Integrated Dell Remote Access Controller 7（iDRAC7）

バージョン 1.00.00 ユーザーズガイド

メモ、注意、警告

メモ: コンピュータを使いやすくするための重要な情報を説明しています。

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

警告: 物的損害、けが、または死亡の原因となる可能性があることを示しています。

2012 - 03

Rev. A00

目次

1

概要

Integrated Dell Remote Access Controller 7（iDRAC7）は、サーバー管理者の生産性を向上させ、Dell サーバーの総合的な可用性を高めるように設計されています。iDRAC7 は、管理者へのサーバー問題のアラート送信、リモートサーバー管理の実施の支援や、サーバーへの物理的なアクセスの必要性の軽減を行います。

Lifecycle Controller テクノロジを搭載した iDRAC7 は、より大きなデータセンターソリューションの一部であり、ビジネスに不可欠なアプリケーションと負荷をいつでも使用できる状態に維持するために役立ちます。このテクノロジを利用することで、管理者はエージェントを使用することなく、あらゆる場所から Dell サーバーを導入、監視、管理、設定、アップデート、トラブルシューティング、および修復することが可能になります。これらの機能は、オペレーティングシステムに依存することなく、またハイパーバイザの有無や状態にも関係なく利用できます。

IT の操作を簡素化および能率化するため、iDRAC7 および Lifecycle Controller と連動する次のような製品もあります。

- VMware vCenter 用の Dell Management プラグイン
- Dell Repository Manager
- Microsoft System Center Operations Manager（SCOM）および Microsoft System Center Configuration Manager（SCCM）用の Dell Management Packs
- BMC Bladelogic
- Dell OpenManage Essentials
- Dell OpenManage Power Center

iDRAC7 には次のタイプが用意されています。

- Basic Management with IPMI
- iDRAC7 Express
- iDRAC7 Express for Blades
- iDRAC7 Enterprise

詳細については、**support.dell.com** にある『*iDRAC7 概要および機能ガイド*』を参照してください。

iDRAC7 With Lifecycle Controller を使用するメリット

次のメリットが挙げられます。

- 可用性の向上 — 不具合発生からの復帰時間を短縮するために役立つ、エラーの可能性または実際のエラーの早期通知を行います。
- 生産性の向上および総所有コスト（TCO）の削減 — 遠隔地に多数存在するサーバーへの管理者の管理範囲を拡大は、交通費などの運用コストを削減しながら IT スタッフの生産性を向上させることができます。
- セキュアな環境 — リモートサーバーへのセキュアなアクセスを提供することにより、管理者はサーバーおよびネットワークのセキュリティを維持しながら、重要な管理作業を行うことができます。
- Lifecycle Controller による内蔵システム管理の強化 – ローカル展開においては Lifecycle Controller の GUI による展開および保守性の簡略化を提供し、リモート展開においては Dell OpenManage Essentials およびパートナーコンソールと統合された Remote Services（WS-Management）インターフェースを提供します。

Lifecycle Controller GUI の詳細については、**support.dell.com/manuals** にある『*Lifecycle Controller ユーザーズガイド*』を参照してください。またリモートサービスに関しては、『*Lifecycle Controller Remote Services ユーザーズガイド*』を参照してください。

主な機能

iDRAC7 の主要機能は次の通りです。

インベントリと監視

- 管理下サーバーの正常性の表示。
- オペレーティングシステムエージェントを使用しないネットワークアダプタおよびストレージサブシステムのインベントリと監視。
- システムインベントリの表示。
- センサー情報の表示。
- 電力消費の監視および制御。
- ブレードサーバーでは、シャーシ管理コントローラ（CMC）ウェブインタフェースの起動、CMC 情報および WWN/MAC アドレスの表示。

メモ: CMC は、M1000E シャーシ LCD パネルおよびローカルコンソール接続を介して、iDRAC7 へのアクセスを提供します。詳細については、**support.dell.com/manuals** にある『*Chassis Management Controller ユーザーズガイド*』を参照してください。

展開

- vFlash SD カードのパーティションの管理。
- 前面パネルディスプレイの設定。
- BIOS およびサポートされるネットワークとストレージアダプタの設定とアップデートが可能になる Lifecycle Controller の起動。
- iDRAC7 ネットワーク設定の管理。
- 仮想コンソールおよび仮想メディアの設定と使用。
- リモートファイル共有、仮想メディア、および VMCLI を使用したオペレーティングシステムの展開。
- 自動検出の有効化。

アップデート

- iDRAC7 ライセンスの管理。
- iDRAC7 ファームウェアのアップデートまたはロールバック。

メンテナンスとトラブルシューティング

- 電源関連の操作の実行および消費電力の監視。
- Server Administrator に依存しないアラートの生成。
- イベントデータのログ：Lifecycle ログおよび RAC ログ。
- イベント、およびより良い電子メールアラート通知のための、電子メール、IPMI、または SNMP アラートの設定。
- 前回のシステムクラッシュイメージのキャプチャ。
- 起動キャプチャビデオおよびクラッシュキャプチャビデオの表示。

セキュアな接続

重要なネットワークリソースへのアクセスのセキュア化は非常に大切です。iDRAC7 には、次のようなさまざまなセキュリティ機能が実装されています。

- セキュアソケットレイヤー（SSL）

- 署名付きファームウェアアップデート。
- Microsoft Active Directory、汎用 LDAP ディレクトリサービス、またはローカル管理のユーザー ID およびパスワードを使用したユーザー認証。
- スマートカードログイン機能を使用した 2 要素認証。2 要素認証は、物理的なスマートカードとスマートカードの PIN に基づいています。
- シングルサインオンおよび公開キー認証。
- 各ユーザーに特定の権限を設定するための役割ベースの許可。
- ユーザー ID とパスワード設定。
- SMCLP とウェブインタフェースが SSL 3.0 規格を使用して、128 ビットと 40 ビット（128 ビットが認められていない国の場合）の暗号化をサポート
- セッションタイムアウトの設定（秒数指定）。
- 設定可能な IP ポート（HTTP、HTTPS、SSH、Telnet、仮想コンソール、および仮想メディア向け）。

メモ: Telnet は SSL 暗号化をサポートせず、デフォルトで無効になっています。

- 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回数の制限により、制限を超えた IP アドレスからのログインの阻止。
- iDRAC7 に接続するクライアントの IP アドレス範囲の限定。
- Enterprise ライセンスを備えたラックサーバーおよびタワーサーバー専用のギガビットイーサネットアダプタ。

ライセンスの管理

iDRAC7 機能は、購入済みのライセンス（Basic Management、iDRAC7 Express、iDRAC7 Express for Blades、または iDRAC7 Enterprise）に基づいて利用できます。iDRAC7 の設定または使用を可能にするインタフェースで利用できるのはライセンスされた機能のみです。たとえば、iDRAC7 ウェブインタフェース、RACADM、WS-MAN, OpenManage Server Administrator などがあります。専用 NIC または iDRAC ポートカードを必要とする vFlash などの機能の一部は、200～500 サーバーシリーズ向けのオプションになっています。

iDRAC7 のライセンス管理とファームウェアアップデート機能は、iDRAC7 ウェブインタフェースと RACADM から常に利用できます。

ライセンスのタイプ

提供されるライセンスには次のタイプがあります。

- 30 日間の評価および延長 — このライセンスは 30 日後に失効しますが、期限を 30 日間延長することもできます。評価ライセンスは継続時間ベースであり、電力がシステムに供給されているときにタイマーが稼動します。
- 永続 — サービスタグにバインドされたライセンスで、永続的です。

ライセンスの取得

次のいずれかの方法を使用して、ライセンスを取得できます。

- 電子メール — テクニカルサポートセンターにライセンスを要求すると、ライセンスが添付された電子メールが送付されます。
- セルフサービスポータル — iDRAC7 から、セルフサービスポータルへのリンクを利用できます。このリンクをクリックして、インターネット上でライセンスを購入できるライセンスセルフサービスポータルを開きます。詳細については、セルフサービスポータルページのオンラインヘルプを参照してください。
- 販売時 — システムの発注時にライセンスを取得します。

ライセンス操作

ライセンス管理の作業を実行する前に、ライセンスを取得しておく必要があります。詳細については、**support.dell.com** にある『*概要および機能ガイド*』を参照してください。

メモ: すべてのライセンスが事前にインストールされているシステムを購入した場合、ライセンス管理は必要ありません。

一対一のライセンス管理には iDRAC7、RACADM、WS-MAN、および Lifecycle Controller-Remote Services を使用して、一対多のライセンス管理には Dell License Manager を使用して、次のライセンス操作を実行できます。

- 表示 — 現在のライセンス情報を表示します。
- インポート — ライセンスの取得後、ライセンスをローカルストレージに保存し、サポートされているいずれかのインタフェースを使用して iDRAC7 にインポートします。検証チェックに合格すれば、ライセンスがインポートされます。

メモ: 一部の機能では、機能の有効化にはシステムの再起動が必要になります。

- エクスポート — バックアップ目的で、あるいは部品やマザーボードを交換した後の再インストールのために、インストールされているライセンスを外部ストレージデバイスにエクスポートします。エクスポートされたライセンスのファイル名と形式は **<EntitlementID>.xml** になります。
- 削除 — コンポーネントが欠落している場合に、そのコンポーネントに割り当てられているライセンスを削除します。ライセンスが削除されると、そのライセンスは iDRAC7 に保存されず、基本的な製品機能が有効になります。
- 置き換え — 評価ライセンスの有効期限を延長したり、評価ライセンスなどのライセンスタイプを購入ライセンスに変更したり、有効期限の切れたライセンスを延長するために、ライセンスを置換します。
  - 評価ライセンスは、アップグレードされた評価ライセンスまたは購入したライセンスと置換できます。
  - 購入したライセンスは、更新されたライセンスまたはアップグレードされたライセンスと置換できます。
- 詳細表示 — インストールされているライセンス、またはサーバーにインストールされているコンポーネントに使用可能なライセンスの詳細を表示します。

メモ: 詳細オプションが正しいページを表示するため、セキュリティ設定の信頼済みサイトのリストに ***.dell.com** が追加されているようにしてください。詳細については、Internet Explorer のヘルプマニュアルを参照してください。

一対多のライセンス展開には、Dell License Manager を使用できます。詳細については、**support.dell.com/manuals** にある『*Dell License Manager ユーザーズガイド*』を参照してください。

ライセンスコンポーネントの状態または状況と使用可能な操作

次の表は、ライセンスの状態または状況に基づいて使用できるライセンス操作をリストしています。

表 1. 状態および状況に基づいたライセンス操作

ライセンス / コンポーネントの状態または状況	インポート	エクスポート	削除	置き換え	詳細表示
非システム管理者ログイン	なし	なし	なし	なし	あり
アクティブなライセンス	あり	あり	あり	あり	あり
期限切れのライセンス	なし	あり	あり	あり	あり

ライセンス / コンポーネントの状態または状況	インポート	エクスポート	削除	置き換え	詳細表示
ランセンスがインストールされているが、コンポーネントが欠落している	なし	あり	あり	なし	あり

iDRAC7 ウェブインタフェースを使用したライセンスの管理

iDRAC7 ウェブインタフェースを使用してライセンスを管理するには、**概要 サーバー ライセンス** と移動します。

ライセンス ページに、デバイスに関連付けられたライセンス、またはインストールされているもののデバイスがシステムに存在しないライセンスが表示されます。ライセンスのインポート、エクスポート、削除、または置き換えの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。

RACADM を使用したライセンスの管理

RACADM を使用してライセンスを管理するには、**ライセンス** サブコマンドを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

関連項目

- ライセンスの管理
- ライセンスのタイプ
- ライセンスの取得
- iDRAC7 でライセンス可能な機能

iDRAC7 でライセンス可能な機能

次の表に、購入したライセンスに基づいて有効化される iDRAC7 機能を示します。

表 2. iDRAC7 のライセンス可能な機能

機能	IPMI 付き Base Management	iDRAC7 Express	iDRAC7 Express for Blades	iDRAC7 Enterprise
インタフェースと標準サポート				
IPMI 2.0	あり	あり	あり	あり
ウェブインタフェース［1］	なし	あり	あり	あり
SNMP	なし	あり	あり	あり
WS-MAN	あり	あり	あり	あり
SMASH-CLP（SSH）	なし	あり	あり	あり
RACADM（SSH、ローカル、およびリモート）［1］	なし	あり	あり	あり
Telnet	なし	あり	あり	あり
接続性				
共有またはフェイルオーバーネットワークモード（ラッ	あり	あり	なし	あり

機能	IPMI 付き Base Management	iDRAC7 Express	iDRAC7 Express for Blades	iDRAC7 Enterprise
クおよびタワーサーバーのみ）				
専用 NIC	なし	なし	あり［2］	あり［2、6］
DNS	あり	あり	あり	あり
VLAN タグ付け	あり	あり	あり	あり
IPv4	あり	あり	あり	あり
IPv6	なし	あり	あり	あり
ダイナミック DNS	なし	あり	あり	あり
セキュリティと認証				
役割ベースの権限	あり	あり	あり	あり
ローカルユーザー	あり	あり	あり	あり
ディレクトリサービス（Active Directory および汎用 LDAP）	なし	なし	なし	あり
SSL 暗号化	あり	あり	あり	あり
2 要素認証［3］	なし	なし	なし	あり
シングルサインオン（SSO）	なし	なし	なし	あり
PK 認証（SSH 用）	なし	なし	なし	あり
セキュリティロックアウト	なし	あり	あり	あり
リモート管理と修正				
内蔵診断	あり	あり	あり	あり
シリアルオーバー LAN（プロキシあり）	あり	あり	あり	あり
シリアルオーバー LAN（プロキシあり）	なし	あり	あり	あり
クラッシュ画面キャプチャ	なし	あり	あり	あり
クラッシュビデオキャプチャ	なし	なし	なし	あり
起動キャプチャ	なし	なし	なし	あり
仮想メディア［4］	なし	なし	あり	あり
仮想コンソール［4］	なし	なし	あり［5］	あり
コンソールコラボレーション［4］	なし	なし	なし	あり
仮想フォルダ	なし	なし	なし	あり
仮想コンソールチャット	なし	なし	なし	あり
リモートファイル共有	なし	なし	なし	あり
vFlash［6］	なし	なし	なし	あり
vFlash パーティション［6］	なし-	なし	なし	あり

機能	IPMI 付き Base Management	iDRAC7 Express	iDRAC7 Express for Blades	iDRAC7 Enterprise
自動検出	なし	あり	あり	あり
監視と電源				
センサー監視とアラート	あり	あり	あり	あり
デバイス監視	なし	あり	あり	あり
ストレージ監視	なし	あり	あり	あり
電子メールアラート	なし-	あり	あり	あり
電源カウンタ履歴	あり	あり	あり	あり
電力制限	なし	なし	なし	あり
リアルタイムの電源監視	あり	あり	あり	あり
リアルタイムの電源グラフ	なし	あり	あり	あり
ロギング				
システムイベントログ	あり	あり	あり	あり
RAC ログ［7］	なし	あり	あり	あり
トレースログ［7］	なし	あり	あり	あり
リモート Syslog	なし	なし	なし	あり

