コマンドに入力する引数を間違えた場合や、、`-h` オプションを入力した場合は、使用法の出力に追加オプションの `-nopresconfig` が表示されます。このオプションは、設定情報を保存せずにファームウェアをアップデートする場合に使用します。IP アドレス、ユーザー、パスワードなどの iDRAC の既存の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の署名者の身元を認証するために使用され、署名後に内容が変更されていないことを証明します。

デジタル署名を検証する Gnu Privacy Guard(GPG)をまだシステムにインストールしていない場合は、これをインストールしてください。標準的な検証方法を使用するには、次の手順に従います。

1. Dell Linux GPG 公開キーがまだない場合は、**lists.us.dell.com** に移動し、**Dell GPG 公開キー** リンクをクリックして 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て、公開キーを `gpg` 信用データベースにインポートします。

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

メモ: プロセスを完了するには秘密キーが必要です。

3. 疑わしいキー警告を回避するには、Dell GPG 公開キーの信用レベルを変更します。

   e. 次のコマンドを入力します。

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

   f. GPG キーエディタ内で、`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. (Product Group) <linux-security@dell.com>
      Primary key fingerprint: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D D
      ```

      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。

   g. GPG キーエディタに「`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.)
      (（パスポートや異なるソースのフィンガープリントの確認などによって）他のユーザーのキーを検証するうえで、このユーザーをどこまで信用するかを決定します。)


        1 = I don't know or won't say (不明または判断できない)
        2 = I do NOT trust (信用しない)
        3 = I trust marginally (少しだけ信用する)
        4 = I trust fully (全面的に信用する)
        5 = I trust ultimately (絶対的に信用する)
        m = back to the main menu (メインメニューに戻る)

      Your decision? ( どこまで信用しますか？)
      ```

   h. `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)
      このキーを絶対的な信用に設定しますか? (y/N)
      ```

   i. `y <Enter>` と入力して選択を確認します。

   j. `quit <Enter>` と入力して、GPG キーエディタを終了します。

   公開キーのインポートと検証は 1 回だけ実行します。

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)と関連する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** からダウンロードします。

   メモ: 各 Linux アップデートパッケージには、個別の署名ファイルがあり、同じウェブページにアップデートパッケージとして表示されます。検証には、アップデートパッケージおよびそれに関連する署名ファイルの両方が必要です。デフォルトでは、署名ファイルの名前は DUP のファイル名と同じで、拡張子は **.sign** です。たとえば、Linux DUP 名が **PE1850-BIOS-LX-A02.BIN** の場合、署名ファイル名は **PE1850-BIOS-LX-A02.BIN.sign** となります。iDRAC ファームウェアイメージには、ファームウェアイメージと共に自己解凍式アーカイブに含まれる **.sign** ファイルが関連付けられています。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、ファイルオプションの **名前を付けて保存...** を選択します。

5. アップデートパッケージの検証:

   ```
   gpg --verify <Linux DUP の署名ファイル名> <Linux DUP のファイル名>
   ```

次に、1425SC BIOS アップデートパッケージを検証する手順の例を示します。

1. 次の 2 ファイルを **support.dell.com** から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 信用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> と入力して選択を確認します。
   e. quit <Enter> と入力して、GPG キーエディタを終了します。

   これで、Dell 公開キーの検証が完了します。

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: 「手順 3」で示したようにキーを検証しなかった場合は、次の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 the owner.
   Primary key fingerprint: 4172 E2CE 955A 1776 A5E6 1BB7 CA77 951D 23B6 6A9D

   (gpg : 警告 : このキーは信頼性のある署名で認証されていません。
   gpg: この署名が所有者のものかどうか識別できません。
   プライマリキーのフィンガープリント: 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 1.11 ユーザー 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の監視と管理に使用するコンピュータです。この項では、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、この項の手順に従って必要なツールのインストールと設定を行ってください。

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」というラベルの 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LAN 経由で iDRAC に 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、管理下サーバーのネットワークから CMC ネットワークを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(GUI コンソールリダイレクトの使用を参照)を使用すると、サーバーのポートにネットワークアクセスできない場合でも、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の NIC が必要な場合があります。

対応ウェブブラウザの設定

この項では、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については、「対応ウェブブラウザ」のリスト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は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、インストール手順に失敗します。このエラーを確認しないでこの手順を繰り返すと、最初の試みでプラグインのインストールに失敗したにも関わらず、コンソールリダイレクトページがロードされます。これは、プラグインのインストールに失敗しても、ウェブブラウザがプロファイルディレクトリにプラグイン情報を保存するからです。この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実行し、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

プロキシサーバー経由で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. ウェブブラウザのウィンドウを開きます。
2. **ツール** をクリックして、**インターネットオプション** をクリックします。
3. **インターネットオプション** ウィンドウで **接続** タブをクリックします。
4. **ローカルエリアネットワーク(LAN)設定** で **LAN 設定** をクリックします。

5. **プロキシサーバーを使用** チェックボックスがオンになっている場合は、**ローカルアドレスにはプロキシサーバーを使用しない** チェックボックスをオンにします。

6. **OK** を 2 度クリックします。

信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際、iDRAC の IP アドレスが信用するドメインのリストにない場合は、IP アドレスをリストに加えるように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。

他言語のウェブインタフェースの表示

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
- 簡体字中国語

Internet Explorer 6.0（Windows）

Internet Explorer で iDRAC ウェブインタフェースを他の言語で表示するには、次の手順を実行してください。

1. **ツール** をクリックして、**インターネットオプション** を選択します。

2. **インターネットオプション** ウィンドウで **言語** をクリックします。

3. **言語の優先順位** ウィンドウで **追加** をクリックします。

4. **言語の追加** ウィンドウでサポートされている言語を選択します。

   複数の言語を選択するには、<Ctrl> を押しながら選択します。

5. 優先言語を選択して **上に移動** をクリックし、その言語をリストの先頭に移動します。

6. **言語設定** 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を他の言語で表示するには、次の手順を実行してください。

1. **編集→ 設定** の順にクリックし、**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. コマンド端末を開きます。
2. locale と入力し、<Enter> 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、変更する必要はありません。値に「zh_CN.UTF-8」が含まれない場合は、手順 4 に進みます。
4. テキストエディタで **/etc/sysconfig/i18n** ファイルを編集します。
5. ファイルに次の変更を加えます。

   現在のエントリ:

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

   更新後のエントリ:

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

6. 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、この修正が反映されていることを確認してください。有効になっていない場合は、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プラグインをインストールするときに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が有効な場合、ビューアのバージョンは同じでも iDRAC にアクセスするたびにコンソールリダイレクトビューアのインストールが要求されます。

ホワイトリスト機能を無効にし、プラグインの不要なインストールを回避するには、次の手順を実行してください。

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. **Preference Name** 列で、**xpinstall.whitelist.required** を見つけてダブルクリックします。

   Preference Name、**Status**、**Type**、**Value** の値が太字で表示されます。**Status** の値は **user set** に変わり、**Value** の値は **false** に変わります。
4. **Preferences Name** 列で、**xpinstall.enabled** を見つけます。

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

Java Runtime Environment (JRE) のインストール

メモ: Internet Explorer ブラウザを使用している場合、コンソールビューア用に ActiveX コントロールが提供されます。JRE をインストールし、ビューアの起動前に 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。詳細については、「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 を使用する選択もできます。

Firefox ブラウザを使用している場合、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 はセキュアではないプロトコルのため、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にのみ使用してください。

メモ: iDRAC へのアクティブな Telnet または SSH 接続は、1 度に 1 つのみが可能です。アクティブな接続が存在する場合、他の接続試行は拒否されます。

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含まれており、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組み込まれている標準バージョンのほかに、さらに便利な機能の付いた有料 / 無料の Telnet クライアントをインストール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、ログインのフリーズ状態が発生することがあります。

この問題を解決するには、hotfix 824810 を Microsoft サポートウェブサイト **support.microsoft.com** からダウンロードししてください。詳細については、Microsoft 技術情報の記事 824810 を参照してください。

Telnet セッションのための Backspace キーの設定

一部のTelnet クライアントでは、<Backspace> キーを使用すると予想外の結果が生じることがあります。たとえば、セッションが ^h をエコーすることがあります。Microsoft と Linux の telnet クライアントではほとんどの場合、<Backspace> キーの使用を設定できます。

Microsoft telnet クライアントで <Backspace> キーを使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. コマンドプロンプトで、次のコマンドを入力します。

   ```
   set bsasdel
   ```

   次のメッセージが表示されます。

   ```
   Backspace will be sent as delete. (Backspace が Delete 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. シェルを開いて次のように入力します。

   ```
   stty erase ^h
   ```
2. コマンドプロンプトで、次のコマンドを入力します。

   ```
   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、セキュリティを強化する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。iDRAC の場合、SSH はデフォルトで有効になっています。

管理下サーバーの iDRAC に接続する際に、管理ステーションで PuTTY（Windows）または OpenSSH（Linux）を使用できます。ログイン時にエラーが発生した場合は、**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 によって制御されたものではありません。

メモ: OpenSSH は Windows の VT100 または ANSI 端末エミュレータから実行してください。Windows のコマンドプロンプトから OpenSSH を実行した場合は、一部の機能を使用できません（複数のキーが機能せず、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」で説明したように、`cfgSsnMgtSshIdleTimeout` プロパティによって制御されます。

DRAC 5 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 暗号化スキーマ

スキーマの種類	スキーム
非対称暗号	Diffie-Hellman DSA/DSS 512-1024(ランダム)ビット(NIST 仕様)
対称暗号	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
メッセージの整合性	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
認証	• パスワード

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のみに iDRAC ウェブインタフェースを使用する場合、TFTP サーバーは不要です。

簡易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)を簡単にしたものです。iDRAC とのファイル転送に、SM-CLP および RACADM コマンドラインインタフェースと併用されます。

iDRAC と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か、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ときに SM-CLP または RACADM を使用する場合は、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 サーバーが既にリッスン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。サーバーが実行していない場合は、次の選択肢があります。

- ネットワーク上で TFTP サービスを実行している別のコンピュータを検索する
- Linux を使用している場合は、ディストリビューションで提供される TFTP サーバーをインストールする
- Windows を使用している場合は、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 が同梱されています。このキットには次のコンポーネントが含まれますが、この限りではありません。

- 『Dell Systems Management Consoles CD』- Dell OpenManage IT Assistant をはじめとする最新の 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、システムのファームウェア、診断および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、周辺機器および RAID コントローラなどについて説明した最新のマニュアルが含まれています。
- デルのサポートウェブサイトおよび Readme ファイル - Dell 製品に関する最新情報については、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については、『クイックインストールガイド』を参照してください。

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 1.11 ユーザー ガイド

ここでは、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。

管理下サーバーへ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、次の機能が含まれています。

- 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ト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表示します。
- 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発行される、またはこれらによって発行されるコマンドのログを表示します。ログはホームページで表示したり、レポートとして印刷または保存したり、指定のサービス担当者に電子メールで送信できます。

Server Administrator 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。

管理下サーバーを使用して前回クラッシュ画面をキャプチャする設定

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支援するために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の詳細については、『Server Administrator ユーザーズガイド』を参照してください。
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 の **起動と回復** で 自動的に再起動する 機能が選択解除されていることを確認してください。Windows の 自動再起動オプションを無効にするを参照してください。
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の下にある **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 の設定手順の詳細については、『 Server Administrator ユーザーズガイド』を参照してください。前回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 の 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 **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 1.11 ユーザー 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に、iDRAC のウェブインタフェースを使用してください。この章では、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ています。

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。

SM-CLP コマンドは、Telnet または SSH 接続によってリモートアクセス可能なシェルにて実行できます。SM-CLP の詳細については、「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ウェブブラウザのウィンドウを開きます。

   詳細については、対応ウェブ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 キーを押します。

   デフォルトの HTTPS ポート番号(ポート 443)が変更されている場合は、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 **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とパスワードはそれぞれ **root** と **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** 権限が与えられている必要があります。

ログインするには、次の手順に従ってください。

1. **ユーザー名** フィールドで、以下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。たとえば、`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。たとえば、`dell.com\john_doe` または `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。パスワードでは大文字と小文字が区別されます。

3. **OK** をクリックするか、Enter キーを押します。

ログアウト

1. 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アクティブな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ください。

---

iDRAC NIC の設定

ここでは、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。

ネットワークおよびIPMI LAN 設定の設定

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

メモ: ほとんどの DHCP サーバーは、予約テーブルにクライアントの ID トークンを保存するためのサーバーを必要とします。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、1 バイトのインタフェース 番号(0)に続く 6 バイトの MAC アドレスを使用してクライアント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** の順にクリックします。
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 に、**ネットワークの設定**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 ネットワークの設定

設定	説明
NIC を有効にする	選択すると、NIC が有効になり、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。
NIC IPアドレスにDHCPを使用	iDRAC に動的ホスト構成プロトコル(DHCP)サーバーから NIC 用の IP アドレスを取得するように指示します。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 アドレスの入力または編集ができます。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	セカンダリ DNS サーバー IP アドレスは、**DHCP を使って DNS サーバーアドレス** が **選択されていない** であるときにだけ使用します。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 に 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 に iDRAC を登録** が選択されている場合にのみ iDRAC 名を表示します。デフォルト名は idrac-サービスタグで、サービスタグは Dell サーバーのサービスタグ番号を示します。例:idrac-00002
DNS ドメイン名に DHCP を使用	デフォルトの DNS ドメイン名を使用します。このチェックボックスが選択されておらず、**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 ドメイン名に DHCP を使用** チェックボックスを選択する場合は、**DHCP の使用(NIC IP アドレス用)**チェックボックスが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 ドメイン名に 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の発生時に、iDRAC 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。
チャネル権限レベルの制限	LAN チャネルで受け入れられるユーザーの最大権限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。
暗号鍵	暗号鍵の文字形式の設定では、0 ～ 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	画面に表示されている **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。その他の変更では NIC の NIC をリセットする必要があり、このため接続が一時的に途絶える場合があります。

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** の順にクリックし、**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 に、**ネットワークセキュリティ** ページの設定を示します。
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 範囲を有効にする	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指定します。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 アドレスの有意ビット位置を定義します。サブネットマスクは、上位ビットがすべて 1 で、下位ビットがすべてゼロであるネットマスク形式です。デフォルトは **255.255.255.0** です。
IP ブロックを有効にする	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 ブロックエラーカウント	IP アドレスからのログイン失敗回数を設定して、それを超えた場合にそのアドレスからのログインを拒否します。デフォルトは **10** です。
IP ブロックエラー時間枠	IP ブロック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 ブロックペナルティ時間	ログイン失敗回数が制限値を超えた IP アドレスからの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では、個々のイベントメッセージが返されたときに iDRAC が選択した処置を実行するように設定します。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直す、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] 、電子メール）があります。

表 5-6 に、フィルタ可能なプラットフォームイベントを示します

索引	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）を生成するように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イベントフィルタで別の動作（システムの再起動など）を実行するように設定すると、その動作が行われます。

プラットフォームイベントフィルタ (PEF) の設定

メモ: プラットフォームイベントトラップまたは電子メール警告設定を行う前に、プラットフォームイベントフィルタを設定してください。

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、該当するイベントの **警告の生成** チェックボックスをクリックし、**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する 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: 設定されている有効な宛先（PET または電子メール）に警告を送信するためには、**警告の生成** を有効にする必要があります。

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っ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 の手順に必ず従ってください。
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選択します。
   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: トラップを確実に送信するには、**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の発生時に iDRAC 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、設定した警告をテストします。
   e. 残りの送信先番号に対してもステップ 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っ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 の手順に必ず従ってください。
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. 電子メール警告の宛先を指定します。
   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送信できます。
   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. **宛先の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: テストメールを正しく送信するには、**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。プラットフォームイベントが発生すると、設定した IP アドレスにある **SMTP サーバー** は 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、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 ステップ a ～ ステップ 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っ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 の順にクリックして、**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 チャネルの権限を更新します。

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

   IPMI LAN 設定 で **チャネル権限レベルの制限** ドロップダウンメニューをクリックし、**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. 必要なら IPMI LAN チャネルの暗号鍵を設定します。

メモ: iDRAC IPMI は RMCP+ プロトコルに対応しています。

メモ: 暗号鍵は、最大 20 文字の偶数の 16 進数文字で指定する必要があります。

IPMI LAN 設定 の **暗号鍵** フィールドに暗号鍵を入力します。

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選択して、シリアルオーバー LAN を有効にします。
   d. IPMI SOL ボーレートを更新します。