［1］ iDRAC7 ライセンス管理およびファームウェアアップデート機能は、常に iDRAC7 ウェブインタフェースと RACADM を介して使用できます。

［2］ すべてのブレードサーバーは、常に iDRAC7 専用の NIC を使用しますが、速度は 100 Mbps に制限されます。ギガバイト Ethernet カードは、シャーシの制限によりブレードサーバーでは機能しませんが、エンタープライズライセンスのあるラックおよびタワーサーバーでは機能します。共有 LOM はブレードサーバーでは無効になります。

［3］ 2 要素認証は Active-X を介して使用できるので、Internet Explorer のみをサポートします。

［4］ 仮想コンソールと仮想メディアは Java と Active-X プラグインの両方を使って使用できます。

［5］ リモート起動付きの単一ユーザーの仮想コンソール

［6］ 一部のシステムでは、オプションの iDRAC7 ポートカードが必要です。

［7］ RAC およびトレースログは、WS-MAN を介して基本バージョンで使用できます。

iDRAC7 にアクセスするインタフェースおよびプロトコル

次の表に iDRAC7 にアクセスするインタフェースを一覧表示します。

メモ: 複数のインタフェースを同時に使用すると、予期しない結果が生じることがあります。

表 3. iDRAC7 にアクセスするインタフェースおよびプロトコル

インタフェースまたはプロトコル	説明
iDRAC 設定ユーティリティ	iDRAC 設定ユーティリティを使用して、プレオペレーティングシステム処理を実行します。iDRAC 設定ユーティリティには、他の機能とともに iDRAC7 ウェブインタフェースで使用可能な機能のサブセットが含まれます。 iDRAC 設定ユーティリティにアクセスするには、起動中に <F2> を押し、**セットアップユーティリティメインメニュー** ページで **iDRAC 設定** をクリックします。
iDRAC7 ウェブインタフェース	iDRAC7 ウェブインタフェースを使用して、iDRAC7 の管理および管理下システムの監視を行います。ブラウザは、HTTPS ポートを介してウェブサーバーに接続されます。データストリームは 128 ビット SSL を使用して暗号化され、プライバシーと整合性を提供します。HTTP ポートへの接続はすべて HTTPS にリダイレクトされます。システム管理者は、SSL CSR 生成プロセスで独自の SSL 証明書をアップロードして、ウェブサーバーをセキュア化できます。デフォルトの HTTP および HTTPS ポートは変更可能です。ユーザーアクセスはユーザー権限に基づきます。
RACADM	このコマンドラインユーティリティを使用して、iDRAC7 およびサーバーの管理を実行します。RACADM はローカルおよびリモートで使用できます。 • ローカル RACADM コマンドラインインタフェースは、Server Administrator がインストールされた管理下システムで実行されます。ローカル RACADM は、帯域内 IPMI ホストインタフェースを介して iDRAC7 と通信します。これはローカルの管理下システムにインストールされるため、このユーティリティを実行するには、ユーザーはオペレーティングシステムにログインする必要があります。ユーザーがこのユーティリティを使用するには、完全な Administrator 権限を持っているか、ルートユーザーである必要があります。 • リモート RACADM は、管理ステーションで実行されるクライアントユーティリティです。これは、管理下システムで RACADM コマンドを使用するために帯域外ネットワークインタフェースを使用し、HTTP チャネルも使用します。**–r** オプションは、ネットワークで RACADM コマンドを実行します。 • ファームウェア RACADM は、SSH または Telnet を使用して iDRAC7 にログインしすることによってアクセスできます。ファームウェア RACADM コマンドは、iDRAC7 IP、ユーザー名、またはパスワードを指定しないで実行できます。 • ファームウェア RACADM コマンドを実行するために、iDRAC7 IP、ユーザー名、またはパスワードを指定する必要はありません。RACADM プロンプトの起動後、racadm プレフィックスを付けずに直接コマンドを実行できます。
サーバー LCD パネル / シャーシ LCD パネル	サーバー前面パネルの LCD を使用して、次の操作を行うことができます。 • アラート、iDRAC7 IP または MAC アドレス、ユーザーによるプログラムが能な文字列の表示 • DHCP の設定 • iDRAC7 静的 IP 設定の設定。 ブレードサーバーでは、LCD はシャーシの前面パネルにあり、すべてのブレード間で共有されています。 サーバーを再起動しないで iDRAC をリセットするには、 ボタンを 16 秒間押し続けます。
CMC ウェブインタフェース	シャーシの監視と管理の他、CMC ウェブインタフェースでは次の操作が可能です。 • 管理下システムのステータスの表示 • iDRAC7 ファームウェアのアップデート • iDRAC7 ネットワークの設定 • iDRAC7 ウェブインタフェースへのログイン • 管理下システムの開始、停止、またはリセット • BIOS、PERC、および対応ネットワークアダプタのアップデート

インタフェースまたはプロトコル	説明
Lifecycle Controller	iDRAC7 の設定には Lifecycle Controller を使用します。Lifecycle Controller にアクセスするには、起動中に <F10> を押し、**セットアップユーティリティ → ハードウェア詳細設定 → iDRAC 設定** と移動します。詳細については、**support.dell.com/manuals** にある『*Lifecycle Controller ユーザーズガイド*』を参照してください。
Telnet	Telnet を使用して、RACADM および SMCLP コマンドを実行できる iDRAC7 にアクセスします。RACADM の詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。 SMCLP の詳細については、「SMCLP の使用」を参照してください。 **メモ:** Telnet は、セキュアなプロトコルではなく、デフォルトで無効になっています。Telnet は、パスワードのプレーンテキストでの送信を含む、すべてのデータを伝送します。機密情報を伝送する場合は、SSH インタフェースを使用してください。
SSH	SSH を使用して、RACADM および SMCLP コマンドを実行します。これは Telnet コンソールと同じ機能を提供しますが、高度なセキュリティのために暗号化トランスポート層を使用します。SSH サービスはデフォルトで、iDRAC7 で有効になっています。iDRAC7 では SSH サービスを無効にできます。iDRAC7 は、DSA および RSA ホストキーアルゴリズムを使用する SSH バージョン 2 のみをサポートします。iDRAC7 の初回起動時に、固有の 1024 ビット DSA ホストキーおよび 1024 ビット RSA ホストキーが生成されます。
IPMITool	IPMITool を使用して、iDRAC7 経由でリモートシステムの基本管理機能にアクセスします。インタフェースには、ローカル IPMI、IPMI オーバー LAN、IPMI オーバーシリアル、シリアルオーバー LAN があります。IPMITool の詳細については、**support.dell.com/manuals** にある『*Dell OpenManage Baseboard Management Controller ユーティリティユーザーズガイド*』を参照してください。
VMCLI	仮想メディアコマンドラインインタフェース（VMCLI）を使用して管理ステーション経由でリモートメディアにアクセスし、複数の管理下システムにオペレーティングシステムを展開します。
SMCLP	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（SMCLP）を使用して、システム管理タスクを実行します。これは SSH または Telnet 経由で使用できます。SMCLP の詳細については、「SMCLP の使用」を参照してください。
WS-MAN	LC-Remote Services は、WS-Management プロトコルに基づいて一対多のシステム管理タスクを実行します。LC-Remote Services 機能を使用するには、WinRM クライアント（Windows）や OpenWSMAN クライアント（Linux）などの WS-MAN クライアントを使用する必要があります。Power Shell および Python を使用して、WS-MAN インタフェースに対してスクリプトを実行することもできます。 管理用ウェブサービス（WS-Management）は、システム管理に使用されるシンプルオブジェクトアクセスプロトコル（SOAP）ベースのプロトコルです。iDRAC7 は、WS–Management を使用して Distributed Management Task Force（DMTF）の共通情報モデル（CIM）ベースの管理情報を伝送します。CIM 情報は管理下システムでの変更が可能なセマンティックスおよび情報タイプを定義します。WS-Management から使用可能なデータは、DMTF プロファイルおよび拡張プロファイルにマップされた iDRAC7 計装インタフェースによって提供されます。 詳細については、次の文書を参照してください。 • **support.dell.com/manuals** にある『Lifecycle Controller Remote Services ユーザーズガイド』。 • **support.dell.com/manuals** にある『Lifecycle Controller 統合ベストプラクティスガイド』。 • Dell TechCenter の Lifecycle Controller ページ — **delltechcenter.com/page/Lifecycle+Controller** • Lifecycle Controller WS-Management スクリプトセンター — **delltechcenter.com/page/Scripting+the+Dell+Lifecycle+Controller**

インタフェースまたはプロトコル	説明

- MOF およびプロファイル — **delltechcenter.com/page/DCIM.Library**
- DTMF ウェブサイト — **dmtf.org/standards/profiles/**

iDRAC7 ポート情報

次の情報ポートは、ファイアウォールを介してリモートで iDRAC7 にアクセスするために必要です。これらのポートは、iDRAC7 が接続のためにリッスンするポートです。

表 4. iDRAC7 が接続のためにリッスンするポート

ポート番号	機能
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
5900*	仮想コンソールのキーボードおよびマウスのリダイレクション、仮想メディア、仮想フォルダ、およびリモートファイル共有

*設定可能なポート

次の表に、iDRAC7 がクライアントとして使用するポートを示します。

表 5. iDRAC7 がクライアントとして使用するポート

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
445	共通インターネットファイルシステム（CIFS）
636	LDAP Over SSL（LDAPS）
2049	ネットワークファイルシステム（NFS）
3269	グローバルカタログ（GC）用 LDAPS

その他の必要マニュアル

本書に加え、デルサポートサイト（**support.dell.com/manuals**）の次のマニュアルは、お使いのシステムでの iDRAC7 のセットアップおよび操作に関する追加情報を提供します。**マニュアル** ページで、**ソフトウェア → システム管理** をクリックします。右側にある適切な製品リンクをクリックして、マニュアルにアクセスします。

- 『*iDRAC7 オンラインヘルプ*』には、iDRAC7 ウェブインタフェースで使用可能なフィールドの詳細情報、および iDRAC7 ウェブインタフェースの説明が記載されています。このオンラインヘルプには、iDRAC7 のインストール後にアクセスできます。

- 『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』には、RACADM サブコマンド、サポートされているインタフェース、および iDRAC7 プロパティデータベースグループとオブジェクト定義に関する情報が記載されています。
- 『*システム管理概要ガイド*』にはシステム管理タスクを実行するために使用できる様々なソフトウェアに関する簡潔な情報が記載されています。
- 『*Dell Lifecycle Controller ユーザーズガイドと Remote Services ユーザーガイド*』には、Lifecycle Controller と Remote Services の使用に関する情報がそれぞれ記載されています。
- 『Dell Remote Access 設定ツールユーザーズガイド』には、ツールを使用してネットワーク内の iDRAC IP アドレスを検出し、検出された IP アドレスに対して一対多のファームウェアアップデートおよび Active Directory 設定を実行する方法について記載されています。
- 『*Dell システムソフトウェアサポートマトリックス*』は、各種 Dell システム、これらのシステムでサポートされているオペレーティングシステム、これらのシステムにインストールできる Dell OpenManage コンポーネントについての情報を提供しています。
- 『*Dell OpenManage Server Administrator インストールガイド*』では、Dell OpenManage Server Administrator のインストール手順が説明されています。
- 『*Dell OpenManage Management Station Software インストールガイド*』では、Dell OpenManage Management Station Software（ベースボード管理ユーティリティ、DRAC ツール、Active Directory スナップインを含む）のインストール手順が説明されています。
- 『*Dell OpenManage Baseboard Management Controller Management ユーティリティユーザーズガイド*』には、IPMI インタフェースに関する情報が記載されています。
- 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。
- 「*用語集*」では、本書で使用されている用語が説明されています。

詳細については、次のシステムマニュアルを参照することができます。

- 『*iDRAC7 概要および機能ガイド*』では、iDRAC7 とそのライセンス可能機能、およびライセンスのアップグレードオプションに関する情報が記載されています。
- システムに付属している「安全にお使いただくために」には安全や規制に関する重要な情報が記載されています。規制に関する詳細な情報については、**dell.com/regulatory_compliance** にある 法規制の順守ホームページを参照してください。保証に関する情報は、このマニュアルに含まれているか、別の文書として同梱されています。
- ラックソリューションに付属の『*ラック取り付けガイド*』では、システムをラックに取り付ける方法について説明しています。
- 『*はじめに*』では、システムの機能、システムのセットアップ、および仕様の概要を説明しています。
- 『*オーナーズマニュアル*』では、システムの機能、システムのトラブルシューティング方法、およびシステムコンポーネントの取り付けまたは交換方法について説明しています。

デルへのお問い合わせ

メモ: お使いのコンピュータがインターネットに接続されていない場合は、購入時の納品書、出荷伝票、請求書、またはデルの製品カタログで連絡先をご確認ください。

デルでは、オンラインまたは電話によるサポートとサービスのオプションを複数提供しています。サポートやサービスの提供状況は国や製品ごとに異なり、国 / 地域によってはご利用いただけないサービスもございます。デルのセールス、テクニカルサポート、またはカスタマーサービスへは、次の手順でお問い合わせいただけます。

1. **support.dell.com** にアクセスします。
2. サポートカテゴリを選択します。
3. 米国在住以外のお客様は、**support.dell.com** ページ下の国コードを選択してください。**All** を選択するとすべての選択肢が表示されます。
4. 必要なサービスまたはサポートのリンクを選択します。

2

iDRAC7 へのログイン

iDRAC7 には、iDRAC7 ユーザー、Microsoft Active Directory ユーザー、または LDAP 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 および calvin です。シングルサインオンまたはスマートカードを使用してログインすることもできます。

メモ: iDRAC7 へログインするには、iDRAC へのログイン権限が必要です。

関連リンク

ローカルユーザー、Active Directory ユーザー、または LDAP ユーザーとしての iDRAC7 へのログイン
スマートカードを使用した iDRAC7 へのログイン
シングルサインオンを使用した iDRAC7 へのログイン

ローカルユーザー、Active Directory ユーザー、または LDAP ユーザーとしての iDRAC7 へのログイン

ウェブインタフェースを使用して iDRAC7 にログインする前に、サポートされているウェブブラウザ（Internet Explorer または Firefox）が設定されており、必要な権限を持つユーザーアカウントが作成されていることを確認してください。

メモ: Active Directory ユーザーのユーザー名は、大文字と小文字が区別*されません*。パスワードはどのユーザーも、大文字と小文字が区別されます。

メモ: Active Directory のほか、openLDAP、openDS、Novell eDir、および Fedora ベースのディレクトリサービスがサポートされています。「<」文字と「>」文字は、ユーザー名には使用できません。

ローカルユーザー、Active Directory ユーザー、または LDAP ユーザーとして iDRAC7 にログインするには、次の手順を実行します。

1. サポートされているウェブブラウザを開きます。
2. **アドレス** フィールドに、`https://[iDRAC IP アドレス]` を入力し、**Enter** を押します。

   メモ: 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、`https://[iDRAC7 IP アドレス]:[ポート番号]` を入力します。ここで、`[iDRAC7 IP アドレス]` は iDRAC7 IPv4 または IPv6 アドレスであり、`[ポート番号]` は HTTPS ポート番号です。

   ログイン ページが表示されます。
3. ローカルユーザーの場合は、次の手順を実行します。
   - **ユーザー名** フィールドと **パスワード** フィールドに、iDRAC7 ユーザーの名前とパスワードを入力します。
   - **ドメイン** ドロップダウンメニューから、**この iDRAC** を選択します。
4. Active Directory ユーザーの場合は、**ユーザー名** フィールドと **パスワード** フィールドに Active Directory ユーザーの名前とパスワードを入力します。ユーザー名の一部としてドメイン名を指定している場合は、ドロップダウンメニューから **この iDRAC** を選択します。ユーザー名の形式は <ドメイン>\<ユーザー名>、<ドメイン>/<ユーザー名>、または <ユーザー>@<ドメイン> にすることができます。

   たとえば、dell.com\john_doe、または JOHN_DOE@DELL.COM となります。

   ユーザー名にドメインが指定されていない場合は、**ドメイン** ドロップダウンメニューから Active Directory ドメインを選択します。

5. LDAP ユーザーの場合は、**ユーザー名** フィールドと **パスワード** フィールドに LDAP ユーザーの名前とパスワードを入力します。LDAP ログインにはドメイン名は必要ありません。デフォルトでは、ドロップダウンメニューの **この iDRAC** が選択されています。
6. **送信** をクリックします。必要なユーザー権限で iDRAC7 にログインされました。

関連リンク

ユーザーアカウントと権限の設定
対応ウェブブラウザの設定

スマートカードを使用した iDRAC7 へのログイン

スマートカードを使用して iDRAC7 にログインできます。スマートカードでは、次の 2 層構造のセキュリティを実現する 2 要素認証（TFA）が提供されます。

- 物理的なスマートカードデバイス。
- パスワードや PIN などの秘密コード。

ユーザーは、スマートカードと PIN を使用して自身の資格情報を検証する必要があります。

関連リンク

スマートカードを使用したローカルユーザーとしての CMC へのログイン
スマートカードを使用した Active Directory ユーザーとしての iDRAC7 へのログイン

スマートカードを使用したローカルユーザーとしての CMC へのログイン

スマートカードを使用してローカルユーザーとしてログインする前に、次を実行する必要があります。

- ユーザーのスマートカード証明書および信頼できる認証局（CA）の証明書を iDRAC7 にアップロードします。
- スマートカードログオンを有効化します

iDRAC7 ウェブインタフェースは、スマートカードを使用するように設定されているユーザーのスマートカードログオンページを表示します。

メモ: ブラウザの設定によっては、この機能を初めて使用するときにスマートカードリーダー ActiveX プラグインのダウンロードとインストールのプロンプトが表示されます。

スマートカードを使用してローカルユーザーとして iDRAC7 にログインするには、次の手順を実行します。

1. リンク `https://[IP アドレス]` を使用して iDRAC7 ウェブインタフェースにアクセスします。
   iDRAC7 ログイン ページが表示され、スマートカードを挿入するプロンプトが表示されます。

メモ: 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、`https://[IP アドレス]:[ポート番号]` と入力します。ここで、`[IP アドレス]` は iDRAC7 の IP アドレスで、`[ポート番号]` は HTTPS ポート番号です。

2. スマートカードをリーダーに挿入して **ログイン** をクリックします。
   スマートカードの PIN のプロンプトが示されます。パスワードは必要ありません。
3. ローカルのスマートカードユーザーのスマートカード PIN を入力します。
   これで、iDRAC6 にログインできます。

メモ: スマートカードログオンの CRL チェックの有効化 を有効にしているローカルユーザーの場合、iDRAC7 は CRL のダウンロードとユーザーの証明書の CRL の確認を試行します。証明書が失効済みとしてリストされている場合や、何らかの理由で CRL をダウンロードできない場合は、ログインに失敗します。

関連リンク

スマートカードログインの有効化または無効化
ローカルユーザー用の iDRAC7 スマートカードログインの設定

スマートカードを使用した Active Directory ユーザーとしての iDRAC7 へのログイン

スマートカードを使用して Active Directory ユーザーとしてログインする前に、次を実行する必要があります。

- 信頼できる認証局（CA）証明書（CA 署名付き Active Directory 証明書）を iDRAC7 にアップロードします。
- DNS サーバーを設定します。
- Active Directory ログインを有効にします。
- スマートカードログインを有効にします。

スマートカードを使用して iDRAC7 に Active Directory ユーザーとしてログインするには、次の手順を実行します。

1. リンク `https://[IP アドレス]` を使用して iDRAC7 にログインします。
   iDRAC7 ログイン ページが表示され、スマートカードを挿入するプロンプトが表示されます。

メモ: 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、`https://[IP アドレス]:[ポート番号]` と入力します。ここで、`[IP アドレス]` は iDRAC7 IP アドレス、`[ポート番号]` は HTTPS ポート番号です。

2. スマートカードを挿入し、**ログイン** をクリックします。
   PIN ポップアップが表示されます。
3. PIN を入力し、**送信** をクリックします。
   Active Directory の資格情報で iDRAC7 にログインされます。

メモ:

スマートカードユーザーが Active Directory に存在する場合、Active Directory のパスワードは必要ありません。

関連リンク

スマートカードログインの有効化または無効化
Active Directory ユーザーのための iDRAC7 スマートカードログインの設定

シングルサインオンを使用した iDRAC7 へのログイン

シングルサインオン（SSO）を有効にすると、ユーザー名やパスワードなどのドメインユーザー認証資格情報を入力せずに、iDRAC7 にログインできます。

関連リンク

Active Directory ユーザーのための iDRAC7 SSO ログインの設定

iDRAC7 ウェブインタフェースを使用した iDRAC7 SSO へのログイン

シングルサインオンを使用して iDRAC7 にログインする前に、次を確認してください。

- 有効な Active Directory ユーザーアカウントを使用して、システムにログインしている。
- Active Directory の設定時に、シングルサインオンオプションを有効にしている。

ウェブインタフェースを使用して iDRAC7 にログインするには、次の手順を実行します。

1. Active Directory の有効なアカウントを使って管理ステーションにログインします。
2. ウェブブラウザで、`https://[FQDN アドレス]` を入力します。

メモ: デフォルトの HTTP ポート番号（ポート 443）が変更されている場合は、`https://[FQDN アドレス]:[ポート番号]` を入力します。ここで、`[FQDN アドレス]` は iDRAC7 FQDN（iDRAC7dnsname.domain.name）であり、`[ポート番号]` は HTTPS ポート番号です。

メモ: FQDN の代わりに IP アドレスを使用すると、SSO に失敗します。

ユーザーが有効な Active Directory アカウントを使用してログインすると、iDRAC7 はオペレーティングシステムにキャッシュされた資格情報を使用して、適切な Microsoft Active Directory 権限でユーザーをログインします。

iDRAC7 ウェブインタフェースを使用した iDRAC7 SSO へのログイン

SSO 機能を使用して、CMC ウェブインタフェースから iDRAC7 ウェブインタフェースを起動できます。CMC ユーザーには、CMC から iDRAC7 を起動する場合の CMC ユーザー権限があります。ユーザーアカウントが CMC にはあるが iDRAC にはない場合でも、そのユーザーは CMC から iDRAC7 にログインできます。

iDRAC6 ネットワーク LAN が無効（LAN を有効にする = No）の場合は、SSO を利用できません。

サーバーがシャーシから取り外されている、iDRAC7 IP アドレスが変更されている、または iDRAC7 ネットワーク接続に問題が発生している場合は、CMC ウェブインタフェースの iDRAC7 起動オプションがグレー表示になります。

詳細については、**support.dell.com/manuals** にある『*Chassis Management Controller ユーザーズガイド*』を参照してください。

リモート RACADM を使用した iDRAC7 へのアクセス

RACADM ユーティリティを使用して、リモート RACADM で iDRAC7 にアクセスできます。

詳細については、**support.dell.com/manuals** にある『*iDRAC7 および CMC 向け RACADM リファレンスガイド*』を参照してください。

管理ステーションのデフォルトの証明書ストレージに iDRAC7 の SSL 証明書が保存されていない場合、RACADM コマンドを実行するときに警告メッセージが表示されます。ただし、コマンドは正常に実行されます。

メモ: iDRAC7 証明書は、セキュアなセッションを確立するために iDRAC7 が RACADM クライアントに送信する証明書です。この証明書は、CA によって発行されるか、自己署名になります。いずれの場合でも、管理ステーションで CA または署名権限が認識されなければ、警告が表示されます。

関連リンク

リモート RACADM を Linux 上で使用するための CA 証明書の検証

リモート RACADM を Linux 上で使用するための CA 証明書の検証

リモート RACADM コマンドを実行する前に、通信のセキュア化に使用される CA 証明書を検証します。

リモート RACADM を使用するために証明書を検証するには、次の手順を実行します。

1. DER フォーマットの証明書を PEM フォーマットに変換します（openssl コマンドラインツールを使用）。

   ```
   openssl x509 -inform pem -in [yourdownloadedderformatcert.crt] -outform pem
   -out [outcertfileinpemformat.pem] -text
   ```

2. 管理ステーションのデフォルトの CA 証明書バンドルの場所を確認します。たとえば、RHEL5 64-bit の場合は **/etc/pki/tls/cert.pem** です。

3. PEM フォーマットの CA 証明書を管理ステーションの CA 証明書に付加します。
   たとえば、`cat command: - cat testcacert.pem >> cert.pem` を使用します。
4. サーバー証明書を生成して iDRAC7 にアップロードします。

ローカル RACADM を使用した iDRAC7 へのアクセス

ローカル RACADM を使用した iDRAC7 へのアクセスについては、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

ファームウェア RACADM を使用した iDRAC7 へのアクセス

SSH または Telnet インタフェースを使用して、iDRAC7 にアクセスし、ファームウェア RACADM のコマンドを実行できます。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

SMCLP を使用した iDRAC7 へのアクセス

SMCLP は、Telnet または SSH を使用して iDRAC7 にログインするときのデフォルトのコマンドラインプロンプトです。詳細については、「SMCLP の使用」を参照してください。

公開キー認証を使用した iDRAC7 へのログイン

パスワードを入力せずに SSH 経由で iDRAC7 にログインできます。また、1 つの RACADM コマンドをコマンドライン引数として SSH アプリケーションに送信できます。コマンドの完了後にセッションが終了するため、コマンドラインオプションはリモート RACADM と同様に動作します。

例えば、次のとおりです。

ログイン：

```
ssh ユーザー名@<ドメイン>
```

または

```
ssh ユーザー名@<IP アドレス>
```

ここで、`IP アドレス` には iDRAC6 の IP アドレスを指定します。

RACADM コマンドの送信：

```
ssh ユーザー名@<ドメイン> racadm getversion
```

```
ssh ユーザー名@<ドメイン> racadm getsel
```

関連リンク

SSH の公開キー認証の使用

複数の iDRAC7 セッション

次の表では、各種インタフェースを使用して実行できる複数の iDRAC7 セッションのリストを提供します。

表 6. 複数の iDRAC7 セッション

インタフェース	セッション数
iDRAC7 ウェブインタフェース	4
リモート RACADM	4
ファームウェア RACADM/SMCLP	SSH - 2 Telnet - 2 シリアル - 1

3

管理下システムと管理ステーションのセットアップ

iDRAC7 を使用して帯域外システム管理を実行するには、iDRAC7 をリモートアクセス用に設定し、管理ステーションと管理対象システムをセットアップして、対応ウェブブラウザを設定する必要があります。

メモ: ブレードサーバーの場合、設定を実行する前に、CMC および I/O モジュールをシャーシに取り付けて、物理的にシステムをシャーシに取り付けます。

関連リンク

iDRAC7 IP アドレスのセットアップ
管理対象システムのセットアップ
iDRAC7 ファームウェアのアップデート
iDRAC7 ファームウェアのロールバック
管理ステーションのセットアップ
対応ウェブブラウザの設定

iDRAC7 IP アドレスのセットアップ

iDRAC7 との双方向通信を有効にするためには、お使いのネットワークインフラストラクチャに基づいて初期ネットワーク設定を行う必要があります。次のいずれかのインタフェースを使用して IP アドレスをセットアップできます。

- iDRAC 設定ユーティリティ
- Lifecycle Controller（『*Lifecycle Controller ユーザーズガイド*』を参照）
- Dell Deployment Toolkit（『*Dell Deployment Toolkit ユーザーズガイド*』を参照）
- シャーシまたはサーバーの LCD パネル（システムの『*ハードウェアオーナーズマニュアル*』を参照）

メモ: ブレードサーバーの場合、CMC の初期設定時にのみ、シャーシの LCD パネルを使用してネットワーク設定を設定できます。シャーシの導入後は、シャーシの LCD パネルを使用して iDRAC7 を再設定することはできません。

- CMC ウェブインタフェース（『*Dell Chassis Management Controller Firmware ユーザーズガイド*』を参照）

ラックサーバーとタワーサーバーの場合、IP アドレスをセットアップするか、デフォルトの iDRAC7 IP アドレス 192.168.0.120 を使用して初期ネットワーク設定を設定できます。これには、iDRAC7 の DHCP または静的 IP のセットアップも含まれます。

ブレードサーバーの場合、iDRAC7 ネットワークインタフェースはデフォルトで無効になっています。

iDRAC7 IP アドレスを設定した後、次の手順を実行します。

- *iDRAC7 IP アドレスをセットアップした後はデフォルトのユーザー名とパスワードを変更する*ようにしてください。
- 次のいずれかのインタフェースでそのアドレスにアクセスします。
  - 対応ブラウザ（Internet Explorer または Firefox）を使用した iDRAC7 ウェブインタフェース
  - セキュアシェル（SSH）— Windows 上では、PuTTY などのクライアントが必要です。ほとんどの Linux システムでは、SSH をデフォルトで利用できるため、クライントは不要です。
  - Telnet（デフォルトでは無効になっているため、有効にする必要あり）

– IPMITool（IPMI コマンドを使用）またはシェルプロンプト（『*Systems Management Documentation and Tools*』DVD または **support.dell.com** から入手できる Windows または Linux のデルカスタム化インストーラが必要。）

関連リンク

iDRAC 設定ユーティリティを使用した iDRAC IP のセットアップ
CMC ウェブインタフェースを使用した iDRAC7 IP のセットアップ
自動検出の有効化

iDRAC 設定ユーティリティを使用した iDRAC IP のセットアップ

iDRAC7 IP アドレスをセットアップするには、次の手順を実行します。

1. 管理下システムの電源を入れます。
2. Power-on Self-test（POST）中に <F2> を押します。
3. **セットアップユーティリティメインメニュー** ページで **iDRAC 設定** をクリックします。
   iDRAC 設定 ページが表示されます。
4. **ネットワーク** をクリックします。
   ネットワーク ページが表示されます。
5. 次の設定を指定します。
   – ネットワーク設定
   – 共通設定
   – IPv4 設定
   – IPv6 設定
   – IPMI 設定
   – VLAN 設定
6. **セットアップユーティリティメインメニュー** ページに戻り、**終了** をクリックします。
   ネットワーク情報が保存され、システムが再起動します。