メモ: シリアルコンソールを LAN 経由でリダイレクトする場合は、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維持するには、特定の管理者権限(またはロールベースの権限)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** の順にクリックして、**ネットワーク/ セキュリティ** をクリックします。
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 権限**、**iDRAC 権限**、**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 の匿名ユーザー用に予約されており、変更できません。

3. **ユーザー ID** 列で、ユーザー ID をクリックします。
4. **ユーザーの設定** ページで、ユーザーのプロパティと権限を設定します。

   表 5-7iDRAC 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ています。

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

   表 5-9 では、**IPMI LAN** 権限 と **iDRAC ユーザー権限**を設定するための **ユーザー**グループ権限 について説明しています。

   表 5-10 では、**iDRAC グループ**権限について説明しています。**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 全般的なプロパティ

プロパティ	説明
ユーザー ID	16 個あるプリセットユーザー ID 番号の 1 つが入っています。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。
ユーザー名	iDRAC ユーザー名は最大 16 文字で指定します。各ユーザーは一意なユーザー名を持つ必要があります。 **メモ:** iDRAC のユーザー名に **/**(フォワードスラッシュ) や **.**(ピリオド) を含めることはできません。 **メモ:** ユーザー名を変更した場合は、新しい名前は次回のユーザーログイン時までユーザーインタフェースに表示されません。

パスワードの変更	**新しいパスワード** と **新しいパスワードの確認** フィールドを有効にします。選択しないと、ユーザーの **パスワード** を変更することはできません。
新しいパスワード	iDRAC ユーザーのパスワードの編集を有効にします。20 文字以内で **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	確認のために iDRAC ユーザーのパスワードを再入力します。

表 5-8 IPMI LAN ユーザー権限

プロパティ	説明
許可される最高 LAN ユーザー権限	IPMI LAN チャネルでのユーザーの最大権限を、**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。選択すると、この権限が有効になります。

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 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	ユーザーが特定のユーザーにシステムへのアクセスを許可できるようにします。
ログのクリア	iDRAC のログをクリアできます。
サーバーコントロールコマンドの実行	RACADM コマンドを実行できます。
コンソールリダイレクトへのアクセス	ユーザーにコンソールリダイレクトの実行を許可します。
仮想メディアへのアクセス	ユーザーに仮想メディアの実行と使用を許可します。
テスト警告	ユーザーがテスト警告(電子メールと PET)を特定のユーザーに送信できるようにします。
診断コマンドの実行	ユーザーに診断コマンドの実行を許可します。

表 5-10 iDRAC グループ権限

ユーザーグループ	与えられる権限
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	**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** の権限を自由に組み合わせて選択できます。
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	画面に表示されている **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

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

- SSL (Secure Sockets Layer)
- 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

SSL (Secure Sockets Layer)

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。公開鍵と秘密鍵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 対応システムは、次のタスクを実行できます。

- SSL 対応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いセキュリティを確保するには、名の通った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企業情報を掲載した証明書署名要求(CSR)を生成します。生成した CSR を VeriSign や Thawte などの CA に送信します。

証明書署名要求 (CSR)

CSR は、認証局 (CA) に対してセキュアサーバー証明書の発行を求めるデジタル要求です。セキュア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ネゴシエートできます。

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 などがあります。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を介したトランザクションを識別する固有の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、証明書に含まれている情報に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** の順にクリックして、**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存されます。

表 5-12 に、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 **SSL メインメニュー** ページ上のボタンについて説明します。

表 5-12 SSL メインメニューオプション

フィールド	説明
新規証明書署名要求(CSR)の生成	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、ファームウェアにある古い CSR を上書きします。CA が CSR を受け入れるためには、ファームウェアにある CSR が CA から返された証明書に一致する必要があります。
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 メインメニューボタン

ボタン	説明
印刷	画面に表示されている **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古い 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 に、**証明書署名要求 (CSR) の生成** ページのオプションを示します。
3. 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 ページのオプション

フィールド	説明
コモンネーム	証明する名前(通常は **www.xyzcompany.com** のような Web サーバーのドメイン名)。英数字、ハイフン、下線、ピリオドのみが有効です。スペースは使用できません。
組織名	この組織に関連付けられた名前(たとえば「XYZ 会社」)。英数字、ハイフン、下線、ピリオド、スペースのみが有効です。
部門名	部門など組織単位に関連付ける名前(例、Information Technology)。英数字、ハイフン、下線、ピリオド、スペースのみが有効です。
地域	証明する会社が所在する都市や地域(たとえば「神戸」)。英数字とスペースのみが有効です。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がある都道府県(たとえば「東京」)。英数字とスペースのみが有効です。略語は使用しないでください。
国番号	証明書を申請している組織が所在する国の名前。
電子メール	CSR に関連付けられてい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。このフィールドは任意選択です。

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 ページが開きます。
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: アップロード中の証明書の対応ファイルパスが **ファイルパス** の値に表示されます。完全ファイル名およびファイル拡張子を含む完全な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	画面に表示されている **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
タイトル情報	タイトルによって入力された証明書のアトリビュート
発行者情報	発行者によって返された証明書のアトリビュート
有効期間の開始	証明書の発行日
有効期間の終了	証明書の失効日

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 での 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** の順にクリックして、**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示します。

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 の設定	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** を設定します。
Active Directory CA 証明書のアップロード	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 CA 証明書の表示	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	画面に表示されている **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 の設定（標準スキーマと拡張スキーマ）

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

   表 5-21 に、**Active Directory の設定と管理** ページの設定を示します。
3. **適用** をクリックして設定を保存します。
4. 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 標準スキーマのロールグループを設定するには、個々のロールグループ (1～5) をクリックします。表 5-23 および 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。
ルードメイン名	Active Directory のルードメイン名。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。
標準スキーマを使用	Active Directory に標準スキーマを使用します。
拡張スキーマを使用	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。
ロールグループ	iDRAC に関連付けられたロールグループのリスト。 ロールグループの設定を変更するには、ロールグループリストでそのロールグループの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 でロール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	ロール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	画面に表示されている **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 ロールグループの権限

設定	説明
ロールグループの権限レベル	ユーザーの最大 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。 **ロールグループ** 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。
サーバーコントロールコマンドの実行	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 ロールグループの権限

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: アップロード中の証明書の対応ファイルパスが **ファイルパス** の値に表示されます。完全ファイル名およびファイル拡張子を含む完全な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、iDRAC にアクセスする管理ステーションにこの証明書があることを確認してください。

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	画面に表示されている **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. **ダウンロードが完了しました** ウィンドウで**閉じる** をクリックします。

Active Directory CA 証明書の表示

Active Directory メインメニュー ページを使用して、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
タイトル情報	タイトルによって入力された証明書の属性
発行者情報	発行者によって返された証明書の属性
有効期間の開始	証明書の発行日。
有効期間の終了	証明書の有効期限日。

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	**画面に表示されている 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 に、**シリアルオーバー LAN の設定** ページの設定を示します。
3. **適用** をクリックします。
4. 必要なら、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 の設定 ページの設定

設定	説明
シリアルオーバー LAN を有効にする	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 の設定 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 の設定 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** ページの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 の設定 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 時間は秒で測定されます。

文字送信しきい値	iDRAC は、このしきい値に設定した文字数を受け取ると、文字を含む SOL 文字データパッケージを送信します。しきい値は文字数で測定されます。

表 5-31 シリアルオーバー LAN の設定 詳細設定 ページのボタン

ボタン	説明
印刷	画面に表示されている **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** ページの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 の設定 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、変更は瞬時に反映されます。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** の順にクリックして、**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
   - SSH - SSH 設定については 表 5-33 を参照
   - Telnet - Telnet 設定については 表 5-34 を参照
   - 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
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 ウェブサーバーの設定

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。
現在のセッション数	システムの現在のセッション数(**最大セッション数** 以下)。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。タイムアウト時間の範囲は 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数	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)。タイムアウト時間の範囲は 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数	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)。タイムアウト時間の範囲は 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損された場合、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** の順にクリックして、**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。

   次に、例を示します。

   `C:\Updates\V1.0\<イメージ名>.`

   デフォルトのファームウェアイメージ名は **firmimg.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。アップロードを完了するまでに、数分かかることがあります。

     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。

- **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正しくアップロードされ、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

  - イメージが正しく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選択されています。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損された場合、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損を検知した場合、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 のウェブベースのインタフェースにログインします。

3. **システムツリーで Chassis**(シャーシ)をクリックします。

4. **Update**(アップデート)タブをクリックします。**Updatable Components**(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 での iDRAC の使用

Integrated Dell™ Remote Access Controller ファームウェア バージョン 1.11 ユーザー 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、その他のデバイスを制御するために必要な全情報に共通するデータベースを管理しています。会社で 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、Active Directory ソフトウェアで 既存のユーザーに iDRAC のユーザー特権を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 通りの方法で定義できます。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でき、標準スキーマソリューションを使うと、Active Directory のグループオブジェクトのみを使用できます。

拡張スキーマと標準スキーマの長所と短所

Active Directory を使用して iDRAC へのアクセスを設定する場合は、拡張スキーマソリューションか標準スキーマソリューション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場合の長所は次のとおりです。

- すべてのアクセス制御オブジェクトを Active Directory で管理可能。
- 特権レベルの異なる iDRAC でユーザーアクセスを設定する際の最大限の柔軟性。

標準スキーマソリューションを使用する場合の長所は次のとおりです。

- 標準スキーマでは Active Directory オブジェクトのみが使用されるためスキーマ拡張が不要。
- Active Directory 側での設定が簡単。

拡張スキーマ Active Directory の概要

拡張スキーマの Active Directory を有効にする方法は 3 通りあります。

- iDRAC ウェブインタフェースの使用。「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 を設定する方法」を参照してください。
- RACADM CLI ツールの使用。「RACADM を使用して拡張スキーマ Active Directory で iDRAC を設定する方法」を参照してください。
- SM-CLP コマンドラインの使用。「SM-CLP を使用して拡張スキーマ Active Directory で iDRAC を設定する方法」を参照してください。

Active Directory スキーマ拡張

Active Directory データは、属性とクラスの分散データベースです。Active Directory スキーマには、データベースに追加または挿入するデータタイプを決定する規則があります。ユーザークラスは、データベースに保存されるクラスの一例です。ユーザークラスの属性の例としては、ユーザーの名、姓、電話番号などがあります。会社は、自社環境に特有のニーズを満たすための独自の属性とクラスを追加することで、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とクラスを加えて、機能を拡張しました。

既存の Active Directory スキーマに追加した属性やクラスは、それぞれ固有の ID で定義する必要があります。業界で固有の ID を維持するため、Microsoft は Active Directory オブジェクト識別子(OID)のデータベースを管理して、会社がスキーマに拡張を追加する際に、それが固有なもので互いに競合しないことが保証されるように図っています。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とクラスについて固有の OID、固有の拡張子、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 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

デルでは、さまざまな顧客環境に柔軟に対応できるように、ユーザーが達成したい成果に応じて設定できるプロパティを用意しています。デルは、関連、デバイス、権限のプロパティを加えて、このスキーマを拡張しました。関連プロパティは、特定の権限セットを持つユーザーまたはグループを 1 台または複数台の RAC デバイスにリンクするために使用します。このモデルでは、ユーザー、RAC 権限、およびネットワーク上の RAC デバイスを組み合わせる際に最大限の柔軟性が得られる一方、複雑になり過ぎることはありません。

Active Directory オブジェクトの概要

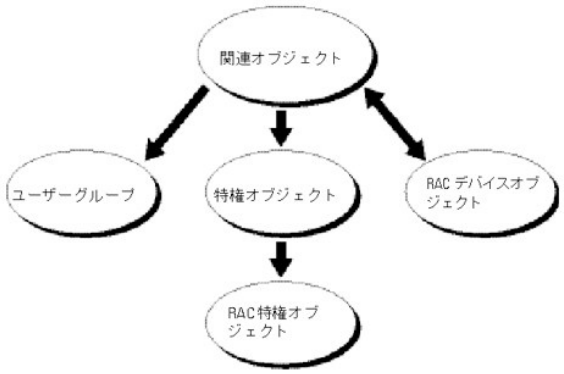
認証と許可のために Active Directory に統合するネットワーク上の物理 RAC の 1 台につき、少なくとも 1 個ずつ関連オブジェクトと RAC デバイスオブジェクトを作成しておきます。関連オブジェクトは必要なだけいくつでも作成でき、各関連オブジェクトにリンクできるユーザー、ユーザーグループ、RAC デバイスオブジェクトの数にも制限はありません。ユーザーと RAC デバイスオブジェクトは、企業内のどのドメインのメンバーでもかまいません。

ただし、各関連オブジェクトは 1 つの権限オブジェクトにしかリンクできず、ユーザー、ユーザーグループ、RAC デバイスオブジェクトを 1 つの権限オブジェクトにしかリンクできません。この例では、システム管理者は特定の RAC で各ユーザーの権限を制御できます。

RAC デバイスオブジェクトは、Active Directory に照会して認証と許可を実行するための RAC ファームウェアへのリンクです。RAC をネットワークに追加した場合、システム管理者は RAC とそのデバイスオブジェクトをその Active Directory 名で設定して、ユーザーが Active Directory で認証と認可を実行できるようにする必要があります。ユーザーが認証できるためには、システム管理者が 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、関連オブジェクトがすべての認証と認可に必要な関連付けを提供する仕組みを示しています。

図 6-1 Active Directory オブジェクトの典型的なセットアップ



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。

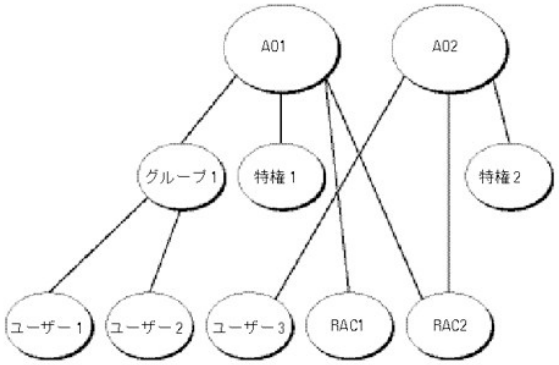
作成する関連オブジェクトの数に制限はありません。ただし、RAC(iDRAC)で認証と許可を実行するには、関連オブジェクトを少なくとも 1 つ作成する必要があり、Active Directory と統合するネットワーク上の各 RAC(iDRAC)に RAC デバイスオブジェクトが 1 つ必要です。

関連オブジェクトに含むことができるユーザー、グループ、RAC デバイスオブジェクトの数に制限はありません。ただし、関連オブジェクトに含むことができる権限オブジェクトは、関連オブジェクト 1 つに 1 つだけです。関連オブジェクトは RAC に「特権」のある「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。たとえば、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、ユニバーサルスコープで関連オブジェクトを作成します。Dell Schema Extender Utility で作成されたデフォルトの関連オブジェクトはドメインローカルグループであり、他のドメインからのユニバーサルグループとは連動しません。

図 6-2 単一ドメインでの Active Directory オブジェクトの設定



単一ドメイン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 つの権限オブジェクト(権限 1 と権限 2)を作成し、権限 1 にはすべての権限(システム管理者)、権限 2 にはログイン権限を与えます。

4. ユーザー 1 とユーザー 2 をまとめてグループ 1 とします。

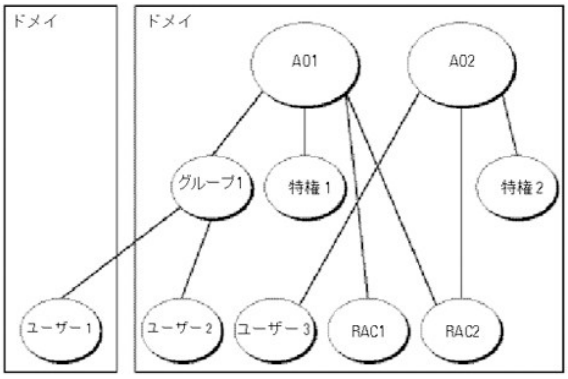
5. グループ 1 をメンバーとして関連オブジェクト 1(AO1)に、権限 1 を権限オブジェクトとして AO1 に、そして RAC1、RAC2 を RAC デバイスとして AO1 にそれぞれ追加します。

6. また、ユーザー 3 をメンバーとして関連オブジェクト 2(AO2)に、権限 2 を権限オブジェクトとして AO2 に、そして RAC2 を RAC デバイスとして AO2 に追加します。