関連リンク

ネットワークの設定
共通設定
IPv4 設定
IPv6 設定
IPMI 設定
VLAN の設定

ネットワークの設定

ネットワーク設定を行うには、次の手順を実行します。

メモ: オプションの詳細については、『*iDRAC 設定ユーティリティオンラインヘルプ*』を参照してください。

1. **NIC の有効化** で、**有効** オプションを選択します。
2. **NIC の選択** ドロップダウンメニューから、ネットワーク要件に基づいて次のポートのうちひとつを選択します。
   – 専用 — リモートアクセスデバイスが、リモートアクセスコントローラ（RAC）上で利用可能な専用ネットワークインタフェースを使用できるようにします。このインタフェースは、ホストオペレーティングシステムとは共有されず、管理トラフィックを別の物理ネットワークにルーティングします。それにより、管理トラフィックをアプリケーショントラフィックから分離することが可能になります。

このオプションは、iDRAC の専用ネットワークポートがそのトラフィックをサーバーの LOM または NIC ポートから切り離してルーティングすることを意味します。ネットワークトラフィックの管理に関しては、専用 オプションを使用すれば、LOM または NIC に割り当てられる IP アドレスと比較して、同じサブネットまたは異なるサブネットからの IP アドレスを iDRAC に割り当てることができます。

メモ: このオプションは、iDRAC7 Enterprise ライセンスを持つラックシステムまたはタワーシステム上でのみ使用できます。ブレードに対しては、デフォルトで使用可能になっています。

- LOM1
- LOM2
- LOM3
- LOM4

メモ: ラックサーバーとタワーサーバーの場合、サーバーモデルに応じて 2 つの LOM オプション（LOM1 と LOM2）または 4 つすべての LOM オプションを使用できます。ブレードサーバーでは、iDRAC7 の通信に LOM は使用されません。

3. **フェイルオーバーネットワーク** ドロップダウンメニューから、残りの LOM のひとつを選択します。ネットワークに障害が発生すると、トラフィックはそのフェイルオーバーネットワーク経由でルーティングされます。

メモ: NIC の選択 ドロップダウンメニューで **専用** を選択した場合、このオプションはグレー表示になります。

たとえば、LOM1 がダウンしたときに iDRAC7 のネットワークトラフィックを LOM2 経由でルーティングするには、**NIC の選択** に **LOM1** を、**フェイルオーバーネットワーク** に **LOM2** を選択します。

4. iDRAC7 で二重モードとネットワーク速度を自動的に設定する必要がある場合は、**オートネゴシエーション** で **オン** を選択します。このオプションは、専用モードの場合にのみ使用できます。有効にすると、iDRAC7 は、そのネットワーク速度に基づいてネットワーク速度を 10、100、または 1000 Mbps に設定します。
5. **ネットワーク速度** で、10 Mbps または 100 Mbps のどちらかを選択します。

メモ: ネットワーク速度を手動で 1000 Mbps に設定することはできません。このオプションは、**オートネゴシエーション** オプションが有効になっている場合にのみ使用できます。

6. **二重モード** で、**半二重** または **全二重** オプションを選択します。

メモ: オートネゴシエーション を有効にすると、このオプションはグレー表示になります。

共通設定

ネットワークインフラストラクチャに DNS サーバーが存在する場合は、DNS に iDRAC7 を登録します。これらは、ディレクトリサービス（Active Directory または LDAP）、シングルサインオン、スマートカードなどの高度な機能に必要な初期設定要件です。
iDRAC7 を登録するには、次の手順を実行します。

1. **DNS に DRAC を登録する** を有効にします。
2. **DNS DRAC 名** を入力します。
3. **ドメイン名の自動設定** を選択して、ドメイン名を DHCP から自動的に取得します。または、**DNS ドメイン名** を入力します。

IPv4 設定

IPv4 の設定を行うには、次の手順を実行します。

1. **IPv4 の有効化** で、**有効** オプションを選択します。
2. **DHCP の有効化** で、**有効** オプションを選択して、DHCP が iDRAC7 に自動で IP アドレス、ゲートウェイ、およびサブネットマスクを割り当てることができるようにします。または、**無効** を選択して次の値を入力します。
   - IP アドレス
   - ゲートウェイ
   - サブネットマスク
3. オプションで、**DHCP を使用して DNS サーバーアドレスを取得する** を有効にして、DHCP サーバーが **優先 DNS サーバー** および **代替 DNS サーバー** を割り当てることができるようにします。または、**優先 DNS サーバー** と **代替 DNS サーバー** の IP アドレスを入力します。

IPv6 設定

代替手段として、インフラストラクチャセットアップに基づいて、IPv6 アドレス プロトコルを使用することもできます。

IPv6 の設定を行うには、次の手順を実行します。

1. **IPv6 の有効化** で、**有効** オプションを選択します。
2. DHCPv6 サーバーが iDRAC7 に自動で IP アドレス、ゲートウェイ、およびサブネットマスクを割り当てることができるようにするには、**自動設定の有効化** で **有効** オプションを選択します。有効にすると、静的な値は無効になります。または、次の手順に進み、静的 IP アドレスを使用して設定を行います。
3. **IP アドレス 1** ボックスに、静的 IPv6 アドレスを入力します。
4. **プレフィックス長** ボックスに、0～128 の範囲の値を入力します。
5. **ゲートウェイ** ボックスに、ゲートウェイアドレスを入力します。
6. DHCP を使用する場合は、**DHCPv6 を使用して DNS サーバーアドレスを取得する** を有効にして、DHCPv6 サーバーからプライマリおよびセカンダリ DNS サーバーアドレスを取得します。
7. オプションで、**DHCP を使用して DNS サーバーアドレスを取得する** を有効にして、DHCPv6 サーバーが **優先 DNS サーバー** および **代替 DNS サーバー** を割り当てることができるようにします。または、**優先 DNS サーバー** と **代替 DNS サーバー** の IP アドレスを入力します。またはその代わりに、
   - **優先 DNS サーバー** ボックスに、静的 DNS サーバー IPv6 アドレスを入力します。
   - **代替 DNS サーバー** ボックスに、静的な代替 DNS サーバーを入力します。

IPMI 設定

IPMI 設定を有効にするには、次の手順を実行します。

1. **IPMI Over LAN の有効化** で **有効** を選択します。
2. **チャネル権限制限** で、**システム管理者**、**オペレータ**、または **ユーザー** を選択します。
3. **暗号化キー** ボックスに、0～40 の 16 進法文字（空白文字なし）のフォーマットで暗号化キーを入力します。デフォルト値はすべてゼロです。

VLAN の設定

VLAN インフラストラクチャ内に iDRAC7 を設定できます。VLAN 設定を行うには、次の手順を実行します。

1. **VLAN ID の有効化** で、**有効** を選択します。
2. **VLAN ID** ボックスに、1～4094 の有効な番号を入力します。
3. **優先度** ボックスに、0～7 の数値を入力して VLAN ID の優先度を設定します。

CMC ウェブインタフェースを使用した iDRAC7 IP のセットアップ

CMC ウェブインタフェースを使用して iDRAC7 IP アドレスをセットアップするには、次の手順を実行します。

メモ: CMC から iDRAC7 ネットワーク設定を行うには、シャーシ設定のシステム管理者権限が必要です。

1. CMC ウェブインタフェースにログインします。
2. **サーバー概要 → セットアップ → iDRAC** と移動します。
   iDRAC の展開 ページが表示されます。
3. **iDRAC ネットワーク設定** で、**LAN の有効化**、およびその他のネットワークパラメータを要件に従って選択します。詳細については、『*CMC オンラインヘルプ*』を参照してください。
4. 各ブレードサーバー固有の追加のネットワーク設定には、**サーバーの概要 → <サーバー名>** と移動します。
   サーバーステータス ページが表示されます。
5. **iDRAC の起動** をクリックし、**概要 → iDRAC 設定 → ネットワーク** と移動します。
6. **ネットワーク** ページで、次の設定を指定します。
   - ネットワーク設定
   - 共通設定
   - IPv4 設定
   - IPv6 設定
   - IPMI 設定
   - VLAN 設定

メモ: 詳細については、『iDRAC7 Online Help』を参照してください。

7. ネットワーク情報を保存するには、**適用** をクリックします。
   詳細については、**support.dell.com/manuals** にある『*Chassis Management Controller ユーザーズガイド*』を参照してください。

自動検出の有効化

自動検出機能を使用すると、新たに設置されたサーバーが、プロビジョニングサーバーをホストしているリモート管理コンソールを自動的に検出できるようになります。プロビジョニングサーバーは、カスタム管理ユーザー資格情報を iDRAC7 に提供し、それにより、管理コンソールからプロビジョニングされていないサーバーを検出し、管理することが可能になります。自動検出の詳細については、**support.dell.com/manuals** にある『*Lifecycle Controller Remote Services ユーザーズガイド*』を参照してください。

自動検出は、静的 IP で動作します。DHCP、DNS サーバー、またはデフォルトの DNS ホスト名ではプロビジョニングサーバーが検出されます。DNS が指定されている場合、プロビジョニングサーバー IP は DNS から取得され、DHCP 設定は不要です。プロビジョニングサーバーが指定されている場合、検出は省略されるので、DHCP も DNS も不要になります。

自動検出機能が工場出荷時のシステム上で有効にされていない場合、デフォルトの管理者アカウント（ユーザー名は root、パスワードは calvin）が有効になっています。自動検出を有効にする前に、この管理者アカウントを無効にするようにしてください。

iDRAC7 設定ユーティリティまたは Lifecycle Controller を使用して自動検出を有効にできます。Lifecycle Controller の使用方法の情報については、**support.dell.com/manuals** にある『*Lifecycle 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を使用して自動検出を有効にするには、次の手順を実行します。

1. 管理下システムの電源を入れます。
2. POST 中に、<F2> を押し、**iDRAC 設定 → リモート有効化** と移動します。
   iDRAC 設定のリモート有効化 ページが表示されます。
3. 自動検出を有効にし、プロビジョニングサーバーの IP アドレスを入力して、**戻る** をクリックします。

メモ: プロビジョニングサーバー IP の指定はオプションです。設定しなければ、DHCP または DNS 設定（手順 7）を使用して検出されます。

4. **ネットワーク** をクリックします。
   iDRAC 設定のネットワーク ページが表示されます。
5. NIC を有効にします。
6. IPv4 を有効にします。

メモ: 自動検出では、IPv6 はサポートされません。

7. DHCP を有効にして、ドメイン名、DNS サーバーアドレス、および DNS ドメイン名を DHCP から取得します。

メモ: プロビジョニングサーバーの IP アドレス（手順 3）を入力した場合、手順 7 はオプションになります。

管理ステーションのセットアップ

管理ステーションとは、iDRAC7 インタフェースにアクセスしてリモートで PowerEdge サーバーを監視および管理するために使用されるコンピュータです。
管理ステーションをセットアップするには、次の手順を実行します。

1. サポートされているオペレーティングシステムをインストールします。詳細については、readme を参照してください。
2. サポートされているウェブブラウザ（Internet Explorer または Firefox）をインストールし、設定します。
3. 最新の Java Runtime Environment（JRE）をインストールします（ウェブブラウザを使用した iDRAC7 へのアクセスに Java プラグインタイプが使用される場合に必要）。
4. 『*Dell Systems Management Tools and Documentation*』DVD から、SYSMGMT フォルダにあるリモート RACADM と VMCLI をインストールします。または、DVD の **セットアップ** を実行して、デフォルトでリモート RACADM をインストールし、その他の OpenManage ソフトウェアをインストールします。RACADM の詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。
5. 要件に基づいて次をインストールします。
   - Telnet
   - SSH クライアント
   - TFTP
   - Dell OpenManage Essentials

関連リンク

VMCLI ユーティリティのインストールと使用
対応ウェブブラウザの設定

iDRAC7 へのリモートアクセス

管理ステーションから iDRAC7 ウェブインタフェースにリモートアクセスするには、管理ステーションが iDRAC7 と同じネットワークに存在することを確認します。次に例を示します。

- ブレードサーバー — 管理ステーションは、CMC と同じネットワークに存在する必要があります。管理対象システムのネットワークから CMC ネットワークを隔離することの詳細については、**support.dell.com/manuals** にある『*Chassis Management Controller ユーザーズガイド*』を参照してください。
- ラックおよびタワーサーバー — iDRAC7 NIC を LOM1 に設定し、管理ステーションが iDRAC7 と同じネットワークに存在することを確認します。

メモ: システムが iDRAC7 Enterprise にアップグレードされた場合は、iDRAC7 NIC を **専用** に設定できます。

管理ステーションから管理下システムのコンソールにアクセスするには、iDRAC7 ウェブインタフェースから仮想コンソールを使用します。

関連リンク

仮想コンソールの起動
ネットワークの設定

管理対象システムのセットアップ

ローカル RACADM を実行する必要がある場合、または前回クラッシュ画面のキャプチャを有効にする必要がある場合は、『*Dell Systems Management Tools and Documentation*』DVD から次をインストールします。

- ローカル RACADM
- Server Administrator

Server Administrator の詳細については、**support.dell.com/manuals** にある『*Dell OpenManage Server Administrator ユーザーズガイド*』を参照してください。

関連リンク

ローカル管理者アカウント設定の変更

ローカル管理者アカウント設定の変更

iDRAC7 IP アドレスを設定した後、iDRAC 設定ユーティリティを使用してローカル管理者アカウント設定（つまり、ユーザー 2）を変更できます。これを行うには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**ユーザー設定** に移動します。
   iDRAC 設定のユーザー設定 ページが表示されます。
2. **ユーザー名**、**LAN ユーザー権限**、**シリアルポートユーザー権限**、および **パスワード** の詳細情報を指定します。
   オプションについては、『*iDRAC 設定ユーティリティオンラインヘルプ*』を参照してください。
3. **戻る**、**終了** の順にクリックし、**はい** をクリックします。
   ローカル管理者アカウント設定が設定されます。

管理下システムの場所のセットアップ

iDRAC7 ウェブインタフェースまたは iDRAC 設定ユーティリティを使用して、データセンタ内の管理下システムの場所の詳細を指定できます。

ウェブインタフェースを使用した管理下システムの場所のセットアップ

システムの場所の詳細情報を指定するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要** → **サーバー** → **プロパティ** → **詳細情報** に移動します。
   システムの詳細情報 ページが表示されます。
2. **システムの場所** で、データセンター内の管理下システムの場所について詳細情報を入力します。
   オプションの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。
3. **適用** をクリックします。システムの場所の詳細情報が iDRAC7 に保存されます。

RACADM を使用した管理下システムの場所のセットアップ

システムの場所の詳細情報を指定するには、System.Location グループオブジェクトを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

iDRAC 設定ユーティリティを使用した管理下システムの場所のセットアップ

システムの場所の詳細を指定するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**システムの場所** に移動します。
   iDRAC 設定のシステムの場所 ページが表示されます。
2. データセンター内の管理下システムの場所の詳細を入力します。このオプションの詳細については、『*iDRAC 設定ユーティリティオンラインヘルプ*』を参照してください。
3. **戻る**、**終了** の順にクリックし、**はい** をクリックします。
   詳細が保存されます。

システムパフォーマンスと電力消費の最適化

iDRAC 設定ユーティリティを使用して、管理下システムのパフォーマンスの最適化、最大排気温度およびファン速度の設定を行うことができます。これには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**温度** に移動します。
   温度の iDRAC 設定 ページが表示されます。
2. 温度、ユーザーオプション、およびファン設定を指定します。
   詳細については、『*iDRAC 設定オンラインヘルプ*』を参照してください。
3. **戻る**、**終了** とクリックし、**はい** をクリックします。
   温度が設定されました。

対応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 iDRAC7 ウェブインタフェースに接続する場合は、そのプロキシサーバー経由でインターネットにアクセスするようにウェブブラウザを設定する必要があります。

Internet Explorer ウェブブラウザを設定するには、次の手順を実行します。

1. ウェブブラウザで、**ツール → インターネットオプション → セキュリティ → ローカルネットワーク** と移動します。
2. **カスタムレベル** をクリックして **中低** を選択し、**リセット** をクリックして **OK** のクリックで確定します。
   カスタムレベル をクリックしてダイアログを開きます。
3. ActiveX コントロールとプラグインと表題のついたセクションまでスクロールダウンし、次を設定します。

メモ: 中低状態の設定は、IE のバージョンによって異なります。

- ActiveX コントロールに対して自動的にダイアログを表示：有効
- バイナリ動作とスクリプト動作：有効
- 署名された ActiveX コントロールのダウンロード：プロンプトを表示
- 安全だとマークされていない ActiveX コントロールの初期化とスクリプトの実行：プロンプトを表示
- ActiveX コントロールとプラグインの実行：有効
- 安全とマークされている ActiveX のスクリプトの実行：有効

ダウンロード で、次を設定します。

- ファイルのダウンロード時に自動的にダイアログを表示：有効
- ファイルのダウンロード：有効
- フォントのダウンロード：有効

その他 で、次を設定します。

- META-REFRESH を許可：有効
- Internet Explorer のウェブブラウザコントロールのスクリプト実行の許可：有効
- サイズや位置の制限なしでスクリプトでウィンドウを開くことを許可：有効
- クライアント証明書が 1 つしかない、または存在しない場合、証明書の選択プロンプトを表示しない：有効
- IFRAME でのプログラムとファイルの起動：有効
- 拡張子ではなく、内容によってファイルを開く：有効
- ソフトウェアチャンネルのアクセス許可：安全性 - 低
- 非暗号化形式データの送信：有効
- ポップアップブロッカーの使用：無効

スクリプト で、次を設定します。

- アクティブスクリプト：有効
- スクリプトによる貼り付け処理の許可：有効
- Java アプレットのスクリプト：有効

4. **ツール → インターネットオプション → 詳細設定** と移動します。
5. **参照** で、次を設定します。

- URL を常に UTF-8 として送信：選択
- スクリプトのデバッグを無効化（Internet Explorer）：選択
- スクリプトのデバッグを無効化（その他）：選択
- スクリプトエラーごとに通知を表示：選択解除
- インストールオンデマンドを有効化（その他）：選択
- ページの切り替えを有効化：選択
- サードパーティのブラウザ拡張を有効化：選択
- ショートカットの起動にウィンドウを再使用：選択解除

HTTP 1.1 設定 で、次を設定します。

- HTTP 1.1 を使用：選択
- プロキシ接続で HTTP 1.1 を使用：選択

Java（Sun） で、次を設定します。

- JRE 1.6.x_yz を使用：選択（オプション。バージョンが異なることがあります）

マルチメディア で、次を設定します。

- イメージサイズの自動変更を有効化：選択
- ウェブページのアニメーションを再生：選択
- ウェブページのビデオを再生：選択
- 画像を表示：選択

セキュリティで、次を設定します。

- 発行元証明書の取り消しを確認：選択解除
- ダウンロードしたプログラムの署名を確認：選択解除
- ダウンロードしたプログラムの署名を確認：選択
- SSL 2.0 を使用：選択解除
- SSL 3.0 を使用：選択
- TLS 1.0 を使用：選択
- 無効なサイト証明書について警告：選択
- セキュアモードと非セキュアモードの切り替えを警告：選択
- フォームの送信がリダイレクトされた場合に警告：選択

メモ: 設定を変更するには、変更による影響について確認し、理解しておくことをお勧めします。たとえば、ポップアップをブロックすると、iDRAC7 ウェブインタフェースの一部が正常に動作しない場合があります。

6. **適用**、**OK** の順にクリックします。
7. **接続** タブをクリックします。
8. **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。
9. **プロキシサーバーを使用** チェックボックスが選択されている場合は、**ローカルアドレスにはプロキシサーバーを使用しない** チェックボックスを選択します。
10. **OK** を 2 回クリックします。
11. ブラウザを閉じてから再起動し、すべての変更が実施されていることを確認します。

関連リンク

各言語のウェブインタフェースの表示
信頼済みドメインリストへの iDRAC7 の追加
Firefox のホワイトリスト機能を無効にする

信頼済みドメインリストへの iDRAC7 の追加

iDRAC7 ウェブインタフェースにアクセスすると、信頼済みドメインのリストに iDRAC7 の IP アドレスを追加するよう求められます（iDRAC7 の IP アドレスがリストにない場合）。追加したら、**更新** をクリックするか、ウェブブラウザを再び起動し、iDRAC7 ウェブインタフェースへの接続を確立します。

一部のオペレーティングシステムでは、iDRAC7 の IP アドレスが Internet Explorer（IE）8 の信頼済みドメインのリストに含まれていなくても、同アドレスをリストに追加するように求められない場合があります。

メモ: ブラウザが信頼しない証明書を使用して iDRAC7 ウェブインタフェースに接続する場合は、ブラウザの最初の証明書エラー警告を確認した後で、その警告が再び表示されることがあります。これは、セキュリティの予期された動作です。

IE8 の信頼済みドメインのリストに iDRAC7 の IP アドレスを追加するには、次の手順を実行します。

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 → サイト** と選択します。
2. **このウェブサイトをゾーンに追加する** に、iDRAC7 の IP アドレスを入力します。
3. **追加** をクリックし、**OK** をクリックして、次に **閉じる** をクリックします。
4. **OK** をクリックし、ブラウザを更新します。

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個別サイトのそれぞれのために、プラグインをインストールするユーザー許可が必要な「ホワイトリスト」セキュリティ機能があります。有効化すると、ホワイトリスト機能は、

アクセスする各 iDRAC7 に仮想コンソールビューアーをインストールすることを必須とします。これは、ビューアーのバージョン同一であっても同じです。

ホワイトリスト機能を無効にし、不必要なプラグインインストールを避けるには、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. **プリファレンス名** 列で、**xpinstall.whitelist.required** を見つけてダブルクリックします。
   プリファレンス名、**ステータス**、**タイプ**、および **値** の値が太字のテキストに変更されます。**ステータス** の値はユーザーセットに変更され、**値** は false に変更されます。
4. **プリファレンス名** 列で、**xpinstall.enabled** を見つけます。
   値 が **true** であることを確認します。そうでない場合は、**xpinstall.enabled** をダブルクリックして **値** を **true** に設定します。

各言語のウェブインタフェースの表示

iDRAC7 ウェブインタフェースは、次の言語でサポートされています。

- 英語（en-us）
- フランス語（fr）
- ドイツ語（de）
- スペイン語（es）
- 日本語（ja）
- 簡体字中国語（zh-cn）

括弧で囲まれた ISO ID は、対応言語の種類を示しています。対応言語の一部では、すべての機能を表示するために、ブラウザウィンドウのサイズを 1024 ピクセル幅に変更することが必要になります。

iDRAC7 ウェブインタフェースは、対応言語異体向けにローカライズされたキーボードで動作するよう設計されています。仮想コンソールなどの、iDRAC7 ウェブインタフェースの一部の機能では、特定の機能や文字にアクセスするために追加の手順を実行することが必要になる場合があります。他のキーボードはサポートされず、これらを使用すると、予期しない問題が発生することがあります。

メモ: 異なる言語の設定方法と、iDRAC7 ウェブインタフェースの各言語バージョンを表示する方法については、ブラウザのマニュアルを参照してください。

iDRAC7 ファームウェアのアップデート

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。

- iDRAC7 ウェブインタフェース
- RACADM CLI（iDRAC7 および CMC）
- Dell Update Package（DUP）
- CMC ウェブインタフェース
- Lifecycle Controller-Remote Services
- Lifecycle Controller

ファームウェアのアップデート中は、次の動作が行われます。

- ファームウェアのアップデートが完了すると、iDRAC7 はリセットされます。これにより、すべての接続とセッションが切断されます。

- ラックとタワーサーバーにあるファンは、システムを過熱から保護します。アップデートが完了すると、通常のファンの速度調整に戻ります。
- 設定が維持されない場合、iDRAC7 は SSL 証明書用に新しい SHA1 キーと MD5 キーを生成します。

メモ: ファームウェアのアップデートが完了すると、iDRAC7 に連結しているすべてのブラウザのウィンドウが閉じます。そうでない場合は、キーがアップデート前のブラウザセッションのキーと異なるという無効な証明書のエラーメッセージが表示されます。

- 何らかの理由で中断が発生すると、ファームウェアのアップデート機能は最大 30 分間有効になりません。

関連リンク

iDRAC7 ファームウェアのダウンロード
iDRAC7 ウェブインタフェースを使用したファームウェアのアップデート
CMC ウェブインタフェースを使用したファームウェアのアップデート
DUP を使用したファームウェアのアップデート
リモート RACADM を使用したファームウェアのアップデート
Lifecycle Controller Remote Services を使用したファームウェアのアップデート

iDRAC7 ファームウェアのダウンロード

ダウンロードするイメージファイルの形式は、アップデート方法によって異なります。

- iDRAC7 ウェブインタフェース — 自己解凍型アーカイブとしてパッケージ化されたバイナリイメージをダウンロードします。デフォルトのファームウェアイメージファイルは **firmimg.d7** です。

メモ: CMC ウェブインタフェースを使用した iDRAC7 の復元には、同じファイル形式が使用されます。

- 管理下システム — オペレーティングシステム固有の Dell Update Package（DUP）をダウンロードします。ファイル拡張子は、Linux オペレーティングシステムの場合は **.bin**、Windows オペレーティングシステムの場合は **.exe** です。
- Lifecycle Controller — 最新のカタログファイルと DUP をダウンロードし、Lifecycle Controller の *プラットフォームアップデート*機能を使用して iDRAC7 ファームウェアを更新します。プラットフォームアップデートの詳細については、**support.dell.com/manuals** にある『*Lifecycle Controller ユーザーズガイド*』を参照してください。

iDRAC7 ウェブインタフェースを使用したファームウェアのアップデート

iDRAC7 ウェブインタフェースを使用してアップデートするには、次の手順を実行します。

1. 最新の iDRAC7 ファームウェアイメージをダウンロードします。
2. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → iDRAC ファームウェアアップデート** と移動します。

   ファームウェアのアップデート ページが表示されます。
3. **ファイルパス** で、**参照** をクリックしてダウンロード済みのファームウェアイメージを選択し、**アップロード** をクリックします。

   ステータス（手順 3 の 2） ページが表示されます。アップロードが完了すると、現在のファームウェアと新規のファームウェアバージョンが表示されます。

   イメージがアップロードされず、すべての検証チェックに合格すると、エラーメッセージが表示され、このアップデートはファームウェアのアップデートページに戻ります。この場合は、iDRAC7 のアップデートを再試行、または **キャンセル** をクリックして iDRAC7 を通常動作モードにリセットすることができます。

   ファームウェアアップグレード中、ネットワークの問題によりイメージがアップロードされなくても、ファームウェアアップデートが進行中であると引き続き表示されます。30 分経過すると、**ファームウェアのアップデート** ページに戻ります。

メモ: この 30 分の間は、ファームウェアアップグレードの操作を一切実行できません。

4. デフォルトで、ファームウェアアップデート後に既存の iDRAC7 設定を保存する **設定の保存** オプションが選択されています。このオプションの選択を解除すると、すべての iDRAC7 設定がデフォルト値にリセットされます。

メモ: iDRAC7 設定がデフォルト値にリセットされると、iDRAC7 IP アドレスは 192.168.0.120 にリセットされ、この IP を使用して iDRAC7 にアクセスできます。または、ローカル RACADM や前面パネル（LCD）を使用するか、F2 を押して（リモート RACADM でネットワークアクセスが必要）、iDRAC7 IP アドレスを再設定できます。

現在の設定を残すには、ローカル RACADM またはリモート RACADM を使用して iDRAC7 設定をファイルにエクスポートし、ファームウェアがアップデートされ、設定がデフォルト値にリセットされた後に、その設定をインポートして iDRAC7 に戻します。ファームウェアアップデート時に設定を保存する場合は、この作業は必要ありません。

iDRAC7 設定を RACADM インタフェースを介して iDRAC7 からファイルにエクスポートする場合は、次のコマンドを使用します。

- ローカル RACADM コマンド：`racadm getconfig -f iDRAC-config.txt`
- リモート RACADM コマンド：`racadm -r <iDRAC IP アドレス> -u <idrac ユーザー名> -p <パスワード> getconfig -f iDRAC-config.txt`。ここで、**iDRAC-config.txt** は設定を保持するファイルです。

iDRAC 設定を RACADM でファイルから iDRAC7 にインポートする場合は、次のコマンドを使用します。

- ローカル RACADM コマンド：`racadm config -f iDRAC-config.txt`
- リモート RACADM コマンド：`racadm -r <iDRAC IP アドレス> -u <idrac ユーザー名> -p <パスワード> getconfig -f iDRAC-config.txt`。ここで、**iDRAC-config.txt** は設定を保持するファイルです。

5. **次へ** をクリックします。
アップデート中（手順 3 の 3） ページが表示され、アップデートの進行状況（パーセント表示）が **進行状況** 列に表示されます。

メモ: アップデートモードでは、このページから移動してもアップデートプロセスはバックグラウンドで継続されます。

6. アップデートの完了後に iDRAC7 を使用するには、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用して接続し直します。
7. 次のページのいずれかで iDRAC7 ファームウェアのバージョンを表示するには、次の手順を行います。
   - **概要 → サーバー → プロパティ → サマリ** に移動し、**サーバー情報** セクションでファームウェアバージョンを表示します。
   - **概要 → iDRAC 設定 → プロパティ** に移動し、**Integrated Dell Remote Access Controller 7** セクションでファームウェアバージョンを表示します。

関連リンク

iDRAC7 ファームウェアのアップデート
iDRAC7 ファームウェアのダウンロード

CMC ウェブインタフェースを使用したファームウェアのアップデート

CMC ウェブインタフェースを使用してブレードサーバー用の iDRAC7 ファームウェアをアップデートできます。
CMC ウェブインタフェースを使用して iDRAC7 ファームウェアをアップデートするには、次の手順を実行します。

1. CMC ウェブインタフェースにログインします。
2. **サーバーの概要 → <サーバー名>** に移動します。
   サーバーステータス ページが表示されます。
3. **iDRAC の起動** ウェブインタフェースをクリックし、**iDRAC ファームウェアアップデート** を実行します。