詳細については、「Active Directory への 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 に存在し、ユーザー 2 とユーザー 3 はドメイン 2 に存在しています。このシナリオでは、両方の 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 複数ドメインでの Active Directory オブジェクトの設定



複数ドメインのシナリオでオブジェクトを設定するには、次の手順を実行してください。

1. ドメインのフォレスト機能がネイティブまたは Windows 2003 モードになっていることを確認します。

2. 2 つの関連オブジェクト AO1(ユニバーサルスコープの)と AO2 をいずれか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 つの権限オブジェクト(権限 1 と権限 2) を作成し、権限 1 にはすべての権限(システム管理者)、権限 2 にはログイン権限を与えます。

5. ユーザー 1 とユーザー 2 をまとめてグループ 1 とします。グループ 1 のグループスコープはユニバーサルでなければなりません。

6. グループ 1 をメンバーとして関連オブジェクト 1(AO1)に、権限 1 を権限オブジェクトとして AO1 に、そして RAC1、RAC2 を RAC デバイスとして AO1 にそれぞれ追加します。

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

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 を参照)

2. Active Directory ユーザーおよびコンピュータのスナップイン を拡張します(「Active Directory ユーザーとコンピュータスナップインへの Dell 拡張のインストール」を参照)。

3. 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」 を参照)。

4. SSL を各ドメインコントローラで有効にします(ドメインコントローラの SSL を有効にする を参照)。

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

Active Directory スキーマの拡張

Active Directory スキーマを拡張すると、Dell の組織単位、スキーマのクラスと属性、サンプル権限、および関連オブジェクトが Active Directory スキーマに追加されます。スキーマを拡張するには、ドメインフォレストのスキーママスター FSMO(Flexible Single Master Operation)ロールオーナーのスキーマ管理者権限が必要です。

次のいずれかの方法でスキーマを拡張できます。

- Dell Schema Extender ユーティリティ
- LDIF スクリプトファイル

LDIF スクリプトファイルを使用すると、デルの組織単位は追加されません。

LDIF ファイルおよび 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\LDIF_Files**

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

Schema Extender または LDIF ファイルのコピーと実行はどの場所からでもできます。

Dell Schema Extender の使用

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

1. **ようこそ** 画面で、**次へ** をクリックします。
2. 警告を読んでから、もう一度 **次へ** をクリックします。
3. **資格情報で現在のログの使用** を選択するか、スキーマ管理者権限でユーザー名とパスワードを入力します。
4. Dell Schema Extender を実行するには、**次へ**をクリックします。
5. **完了** をクリックします。

   スキーマが拡張されます。スキーマの拡張を確認するには、Microsoft 管理コンソール(MMC)と Active Directory スキーマスナップインを使用して、次のものがあることを確認します。

   - クラス(「表 6-2」～「表 6-7」を参照)。
   - 属性(「表 6-8」)

   MMC で Active Directory のスキーマスナップインを有効にして使用する方法については、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
SuperClasses	dellProduct
属性	dellSchemaVersion dellRacType

表 6-4 dellAssociationObject クラス

OID	**1.2.840.113556.1.8000.1280.1.1.1.2**
説明	Dell 関連オブジェクトを表します。この関連オブジェクトはユーザーとデバイスを結び付けます。
クラスの種類	構造体クラス
SuperClasses	グループ
属性	dellProductMembers dellPrivilegeMember

表 6-5 dellRAC4Privileges クラス

OID	**1.2.840.113556.1.8000.1280.1.1.1.3**
説明	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
SuperClasses	なし
属性	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

表 6-6 dellPrivileges クラス

OID	**1.2.840.113556.1.8000.1280.1.1.1.4**
説明	デルの権限(承認権限)のコンテナクラスとして使用されます。
クラスの種類	構造体クラス
SuperClasses	ユーザー
属性	dellRAC4Privileges

表 6-7 dellProduct クラス

OID	**1.2.840.113556.1.8000.1280.1.1.1.5**
説明	すべての Dell 製品が派生するメインクラス。
クラスの種類	構造体クラス
SuperClasses	コンピュータ
属性	dellAssociationMembers

表 6-8 Active Directory スキーマに追加された属性のリスト

属性名 / 説明	**割り当てられる 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 この属性に属する dellRacDevices オブジェクトのリスト。この属性は dellAssociationMembers バックワードリンクへのフォワードリンクです。 リンク ID: 12070	1.2.840.113556.1.8000.1280.1.1.2.2 識別名 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

dellIsLoginUser ユーザーにデバイスへのログイン権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.3 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin ユーザーにデバイスのカード設定権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.4 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin ユーザーにデバイスのユーザー設定権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.5 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
delIsLogClearAdmin ユーザーにデバイスのログクリア権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.6 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser ユーザーにデバイスのサーバーリセット権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.7 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser ユーザーにデバイスのコンソールリダイレクト権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.8 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser ユーザーにデバイスの仮想メディア権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.9 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser ユーザーにデバイスのテスト警告ユーザー権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.10 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin ユーザーにデバイスのデバッグコマンド管理者権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.11 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion スキーマの更新に現在のバージョンが使用されます。	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 タイプで dellAssociationObjectMembers フォワードリンクへのバックワードリンクです。	1.2.840.113556.1.8000.1280.1.1.2.13 大文字小文字の区別無視の文字列 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers この製品に属する dellAssociationObjectMembers のリスト。この属性は dellProductMembers リンク属性へのバックワードリンクです。 リンク ID: 12071	1.2.840.113556.1.8000.1280.1.1.2.14 識別名 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

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

Active Directory でスキーマを拡張する場合は、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、インストール過程で **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** オプションを選択すると、スナップインを拡張できます。Systems Management Software のインストールの手順については、『Dell OpenManage ソフトウェアクイックインストールガイド』を参照してください。

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

Administrator Pack のインストール

Active Directory iDRAC オブジェクトを管理している各システムに Administrator Pack をインストールする必要があります。Administrator Pack をインストールしないと、コンテナ内の Dell RAC オブジェクトを表示できません。

詳細については、「Active Directory ユーザーとコンピュータの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の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、次の手順に従います。

1. ドメインコントローラにログインしている場合は、**スタート**→**管理ツール**→**Active Directory ユーザーとコンピュータ** の順にクリックします。

   ドメインコントローラにログインしていない場合は、適切な Microsoft Administrator Pack がローカルシステムにインストールされている必要があります。この Administrator Pack をインストールするには、**スタート**→ **実行** の順にクリックし、MMC と入力して **<Enter>** を押します。

   Microsoft 管理コンソール(MMC)ウィンドウが表示されます。

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て **追加** をクリックします。

5. **閉じる** をクリックして **OK** をクリックします。

Active Directory への 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、次の手順に従います。

- RAC デバイスオブジェクトの作成
- 特権オブジェクトの作成
- 関連オブジェクトの作成
- 関連オブジェクトへのオブジェクトの追加

RAC デバイスオブジェクトの作成

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

2. Select **新規**→ **Dell RAC オブジェクト** を選択します。

   新規オブジェクト ウィンドウが表示されます。

3. 新しいオブジェクトの名前を入力します。この名前は、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 を設定する方法 の手順 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: 権限オブジェクトは、関係する関連オブジェクトと同じドメインに作成する必要があります。

1. **コンソールのルート**(MMC)ウィンドウでコンテナを右クリックします。

2. **新規**→ **Dell RAC オブジェクト** の順に選択します。

   新規オブジェクト ウィンドウが表示されます。

3. 新しいオブジェクトの名前を入力します。

4. **権限オブジェクト** を選択します。

5. **OK** をクリックします。

6. 作成した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 権限** タブをクリックして、ユーザーに与える権限を選択します(詳細は「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。関連スコープは関連オブジェクトのセキュリティグループの種類を指定します。関連オブジェクトを作成する場合は、追加するオブジェクトの種類に適用される関連スコープを選択します。

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

1. **コンソールのルート**(MMC)ウィンドウでコンテナを右クリックします。
2. **新規→ Dell RAC オブジェクト** の順に選択します。

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

関連オブジェクトへのオブジェクトの追加

関連オブジェクトプロパティ ウィンドウを使用すると、ユーザーまたはユーザーグループ、権限オブジェクト、RAC デバイスまたは RAC デバイスグループ間の関連付けができます。Windows 2000 モード以降のシステムを使用している場合は、ユニバーサルグループを使ってユーザーまたは RAC オブジェクトでドメインを拡張する必要があります。

ユーザーおよび RAC デバイスのグループを追加できます。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、**プロパティ** を選択します。
2. **ユーザー** タブを選択して、**追加** を選択します。
3. ユーザーまたはユーザーグループの名前を入力し、**OK** をクリックします。

権限オブジェクト タブをクリックして、システムで認証するときにユーザーまたはユーザーグループの権限を定義する関連を権限オブジェクトに追加します。関連オブジェクトに追加できる権限ブジェクトは 1 つだけです。

権限の追加

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. 権限オブジェクト名を入力し、**OK** をクリックします。

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

RAC デバイスまたは RAC デバイスグループの追加

RAC デバイスまたは RAC デバイスグループを追加するには、次の手順に従います。

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

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 を設定する方法

1. サポートされているウェブブラウザのウィンドウを開きます。
2. 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** の順にクリックします。
4. **設定** タブをクリックして、**Active Directory**を選択します。
5. **Active Directory メインメニュー** ページで、**Active Directory の設定** を選択し、**次へ** をクリックします。
6. 全般設定セクションでは以下の操作を行います。
   e. **Active Directory を有効にする** チェックボックスをオンにします。
   f. **ルートドメイン名** を入力します。**ルートドメイン名** はフォレストのルートドメインの完全修飾名です。
   g. **タイムアウト**時間を秒単位で入力します。
7. Active Directory スキーマの選択セクションで **拡張スキーマの使用** をクリックします。
8. 拡張スキーマの設定セクションでは、以下の操作を行います。
   a. **DRAC 名** を入力します。この名前は、ドメインコントローラで作成した RAC オブジェクトの共通名と同じにしてください(「RAC デバイスオブジェクトの作成」の「手順 3」を参照)。
   b. **DRAC ドメイン名** を入力します(例、iDRAC.com)。NetBIOS 名を使用しないでください。**DRAC ドメイン名** は、RAC デバイスオブジェクトがあるサブドメインの完全修飾ドメイン名です。
9. **適用** をクリックして Active Directory の設定を保存します。
10. **Active Directory メインメニューに戻る** をクリックします。
11. ドメインフォレストのルート 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、証明書ファイルの場所まで移動します。

    メモ: アップロードする証明書の相対ファイルパスが **ファイルパス** の値に表示されます。正しいファイル名とファイル拡張子を含む完全な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 によって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でルート CA 証明書を使用可能にします(ドメインコントローラルート CA 証明書のエクスポート を参照)。

    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** の順にクリックします。
14. **設定** タブをクリックし、**ネットワーク** をクリックします。
15. **ネットワーク設定** で **DHCP を使用(NIC IP アドレス用)** が選択されている場合は、**DHCP を使用 を選択して DNS サーバーアドレスを取得** を選択します。

    DNS サーバーの IP アドレスを手動で入力するには、**DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスをオフにし、プライマリおよび代替 DNS サーバーの IP アドレスを入力します。
16. **変更の適用** をクリックします。

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

RACADM を使用して拡張スキーマ Active Directory で iDRAC を設定する方法

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 共通名>
```

```
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 <プライマリ DNS IP アドレス>

racadm config -g cfgLanNetworking -o cfgDNSServer2 <セカンダリ DNS IP アドレス>
```

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

SM-CLP を使用して拡張スキーマ Active Directory で iDRAC を設定する方法

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 共通名>

set /system1/sp1/oemdell_ssl1 oemdell_certtype=AD

load -source <ActiveDirectory 証明書 TFTP URI> /system1/sp1/oemdell_ssl1

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=<プライマリ DNS IP アドレス>

set /system1/sp1/enetport1/lanendpt1/ipendpt1/\
dnsendpt1/remotesap1 dnsserveraddress=<セカンダリ 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になります。Active Directory 側では、標準グループオブジェクトがロールグループとして使用されます。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。指定した iDRAC へのアクセスをこのユーザーに与えるには、役割グループ名とそのドメイン名を特定の 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、ロールグループの権限レベルを、表 6-9 はロールグループのデフォルト設定を示したものです。

図 6-4 Microsoft Active Directory と標準スキーマを使用して iDRAC を設定する方法

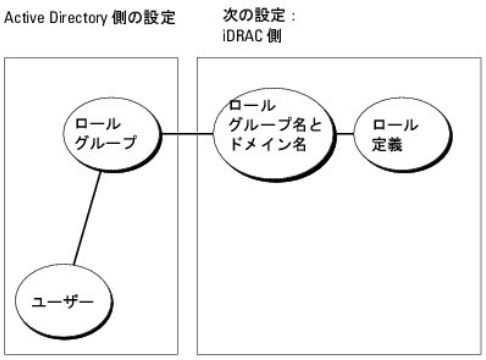


表 6-9 ロールグループのデフォルト権限

デフォルトの権限レベル	許可する権限	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: ビットマスク値の使用は、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 通りの方法があります。

- iDRAC ウェブユーザーインタフェースの使用。「標準スキーマ Active Directory とウェブインタフェースを使用して iDRAC を設定する方法」を参照してください。
- RACADM CLI ツールの使用。「標準スキーマ Active Directory と RACADM を使用して iDRAC を設定する方法」を参照してください。

iDRAC にアクセスするために標準スキーマ Active Directory を設定する方法

Active Directory ユーザーが iDRAC にアクセスできるためには、まず次の手順に従って 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。ウェブインタフェース、RACADM、または SM-CLP を使用してグループ名とドメイン名を iDRAC で設定する必要があります(「標準スキーマ Active Directory とウェブインタフェースを使用して iDRAC を設定する方法」または「標準スキーマ Active Directory と RACADM を使用して iDRAC を設定する方法」を参照)。
3. iDRAC にアクセスする Active Directory グループのメンバーとして Active Directory ユーザーを追加します。

標準スキーマ Active Directory とウェブインタフェースを使用して iDRAC を設定する方法

1. サポートされているウェブブラウザのウィンドウを開きます。
2. 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** の順にクリックして、**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、**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操作を行います。
   a. **Active Directory を有効にする** チェックボックスをオンにします。
   b. **ルートドメイン名** を入力します。**ルートドメイン名** はフォレストのルートドメインの完全修飾名です。
   c. **タイムアウト** の時間を秒単位で入力します。

7. Active Directory スキーマの選択セクションで **標準スキーマの使用** をクリックします。

8. **適用** をクリックして Active Directory の設定を保存します。

9. I標準スキーマ設定セクションの **ロールグループ** 列で **ロールグループ** をクリックします。

   ロールグループの設定 ページが表示されます。このページには、ロールグループの **グループ名**、**グループドメイン**、**ロールグループの権限** が含まれています。

10. **グループ名** を入力します。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** はフォレストのルートドメインの完全修飾名です。

12. **ロールグループの権限** で、グループの権限を設定します。

    表 5-10 に**ロールグループの権限** を示します。

    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、ロール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、証明書ファイルの場所まで移動します。

    メモ: アップロードする証明書の相対ファイルパスが **ファイルパス** の値に表示されます。正しいファイル名とファイル拡張子を含む完全な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 によって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 を参照）。

    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** の順にクリックします。

19. **設定** タブをクリックし、**ネットワーク** をクリックします。

20. **ネットワーク設定** で **DHCP を使用（NIC IP アドレス用）**が選択されている場合、**DHCP を使用 を選択して DNS サーバーアドレスを取得** を選択します。

    DNS サーバーの IP アドレスを手動で入力するには、**DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスをオフにし、プライマリおよび代替 DNS サーバーの IP アドレスを入力します。

21. **変更の適用** をクリックします。

    これで 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 と RACADM を使用して iDRAC を設定する方法

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 <役割グループの共通名>

   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 <プライマリ DNS IP アドレス>

racadm config -g cfgLanNetworking -o cfgDNSServer2 <セカンダリ DNS IP アドレス>
```

標準スキーマ Active Directory と SM-CLP を使用して iDRAC を設定する方法

メモ: 証明書は SM-CLP では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 コマンドを使用してください。

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 共通名>

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 <ActiveDirectory 証明書 TFTP URI> /system1/sp1/oemdell_ssl1

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/\
dnsendpt1/remotesap1 dnsserveraddress=<プライマリ DNS IP アドレス>