関連リンク

iDRAC7 ファームウェアのアップデート
iDRAC7 ファームウェアのダウンロード
iDRAC7 ウェブインタフェースを使用したファームウェアのアップデート

DUP を使用したファームウェアのアップデート

Dell Update Package（DUP）を使用してファームウェアをアップデートする前に、次を実行しておく必要があります。

- IPMI と管理下システムのドライバをインストールして有効化します。
- システムで Windows オペレーティングシステムが実行されている場合は、Windows Management Instrumentation（WMI）サービスを有効にして起動します。

メモ: Linux で DUP ユーティリティを使用して iDRAC7 ファームウェアをアップデートしているときは、コンソールに `usb 5-2: device descriptor read/64, error -71` というエラーメッセージが表示されても無視してください。

- システムに ESX ハイパーバイザがインストールされている場合は、DUP ファイルが実行できるように、`service usbarbitrator stop` コマンドを使用して「usbarbitrator」サービスが停止されていることを確認します。

DUP を使用して iDRAC7 をアップデートするには、次の手順を実行します。

1. インストールされているオペレーティングシステムに対応した DUP をダウンロードし、管理下システム上で実行します。
2. DUP を実行します。
   ファームウェアがアップデートされます。ファームウェアのアップデート完了後に、システムを再起動する必要はありません。

リモート RACADM を使用したファームウェアのアップデート

リモート RACADM を使用してアップデートするには、次の手順を実行します。

1. ファームウェアイメージを TFTP または FTP サーバーにダウンロードします（たとえば、**C:\downloads\firmimg.d7**）。
2. 次の RACADM コマンドを実行します。
   TFTP サーバー：

   ```
   racadm -r <iDRAC7 IP アドレス> -u <ユーザー名> -p <パスワード> fwupdate -g -u -a <パス>
   ```

   ここで、*パス*は、**firmimg.d7** が保存されている TFTP サーバー上の場所です。
   FTP サーバー：

   ```
   racadm -r <iDRAC7 IP アドレス> -u <ユーザー名> -p <パスワード> fwupdate -f <FTP サーバー IP> <FTP サーバーユーザー名> <FTP サーバーパスワード> -d <パス>
   ```

   ここで、*パス*は、**firmimg.d7** が保存されている FTP サーバー上の場所です。
   詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』の `fwupdate` コマンドを参照してください。

Lifecycle Controller Remote Services を使用したファームウェアのアップデート

Lifecycle Controller Remote Services を使用したファームウェアのアップデートについては、**support.dell.com/manuals** にある『*Lifecycle Controller–Remote Services ユーザーズガイド*』を参照してください。

iDRAC7 ファームウェアのロールバック

次のいずれかの方法を使用して、ファームウェアを以前にインストールしたバージョンにロールバックできます。

- iDRAC7 ウェブインタフェース
- CMC ウェブインタフェース
- RACADM CLI（iDRAC7 および CMC）
- Lifecycle Controller
- Lifecycle Controller-Remote Services

関連リンク

iDRAC7 ウェブインタフェースを使用したファームウェアのロールバック
CMC ウェブインタフェースを使用したファームウェアのロールバック
RACADM を使用したファームウェアのロールバック
Lifecycle Controller を使用したファームウェアのロールバック
Lifecycle Controller-Remote Services を使用したファームウェアのロールバック

iDRAC7 ウェブインタフェースを使用したファームウェアのロールバック

iDRAC7 ウェブインタフェースを使用してロールバックするには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → iDRAC ファームウェアアップデート** と移動します。
   ファームウェア - アップロード / ロールバック（手順 3 の 1） ページが表示されます。
2. **ロールバック** をクリックします。
   ステータス（手順 3 の 2） ページに、現在のファームウェアとロールバックするファームウェアのバージョンが表示されます。
3. デフォルトで **設定の保存** チェックボックスが選択されており、これにより、ファームウェアのロールバック後に既存の iDRAC7 設定が保存されます。iDRAC7 をデフォルト設定にリセットするには、このチェックボックスをオフにします。

メモ: iDRAC7 設定がデフォルト値にリセットされると、iDRAC7 の IP アドレスが 192.168.0.120 にリセットされます。この IP を使用して iDRAC7 にアクセス、またはローカル RACADM か F2 を使用して iDRAC7 アドレスを再設定することもできます（リモート RACADM にはネットワークアクセスが必要です）。

4. **次へ** をクリックします。
   アップデート中（手順 3 の 3） ページが表示されます。

メモ: ロールバックモード中は、ユーザーがこのページから移動してもロールバック処理がバックグラウンドで継続されます。

5. ロールバックが完了すると、iDRAC7 がリセットされます。iDRAC7 を使用するには、現在のブラウザウィンドウを閉じ、新規のブラウザウィンドウを使用して再接続する必要があります。
6. iDRAC7 ファームウェアバージョンを表示するには、次のいずれかのページに移動します。

- **概要 → サーバー → プロパティ → サマリ** に移動すると、**サーバー情報** のセクションにファームウェアバージョンが表示されます。
- **概要 → iDRAC 設定 → プロパティ** と移動すると、**Integrated Dell Remote Access Controller 7** のセクションにファームウェアバージョンが表示されます。

CMC ウェブインタフェースを使用したファームウェアのロールバック

CMC ウェブインタフェースを使用してロールバックするには、次の手順を実行します。

1. CMC ウェブインタフェースにログインします。
2. **サーバーの概要 → <サーバー名>** に移動します。
   サーバーステータス ページが表示されます。
3. **iDRAC の起動** ウェブインタフェースをクリックし、iDRAC7 ファームウェアのロールバックを実行します。

RACADM を使用したファームウェアのロールバック

以前のファームウェアバージョンにロールバックするには、**fwupdate** コマンドを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

Lifecycle Controller を使用したファームウェアのロールバック

これについての情報は、**support.dell.com/manuals** にある『*Lifecycle Controller ユーザーズガイド*』を参照してください。

Lifecycle Controller-Remote Services を使用したファームウェアのロールバック

これについての情報は、**support.dell.com/manuals** にある『*Lifecycle Controller Remote Services ユーザーズガイド*』を参照してください。

iDRAC7 のリカバリ

iDRAC7 は、起動可能な iDRAC7 を確実にするため、次の 2 つのオペレーティングシステムイメージをサポートします。予期しない破壊的なエラーが発生した場合は、両方の起動パスが失われます。

- iDRAC7 ブートローダーは、起動可能なイメージがないことを検出します。
- システムの正常性と識別 LED が 1/2 秒以下の間隔で点滅します(LED はラックおよびタワーサーバーの背面と、ブレードサーバーの前面にあります)。
- ブートローダーが、SD カードスロットをポーリングします。
- Windows オペレーティングシステムを使用して SD カードを FAT でフォーマットするか、Linux オペレーティングシステムを使用して SD カードを EXT3 でフォーマットします。
- **firmimg.d7** を SD カードにコピーします。
- SD カードをサーバーに挿入します。
- ブートローダーが SD カードを検出し、点滅している LED を橙色に点灯、firmimg.d7 を読み取り、iDRAC7 を再プログラムして、次に iDRAC7 が再起動されます。

TFTP サーバーの使用

Trivial File Transfer Protocol（TFTP）サーバーを使用して iDRAC7 ファームウェアをアップグレードまたはダウングレードしたり、証明書をインストールしたりできます。これは SM-CLP および RACADM コマンドラインインタフェースで iDRAC7 にファイルを転送したり、iDRAC7 からファイルを転送したりするために使用されます。TFTP サーバーには、iDRAC7 の IP アドレスまたは DNS 名を使用してアクセスできる必要があります。

メモ: 証明書の転送およびファームウェアのアップデートに iDRAC7 ウェブインタフェースを使用する場合、TFTP サーバーは必要ありません。

Windows または Linux オペレーティングシステムで `netstat -a` コマンドを使用して、TFTP サーバーが実行中であるかどうかを確認できます。TFTP のデフォルトのポートは 69 です。TFTP サーバーが実行中でない場合は、次のいずれかの操作を実行します。

- 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します。
- オペレーティングシステム上に TFTP サーバーをインストールします。

他のシステム管理ツールを使用した iDRAC7 の監視

iDRAC7 は、IT Assistant、Dell Management Console、および Dell OpenManage Essentials を使用して検出および監視できます。また、Dell Remote Access Configuration Tool（DRACT）を使用して、iDRAC の検出、ファームウェアの更新、および Active Directory の設定を行うこともできます。詳細については、それぞれのユーザーズガイドを参照してください。

4

iDRAC7 の設定

iDRAC7 では、リモート管理タスクを実行するために iDRAC7 プロパティの設定、ユーザーのセットアップ、および警告のセットアップを行うことができます。

iDRAC7 を設定する前に、iDRAC7 ネットワーク設定と対応ブラウザの設定が行われており、必要なライセンスをアップデートされているようにしてください。iDRAC7 でのライセンス可能な機能の詳細については、「ライセンスの管理」を参照してください。

次を使用して iDRAC7 を設定できます。

- iDRAC7 ウェブインタフェース
- RACADM
- Remote Services（『*Lifecycle Controller Remote Services ユーザーズガイド*』を参照）
- IPMITool（『*Baseboard Management Controller Management ユーティリティユーザーズガイド*』を参照）

iDRAC7 を設定するには、次の手順を実行します。

1. iDRAC7 にログインします。
2. 必要に応じてネットワーク設定を変更します。

メモ: iDRAC7 IP アドレスのセットアップ時に iDRAC 設定ユーティリティを使用して iDRAC7 ネットワーク設定を設定した場合、この手順は省略します。

3. iDRAC7 にアクセスするインタフェースを設定します。
4. 前面パネルディスプレイを設定します。
5. 必要に応じてシステムの場所を設定します。
6. iDRAC7 に対して次のいずれかの代替通信方法を確立します。
   - IPMI または RAC シリアル
   - IPMI シリアルオーバー LAN
   - IPMI Over LAN
   - SSH または Telnet クライアント
7. 必要な証明書を取得します。
8. iDRAC7 ユーザーを追加し、権限を設定します。
9. 電子メールアラート、SNMP トラップ、または IPMI アラートを設定し、有効にします。
10. 必要に応じて電力制限ポリシーを設定します。
11. 前回のクラッシュ画面を有効にします。
12. 必要に応じて仮想コンソールと仮想メディアを設定します。
13. 必要に応じて vFlash SD カードを設定します。
14. 必要に応じて最初の起動デバイスを設定します。
15. 必要に応じて内部管理通信を設定します。

関連リンク

iDRAC7 へのログイン
ネットワーク設定の変更
サービスの設定

iDRAC7 情報の表示

iDRAC7 の基本的なプロパティを表示できます。

ウェブインタフェースを使用した iDRAC7 情報の表示

iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → プロパティ** と移動し、iDRAC7 に関連する次の情報を表示します。これらのプロパティについては、『*iDRAC7 オンラインヘルプ*』を参照してください。

- デバイスタイプ
- ハードウェアおよびファームウェアバージョン
- 最後のファームウェアアップデート
- RAC 時間
- アクティブ化可能なセッション数
- 現在のセッション数
- LAN の有効化または無効化
- IPMI バージョン
- ユーザーインタフェースタイトルバー情報
- ネットワーク設定
- IPv4 設定
- IPv6 設定

RACADM を使用した iDRAC7 情報の表示

RACADM を使用して iDRAC7 情報を表示するには、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』で説明されている `getsysinfo` または `get` サブコマンドの詳細を参照してください。

ネットワーク設定の変更

iDRAC 設定ユーティリティを使用して iDRAC7 ネットワーク設定を設定した後も、iDRAC7 ウェブインタフェース、RACADM、Lifecycle Controller、Dell Deployment Toolkit、および Server Administrator から設定を変更することができます（オペレーティングシステムの起動後）。これらのツールと権限設定の詳細については、それぞれのユーザーズガイドを参照してください。

iDRAC7 ウェブインタフェースまたは RACADM を使用してネットワーク設定を変更するには、**iDRAC の設定** 権限が必要です。

メモ: ネットワーク設定を変更すると、iDRAC7 への現在のネットワーク接続が切断される場合があります。

ウェブインタフェースを使用したネットワーク設定の変更

iDRAC7 ネットワーク設定を変更するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ネットワーク** と移動します。
   ネットワーク ページが表示されます。
2. 必要な情報を指定し、**適用** をクリックします。
   各種設定の詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。

ローカル RACADM を使用したネットワーク設定の変更

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
```

次に、必要な LAN ネットワークプロパティを設定するコマンドの使用例を示します。

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1
racadm config -g cfgLanNetworking -o cfgNicIpAddress 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicNetmask 255.255.255.0
racadm config -g cfgLanNetworking -o cfgNicGateway 192.168.0.120
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSServer1 192.168.0.5
racadm config -g cfgLanNetworking -o cfgDNSServer2 192.168.0.6
racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1
racadm config -g cfgLanNetworking -o cfgDNSRacName RAC-EK00002
racadm config -g cfgLanNetworking -o cfgDNSDomainNameFromDHCP 0
racadm config -g cfgLanNetworking -o cfgDNSDomainName MYDOMAIN
```

メモ: cfgNicEnable を **0** に設定すると、DHCP が有効化されても iDRAC7 LAN は無効になります。

IP フィルタと IP ブロックの設定

ユーザー認証に加え、次のオプションを使用して iDRAC7 へのアクセス時のセキュリティを強化します。

- IP フィルタは、iDRAC7 にアクセスするクライアントの IP アドレス範囲を限定します。新規ログインの IP アドレスを指定の範囲と比較し、その範囲内の IP アドレスを持つ管理ステーションからの iDRAC7 アクセスのみを許可します。それ以外のログイン要求はすべて拒否されます。
- IP ブロックは、特定の IP アドレスからの過剰なログイン失敗が発生したことを動的に判断し、事前に選択された時間枠の間、そのアドレスが iDRAC7 にログインするのをブロックします。これには次が含まれます。
  - 許可するログイン失敗回数。

- これらの失敗が発生する時間枠（秒）。
- IP アドレスが許可される失敗回数を超えた後で、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時間枠（秒）。

特定 IP アドレスからのログインに失敗するたびに、その回数が内部カウンタによって記録されます。ユーザーがログインに成功すると、失敗の履歴はクリアされ、内部カウンタがリセットされます。

メモ: クライアント IP アドレスからのログイン試行が拒否されると、SSH クライアントに「ssh 交換識別子：リモートホストによって接続が閉じられました というメッセージが表示される場合があります。

メモ: Dell Deployment Toolkit（DTK）を使用する場合は、権限について『*Dell Deployment Toolkit ユーザーズガイド*』を参照してください。

iDRAC7 ウェブインタフェースを使用した IP フィルタと IP ブロックの設定

これらの手順を実行するには、iDRAC7 の設定権限が必要です。

IP フィルタおよびブロックを設定するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ネットワーク → ネットワーク** と移動します。
   ネットワーク ページが表示されます。
2. **詳細設定** をクリックします。
   ネットワークセキュリティ ページが表示されます。
3. IP フィルタおよびブロックの設定を指定します。
   オプションの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。
4. **適用** をクリックして設定を保存します。

RACADM を使用した IP フィルタと IP ブロックの設定

これらの手順を実行するには、iDRAC7 の設定権限が必要です。

IP フィルタと IP ブロックを設定するには、次の RACADM オブジェクトを使用します。

- cfgRacTuneIpRangeEnable
- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask
- cfgRacTuneIpBlkEnable
- cfgRacTuneIpBlkFailCount
- cfgRacTuneIpBlkFailWindow

cfgRacTuneIpRangeMask プロパティは、入力される IP アドレスと **cfgRacTuneIpRangeAddr** プロパティの両方に適用されます。結果が同じである場合は、入力される着信ログイン要求に iDRAC7 へのアクセスが許可されます。この範囲外の IP アドレスからログインすると、エラーが発生します。

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)
```

ここで & は数量のビットワイズ AND であり、^ はビットワイズ XOR

です。

IP フィルタの例

- 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
```

- 連続する 4 つの IP アドレス（たとえば、192.168.0.212～192.168.0.215）へのログインを制限するには、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 ブロックの例

- 次の例は、管理ステーション IP アドレスが 1 分間にログイン試行を 5 回失敗した場合に、その IP アドレスによるセッションの確立が 5 分間阻止される例です。

  ```
  racadm config -g cfgRacTuning -o cfgRacTuneIpRangeEnable 1
  racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount 5
  racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow 60
  ```

- 次の例では、ログイン試行の失敗回数が 1 分間に 3 回を超えた場合に、1 時間ログイン試行が阻止されます。

  ```
  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 3600
  ```

詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

サービスの設定

iDRAC7 では、次のサービスの設定と有効化ができます。

- ローカル設定 — ローカル RACADM および iDRAC 設定ユーティリティを使用して iDRAC7 設定へのアクセスを（ホストシステムから）無効化します。
- ウェブサーバー — iDRAC7 ウェブインタフェースへのアクセスを有効にします。オプションを無効にした場合は、RACADM を使用してこのオプションを有効にできます。
- SSH — ファームウェア RACADM から iDRAC7 にアクセスします。
- Telnet — ファームウェア RACADM から iDRAC7 にアクセスします。
- リモート RACADM — iDRAC7 にリモートアクセスします。
- SNMP エージェント — イベントに対して SNMP トラップを送信するよう iDRAC7 を有効にします。
- 自動システム復元エージェント — 最後のシステムクラッシュ画面を有効にします。

ウェブインタフェースを使用したサービスの設定

iDRAC7 ウェブインタフェースを使用してサービスを設定するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ネットワーク → サービス** と移動します。
   サービス ページが表示されます。
2. 必要な情報を指定し、**適用** をクリックします。
   各種設定の詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。

RACADM を使用したサービスの設定

さまざまなサービスを有効化し、設定するには、次の RACADM オブジェクトを使用します。

- cfgRacTuneLocalConfigDisable
- cfgRacTuneCtrlEConfigDisable
- cfgSerialSshEnable
- cfgRacTuneSshPort
- cfgSsnMgtSshIdleTimeout
- cfgSerialTelnetEnable
- cfgRacTuneTelnetPort
- cfgSsnMgtTelnetIdleTimeout
- cfgRacTuneWebserverEnable
- cfgSsnMgtWebserverTimeout
- cfgRacTuneHttpPort
- cfgRacTuneHttpsPort
- cfgRacTuneRemoteRacadmEnable
- cfgSsnMgtRacadmTimeout
- cfgOobSnmpAgentEnable
- cfgOobSnmpAgentCommunity

これらのオブジェクトの詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

前面パネルディスプレイの設定

管理下システムの前面パネル LCD および LED ディスプレイを設定することができます。

ラックおよびタワーサーバーには、次の 2 つのタイプの前面パネルがあります。

- LCD 前面パネルとシステム ID LED
- LED 前面パネルとシステム ID LED

ブレードサーバーの場合は、ブレードシャーシに LCD が搭載されているため、サーバーの前面パネルで使用できるのはシステム ID LED のみです。

関連リンク

LCD の設定

システム ID LED の設定

LCD の設定

管理下システムの LCD 前面パネルでは、iDRAC 名や IP などのデフォルト文字列、またはユーザー定義の文字列を設定し、表示できます。

ウェブインタフェースを使用した LCD の設定

サーバーの LCD 前面パネルの表示を設定するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → ハードウェア → 前面パネル** と移動します。
2. **LCD 設定** セクションの **ホームメッセージの設定** ドロップダウンメニューで、次のいずれかを選択します。
   - サービスタグ（デフォルト）
   - Asset Tag
   - DRAC MAC アドレス
   - DRAC IPv4 アドレス
   - DRAC IPv6 アドレス
   - システム電源
   - 環境温度
   - システムモデル
   - ホスト名
   - ユーザー定義
   - なし

   ユーザー定義 を選択した場合は、テキストボックスに必要なメッセージを入力します。

   なし を選択した場合は、サーバーの LCD 前面パネルにホームメッセージは表示されません。
3. **適用** をクリックします。

   サーバーの LCD 前面パネルに、設定したホームメッセージが表示されます。

RACADM を使用した LCD の設定

サーバー LCD 前面パネルディスプレイを設定するには、`System.LCD` グループのオブジェクトを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

iDRAC 設定ユーティリティを使用した LCD の設定

サーバー LCD 前面パネルディスプレイを設定するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**LCD** に移動します。

   iDRAC 設定 LCD ページが表示されます。
2. 必要なオプションを指定します。

   詳細については、『*iDRAC 設定ユーティリティオンラインヘルプ*』を参照してください。
3. **戻る**、**終了** の順にクリックして、**はい** をクリックします。

   設定が保存されます。

システム ID LED の設定

サーバーを識別するには、管理下システムで点滅しているシステム ID LED を有効化または無効化します。

ウェブインタフェースを使用したシステム ID LED の設定

システム ID LED ディスプレイを設定するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → ハードウェア → 前面パネル** と移動します。**前面パネル** ページが表示されます。
2. **システム ID LED 設定** セクションで、次のいずれかのオプションを選択して LED の点滅を有効化または無効化します。
   - 点滅無効
   - 点滅有効

- 点滅有効 1 日タイムアウト
- 点滅有効 1 週間タイムアウト
- 点滅有効 1 か月タイムアウト

3. **適用** をクリックします。
   前面パネルの LED 点滅が設定されます。

RACADM を使用したシステム ID LED の設定

システム ID LED を設定するには、**setled** コマンドを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

最初の起動デバイスの設定

次回起動のみ、または後続のすべての再起動用に、最初の起動デバイスを選択できます。この選択に基づいて、システムの最初の起動デバイスを設定できます。システムは、次回および後続の再起動時に選択されたデバイスから起動し、そのデバイスは iDRAC7 ウェブインタフェースまたは BIOS 起動順序から再び変更されない限り、BIOS 起動順序に最初の起動デバイスとして保持されます。

メモ: iDRAC7 ウェブインタフェースで最初の起動デバイスの設定は、システム BIOS 起動設定を上書きします。

ウェブインタフェースを使用した最初の起動デバイスの設定

iDRAC7 ウェブインタフェースを使用して最初の起動デバイスを設定するには、次の手順を実行します。

1. **概要 → サーバー → セットアップ → 最初の起動デバイス** と移動します。
   最初の起動デバイス ページが表示されます。
2. ドロップダウンリストから必要な最初の起動デバイスを選択し、**適用** をクリックします。
   以降の再起動で、システムは、選択されたデバイスから起動します。
3. 次回の起動で選択されたデバイスから 1 度だけ起動するには、**1 回限りの起動** を選択します。それ以降、システムは BIOS の起動順序に従って最初の起動デバイスから起動します。
   オプションの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。

RACADM を使用した最初の起動デバイスの設定

- 最初の起動デバイスを設定するには、`cfgServerFirstBootDevice` オブジェクトを使用します。
- デバイスで 1 度だけ起動することを有効にするには、`cfgServerBootOnce` オブジェクトを使用します。

これらのオブジェクトの詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

内部システム管理通信の有効化

ネットワークドーターカード（NDC）または LAN On Motherboard（LOM）デバイスが搭載されたラックまたはタワーデバイスでは、共有 LOM を介した iDRAC7 とホストオペレーティングシステム間の高速双方向帯域内通信を提供する内部システム管理通信チャネルを有効にすることができます。このチャネルは、次の条件で有効化できます。

- iDRAC 設定ユーティリティ（プレオペレーティングシステム環境）
- RACADM または WS-MAN（ポストオペレーティングシステム環境）

- iDRAC7 が共有モードである（つまり、NIC の選択が LOM のひとつに割り当てられている）。
- ホストオペレーティングシステムと iDRAC7 が同一サブネットおよび同一 VLAN 内に存在する。

IMC が IPv4 および IPv6 アドレスをサポートしている。
内部システム管理通信を有効にする前に、次を確認してください。

- iDRAC7 が共有モードである（つまり、NIC の選択が LOM のひとつに割り当てられている）。
- ホストオペレーティングシステムと iDRAC7 が同一サブネットおよび同一 VLAN 内に存在する。

iDRAC 設定ユーティリティを使用した IMC の有効化

iDRAC 設定ユーティリティを使用して IMC を有効にするには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**パススルー通信** に移動します。
   パススルー通信 ページが表示されます。
2. **有効** を選択します。
   オプションの詳細については、『*iDRAC 設定ユーティリティオンラインヘルプ*』を参照してください。
3. **戻る**、**終了** の順にクリックし、**はい** をクリックします。
   詳細が保存されます。

RACADM を使用した IMC の有効化

iDRAC7 を共有モードで設定するには（例 LOM1）、次のコマンドを実行します。

```
racadm config -g cfglannetworking -o cfgnicselection 2
```

IMC を有効にするには、次のコマンドを実行します。

```
racadm set idrac.imc.AdministrativeState Enabled
```

前回のクラッシュ画面の有効化

管理下システムのクラッシュの原因をトラブルシューティングするため、iDRAC7 を使用してシステムのクラッシュイメージを取得できます。
前回のクラッシュ画面を有効にするには、次の手順を実行します。

1. 『*Dell Systems Management Tools and Documentation*』DVD から、管理対象システムに Server Administrator をインストールします。
   詳細については、**support.dell.com/manuals** にある『*Dell OpenManage Server Administrator インストールガイド*』を参照してください。
2. **Windows** の起動と回復ウィンドウで、自動再起動オプションが選択されていないことを確認します。
   詳細については、Windows のマニュアルを参照してください。
3. Server Administrator を使用して **自動回復** タイマーを有効化し、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** に設定して、タイマーを秒単位で設定します（60～480 の値）。
   詳細については、**support.dell.com/manuals** にある『*Dell OpenManage Server Administrator インストールガイド*』を参照してください。
4. 次のいずれかを使用して、**自動シャットダウンと回復**（ASR）オプションを有効にします。
   - Server Administrator — **support.dell.com/manuals** にある『*Dell OpenManage Server Administrator ユーザーズガイド*』を参照してください。
   - ローカル RACADM — 次のコマンドを使用します。
     ```
     racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1
     ```
5. **自動システム回復エージェント** を有効にします。これには、**概要 → iDRAC 設定 → ネットワーク → サービス** に移動し、**有効化** を選択して **適用** をクリックします。

証明書の取得

次の表に、ログインタイプに基づいた証明書のタイプを示します。

表 7. ログインタイプに基づいた証明書のタイプ

ログインタイプ	証明書タイプ	取得方法
Active Directory を使用したシングルサインオン	信頼できる CA 証明書	CSR を生成し、認証局の署名を取得します。
ローカルユーザーまたは Active Directory ユーザーとしてのスマートカードログイン	• ユーザー証明書 • 信頼できる CA 証明書	• ユーザー証明書 — スマートカードベンダーが提供するカード管理ソフトウェアを使用して、スマートカードユーザー証明書を Base64 でエンコードされたファイルとしてエクスポートします。 • 信頼できる CA 証明書 — この証明書は、CA によって発行されます。
Active Directory ユーザーログイン	信頼できる CA 証明書	この証明書は、CA によって発行されます。
ローカルユーザーログイン	SSL 証明書	CSR を生成し、認証局の署名を取得します。 **メモ:** iDRAC7 にはデフォルトの自己署名型 SSL サーバー証明書が付属しています。iDRAC7 ウェブサーバー、仮想メディア、および仮想コンソールでは、この証明書を使用します。

関連リンク

SSL サーバー証明書
新しい証明書署名要求の生成

SSL サーバー証明書

iDRAC7 には、ネットワーク上での暗号化データの転送に業界標準の SSL セキュリティプロトコルを使用するよう設定されたウェブサーバーが含まれています。非対称暗号テクノロジを基盤とする SSL は、ネットワーク上の傍受防止するクライアントとサーバー間での認証かつ暗号化された通信を提供するために広く受け入れられています。

SSL 対応システムは、次のタスクを実行できます。

- SSL 対応クライアントに自らを認証する
- 2 つのシステムに暗号化接続の確立を許可する

暗号化プロセスは、高レベルなデータ保護を実現します。iDRAC7 には、北米のインターネットブラウザで一般的に使用できる暗号化形式の中でも最もセキュアな形式である 128 ビット SSL 暗号化標準が採用されています。

iDRAC7 ウェブサーバーには、デフォルトで Dell 自己署名型 SSL デジタル証明書が付属しています。iDRAC7 セッションが本物であることを確認し、システム管理者が不正ユーザーに iDRAC7 資格情報を明かさないようにするため、SSL サーバー証明書を周知の認証局（CA）署名付き証明書に置き換えてください。認証局は、信

頼性のある審査、身元証明、およびその他の重要なセキュリティ基準の高度な水準を満たすことで情報テクノロジ業界で認められている事業体です。CA には、Thawte や VeriSign などがあります。

署名付き証明書を取得するプロセスを開始するには、iDRAC7 ウェブインタフェースまたは RACADM インタフェースを使用して、会社の情報を記した証明書署名要求を生成します。その後、生成した CSR を VerSign や Thawte などの CA に送信します。

関連リンク

新しい証明書署名要求の生成
サーバー証明書のアップロード
サーバー証明書の表示

新しい証明書署名要求の生成

CSR は、認証局（CA）への SSL サーバー証明書のデジタル要求です。SSL サーバー証明書は、サーバーのクライアントがサーバーの ID を信頼し、サーバーとの暗号化セッションのネゴシエーションをできるようにします。

CA が CSR を受け取ると、CA は CSR に含まれる情報を確認し、検証します。申請者が CA のセキュリティ標準を満たす場合、CA はデジタル署名付きの SSL サーバー証明書を発行します。この証明書は、申請者のサーバーが管理ステーションで実行されているブラウザと SSL 接続を確立するときに、そのサーバーを固有識別します。

CA が CSR を承認し、SSL サーバー証明書を発行した後は、その証明書を iDRAC7 にアップロードできます。iDRAC7 ファームウェアに保存されている CSR の生成に使用された情報は、SSL サーバー証明書に含まれる情報と一致する必要があります。つまり、この証明書は、iDRAC7 によって作成された CSR を使用して生成されている必要があります。