->cd /system1/sp1/enetport1/lanendpt1/ipendpt1
dnsendpt1/remotesap1 dnsserveraddress=<プライマリ DNS IP アドレス>
```

ドメインコントローラの SSL を有効にする

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、次の手順に従っ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. ドメインコントローラに Microsoft エンタープライズのルート CA をインストールします。
   a. **スタート→ コントロールパネル→ プログラムの追加と削除** の順に選択します。
   b. **Windows コンポーネントの追加と削除** を選択します。
   c. **Windows コンポーネント ウィザード** で、**証明書サービス** チェックボックスをオンにします。
   d. **CA の種類** で **エンタープライズのルート CA** を選択して **次へ** をクリックします。
   e. **この CA の共通名** を入力して **次へ** をクリックし、**完了** をクリックします。
2. 各コントローラの SSL 証明書をインストールして、各ドメインで SSL を有効にします。
   a. **スタート→ 管理ツール→ ドメインセキュリティポリシー** をクリックします。
   b. **公開キーのポリシー** フォルダを展開し、**自動証明書要求の設定** を右クリックして**自動証明書要求** をクリックします。
   c. **自動証明書要求の設定ウィザード** で **次へ** をクリックし、**ドメインコントローラ** を選択します。
   d. **次へ** をクリックして、**完了** をクリックします。

ドメインコントローラルート CA 証明書のエクスポート

メモ: システムで Windows 2000 を実行している場合は、次の手順が異なる可能性があります。

1. Microsoft Enterprise CA サービスを実行しているドメインコントローラを見つけます。
2. **スタート→ファイル名を指定して実行** の順にクリックします。
3. **ファイル名を指定して実行** のフィールドに「mmc」と入力し、**OK** をクリックします。
4. **コンソール 1**（MMC）ウィンドウで、**ファイル**（または Windows 2000 マシンでは**コンソール**）をクリックし、**スナップインの追加と削除** を選択します。
5. **スナップインの追加と削除** ウィンドウで **追加** をクリックします。
6. **スタンドアロンスナップイン** ウィンドウで **証明書** を選択して **追加** をクリックします。
7. **コンピュータ** アカウントを選択して **次へ** をクリックします。
8. **ローカルコンピュータ** を選択して **完了** をクリックします。
9. **OK** をクリックします。
10. **コンソール 1** ウィンドウで、**証明書** フォルダを展開し、**パーソナル** フォルダを展開して、**証明書** フォルダをクリックします。
11. ルート CA 証明書を見つけて右クリックし、**すべてのタスク** を選択して **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** を選択し、**いいえ、秘密キーをエクスポートしない** を選択します。
13. **次へ** をクリックし、フォーマットとして **Base-64 エンコード X.509 (.cer)** を選択します。
14. **次へ** をクリックし、場所を選択して証明書を保存します。
15. 手順 14 に保存したした証明書を iDRAC にアップロードします。

    RACADM を使って証明書をアップロードするには、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 を設定する方法 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ウェブ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メインメニュー** ページで **サーバー証明書のアップロード** を選択して、**適用** をクリックします。

f. **証明書のアップロード** 画面で、次のいずれかの手順を実行します。
   - **参照** をクリックして、証明書を選択します。
   - **値** フィールドで証明書のパスを入力します。.

g. **Apply**(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: システムで Windows 2000 が実行されている場合は、次の手順は異なっている可能性があります。

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

   独自の証明書をインストールした場合は、その証明書に署名する CA が **信頼できるルート認証局** リストにあるかどうか確認してください。この認証局がリストにない場合、それを使用するすべてのドメインコントローラにインストールする必要があります。
5. **次へ** をクリックし、証明書の種類に基づいて証明書の保存場所を Windows に自動的に選択させるか、希望の場所まで参照します。
6. **完了** 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、ドメイン名ともに空白スペースや特殊文字(\, /, or @ など)は使用できません。

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

よくあるお問い合わせ(FAQ)

表 6-10よくあるお問い合わせの一覧を掲載しています。

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。
混在モード(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)において、Active Directory を使って iDRAC にログインできますか?	はい。混在モードでは、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。 Dell 拡張の Active Directory ユーザーとコンピュータスナップインは混在モードの場合、ドメイン間

	でオブジェクトを作成するために、モードを確認し、ユーザー制限を行います。
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の機能レベルは、ネイティブか Windows 2003 モードであることが必要です。また、関連オブジェクト、RAC ユーザーオブジェクト、および RAC デバイスオブジェクト（関連オブジェクトを含む）にあるグループはユニバーサルグループでなければなりません。
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）をいくつかのドメインに分散できますか?	関連オブジェクトと権限オブジェクトは同じドメインの中に置く必要があります。この 2 種類のオブジェクトは、デル拡張の Active Directory ユーザーとコンピュータのスナップインによって、強制的に同一のドメインに作成されます。その他のオブジェクトは別のドメインに作成することができます。
ドメインコントローラの SSL 設定に何か制限はありますか？	はい。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。	RAC 証明書の生成jに Microsoft 証明書サービスを使用している場合、証明書の作成時に **ウェブ証明書** ではなく誤って **ユーザー証明書** を選択してしまった可能性があります。 回復するには、CSR を生成し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 {filename}] 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？この問題はどのようにトラブルシューティングできますか？	1. ログインに NetBIOS 名でなく、正しいユーザードメイン名が使用されていることを確認します。 2. ローカル 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。 ログインした後、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**、**ルードメイン名**、および **DRAC / MC ドメイン名** が Active Directory の環境設定と一致していることを確認します。 f. 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

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 1.11 ユーザー ガイド

この項では、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、ローカルのコンソールにリモートからグラフィックモードまたはテキストモード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。

日常的なメンテナンスを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、リモートから即座に他のユーザーと情報を共有することもできます。

コンソールリダイレクトの使用

メモ: コンソールリダイレクトセッションを開いたとき、管理下サーバーはそのコンソールがリダイレクトされていることを示しません。

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その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、リモートでソフトウェアのインストールを実行できます。

コンソールリダイレクトセッションには次の規則が適用されます。

- 同時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。
- 管理下システムのウェブブラウザからコンソールリダイレクトセッションを開始しないでください。
- 1 MB/秒以上 のネットワーク帯域幅が必要です。

サポートされている画面解像度とリフレッシュレート

表 7-1 は、管理下システムで実行しているコンソールリダイレクトセッションでサポートされている 画面解像度と、そのリフレッシュレートを示しています。

表 7-1 サポートされている画面解像度とリフレッシュレート

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

管理ステーションの設定

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

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

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

   - 対応ウェブブラウザの設定
   - Firefox を使用している場合、または Internet Explorer で Java ビューアを使用する場合は、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。

- 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、ローカルコンソールでサーバーを選択すると、サーバーのコンソール解像度がリセットされることがあります。サーバーで Linux オペレーティングシステムを実行している場合は、ローカル画面で X11 コンソールが表示されない可能性があります。iKVM で <Ctrl><Alt><F1> キーを押すと、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ています。
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	コンソールリダイレクトを有効または無効にする場合にクリックします。 **チェックボックスがオン** の場合は、コンソールリダイレクトが有効です。 **チェックボックスがオフ** の場合は、コンソールリダイレクトが無効です。 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最大セッション数（**1** または **2**）が表示されます。コンソールリダイレクトの最大セッション数を変更するには、ドロップダウンメニューを使用します。デフォルトは **2** です。
アクティブセッション数	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するネットワークポート番号。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は、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は、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。
ビデオ暗号化有効	**チェックボックスがオン** の場合は、ビデオ暗号化が有効です。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オフ** の場合は、ビデオ暗号化が無効です。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る場合があります。**
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 環境で実行している場合は、**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上で Internet Explorer を使用している場合は、次のビューアから選択できます。 ActiveX - The ActiveX コンソールリダイレクト ビューア Java - Java コンソールリダイレクト ビューア **メモ:** Java ビューアを使用するには、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オンの場合は、コンソールリダイレクト中 iKVM モニターへの出力は無効になります。これにより、**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仮想メディアを使用する方法については、「仮想メディアの設定と使用法」を参照してください。

コンソールリダイレクトの設定 ページには、表 7-5 に示すボタンがあります。

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の設定** ページを印刷します。

更新	**コンソールリダイレクト設定** ページを再ロードします。
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セッションを開くと、Dell デジタル KVM ビューアアプリケーションが開始し、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 に示す情報を使用してコンソールリダイレクトセッションが使用可能であることを確認します。

   表示されているプロパティ値の設定を変更する場合は、「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有効	はい / いいえ
ビデオ暗号化有効	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セッション数を表示します。
現在のセッション数	現在アクティブなコンソールリダイレクトセッション数を表示します。
マウスモード	現在有効なマウスアクセラレータが表示されます。**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が表示されます。 **ActiveX** - Active-X ビューアが起動します。Active-X ビューアは、Windows のオペレーティングシステム上で実行する場合、Internet Explorer でのみ使用できます。 **Java** - Java ビューアが起動します。Java ビューアは、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で実行している場合は、Java ビューア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 を使用して iDRAC にアクセスする場合は、プラグインタイプに Active-X または Java のどちらかを選択できます。
ローカルコンソール	ローカルコンソールが無効になっていない場合は、チェックボックスがオフです。チェックボックスがオンの場合は、シャーシで iKVM 接続を使用しているユーザーがコンソールにアクセスできません。

メモ: コンソールリダイレクトで仮想メディアを使用する方法については、「仮想メディアの設定と使用法」を参照してください。

コンソールリダイレクト ページには、表 7-5 に示すボタンがあります。

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の設定** ページを再ロードします。
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の設定** 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な場合は、**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、メッセージボックスがいくつか表示される場合があります。アプリケーションへの不正アクセスを防ぐために、これらのメッセージボックスは 3 分間内に参照する必要があります。そうしないと、アプリケーションの再起動を要求されます。

   メモ: 以下の手順の途中で **セキュリティ警告** ウィンドウが表示された場合は、その内容を読んでから、**はい** をクリックして続行します。

   管理ステーションが iDRAC に接続し、Dell Digital KVM ビューアアプリケーションにリモートシステムのデスクトップが表示されます。

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 ビューア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に 2 つのマウスポインタを同期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。

ビデオビューアの使用

ビデオビューアは管理ステーションと管理下サーバー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、マウスやキーボードの機能を制御できます。リモートシステムに接続すると、ビデオビューアが別のウィンドウで開始します。

ビデオビューアは、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、さまざまな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、ビデオビューアが表示されたら、カラーモードの調整やマウスポインタの同期が必要になる場合があります。

表 7-6 は、ビューアで使用可能なメニューオプションについて説明しています。

表 7-6 ビューアメニューバーの選択項目

メニュー項目	項目	説明
ビデオ	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	ビューアの画面イメージを更新します。
	現在の画面のキャプチャ	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、指定した場所にファイルを保存できます。
	全画面	ビデオビューア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 **ビデオビューア** 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、**押して放す** 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、**押して放す** を選択します。
	マクロ	マクロを選択するか、マクロに指定されたホットキーを入力すると、リモートシステムでそのアクションが実行されます。ビデオビューアは、次のマクロを提供しています。 • Ctrl-Alt-Del • Alt-Tab • Alt-Esc • Ctrl-Esc • Alt-スペース • 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、クライアントのマウスがサーバーのマウスにリダイレクトされるようにカーソルを同期できます。
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。たとえば、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は、コンソールビューアが使用するネットワーク帯域幅を減らし、メディアからのデータ転送に使用する帯域幅を増やすように、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 仮想メディアの機能については、「仮想メディアの設定と使用法」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	-	**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

コンソールリダイレクトを使用してリモートの PowerEdge システムに接続する場合、リモートシステムのマウスアクセラレータ速度が管理ステーションのマウスポインタと同期せず、ビデオビューアウィンドウに 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** の順にクリックするか、<Alt><M> キーを押します。

[カーソルの同期] メニューアイテムは切り替え式です。メニューの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は、ビューア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。設定の詳細については、「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。iDRAC コンソールリダイレクト画面でマウスの矢印を制御するには、オペレーティングシステムのデフォルトのマウス設定が使用されます。

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に iDRAC を設定できます。ローカルコンソールが無効になると、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ときは、状態ドットが緑色で表示されます。

管理下サーバーのコンソールへの排他的アクセスを確保する場合は、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 に接続しているモニター、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、次の手順を実行してください。

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。詳細については、「ウェブインタフェースへのアクセス」を参照してください。
2. **システム** 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の設定** 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オンにし、**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無効にする(オフにする)場合は、**コンソールリダイレクトの設定** 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オンにし、**適用** をクリックします。

コンソールリダイレクト ページにローカルサーバービデオのステータスが表示されます。

よくあるお問い合わせ(FAQ)

表 7-7 は、よくあるお問い合わせとその回答です。

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開始できますか。	はい、開始できます。
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 秒も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に応じて別の操作を実行できるように配慮されています。
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。	いいえ。ローカルビデオを **オン** にする要求を iDRAC が受信すると、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。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とマウスは無効になるため、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。ローカルビデオのオン / オフを切り替えても、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 / オフにするために必要な権限は何ですか。	iDRAC の設定権限を持つユーザーであれば、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を取得するにはどのようにしますか。	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の設定** ページに表示されます。 RACADM CLI コマンドの **racadm getconfig -g cfgRacTuning** は、**cfgRacTuneLocalServerVideo** のオブジェクトに状態を表示します。 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が表示されます。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からシステム画面の下部が見えません。.	管理ステーションのモニターの解像度が 1280x1024 に設定されていることを確認してください。
コンソール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。詳細については、「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を実行しているときに	Dell BIOS はマウスドライバを PS/2 マウスとしてエミュレートしています。設計上、PS/2 マウスはマウスポインタの相対位置を使用するため、同期

DOS でマウスが同期しないのはなぜでしょうか。	のずれが生じます。iDRAC には USB マウスドライバが搭載されているので、マウスポインタの絶対位置と正確な追跡が可能です。iDRAC が USB の絶対的なマウスの位置を Dell BIOS に通知しても、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の設定でマウスモードを **なし** に設定してください。
Linux テキストコンソールでマウスが同期しないのはなぜでしょうか。	仮想 KVM は USB マウスドライバを必要としますが、USB マウスドライバは X-Window オペレーティングシステムでしか使用できません。
マウスの同期の問題がまだ解決しません。	コンソールリダイレクトセッションの開始前に、オペレーティングシステム用に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。マウスの同期を切り替えるには、**マウス**→ **マウスの同期** の順に選択するか、<Alt><M> キーを押します。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 コンソールリダイレクトを使ってリモートから Microsoft™ オペレーティングシステムをインストール中に、キーボードやマウスを使用できないのはなぜですか。	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らインストールすると、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 で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、コンソールリダイレクトが有効になったことをユーザーに知らせるために Microsoft によって生成されます。このメッセージが表示されないようにするには、オペレーティングシステムをリモートインストールする前に、必ずコンソールリダイレクトを BIOS でオフにしてください。
管理ステーションの Num Lock インジケータにリモートサーバーの Num Lock の状態が反映され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、管理ステーションの Num Lock の状態にかかわらず、リモートセッションが接続されたときのリモートサーバーの設定に依存します。
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、複数のセッションビューア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るからです。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に、ローカルユーザーがリモートシステムにアクセスした場合、警告メッセージが表示されますか。	いいえ。ローカルユーザーがシステムにアクセスした場合は、双方がシステムを制御できます。
コンソールリダイレクトセッションを実行するために必要な帯域幅はどれくらいですか。	良好なパフォーマンスを得るためには、5 MB/秒の接続を推奨します。最低限必要なパフォーマンスを得るためには 1 MB/秒の接続が必要です。
管理ステーションでコンソールリダイレクトを実行するために最低限必要なシステム要件を教えてください。	管理ステーションには、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

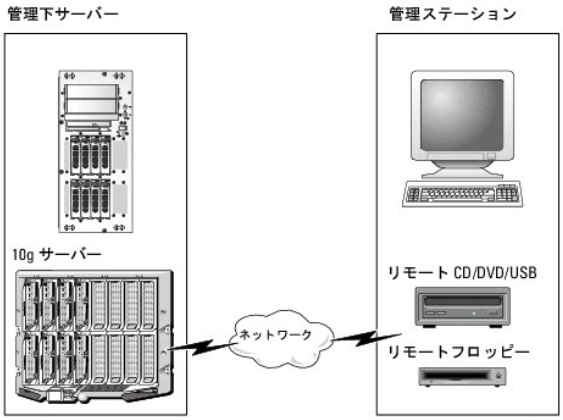
仮想メディアの設定と使用法

Integrated Dell™ Remote Access Controller ファームウェア バージョン 1.11 ユーザー ガイド

概要

コンソールリダイレクトビューアからアクセスする **仮想メディア** 機能は、ネットワーク上のリモートシステムに接続しているメディアへのアクセスを管理下サーバーに提供します。図 8-1 **仮想メディア** の全体的なアーキテクチャを示します。

図 8-1 仮想メディアの全体的なアーキテクチャ



仮想メディア を使用すると、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 およびディスケットドライブからリモートで実行できます。

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

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 2 つのデバイス(フロッピーディスクデバイスと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的なメディアまたはイメージファイルをネットワークを介して提供します。**仮想メディア** が接続していると、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のアクセス要求がネットワーク経由で管理ステーションに転送されます。**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 、サポートされている仮想フロッピーと仮想オプティカルドライブを示します。

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可能性があります。

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 光学ドライブ接続
レガシー 1.44 フロッピードライブ(1.44 フロッピーディスク)	CD-ROM、DVD、CDRW、CD-ROM メディアとのコンボドライブ
USB フロッピードライブ(1.44 フロッピーディスク)	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、Internet Explorer と ActiveX コントロールプラグインの対応バージョンをインストールします。ブラウザのセキュリティを **中** 以下に設定し、Internet Explorer が署名付き ActiveX コントロールをダウンロードできるようにします。

詳細については、「対応ウェブブラウザ」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を実行するには、表示されるセキュリティ警告に答えて ActiveX コントロールを許可します。

Linux ベースの管理ステーション

Linux オペレーティングシステムを実行している管理ステーションで仮想メディア機能を実行するには、Firefox の対応バージョンをインストールします。詳細については、「対応ウェブブラウザ」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** の順に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** の設定値の説明です。
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** - 瞬時に **仮想メディア** をサーバーに連結します。 **分離** -瞬時に **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開始している場合のみ、**仮想メディア** をサーバーに連結します。
最大セッション数	許可されている **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数	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オンの場合は、暗号化が有効で、チェックボックスがオフの場合は、暗号化が無効です。
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。指定したポートに続くポート番号を、その他の iDRAC サービスに設定することはできません。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。指定したポートに続くポート番号を、その他の iDRAC サービスに設定することはできません。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。オフの場合は、USB キードライブとして表示されます。
ブートワンスを有効にする	ブートワンスオプションを有効にするには、このボックスをオンにします。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	画面に表示されている **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しい設定を保存します。

仮想メディアの実行

注意： **仮想メディア**セッションの実行中は、**racreset** コマンドを使用しないでください。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： 仮想メディアにアクセス中、[コンソールビューア] ウィンドウアプリケーションはアクティブなままであることが必要です。

1. 管理ステーションで対応ウェブブラウザを開きます。「対応ウェブブラウザ」を参照してください。

コンソールリダイレクトと **仮想メディア** がサポートしているのは 32 ビットのウェブブラウザのみです。64 ビットウェブブラウザを使用すると、予期しない結果や故障を招きます。

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: このデバイスは仮想フロッピーとして仮想化できるので、**フロッピーイメージファイル** が **フロッピードライブ** （該当する場合）の下に表示されることがあります。1 台のオプティカルドライブと 1 つのフロッピーを同時に選択するか、1 台のドライブだけを選択することができます。

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

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

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で起動します。

5. **メディア**→ **仮想メディアウィザード...** の順にクリックします。

   [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。メディアが接続している場合は、別のメディアソースに接続する前に切断してください。切断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横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を 1 つと、**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は、（ローカルコンピュータ上の）イメージ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横にある接続ボタン** をクリックします。

   メディアは接続し、[状態] ウィンドウが更新されます。

9. **閉じる** ボタンをクリックします。

仮想メディアの切断

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. 切断する メディアの横にある **接続解除** をクリックします。

   メディアは切断され、[状態] ウィンドウが更新されます。

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 を使用すると、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、BIOS セットアップウィンドウを開き、仮想ドライブが有効になっており、正しい順序で表示されていることを確認します。

BIOS 設定を変更するには、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 設定ウィンドウを開きます。

3. 起動シーケンスをスクロールして、<Enter> キーを押します。

   ポップアップウィンドウに、仮想オプティカルデバイス と仮想フロッピードライブのリストがその他の標準起動デバイスと共に表示されます。

4. 仮想ドライブが有効で、起動メディアの最初のデバイスとして表示されていることを確認してください。必要に応じて、画面の指示に従って起動順序を変更します。

5. 変更を保存して終了します。

   管理下サーバーが再起動します。

   管理下サーバーは起動順序に従って、ブータブルデバイスからの起動を試みます。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。起動メディアがない場合は、起動メディアのない物理デバイスの場合と同様にデバイスを無視します。

仮想メディアを使用したオペレーティングシステムのインストール

ここでは、管理ステーションに手動でインタラクティブにオペレーティングシステムをインストールする方法について説明します。完了までに数時間かかる場合があります。**仮想メディア** を使用してスクリプトでオペレーティングシステムをインストールする手順では 15 分以内で完了します。詳細については、「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. 次の点を確認します。
   - 管理ステーションの CD ドライブにオペレーティングシステムのインストール CD が挿入されている。
   - ローカルの 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. 「仮想メディアからの起動」の起動手順に従って、BIOS がインストール元の CD ドライブから起動するように設定されていることを確認してください。
3. 画面の指示に従ってセットアップを完了します。

サーバーのオペレーティングシステムが実行しているときの仮想メディアの使用

Windows ベースシステム

Windows システムでは、仮想メディアドライブは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 からの仮想ドライブの使い方は、物理ドライブの場合とほぼ同じです。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構成によっては、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があります。ドライブが自動的にマウントされない場合は、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とその回答です。

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。どうしてでしょうか。	ネットワークのタイムアウトが発生すると、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て接続を中断します。 仮想メディアの設定を iDRAC ウェブインタフェースまたはローカル RACADM コマンドで変更した場合、設定変更が適用されると、接続しているすべてのメディアが切断されます。 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については、対応オペレーティングシステム のリストを参照してください。.
どのウェブブラウザが iDRAC をサポートしていますか。	対応ウェブブラウザについては、対応ウェブブラウザ のリストを参照してください。
時々クライアントの接続が切れるのはなぜですか。	• ネットワークが低速であるか、クライアント CD ドライブで CD を交換した場合は、クライアントの接続が途切れることがあります。たとえば、クライアントの CD ドライブで CD を交換した場合、新しい CD には自動開始機能が備わっている可能性があります。この場合、クライアントシステムが CD を読み込み準備に時間がかかりすぎて、ファームウェアがタイムアウトになり、接続が途切れることがあります。接続が途切れた場合は、GUI から再接続して、その前の操作を続けることができます。 • ネットワークのタイムアウトが発生した場合、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って、他の人が仮想メディアの設定を変更した可能性があります。仮想ドライブに再接続するには、**仮想メディア** 機能を使用します。
Windows オペレーティングシステムのインストールに時間がかかりすぎるようです。どうしてでしょうか。	『Dell 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ーによって iDRAC ウェブインタフェースへのアクセスに時間がかかることがあります。インストールウィンドウにインストールプロセスが表示されていないのに、インストールが進行しています。
フロッピードライブまたは USB メモリキーの内容を見ているのですが、同じドライブを使って仮想メディア接続を確立し	仮想フロッピードライブへの同時アクセスはできません。ドライブの仮想化を試みる前にドライブの内容を表示するアプリケーションを閉じてください。

ようとすると、接続エラーメッセージが表示されて再試行を求められます。どうしてでしょうか。	
仮想デバイスを起動デバイスとして設定するにはどうしますか。	管理下サーバーの [BIOS 設定] にアクセスして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見つけて、必要に応じてデバイスの起動順序を変更します。たとえば、CD ドライブから起動するには、その CD ドライブを起動順序の最初のドライブとして設定してください。
どのタイプのメディアから起動できますか。	iDRAC では、以下のブータブルメディアから起動できます。 • CDROM/DVD データメディア • ISO 9660 イメージ • 1.44 フロッピーディスクまたはフロッピーイメージ • オペレーティングシステムがリムーバブルディスクとして認識した USB キー • USB キーイメージ
USB キーをブータブルにするには、どうしますか。	**support.dell.com** で、Dell USB キーをブータブルにするための Windows プログラム、Dell 起動ユーティリティを検索してください。 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。たとえば、DOS プロンプトで次のコマンドを入力します。 `sys a: x: /s` x: は、ブータブルにする USB キーです。 Dell 起動ユーティリティを使用して、ブータブル USB キーを作成することもできます。このユーティリティは Dell ブランドの USB キーとしか互換性がありません。ユーティリティをダウンロードするには、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** で R122672.exe を検索してください。

Red Hat® Enterprise Linux® または SUSE® Linux オペレーティングシステムを実行しているシステムでは、仮想フロッピーを検索できません。仮想メディアが連結しているのに、リモートフロッピーに接続してしまいます。どうすればよいでしょうか。	一部の Linux バージョンは仮想フロッピードライブと仮想 CD ドライブを同じ方法で自動マウントしません。仮想フロッピードライブをマウントするには、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。仮想フロッピードライブを見つけてマウントするには、次の手順を実行してください。
	
	1. Linux コマンドプロンプトウィンドウを開き、次のコマンドを入力します。
	
	`grep "Virtual Floppy" /var/log/messages`
	
	2. そのメッセージの最後のエントリを探し、その時刻を書きとめます。
	3. Linux のプロンプトで次のコマンドを入力します。
	
	`grep "hh:mm:ss" /var/log/messages`
	このコマンドで、
	
	hh:mm:ss は、grep から返されたメッセージのタイムスタンプです。
	
	4. 手順 3 で、grep コマンドの結果を読み、DELL 仮想フロッピー のデバイス名を探します。
	5. 仮想フロッピードライブに接続していることを確認します。
	6. Linux のプロンプトで次のコマンドを入力します。
	
	`mount /dev/sdx /mnt/floppy`
	
	このコマンドで、
	
	/dev/sdxはステップ 4 で見つけたデバイス名です。
	
	/mnt/floppy はマウントポイントです。

仮想フロッピードライブまたは仮想フラッシュでサポートされているファイルシステムの種類を教えてください。	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すると、サーバーの仮想ドライブが削除されました。どうしてでしょうか。	ファームウェアのアップデートによって 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 1.11 ユーザー 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 iDRAC の管理機能へのアクセスを提供します。RACADM を使用すると、iDRAC ウェブインタフェースと同じ機能にアクセスできます。RACADM はスクリプトで使用して複数のサーバーと iDRAC の設定を簡易化する一方、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。つまり、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 を設定する方法については、「複数の iDRAC の設定」を参照してください。

この項には次の情報が記載されています。

- 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>
```

オプションを使用しなければ、RACADM コマンド によって一般的な使用情報が表示されます。RACADM サブコマンド一覧を表示するには、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と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 は、RACADM で実行できる各 RACADM サブコマンドについて説明しています。構文と有効なエントリを含む RACADM サブコマンドの詳細については、「RACADM サブコマンドの概要」のリストを参照してください。

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の 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 の時刻を表示します。
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	IP 設定、ハードウェアモデル、ファームウェアバージョンおよびオペレーティングシステム情報を含む 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 トレースログを表示します。-i と共に使用すると、iDRAC のトレースログ内のエントリ数を表示します。
help	iDRAC サブコマンドを一覧にします。

help <サブコマンド>	指定したサブコマンドの使用ステートメントを一覧にします。
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 設定を指定します。
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 で iDRAC に電子メールを送信させます。
testtrap	iDRAC NIC で iDRAC に SNMP 警告を送信させます。
vmdisconnect	仮想メディア接続を強制終了します。

RACADM ユーティリティを使用した iDRAC の設定

この項では、RACADM を使用して、さまざまな iDRAC 設定タスクを実行する方法を説明します。

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 に編成され、オブジェクトには 値 があります。

グループとオブジェクトの詳細については、「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。

iDRAC グループの全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と値を表示するには、次のコマンドを入力します。

```
racadm getconfig -g <グループ>
```

たとえば、**cfgLanNetworking** グループのオブジェクト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と、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。それまでに行った変更がすべて失われます。

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 **root** のみで、パスワードは **calvin** になります。

メモ: ユーザーは経時的に有効にしたり、無効にしたりできます。その結果、ユーザーが各 iDRAC に異なるインデックス番号を持つ場合があります。

iDRAC のプロパティデータベースには、最大 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。)手動で iDRAC ユーザーを有効にする前に、現在のユーザーが存在しているかどうか確認してください。

コマンドプロンプトで次のコマンドを入力すると、ユーザーが存在するかどうかがわかります。

```
racadm getconfig -u <ユーザー名>
```

または

1 ～ 16 の各インデックスに 1 回ずつ次のコマンドを入力します。

```
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と、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 が現在値と共に表示されます。対象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そのインデックス番号は使用可能です。「= 」の後に名前が表示された場合は、インデックスがそのユーザー名に割り当てられています。

iDRAC ユーザーの追加

新しいユーザーを 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 へのログイン特権のある「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、次のいずれかのコマンドを使用します。

```
racadm getconfig -u john

racadm getconfig -g cfgUserAdmin -i 2
```

権限のある iDRAC ユーザーを有効にする

ユーザーに特定の管理者権限（役割ベース）を与えるには、**cfgUserAdminPrivilege** プロパティを、表 9-2 に示した値から構成されるビットマスクに設定します。

表 9-2 ユーザー権限を表すビットマスク

ユーザー権限	権限ビットマスク
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

たとえば、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、0x00000002、0x00000004、0x00000008、0x00000010 の値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 -i 2 0x0000002E
```

iDRAC ユーザーの削除

RACADM を使用している場合は、ユーザーを手動で個別に無効にする必要があります。設定ファイルを使用してユーザーを削除することはできません。

次の例では、RAC ユーザーの削除に使用できるコマンド構文を示します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <インデックス> ""
```

二重引用符の（""）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を使用すると、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を介して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 と 電子メール警告のオプション が設定されていることを確認してください。詳細については、「電子メール警告の設定」を参照してください。

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 とトラップのオプションが正しく設定されていることを確認してください。これらのオプションを設定するには、**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、次のコマンドを使って **cfgNicUseDhcp** オブジェクトを記述し、この機能を有効にします。

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

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の詳細については、「LAN」を参照してください。

次に、LAN ネットワークプロパティの設定に入力できるコマンドの例を示します。

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

racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5

racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6

racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1

racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002

racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

メモ: **cfgNicEnable** を **0** に設定すると、DHCP が有効の場合でも 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。詳細については、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> は次のいずれかです。

      - 2(**ユーザー**)
      - 3(**オペレータ**)

- 4(**システム管理者**)

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

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

b. 必要に応じて、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。詳細については、IPMI 2.0 仕様を参照してください。

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

<鍵> は有効な 16 進数形式の 20 文字からなる暗号鍵です。

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 最低特権レベルは、IPMI SOL をアクティブにするために最低限必要な権限を決定します。詳細については、IPMI 2.0 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更新します。

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

<レベル> は次のいずれかです。

- 2(**ユーザー**)
- 3(**オペレータ**)
- 4(**システム管理者**)

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場合、SOL ボーレートが管理下システムのボーレートと同じであることを確認してください。

b. 次のコマンドを使用して IPMI SOL のボーレートを更新します。

```
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。

次に、例を示します。

```
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。

メモ: SOL は個々のユーザーに対して有効または無効にできます。

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

<ID> はユーザーの一意な ID です。

PEF の設定

各プラットフォーム警告に対し iDRAC が講じる処置を設定できます。表 9-3 は、RACADM で識別される可能な処置と値のリストです。

表 9-3 プラットフォームイベントの処置

処置	値
処置は不要	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」を参照)で、<処置値> は「表 9-3」から取得した値です。

たとえば、プロセッサの重大なイベントが検出されたときに、PEF がシステムを再起動して IPMI 警告を送信できるようにするには、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、PET をインデックス 4 で有効にするには、次のコマンドを入力します。

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 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. コミュニティ名の文字列を設定します。

   コマンドプロンプトで、次のコマンドを入力します。

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

   <名前> は PET コミュニティ名です。

電子メールアラートの設定

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 cfgEmailAlert -o cfgEmailAlertEnable -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。電子メールの送信先インデックスは 1～4 の値が可能です。

   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のオプションを設定します。

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

   1 は電子メール送信先のインデックスで、<電子メールアドレス> は、プラットフォームイベント警告を受け取る送信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 アドレス範囲と比較します。

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

cfgRacTuneIpRangeMask プロパティは着信 IP アドレスと **cfgRacTuneIpRangeAddr** プロパティの両方に適用されます。結果が同じ場合は、着信ログイン要求に 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要求にはエラーが返されます。

次の式の値がゼロに等しい場合は、ログインに進みます。

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

& は数量のビットワイズ AND で ^ はビットワイズ XOR です。

cfgRacTuning プロパティの全リストは、「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が決まります。 このプロパティはビットワイズ and と **cfgRacTuneIpRangeMask** を使用して、許可する IP アドレスの上位ビットを決定します。IP アドレスの上位ビットにこのビットパターンが含まれるすべての IP アドレスにログインが許可されます。この範囲外の IP アドレスからのログインはエラーになります。各プロパティのデフォルト値は、192.168.1.0 ～ 192.168.1.255 のアドレス範囲からのログインを許可しています。
cfgRacTuneIpRangeMask	IP アドレスの有意ビット位置を定義します。マスクは、重要なビットをすべて 1 にし、下位ビットでは 1 つの遷移ですべて 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** の順にクリックします。
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** と **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 フィルタを設定します。

メモ: RACADM と RACADM コマンドの詳細については、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。

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 進数では 11111100b に相当します。

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** は必ずネットマスク形式で設定してください。最重要ビットがすべて(マスクのサブネットを定義)する 1 で、下位ビットではすべて 0 になります。
- 必要な範囲の基底アドレスを **cfgRacTuneIpRangeAddr** の値として使用します。このアドレスの 32 ビットのバイナリ値は、マスクにゼロがある下位ビットがすべてゼロになります。

IP ブロックの設定

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します。

IP ブロックには次の機能が含まれます。

- 許可するログイン失敗回数(**cfgRacTuneIpBlkFailcount**)
- これらの失敗の時間枠(秒)(**cfgRacTuneIpBlkFailWindow**)
- 許可する合計失敗回数を超えてブロックされた IP アドレスのセッション確立が阻止される秒数(**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、失敗履歴がクリアされて、内部カウンタがリセットされます。

メモ: クライアント IP アドレスからのログイン試行が拒否されると、SSH に「ssh exchange identification: Connection closed by remote host」というメッセージが表示される場合があります。

cfgRacTune プロパティの全リストは、「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。

ログイン再試行制限のプロパティ に、ユーザー定義のパラメータを示します。

表 9-5 ログイン再試行制限のプロパティ

プロパティ	定義
cfgRacTuneIpBlkEnable	IP ブロック機能を有効にします。 一定時間内に(**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)。失敗回数がこの制限値を超えると、カウンタはリセットされます。
cfgRacTuneIpBlkPenaltyTime	ログイン失敗回数の制限を越えた 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阻止します。

```
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阻止します。

```
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: この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 設定を変更した場合、既存のすべてのセッションは、警告なく終了します。

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>
```

たとえば、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 コマンドの全リストは、「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 データベースの値が含まれたテキストファイルです。RACADM **getconfig** サブコマンドを使用して iDRAC の現在の値が含まれた設定ファイルを生成できます。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プレーンテキストファイルです。有効なファイル名なら何でも使用できますが、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。

- テキストエディタで作成可能
- RACADM **getconfig** サブコマンドで iDRAC から取得
- RACADM **getconfig** サブコマンドで iDRAC から取得して編集

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、プレーンテキストエディタで設定ファイルを編集します。**racadm** ユーティリティは ASCII テキストのみを解析します。フォーマットすると、パーサが混乱して iDRAC データベースが破損する可能性があります。

この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、行の最初の列で開始する必要があります。その他の列にある # の文字は、単に # 文字として処理されます。

  例:

  ```
  #
  # This is a comment (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。

  グループ名を示す開始の **[** 文字は、一列目で始まる必要があります。このグループ名はそのグループ内の他のオブジェクトよりも前に指定する必要があります。関連するグループ名が含まれていないオブジェクトは、エラーを生成します。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 で定義したように、設定データはグループに分類されています。

  次に、グループ名、オブジェクト、およびオブジェクトのプロパティ値の使用例を示します。

  例:

  ```
  [cfgLanNetworking] (グループ名)
  cfgNicIpAddress=143.154.133.121 (オブジェクト名)
  ```

- パラメータは、object、=、値 の間に空白を入れずに「object=値」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変更されません。= の右側の文字はすべてそのまま解釈されます（たとえば 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。

  ユーザーは使用するインデックスを指定できません。インデックスがすでに存在する場合は、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しい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すると、インデックスグループを手動で作成できます。
racadm config -g <グループ名> -o <アンカー付きオブジェクト> -i <インデックス> <固有アンカー名>

- 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、手動でインデックスオブジェクトを削除する必要があります。

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

メモ: NULL 文字列（2 つの "" 文字）は、指定したグループのインデックスを削除するように iDRAC に命令します。

  インデックス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。次は、現在のインデックス付きグループの例です。

  [cfgUserAdmin]

  cfgUserAdminUserName=<ユーザー名>

- パーサーがインデックス付けされたグループを見つけた場合、これはさまざまなインデックスとの差を表す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 設定されたときに簡単な変更が加えられたものです。変更されたオブジェクトが新しいインデックスを表す場合、設定中にその iDRAC のインデックスが作成されます。

- 設定ファイルで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と削除が繰り返されるため、グループは次第に使用中のインデックスと未使用インデックスで断片化してくる可能性があります。インデックスが存在する場合は、変更されます。インデックスが存在しない場合は、最初に使用できるインデックスが使用されます。この方法では、管理されているすべての RAC 間でインデックスを正確に一致させる必要のない場合に、インデックス付きエントリを追加できるという柔軟性が得られます。新しいユーザーは、最初に使用可能なインデックスに追加されます。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は、1 つの iDRAC で正しく解析および実行される設定ファイルが別の iDRAC でも正しく実行されるとは限りません。

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場合は、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> エントリを含め、"[" 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。

次に、例を示します。

```
#

# Object Group (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更新されます。

```
#

# Object Group (オブジェクトグループ) "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored (コメント、以下の行は無視されます)

cfgNicGateway=10.35.9.1
```

iDRAC への設定ファイルのロード

`racadm config -f <ファイル名>` のコマンドは、有効なグループと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ために設定ファイルを解析します。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 データベースを更新します。

メモ: 構文のみを検証し、iDRAC データベースを更新しない場合は、**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 を更新する前に、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、ユーザーと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できます。ロードする設定ファイルに目的のオブジェクト、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 を更新するには、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すると、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、同じプロパティの他の IDRAC を設定できます。複数の iDRAC を設定するには、次の手順に従ってください。

1. 他の iDRAC にコピーしたい設定がある 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>
   ```

   <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が必要な固有の iDRAC 情報（静的 IP アドレスなど）が含まれています。

2. 前の手順で作成した設定ファイルを編集し、コピーしたくない設定を削除またはコメントアウトします。
3. 設定したい iDRAC がある管理下サーバーのそれぞれにアクセスできる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 に次の設定を行います。
   a. 管理下サーバーにログインし、コマンドプロンプトを開始します。
   b. iDRAC の設定をデフォルト設定から変更するには、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>
      ```

      <ファイル名> は、作成した設定ファイルの名前です。ファイルが作業ディレクトリにない場合は、完全パスを含めてください。

   d. 次のコマンドを入力して、設定済みの 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 1.11 ユーザー ガイド

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

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

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 実装の標準となっています。その原動力は、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に定義された SMASH アーキテクチャです。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、ローカルの 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 専用のインタフェースであるのに対し、SM-CLP は業界標準の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 との対応付け」を参照してください。

SM-CLP を使用したシステム管理

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)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 接続と 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 機能の概要を述べます。

SM-CLP の機能

SM-CLP 仕様は、CLI を使用した単純なシステム管理に使用できる標準的な SM-CLP バーブ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発展させて、CLI を使用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、およびバーブがサポートするオプションのリストを示しています。

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のアドレス領域を移動します。	-default, -examine, -help, -output, -version

	構文: cd [オプション] [ターゲット]	
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。 ヘルプ	-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設定します。 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: set [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 は、SM-CLP オプションについて説明しています。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	実行可能な機能のすべてを実行するようにバーブに指示します。
-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 | all>
-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 アドレス領域の移動

メモ: SM-CLP アドレスパスでスラッシュ(/)とバックスラッシュ(\)は置き換え可能です。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空間に分類されたターゲットで表されます。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(\)で表されます。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移動します。たとえば、システムイベントログ(SEL)で 3 番目のレコードに移動するには、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。. .と . の機能は、Windows および Linux の場合と同様です。. . は、親レベルを参照し、. は、現在のレベルを参照します。

ターゲット

表 10-3 は、SM-CLP で使用可能なターゲットの一覧です。

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 が root アカウント。
/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と状態。

show バーブ の使用

ターゲットの詳細を知るには、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、および 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、バーブに制限できます。たとえば、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表示するには、次のコマンドのように修飾します。

```
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、指定ターゲットの下の他のレベルに **show** を実行します。たとえば、**account1** の **username** および **userid** プロパティを、**/system1/sp1** の下の **account16** ターゲットから表示する場合は、次のコマンドを入力します。

```
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、最も読みやすい出力です。**clpcsv** フォーマットはカンマ区切りの値のフォーマットで、表計算プログラムへの読み込みに適しています。**キーワード** フォーマットは、キーワード=値 のペアを 1 行に 1 つずつ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。

次の例は、SEL の内容を XML で出力する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 を使用して次の処理を実行する例を示します。

- サーバーの電源管理
- SEL の管理
- MAP ターゲットの移動
- システムプロパティの表示
- 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

サーバの電源管理

表 10-4 は、SM-CLP を使用して管理下システムの電源管理操作を実行する例を示しています。

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 管理

表 10-5 は、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ています。

表 10-5 SEL の管理操作

操作	構文
SEL の表示	->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 レコードの表示	->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 のクリア	->delete /system1/sp1/logs1 All records deleted successfully

MAP ターゲットの移動

表 10-6 は、**cd** バーブを使用して MAP をナビゲートする例を示しています。すべての例で、最初のデフォルトターゲットは / であると想定されます。

表 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 ターゲットまで移動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、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、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 コマンドはすべて瞬時に有効になります。

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、変更内容は瞬時に反映されます。

変更をコミットすると、新しいネットワーク設定が有効になり、Telnet または SSH セッションが終了します。このコミット手順を導入すると、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期できます。

表 10-7 は、SM-CLP を使用した iDRAC プロパティの設定例を示しています。

表 10-7 SM-CLP を使用した iDRAC ネットワークプロパティの設定

操作	構文
iDRAC NIC プロパティの場所へ移動します。	`->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`
変更をコミットします。	`->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
    ```

    <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のパスです。

    開いている Telnet または SSH セッションは終了します。ファームウェアアップデートが完了するまで数分かかる場合があります。

4. 新しいファームウェアが書き込まれたことを確認するには、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 に接続し、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。この機能は、シリアルストリームとネットワークパケット間の変換に **solproxy** などのユーティリティを必要とする IPMI SOL の代わりになります。iDRAC SOL の実装によって、シリアルとネットワーク間の変換は iDRAC 内で行われるため、追加のユーティリティは不要になります。

使用する Telnet または SSH コンソールは、管理下サーバーのシリアルポートから届くデータを解釈して応答できることが必要です。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-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 に接続する場合と同様に iDRAC に接続できます。その後、SOL リダイレクトは **/system1/sol1** ターゲットから開始できます。

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**→ **プログラム**→ **アクセサリ**→ **通信**→ **ハイパーターミナル** の順に選択します。
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切断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（コントロールを押しながら右の角括弧を入力して放します）。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 コマンドは使用できなくなりました。

SOL リダイレクトを終了する場合は、<Enter>、<Esc>、<T> の順に各キーを続けて押します。SSH セッションが終了します。

いったん SOL を開始すると、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 1.11 ユーザー 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。

この項では、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。

始める前に

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。

リモートシステム要件

- 各リモートシステムで iDRAC が設定されている。

ネットワーク要件

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。

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

  イメージファイルは、業界標準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。

起動イメージファイルの作成

イメージファイルをリモートシステムに導入する前に、サポートされているシステムがそのファイルから起動できることを確認してください。イメージファイルをテストするには、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 と Windows システム用のイメージファイルの作成方法について説明します。

Linux システム用の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いて次のように入力します。

```
dd if=<入力デバイス> of=<出力ファイル>
```

次に、例を示します。

```
dd if=/dev/sdc0 of=mycd.img
```

Windows システム用のイメージファイルの作成

Windows 用のデータ複製ユーティリティを選択する際、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てください。

導入の準備

リモートシステムの設定

1. 管理ステーションからアクセスできるネットワーク共有フォルダを作成します。
2. オペレーティングシステムファイルをネットワーク共有フォルダにコピーします。
3. オペレーティングシステムをリモートシステムに導入するためのブータブルな設定済み展開イメージファイルがある場合は、このステップをスキップしてください。

   設定済みのブータブルな展開イメージファイルがない場合は、このファイルを作成します。オペレーティングシステムの導入手順に使用されるプログラムやスクリプトをすべて含めます。

   たとえば、Microsoft® Windows® オペレーティングシステムを導入する場合は、Microsoft Systems Management Server (SMS) で使用される導入方法に類似するプログラムをイメージファイルに含めることができます。

   イメージファイルを作成するときは、以下の操作を行ってください。

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

- 次のいずれかの手順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。ユーティリティを使用する際の手引きとして **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 **ivmdeploy** 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(1 行に 1 つの IP アドレス)を入力しします。
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>}
```

上記のコマンドで、

- <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の詳細については、「コマンドラインオプション」を参照してください。このスクリプトの **-r** オプションの処理方法は、**ivmcli -r** オプションとは若干異なります。**-r** オプションの引数が既存のファイル名である場合、スクリプトは指定したファイルから iDRAC IP アドレスを読み取り、各行に **ivmcli** ユーティリティを一度実行します。**-r** オプションの引数が既存のファイル名でない場合は。単独の iDRAC のアドレスになります。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 イメージからのインストールのみをサポートしています。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** オプションを使用してください。

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とき、複数セッションで同一イメージメディアを共有できる。物理ドライブを仮想化するとき、1 度に 1 つのセッションが指定の物理ドライブにアクセスできる。

- 仮想メディアプラグインに対応したリムーバブルデバイスまたはイメージファイル
- iDRAC ファームウェアのブートワンス機能が有効の場合の自動終了

- セキュアソケットレイヤ(SSL)を使用した iDRAC 通信のセキュリティ保護

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

Windows システムの場合は、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、システム管理者の権限がなくても、**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権を一元的に与える手段となり、すべてのユーザーコマンドをログに記録します。iVM-CLI グループにユーザーを追加または編集する場合、システム管理者は **visudo** コマンドを使用します。システム管理者の権限がないユーザーは、**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 キットに同梱されています。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、画面の説明に従ってください。

『Systems Management Consoles CD』には、診断、ストレージ管理、リモートアクセスサービス、RACADM ユーティリティなどの最新のシステム管理ソフトウェア製品が含まれています。システム管理ソフトウェアの最新の製品情報が含まれた Readme ファイルも付いています。

さらに、『Systems Management Consoles CD』には、**ivmdeploy**(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)が含まれています。

メモ: ivmdeploy スクリプトは、インストール時に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。別のディレクトリからスクリプトを使用する場合は、一緒にすべてのファイルをコピーする必要があります。

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のオプションは RACADM ユーティリティのオプションと整合性があります。たとえば、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とおりです。

`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では、大文字と小文字が区別されます。詳細については、「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。

- 何らかの理由で iVM-CLI 接続が終了した場合。
- オペレーティングシステムのコントロールを使用して処理が手動で中止された場合。たとえば、Windows でタスク マネージャを使うと処理を終了できます。

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、ユーティリティにがターゲット iDRAC と仮想メディア接続を確立するために必要です。無効な IP アドレスまたは DDNS 名を入力すると、エラーメッセージが表示されてコマンドは終了します。

<iDRAC IP アドレス> は有効な固有の IP アドレスまたは iDRAC 動的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て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て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 {<device-name> | <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ファイルシステムパーティション番号などを含む有効なデバイスファイル名(Linux システム)です。<イメージファイル> は有効なイメージファイルのファイル名とパスです。

このパラメータは、仮想フロッピー / ディスクメディアを提供するデバイスまたはファイルを指定します。

たとえば、イメージファイルは次のように指定できます。

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

```
-f /tmp/myfloppy.img (Linux システム)
```

イメージファイルが書き込み保護されていない場合、仮想メディアはそのファイルに書き込むことができます。上書きしてはならないフロッピーイメージファイルへの書き込みを保護するようにオペレーティングシステムで設定します。

たとえば、デバイスを次のように指定します。

```
-f a:\ (Windows システム)
```

```
-f /dev/sdb4 # 4th partition on device /dev/sdb (Linux システム)
```

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

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ら、エラーメッセージが表示されてコマンドが終了します。

CD / DVD デバイスまたはイメージファイル

```
-c {<デバイス名> | <イメージファイル>}
```

<デバイス名> は有効な CD/DVD ドライブ文字(Windows システム)または有効な CD/DVD デバイスファイル名 (Linux システム)で、 <イメージファイル> は有効な ISO-9660 イメージファイルのファイル名とパスです。

このパラメータは、仮想 CD/DVD-ROM メディアを提供するデバイスまたはファイルを指定します。

たとえば、イメージファイルは次のように指定します。

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

```
-c /tmp/mydvd.img (Linux システム)
```

たとえば、デバイスは次のように指定します。

```
-c d:\ (Windows システム)
```

```
-c /dev/cdrom (Linux システム)
```

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ら、エラーメッセージが表示されてコマンドが終了します。

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

バージョン表示

```
-v
```

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

ヘルプの表示

```
-h
```

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

手動表示

-m

このパラメータは、可能なオプションすべてに関する説明が記載された iVKM-CLI ユーティリティの詳細ページを表示します。

暗号化データ

-e

このパラメータがコマンドラインに含まれていると、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 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含まれていない場合は、データ転送が暗号化されません。

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

  たとえば、大なり記号(>)の後にファイル名を入力すると、iVM-CLI ユーティリティの印刷出力で指定したファイルが上書きされます。

  メモ: VM-CLI ユーティリティは標準入力 (**stdin**)からは読み取りません。このため、**stdin** リダイレクションは不要です。

- 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。オペレーティングシステムのコマンドシェル機能を使用すると、ユーティリティをバックグラウンドで実行できます。たとえば、Linux オペレーティングシステムでは、コマンドに続いてアンパーサンド(&)を指定すると、プログラムから新しいバックグラウンドプロセスが生成されます。

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、スクリプトを継続できます(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 つ以上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用して、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 = 接続できない

2 = iVM-CLI コマンドラインエラー

3 = RAC ファームウェア接続の切断

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

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 1.11 ユーザー 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。具体的には、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を設定する、有効または無効にする
- IPMI オーバー LAN を有効または無効にする
- 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接続または切断する
- 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戻す
- 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 ソフトウェアで提供され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に iDRAC 設定ユーティリティにアクセスするには、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、Print Screen キーを押して iKVM の On Screen Configuration and Reporting(OSCAR)メニューを表示します。上向き矢印 キーと下向き矢印キーを使用してサーバーが実装されているスロットを強調表示し、Enter キーを押します。
2. サーバーの前面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.....** というメッセージが表示されたら、すぐに Ctrl キーを押しながら E キーを押します。

メモ: Ctrl-E キー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、もう一度やり直してください。

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、上向き矢印キーと下向き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。

- メニュー項目から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 キーを押してその項目にアクセスし、設定が終了したら Esc キーを押します。
- 項目に はい / いいえ、有効 / 無効 など選択可能な値がある場合は、左向き矢印 キーまたは右向き矢印キー、スペース キーを押して値を選択します。
- 編集不可能な項目は青色で表示されます。項目によっては、他の選択内容によって編集可能になるものがあります。
- 画面の下部に現在の項目の操作手順が表示されます。F1 キーを押すと現在の項目の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えたら、Esc キーを押して 終了 メニューを表示します。このメニューでは、変更の保存または無視を選択できるほか、ユーティリティに戻ることもできます。

次の項では、iDRAC 設定ユーティリティのメニュー項目について説明します。

LAN

左向き矢印、右向き矢印、スペースキーを使用して **有効** または **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。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場合、LAN が有効になっている必要があります。

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。)

Press any key to clear the message and continue.
(任意のキーを押してメッセージをクリアし、続行します。)
```

このメッセージでは、LAN が無効になっていると、iDRAC HTTP、HTTPS、Telnet、SSH ポートに直接接続されている装置にアクセスできないだけでなく、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 の再設定に使用できます。

IPMI オーバー LAN(オン / オフ)

左向き矢印、右向き矢印、スペースキーを押して **オン** または **オフ** を選択します。**オフ** を選択すると、iDRAC は LAN インタフェース経由での 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。)
```

任意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 パラメータの設定を終えた後、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

項目	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 のエクステンションです。デフォルト値は 0 を 40 個連ねたものです。
IP アドレスソース	**DHCP** または **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、サーバーの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 から取得し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 から取得した 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、最初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、最初の 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。ユーザーが DNS 内で iDRAC 名を見え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** に設定すると、Enter キーを押して **現在の DNS iDRAC 名** テキストフィールドを編集できます。iDRAC 名の編集を終えたら 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 からのドメイン名	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。

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。編集を終えたら 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

左向き矢印 と 右向き矢印 キー を使用して **節ぞkう** または **切断** を選択します。**接続** を選択すると、仮想メディアデバイスが USB バスに接続され、**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。

切断 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で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 ユーザーの設定を終えて、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

項目	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。
アカウント権限	**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、パスワードを再度入力する必要があります。

デフォルトに戻す

デフォルトに戻す メニュー項目を使用すると、iDRAC 設定項目がすべて出荷時のデフォルトに戻されます。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 キーを押して項目を選択します。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?
出荷時のデフォルト設定に戻す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 ?)

< NO (Cancel) > (<いいえ (キャンセル) >)

< YES (Continue) > (<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戻ります。

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。左向き矢印 キーを使用すると前の(古い)メッセージに移動し、右向き矢印 キー 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そ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には 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えて、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 1.11 ユーザー ガイド

ここでは、iDRAC 項目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。以下の項があります。

- 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

一部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な場合があります。このガイド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修理は試みないでください。

警告: 修理作業の多くは、認定されたサービス技術者のみが行うことができます。製品マニュアルで許可されている、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行ってください。デルの許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。

問題の兆候

ここでは、システムに問題がある可能性を示す兆候について説明します。

LED インジケータ

システム上の問題の初期兆候は、シャーシまたはシャーシに実装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、システムコンポーネント全体の状態を示します。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 で黄色の LED が点滅している場合は、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 で黄色の LED が点滅している場合、LCD メニューを使用してエラーのあるコンポーネントを特定できます。LCD の使い方については、『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 に、PowerEdge サーバー上の LED とその意味を示します。

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 が点灯していない場合、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。

ハードウェア問題の兆候

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。

- 電源が入らない

- 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、その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、次の方法で問題の解決を試みてください。

- モジュールを抜き差しして、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

これらの手順で問題が解決されない場合、『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。

その他の問題の兆候

表 13-2 問題の兆候

注目すべき点:	処置:
システム管理ソフトウェアからの警告メッセージ	システム管理ソフトウェア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。
起動時 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	前回のシステムクラッシュ画面 の表示を参照してください。
LCD のサーバー状態画面の警告メッセージ	サーバーステータス画面でエラーメッセージの確認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。

問題解決ツール

ここでは、特にリモートで問題解決を試みる場合、システムの問題を診断するのに使用できる iDRAC 機能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
- LCD 上のサーバー状態画面でエラーメッセージを確認
- 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システムコンポーネントの正常性状態が示されます。表 13-3 に、システム正常性インジケータの意味を示します。

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(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、重要(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をクリックすると、その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。不具合の種類の診断に役立ててください。iDRAC および CMC 情報ページには、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したイベントの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並び順に SEL を印刷します。**
ログのクリア	**SEL** をクリアします。 **メモ: ログのクリア** ボタンは、**ログのクリア** 権限がある場合にのみ表示されます。
名前を付けて保存	ポップアップウィンドウが開き、選択したディレクトリに **SEL** を保存できます。 **メモ:** Internet Explorer を使用しているときに保存中に問題が発生した場合、Microsoft™ サポートウェブサイト support.microsoft.com から Internet Explorer 用の累積セキュリティ更新プログラムをダウンロードしてください。
更新	**SEL** ページを再ロードします。

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 から返される進行状況を示すコードで、電源オンリセットからの起動順序の異なる段階を示し、システム起動に関するあらゆるエラーを診断できます。

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説明文を参照してください。

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、システム正常性状態 (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	対応処置
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。

前回のシステムクラッシュ画面 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。この機能を設定する手順については、管理下サーバーを使用して前回クラッシュ画面をキャプチャする設定 を参照してください。

前回のクラッシュ画面 ページには、システムクラッシュ前に発生したイベントに関する情報を含む最新クラッシュ画面が表示されます。前回システムクラッシュ情報は、DRAC 5 メモリに保存され、リモートアクセスできます。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 前回のクラッシュ画面ページのボタン

ボタン	対応処置
印刷	**前回のクラッシュ画面** ページを印刷します。
保存	ポップアップウィンドウが開き、選択したディレクトリに 前回クラッシュ画面 ページを保存できます。
削除	**前回のクラッシュ画面** ページを削除します。
更新	**前回のクラッシュ画面** ページを再ロードします。

メモ: 自動回復タイマーの変動により、システムリセットタイマーの値が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。詳細については、管理下サーバーを使用して前回クラッシュ画面をキャプチャする設定 を参照してください。

サーバーステータス画面でエラーメッセージの確認

LED が黄色に点滅し、特定のサーバーにエラーが発生した場合、LCD 上のメインサーバーステータス画面に影響があったサーバーを橙色でハイライトします。LCD ナビゲーションボタンを使用して、影響があるサーバーをハイライト表示し、中央のボタンをクリックします。2 行目にエラーおよび警告メッセージが表示されます。下記の表には、すべてのエラーメッセージおよびそれの重要度が示されています。

表 13-7 サービスステータス画面

重要度	メッセージ	原因
Warning (警告)	システム基板の周辺温度: システム基板の温度センサー、警告イベント	サーバー周辺温度が警告しきい値を超えました。
Critical (重要)	システム基板の周辺温度: システム基板の温度センサー、エラーイベント	サーバー周辺温度がエラーしきい値を超えました。
Critical (重要)	システム基板の CMOS バッテリー:システム基板のバッテリーセンサー、エラーがアサートされました	CMOS バッテリーが存在しないか、電圧がありません。
Warning (警告)	システム基板のシステムレベル:システム基板の電流センサー、警告イベント	電流 が警告しきい値を超えました。
Critical (重要)	システム基板のシステムレベル:システム基板の電流センサー、エラーイベント	電流 がエラーしきい値を超えました。
Critical (重要)	CPU<番号> <電圧センサー名>: CPU<番号>の電圧センサー、状態アサートがアサートされました	電圧が許容範囲を超えています。
Critical (重要)	システム基板 <電圧センサー名>: システム基板の電圧センサー、状態アサートがアサートされました	電圧が適性範囲を超えています。
Critical (重要)	CPU<番号> <電圧センサー名>: CPU<番号>の電圧センサー、、状態アサートがアサートされました	電圧が許容範囲を超えています。
Critical (重要)	CPU<番号> 状態: CPU<番号>のプロセッサセンサー、IERR がアサートされました	CPU エラー
Critical (重要)	CPU<番号> 状態: CPU<番号>のプロセッサセンサー、サーマルトリップがアサートされました	CPU が過熱状態
Critical (重要)	CPU<番号> 状態: CPU<番号>のプロセッサセンサー、構成エラーがアサートされました	不正なプロセッサタイプまたは間違った位置に取り付けられています。
Critical (重要)	CPU<番号> 状態: CPU<番号>のプロセッサセンサー、CPUの不在がアサートされました	必要な CPU が存在しません。
Critical (重要)	システム基板 Video Riser: システム基板のモジュールセンサー、デバイスの取り外しがアサートされました	必要なモジュールが取り外されました。
Critical (重要)	Mezz B<スロット番号> 状態: Mezz B のアドインカードセンサー<スロット番号>、インストールエラーがアサートされました	IO ファブリックに間違った Mezzanine カードが取り付けられています。
Critical (重要)	Mezz C<スロット番号> 状態: Mezz Cのアドインカードセンサー<スロット番号>、インストールエラーがアサートされました	I/O ファブリックに間違った Mezzanine カードが取り付けられています。
Critical (重要)	バックプレーンドライブ <番号>: バックプレーンのドライブスロットセンサー、ドライブが取り外されました	ストレージドライブが取り外されました
Critical (重要)	バックプレーンドライブ <番号>: バックプレーンのドライブスロットセンサー、ドライブ障害がアサートされました	ストレージドライブの障害
Critical (重要)	システム基板 PFault フェールセーフ: システム基板の電圧センサー、状態アサートがアサートされました	システム基板の電圧が異常レベルに達した場合に、このイベントが生成されます。
Critical (重要)	システム基板 OS ウォッチドッグ: システム基板のウォッチドッグセンサー、タイマー期限切れがアサートされました	iDRAC ウォッチドッグのタイマー期限切れ。特に処置は設定されていません。
Critical (重要)	システム基板 OS ウォッチドッグ: システム基板のウォッチドッグセンサー、再起動がアサートされました	iDRAC ウォッチドッグは、システムのクラッシュ（ホストからの応答がないためのタイマー期限切れ）を検知し、再起動の処置が設定されていますÂB
Critical (重要)	システム基板 OS ウォッチドッグ: システム基板のウォッチドッグセンサー、電源オフがアサートされました	iDRAC ウォッチドッグは、システムのクラッシュ（ホストからの応答がないためのタイマー期限切れ）を検知し、電源オフの処置が設定されていますÂB

Critical (重要)	システム基板 OS ウォッチドッグ: システム基板のウォッチドッグセンサー、電源の入れ直しがアサートされました	iDRAC ウォッチドッグは、システムのクラッシュ(ホストからの応答がないためのタイマー期限切れ)を検知し、電源入れ直しの処置が設定されていますÅB
Critical (重要)	システム基板 SEL: システム基板のイベントログセンサー、ログがいっぱいであることがアサートされました	SEL デバイスは、SEL がいっぱいになる前に 1 つしかエントリを追加できないことを検出しましたÅB
Warning (警告)	ECC 訂正可能エラー: メモリセンサー、訂正可能な ECC (<DIMM の位置>) がアサートされました	訂正可能 ECC エラー数が重要レートに達しました。
Critical (重要)	ECC 訂正不能エラー: メモリセンサー、訂正不能 ECC (<DIMM の位置>) がアサートされました	訂正不能 ECC エラーが検知されました。
Critical (重要)	I/O チャネルチェック: 重要なイベントセンサー、I/O チャネルチェック NMI がアサートされました	I/O チャネルに重要な割り込みが発生しています。
Critical (重要)	PCI パリティエラー: 重要なイベントセンサー、PCI PERR がアサートされました	PCI バスにパリティエラーが検知されました。
Critical (重要)	PCI システムエラー: 重要イベントセンサー、PCI SERR (<スロット番号または PCI デバイス ID>) がアサートされました	デバイスにより、PCI エラーが検知されました。
Critical (重要)	SBE ログ無効: イベントログセンサー、訂正可能なメモリエラーのログ無効がアサートされました	ログされるシングルビットエラーの数が多すぎると、シングルビットエラーのログは無効になります。
Critical (重要)	ログ無効: イベントログセンサー、すべてのイベントログ無効がアサートされました	すべてのエラーログは無効になります。
Non-Recoverable (回復不可)	CPU プロトコルエラー: プロセッササンサー、回復不可がアサートされました	プロセッサプロトコルが回復不可の状態になりました。
Non-Recoverable (回復不可)	CPU バスエラー: プロセッササンサー、回復不可がアサートされました	プロセッサバス PERR が回復不可の状態になりました。
Non-Recoverable (回復不可)	CPU 初期化エラー: プロセッササンサー、回復不可がアサートされました	プロセッサ初期化が回復不可の状態になりました。
Non-Recoverable (回復不可)	CPU マシンチェック: プロセッササンサー、回復不可がアサートされました	プロセッサマシンチェックが回復不可の状態になりました。
Critical (重要)	メモリスペア: メモリセンサー、冗長性喪失 (<DIMM の位置>) がアサートされました	メモリスペアの冗長性が無くなりました。
Critical (重要)	メモリミラー: メモリセンサー、冗長性喪失 (<DIMM の位置>) がアサートされました	メモリミラーの冗長性が無くなりました。
Critical (重要)	メモリ RAID: メモリセンサー、冗長性喪失 (<DIMM の位置>) がアサートされました	RAID メモリの冗長性が無くなりました。
Warning (警告)	メモリ追加: メモリセンサー、メモリの存在 (<DIMM の位置>) がアサート解除されました	増設されたメモリモジュールが取り外されました。
Warning (警告)	メモリ除去: メモリセンサー、メモリの存在 (<DIMM の位置>) がアサート解除されました	メモリモジュールが取り外されました。
Critical (重要)	メモリ構成エラー: メモリセンサー、構成エラー (<DIMM の位置>) がアサートされました	システムのメモリ構成が正しくありません。
Warning (警告)	メモリ冗長性低下: メモリセンサー、冗長性低下 (<DIMM の位置>) がアサートされました	メモリの冗長性は低下しましたが、喪失されていません。
Critical (重要)	PCIE 致命的エラー: 重要なイベントセンサー、バスの致命的エラーがアサートされました	PCIE バスに致命的なエラーが検知されました。
Critical (重要)	チップセットエラー: 致命的なイベントセンサー、PCI PERR がアサートされました	チップエラーが検出されました。
Warning (警告)	メモリ ECC 警告: メモリセンサー、OK から 非重要 (<DIMM の場所) へのステータス移行がアサートされました	訂正可能な ECC エラー率が通常率より増加しました。
Critical (重要)	メモリ ECC 警告: メモリセンサー、やや重大 から 重要 (<DIMM の場所) へのステータス移行がアサートされました	訂正可能な ECC エラー率が重要率に達しました。
Critical (重要)	POST エラー: POST センサー、メモリ非搭載	システム基板にメモリが搭載されていません
Critical (重要)	POST エラー: POST センサー、メモリ構成エラー	メモリが検出されましたが、構成不能です。
Critical (重要)	POST エラー: POST センサー、使用不可メモリエラー	メモリが構成されましたが、使用できません。
Critical (重要)	POST エラー: POST センサー、シャドウ BIOS にエラーが発生しました	システム BIOS シャドウの障害
Critical (重要)	POST エラー: POST センサー、CMOS にエラーが発生しました	CMOS の障害
Critical (重要)	POST エラー: POST センサー、DMA コントローラにエラーが発生しました	DMA コントローラの障害
Critical (重要)	POST エラー: POST センサー、割り込み信号コントローラにエラーが発生しました	割り込み信号コントローラの障害
Critical (重要)	POST エラー: POST センサー、タイマー更新が失敗しました	タイマー更新エラー
Critical (重要)	POST エラー: POST センサー、設定可能インターバルタイマーエラー	設定可能インターバルタイマーのエラー
Critical (重要)	POST エラー: POST センサー、パリティエラー	パリティエラー
Critical (重要)	POST エラー: POST センサー、SIO にエラーが発生しました	SIO の障害
Critical (重要)	POST エラー: POST センサー、キーボードコントローラにエラーが発生しました	キーボードコントローラエラー
Critical (重要)	POST エラー: POST センサー、システム管理割り込みの初期化に失敗しました	SMI(システム管理割り込み)の初期化エラー。
Critical (重要)	POST エラー: POST センサー、BIOS シャットダウンテストに失敗しました	BIOS シャットダウンテストエラー
Critical (重要)	POST エラー: POST センサー、BIOS POST メモリテストに失敗しました	BIOS POST メモリテストエラー
Critical (重要)	POST エラー: POST センサー、Dell リモートアクセスコントローラの構成に失敗しました	DRAC(Dell Remote Access Controller)の構成エラー
Critical (重要)	POST エラー: POST センサー、CPU 構成に失敗しました	CPU 構成エラー
Critical (重要)	POST エラー: POST センサー、不正メモリ構成エラー	メモリ構成が正しくありません
Critical (重要)	POST エラー: POST センサー、POST にエラーが発生しました	ビデオ初期化後の一般的エラー。
Critical (重要)	ハードウェアバージョンエラー: バージョン変更センサー、ハードウェアの非互換性がアサートされました	互換性のないハードウェアが検知されました
Critical (重要)	ハードウェアバージョンエラー: バージョン変更センサー、ハードウェアの非互換性(BMC ファームウェア)がアサートされました	ハードウェアはファームウェアとの互換性がありません。

Critical (重要)	ハードウェアバージョンエラー: バージョン変更センサー、ハードウェアの非互換性(BMC ファームウェアと CPU の不一致)がアサートされました	CPU はファームウェアとの互換性がありません
Critical (重要)	メモリ過熱: メモリセンサー、訂正可能な ECC <DIMM の位置> がアサートされました	メモリモジュールの過熱
Critical (重要)	メモリ致命的 SB CRC: メモリセンサー、訂正不能な ECC がアサートされました	South bridge メモリの障害
Critical (重要)	メモリ致命的 NB CRC: メモリセンサー、訂正不能な ECC がアサートされました	North bridge メモリの障害
Critical (重要)	ウォッチドッグタイマー: ウォッチドッグセンサー、再起動がアサートされました	ウォッチドッグタイマーがシステムを再起動させました
Critical (重要)	ウォッチドッグタイマー: ウォッチドッグ センサー、タイマー期限切れがアサートされました	ウォッチドッグタイマーが期限切れになりましたが、処置の必要なし
Warning (警告)	リンクチューニング: バージョン変更センサー、ソフトウェアまたはファイアウォールの変更がアサート解除されました	正常な NIC 操作を可能にするリンクチューニング設定のアップデートに失敗しました
Warning (警告)	リンクチューニング: バージョン変更センサー、ハードウェアの変更 <デバイスのスロット番号> がアサート解除されました	正常な NIC 操作を可能にするリンクチューニング設定のアップデートに失敗しました
Critical (重要)	リンクチューニング/フレックスアドレス: リンクチューニングセンサー、仮想 MAC アドレス (バス # デバイス # 機能 #) の設定失敗がアサートされました	このデバイスでは、フレックスアドレスを設定できません
Critical (重要)	リンクチューニング/フレックスアドレス: リンクチューニングセンサー、デバイスオプション ROM がリンクチューニングまたは アドレス (Mezz <位置>) のサポートの失敗がアサートされました	オプション ROM が Flex アドレスまたはリンクチューニングをサポートしていません。
Critical (重要)	リンクチューニング/フレックスアドレス: リンクチューニングセンサー、BMC/iDRAC からリンクチューニングまたはフレックスアドレスデータの取得に失敗 がアサートされました	BMC/iDRAC からリンクチューニングまたはフレックスアドレス情報の取得に失敗しました。

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格納されています。ログがいっぱいになると、最も古いエントリから上書きされます。

システムイベントログ(SEL)には管理下サーバーで発生するイベントのレコードが格納され、**iDRAC ログ** には iDRAC で発生するイベントのレコードが格納されます。

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** の順に クリックし、**iDRAC ログ** をクリックします。

iDRAC ログ は、表 13-8 の情報を提供します。

表 13-8 iDRAC ログページ情報

フィールド	説明
日時	日付と時刻(Dec 19 16:55:47など)。 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、システム起動の文字列として時刻が表示されます。
ソース	イベントを引き起こしたインタフェース
説明	イベントの概要と iDRAC にログインしたユーザー名。

iDRAC ログページのボタンの使用

iDRAC ログ ページには、次のボタンがあります(表 13-9 を参照)。

表 13-9 iDRAC ログボタン

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、**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 を使用しているときに保存中に問題が発生した場合、Microsoft サポートウェブサイト **support.microsoft.com** から Internet Explorer 用の累積セキュリティ更新プログラムをダウンロードしてください。
更新	**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** の順にクリックします。

メインシステムエンクロージャ

表 13-10 と 表 13-11 に、メインシステムエンクロージャのプロパティについて説明しています。

表 13-10 システム情報フィールド

フィールド	説明
説明	システムの情報を表示します。
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 13-11 自動回復フィールド

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 13-12 iDRAC プロパティについて説明しています。

表 13-12 iDRAC 情報フィールド

フィールド	説明
日時	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 台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見つけるために、iDRAC ウェブインタフェースを使用してサーバー上の青色の点滅 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** の順にクリックします。
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 が指定した秒数ほど点滅します。

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** の順にクリックします。
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

DRAC 5 には、Microsoft®Windows® や Linux 搭載システムに含まれているものと同様なネットワーク診断ツールが標準装備されています(表 13-13 を参照)。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** の順にクリックします。
2. **診断** タブをクリックします。

表 13-13 に、**診断コンソール** ページに入力できるコマンドを示します。コマンドを入力して **送信** をクリックします。デバッグの結果が **診断コンソール** ページに表示されます。

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 13-13 診断コマンド

コマンド	説明
arp	ARP (Address Resolution Protocol) テーブルの内容を表示します。ARP エントリの追加や削除はできません。
ifconfig	ネットワークインタフェーステーブルの内容を表示します。
netstat	ルーティングテーブルの内容を印刷します。
ping <IP アドレス>	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。宛先 IP アドレスをこのオプションの右にあるフィールドに入力してください。ICMP(インターネットコントロールメッセージプロトコル)エコーパケットが現在のルーティングテーブルの内容に基づいて宛先 IP アドレスに送信されます。
gettracelog	iDRAC トレースログを表示します。詳細については、gettracelogを参照してください。

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方法については、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 13-14 に、電源制御処置について説明します。
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 13-15を参照してください。

表 13-14 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正常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、システムによる電源管理を可能にする ACPI (Advanced Configuration and Power Interface) 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(ウォームブート)。
システムの電源を入れ直す	電源を切ってからシステムを再起動します(コールドブート)。

表 13-15 電源管理ページのボタン

ボタン	処置
印刷	画面に表示されている **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 ページ表示中に加え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 13-16 に、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) を掲載します。

表 13-16 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 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詳細は、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** の順にクリックし、**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 サブコマンドのリストは、『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)	次に、例を示します。
	
	`$ 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** の順にクリックします。 **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 サブコマンドのリストは、『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 Enabled = 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 Current 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。 詳細については、デフォルトに戻す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. **セットアップ** タブをクリックします。 4. 該当するサーバーの行に、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** の順にクリックします。 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したとき、ビューアの画面が空白です。	**仮想メディア** 権限があるが、**コンソールリダイレクト** 権限がない場合、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。	サーバーを取り外し、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。表示される場合は、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

Integrated Dell™ Remote Access Controller ファームウェア バージョン 1.11 ユーザー ガイド

Active Directory

Active Directory は、ユーザーデータ、セキュリティ、分散リソースのネットワーク管理を自動化する標準化された一元管理システムで、他のディレクトリとの相互動作ができるようにします。Active Directory は、分散ネットワーク環境用に特にデザインされています。

AGP

Accelerated Graphics Port の略語。グラフィックカードがメインシステムメモリに高速にアクセスできるようにするバス仕様。

ARP

アドレス解決プロトコル(Address Resolution Protocol)の略語。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

情報交換用アメリカ標準コード(American Standard Code for Information Interchange)の略語。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 の略語。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。

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。

CA

認証局(CA)は、IT 業界で認知さ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提供しています。CA には、Thawte や VeriSign などがあります。CA は CSR を受理すると、CSR に含まれる情報を調べ、検証します。申請者が CA のセキュリティ標準を満たしていると、CA はネットワークおよびインターネット経由でトランザクションを行う申請者を一意に識別する証明書を発行します。

CD

コンパクトディスク(Compact Disc)の略語。

CHAP

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

CIM

Common Information Model の略語。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

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

CLP

コマンドラインプロトコル(Command Line Protocol)の略語。

CSR

認証署名要求(Certificate signing request)の略語。

DHCP

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

DLL

Dynamic Link Library(ダイナミックリンクライブラリ) 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の特定のデバイスと通信できるように、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ることがよくあります。

DDNS

Domain Name System(ドメイン名システム)

DMTF

分散管理タスクフォース (Distributed Management Task Force) の略語。

DNS

ドメイン名システム (Domain Name System) の略語。

iDRAC

Dell® Remote Access Controller 5 の略語。

DSU

ディスクストレージユニット(Disk Storage Unit)の略語。

FQDN

完全修飾ドメイン名 (Fully Qualified Domain Names) の略語。Microsoft® Active Directory? は、64 バイト以下の FQDN しかサポートしていません。

FSMO

Flexible Single Master Operation の略語。Microsoft が拡張動作の一律性を保証する方法。

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 は一般的に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するものです。

GPIO

汎用入力 / 出力(General Purpose Input/Output)の略語。

GRUB

GRand Unified Bootloader の略語。一般的に使用される新しい Linux ローダー。

GUI

グラフィカルユーザーインタフェース(Graphical User Interface)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した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 の略語。

ID

識別子(Identifier)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

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

インターネットプロトコル(Internet Protocol)の略語。TCP/IP のネットワーク層。IP はパケットの経路選択、断片化、再構成などを行います。

IPMB

intelligent platform management bus 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 の略語。システム管理テクノロジの一部。

Kbps

1 秒あたりのキロビット数(Kilobits per second)の略語で、データ転送速度を表します。

LAN

構内通信網(Local Area Network)の略語。

LDAP

軽量ディレクトリアクセスプロトコル(Lightweight Directory Access Protocol)の略語。

LED

発光ダイオード(light-emitting diode)の略語。

LOM

構内通信網(Local Area Network)の略語。

MAC

媒体アクセス制御(Media Access Control)の略語。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

媒体アクセス制御アドレス(Media Access Control address)の略語。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

1 秒あたりのメガビット数(Megabits per second)の略語で、データ転送速度を表します。

MIB

管理情報ベース(Management Information Base)の略語。

MII

Media Independent Interface の略語。

NAS

ネットワーク接続ストレージ(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。Print Screen 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です。

POST

電源投入時自己診断(power-on self-test)の略語。コンピュータの電源を入れると、システムによって自動的に一連の診断テストが実行されます。

PPP

Point-to-Point Protocolの略語。一連のポイントツーポイントリンクを通じて、ネットワークレイヤデータグラム(IP パケットなど)の転送に使うインターネット標準プロトコル。

RAM

ランダムアクセスメモリ(random-access memory)の略語。システムおよび iDRAC の読み書き可能な汎用メモリ。

RAM fBXN

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。

RAC

Remote Access Controller の略語。

ROM

読み取り専用メモリ(Read-Only Memory)の略語。データの読み取りはできますが、書き込みはできません。

RPM

Red Hat® Package Manager の略語。Red Hat Enterprise Linux® オペレーションシステム用のパッケージ管理システムで、ソフトウェアパッケージのインストールを支援します。インストールプログラムに似ています。

SAC

Microsoft® Special Administration Console の略語。

SAP

サービスアクセスポイント(Service Access Point)の略語。

SEL

システムイベントログ(system event log)の略語。

SMI

システム管理割り込み(Systems Management Interrupt)の略語。

SMTP

簡易メール転送プロトコル(Simple Mail Transfer Protocol)の略語。システム間の電子メールの転送に使用するプロトコル。SMTP は通常、イーザネット上で使用されます。

SMWG

Systems Management Working Group(システム管理ワークグループ)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

セキュアシェル(Secure Shell)の略語。

SSL

セキュアソケットレイヤ(Secure Sockets Layer)の略語。

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。

TAP

Telelocator Alphanumeric Protocol の略語。ページャサービスに要求を送信するために使用するプロトコル。

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のプロトコルを持つ標準 Ethernet プロトコルのセットを指します。

TFTP

簡易ファイル転送プロトコル(Trivial File Transfer Protocol)の略語。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簡易ファイル転送プロトコル。

UPS

無停電電源装置 (Uninterruptible power supply) の略語。

USB

Universal Serial Bus の略語。

UTC

協定世界時(Universal Coordinated Time)の略語。「GMT」を参照してください。

VLAN

仮想構内通信網(Virtual Local Area Network)の略語。

VNC

仮想ネットワークコンピューティング(Virtual Network Computing)の略語。

VT-100

ビデオ端末(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によって使用されています。

WAN

広域通信網(Wide Area Network)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

コンソールリダイレクトとは、管理下システムのディスプレイ画面、マウス機能およびキーボード機能を管理ステーションの該当するデバイスへ転送する機能のこと。これを使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システムを制御できます。

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によって、データバス、アドレスバス、PCI バスなどと名付けられます。

目次ページに戻る

目次ページに戻る

Integrated Dell™ Remote Access Controller ファームウェア バージョン 1.11 ユーザー ガイド

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

注意: 注意は、ハードウェアの損傷やデータの損失の可能性があることを示し、その危険を回避する方法を説明しています。

_____

2008 年 6 月 Rev.A02

目次ページに戻る