関連リンク

SSL サーバー証明書

ウェブインタフェースを使用した CSR の生成

新規の CSR を生成するには、次の手順を実行します。

メモ: 新規の CSR はそれぞれ、ファームウェアに保存された以前の CSR データを上書きします。CSR 内の情報は、SSL サーバー証明書内の情報に一致する必要があります。そうでない場合、iDRAC7 は証明書を受け入れません。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ネットワーク → SSL** と移動し、**新規の証明書署名要求（CSR）の生成** を選択して **次へ** をクリックします。
   新規の証明書署名要求の生成 ページが表示されます。
2. 各 CSR 属性の値を入力します。
   詳細については、『*iDRAC7 Online Help*』を参照してください。
3. **生成** をクリックします。
   新規の CSR が生成されます。
4. **ダウンロード** をクリックして CSR ファイルを管理ステーションに保存します。

RACADM を使用した CSR の生成

CSR を生成するには、`cfgRacSecurityData` グループ内のオブジェクトを使用して値を指定し、`sslcsrgen` コマンドを使用して CSR を生成します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

サーバー証明書のアップロード

CSR の生成後、署名された SSL サーバー証明書を iDRAC7 ファームウェアにアップロードできます。iDRAC7 は、証明書のアップロード後にリセットされます。iDRAC7 は、X509 Base-64 エンコードの Web サーバー証明書のみを受け入れます。

注意: 証明書のアップロード中は、iDRAC7 を使用できません。

関連リンク

SSL サーバー証明書

ウェブインタフェースを使用したサーバー証明書のアップロード

SSL サーバー証明書をアップロードするには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ネットワーク → SSL** と移動し、**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。
   証明書アップロード ページが表示されます。
2. **ファイルパス** で **参照** をクリックして、管理ステーションの証明書を選択します。
3. **適用** をクリックします。
   SSL サーバー証明書が iDRAC7 ファームウェアにアップロードされ、既存の証明書と交換されます。

RACADM を使用したサーバー証明書のアップロード

SSL サーバー証明書をアップロードするには、`sslcertupload` コマンドを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

サーバー証明書の表示

現在 iDRAC7 で使用されている SSL サーバー証明書を表示できます。

関連リンク

SSL サーバー証明書

ウェブインタフェースを使用したサーバー証明書の表示

iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ネットワーク → SSL** と移動し、**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。**サーバー証明書の表示** ページに、現在使用中の SSL サーバー証明書が表示されます。

RACADM を使用したサーバー証明書の表示

SSL サーバー証明書を表示するには、`sslcertview` コマンドを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

RACADM を使用した複数の iDRAC7 の設定

RACADM を使用して、1 つ、または複数の iDRAC7 を同じプロパティで設定できます。iDRAC7 のグループ ID とオブジェクト ID を使用して特定の iDRAC7 をクエリすると、RACADM は取得した情報から **.cfg** 設定ファイルを作成します。ファイル名はユーザーが指定します。ファイルを他の iDRAC7 にインポートして、それらの iDRAC7 を同様に設定します。

メモ: いくつかの設定ファイルには固有の iDRAC7 情報（静的 IP アドレスなど）が含まれており、そのファイルを他の iDRAC7 にエクスポートする前に、あらかじめその情報を変更しておく必要があります。

複数の iDRAC7 を設定するには、次の手順を実行します。

1. コマンド `racadm getconfig -f myfile.cfg` を使用して、必要な設定を含むターゲット iDRAC7 をクエリします。
   このコマンドは、iDRAC7 設定を要求し、**myfile.cfg** ファイルを生成します。このファイルは、必要に応じて別の名前に設定できます。

メモ: getconfig -f を使った iDRAC7 設定のファイルへのリダイレクトは、ローカルまたはリモート RACADM インタフェースでのみサポートされています。

メモ: 生成された .cfg ファイルにはユーザーパスワードは含まれていません。

   getconfig コマンドは、グループ内のすべての設定プロパティ（グループ名とインデックスで指定）と、ユーザー名別のユーザーのすべての設定プロパティを表示します。
2. シンプルテキストエディタを使用して、設定ファイルに変更を加えます（オプション）。

メモ: このファイルの編集はシンプルテキストエディタで行うようにお勧めします。RACADM ユーティリティは ASCII 形式のテキスト解析を用いるため、書式が混在するとこの解析に混乱を招き、RACADM データベースが破壊される可能性があります。

3. 新規の設定ファイルを使用して、`racadm config -f myfile.cfg` コマンドでターゲットの iDRAC7 を変更します。
   これによって、その他の iDRAC7 に情報がロードされます。ユーザーおよびパスワードデータベースを Server Administrator と同期するには、config サブコマンドを使用します。
4. `racadm racreset` コマンドを使用して、ターゲットの iDRAC7 をリセットします。

iDRAC7 設定ファイルの作成

設定ファイル **.cfg** には、次の操作を実行できます。

- 作成する
- `racadm getconfig -f <ファイル名>.cfg` コマンドで取得する
- `racadm getconfig -f <ファイル名>.cfg` コマンドで取得した後、編集する
  `getconfig` コマンドについては、**support.dell.com/manuals** にある『*RACADM Command Line Reference Guide for iDRAC7 and CMC*』を参照してください。

.cfg ファイルはまず、有効なグループとオブジェクト名が存在し、基本構文規則に従っていることを検証するために構文解析されます。エラーには、エラーが検出された行番号を示すフラグが付き、問題を説明するメッセージが表示されます。正確性のためにファイル全体が構文解析され、すべてのエラーが表示されます。**.cfg** ファイルにエラーが検出された場合、書き込みコマンドは iDRAC7 に送信されません。ユーザーは、そのファイルを使用して iDRAC7 を設定する前に、すべてのエラーを修正する必要があります。`config` サブコマンドに `-c` オプションを使用すると、構文が検証され、iDRAC7 への書き込み操作は実行されません。

.cfg ファイルを作成するときは、次のガイドラインに従ってください。

- 構文解析でインデックス付きグループが検出されると、そのグループのインデックスがアンカーとして使用されます。インデックス付きグループ内のオブジェクトに対する変更は、インデックス値にも関連付けられます。たとえば、次のとおりです。

```
[cfgUserAdmin]
# cfgUserAdminIndex=11
cfgUserAdminUserName=
# cfgUserAdminPassword=********  （書き込み専用）
```

```
cfgUserAdminEnable=0
cfgUserAdminPrivilege=0x00000000
cfgUserAdminIpmiLanPrivilege=15
cfgUserAdminIpmiSerialPrivilege=15
cfgUserAdminSolEnable=0
```

- インデックスは読み取り専用であり、変更できません。インデックス付きグループのオブジェクトは、それらのグループがリストされているインデックスにバインドされ、オブジェクト値の有効な設定は、その特定のインデックスにのみ適用されます。
- インデックス付きグループごとに、事前定義されたインデックスのセットを使用できます。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。
- racresetcfg サブコマンドを使用して、iDRAC7 を元のデフォルトにリセットしてから、racadm config -f <ファイル名>.cfg コマンドを実行します。**.cfg** ファイルに必要なオブジェクト、ユーザー、インデックス、およびその他のパラメータが含まれていることを確認してください。

△ **注意: racresetcfg サブコマンドを使用して、データベースと iDRAC7 NIC 設定を元のデフォルト設定にリセットし、すべてのユーザーとユーザー設定を削除します。root ユーザーは使用可能ですが、その他のユーザー設定もデフォルト設定にリセットされます。**

構文解析規則

- 「#」から始まる行はすべてコメントとして扱われます。コメント行は、1 列目で始まる必要があります。他の列の「#」文字は、「#」文字として扱われます。一部のモデムパラメータには、文字列に「#」文字が含まれる場合があります。エスケープ文字は必要ありません。racadm getconfig -f <ファイル名> **.cfg** コマンドで .cfg を生成し、エスケープ文字を追加せずに別の iDRAC7 に対して racadm config -f <ファイル名> .cfg コマンドを実行することができます。

  ```
  #

  # これはコメントです。

  [cfgUserAdmin]

  cfgUserAdminPageModemInitString=<モデム初期化文字列 # コメントではありません>
  ```

- すべてのグループエントリは、「[」と「]」で囲む必要があります。グループ名を示す始まりの「[」文字は、1 列目で*開始する必要*があり、このグループ名は、そのグループ内のどのオブジェクトよりも*前に指定する必要*もあります。関連付けられたグループ名を含まないオブジェクトがあると、エラーが発生します。設定データは、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』に定義されているとおりにグループにまとめられます。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例を示します。

  ```
  [cfgLanNetworking] -{グループ名}

  cfgNicIpAddress=143.154.133.121 {オブジェクト名}
  ```

- すべてのパラメータは、「object」、「=」、または「value」の間に空白を入れず、「object=value」のペアとして指定されます。

  値の後ろにある空白は無視されます。値文字列内の空白は未変更のままとなります。「=」の右側の文字はすべてそのまま使用されます（たとえば、2 番目の「=」、または「#」、「[」、「]」など）。これらの文字は、有効なモデムチャットスクリプト文字です。

  上記の例を参照してください。

  racadm getconfig -f <ファイル名>.cfg コマンドを実行するとインデックスオブジェクトの前にコメントが置かれ、ユーザーが含まれているコメントを参照できます。

  インデックス付きグループの内容を表示するには、次のコマンドを使用します。

  ```
  racadm getconfig -g <グループ名> -i <インデックス 1〜16>
  ```

- インデックス付きグループの場合、オブジェクトアンカーが「[ ]」ペアの後の最初のオブジェクトである必要があります。次に、現在のインデックス付きグループの例を示します。

  ```
  [cfgUserAdmin]
  ```

```
cfgUserAdminIndex=11
```

`racadm getconfig -f <myexample>.cfg` と入力すると、このコマンドは現在の iDRAC7 設定のために **.cfg** ファイルを作成します。この設定ファイルは例として、および固有の **.cfg** ファイルの開始点として使用できます。

iDRAC7 IP アドレスの変更

設定ファイルで iDRAC7 の IP アドレスを変更する場合は、不必要なすべての *<変数>*=**value** エントリを削除します。IP アドレスの変更に関する 2 つの *<変数>*=**value** エントリを含む、「[」と「]」で囲まれた実際の変数グループのラベルのみが残ります。

例えば、次のとおりです。

```
#
# Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

このファイルは次のように更新されます。

```
#
# Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# comment, the rest of this line is ignored
cfgNicGateway=10.35.9.1
```

コマンド `racadm config -f myfile.cfg` はファイルを解析し、行番号によってすべてのエラーを識別します。正しいファイルは適切なエントリをアップデートします。また、前の例で示されたのと同じ `getconfig` コマンドを使用して、更新を確認することもできます。

このファイルを使用して会社全体の変更をダウンロードしたり、ネットワーク上で新しいシステムを設定したりできます。

メモ:「Anchor」は内部的な用語であるため、ファイルでは使用しないでください。

ホストシステムで iDRAC7 設定を変更するためのアクセスの無効化

ローカル RACADM または iDRAC 設定ユーティリティを使用して iDRAC7 設定を変更するためのアクセスを無効化できますが、これらの設定は、次の手順を実行して表示することができます。

1. iDRAC7 Web インタフェースで、**概要 → iDRAC 設定 → ネットワーク → サービス** と移動します。
2. 次のいずれか、または両方を選択します。
   - **iDRAC 設定を使用した iDRAC ローカル設定の無効化** — iDRAC 設定ユーティリティで設定を変更するためのアクセスを無効化します。
   - **RACADM を使用した iDRAC ローカル設定の無効化** — ローカル RACADM で設定を変更するためのアクセスを無効化します。
3. **適用** をクリックします。

メモ: アクセスが無効化されると、サーバー管理者または IPMITool を使用して iDRAC7 設定を実行できません。ただし、IPMI Over LAN を使用できます。

5

iDRAC7 と管理下システム情報の表示

iDRAC7 と管理下システムの正常性とプロパティ、ハードウェアとファームウェアのインベントリ、センサーの正常性、ストレージデバイス、ネットワークデバイスを表示できます。また、ユーザーセッションの表示および終了も行うことができます。ブレードサーバーの場合、フレックスアドレスの情報も表示できます。

関連リンク

管理下システムの正常性とプロパティの表示
システムインベントリの表示
センサー情報の表示
ストレージデバイスのインベントリと監視
ネットワークデバイスのインベントリおよび監視
FlexAddress メザニンカードのファブリック接続の表示
iDRAC7 セッションの表示または終了

管理下システムの正常性とプロパティの表示

iDRAC7 ウェブインタフェースにログインすると、**システムサマリ** ページでは、管理下システムの正常性、基本的な iDRAC7 情報の表示、仮想コンソールのプレビュー、作業メモの追加と表示が可能になり、電源オン / オフ、パワーサイクル、ログの表示、ファームウェイのアップデート、iDRAC7 のリセットなどの作業を迅速に開始することができます。

システムサマリ ページにアクセスするには、**概要 → サーバー → プロパティ → サマリ** に移動します。**システムサマリ** ページが表示されます。詳細については、『*iDRAC7 Online Help*』を参照してください。

iDRAC 設定ユーティリティを使用して、基本的なシステムサマリ情報を表示することもできます。これには、iDRAC 設定ユーティリティで、**システムサマリ** に移動します。**iDRAC 設定 システムサマリ** ページが表示されます。詳細については、『*iDRAC 設定ユーティリティオンラインヘルプ*』を参照してください。

システムインベントリの表示

管理下システムに取り付けられたハードウェアおよびファームウェアコンポーネントに関する情報を表示できます。これを行うには、iDRAC7 ウェブインタフェースで、**概要 → サーバー → プロパティ → システムインベントリ** と移動します。表示されたプロパティについては、『iDRAC7 オンラインヘルプ』を参照してください。

ハードウェアコンポーネントを交換する、またはファームウェアバージョンをアップデートする場合は、再起動時におけるシステムインベントリの収集のため、**再起動時のシステムインベントリの収集**（CSIOR）オプションを有効化して実行するようにします。数分後に、iDRAC7 にログインし、**システムインベントリ** ページに移動して詳細を表示します。サーバーに取り付けられたハードウェアによっては、情報が利用可能になるまでに最大 5 分間かかることがあります。

メモ: CSIOR オプションはデフォルトで有効化されます。

センサー情報の表示

次のセンサーは、管理下システムの正常性を監視するために役に立ちます。

- **バッテリセンサー** — システム基板 CMOS およびストレージの RAID On Motherboard（ROMB）上のバッテリに関する情報を提供します。

メモ: ストレージ ROMB のバッテリ設定は、システムにバッテリ装備の ROMB がある場合にのみ利用可能です。

- **ファンセンサー**（ラックおよびタワーサーバーの場合のみ利用可能） — システムファンに関する情報（ファンの冗長性や、ファン速度としきい値が示されたファンのリスト）を提供します。
- **CPU センサー** — 管理下システムの CPU の正常性および状態を示します。
- **イントルージョンセンサー** — シャーシに関する情報を提供します。
- **電源装置センサー**（ラックおよびタワーサーバーの場合のみ利用可能） — 電源装置と電源装置の冗長性ステータスに関する情報を提供します。

メモ: システムに電源装置が 1 つしかない場合、電源装置の冗長性は **無効** に設定されます。

- **リムーバブルフラッシュメディアセンサー** — 内部 SD モジュール（vFlash および 内部デュアル SD モジュール（IDSDM））に関する情報を提供します。
  - IDSDM の冗長性が有効な場合は、「IDSDM Redundancy Status, IDSDM SD1, IDSDM SD2」という IDSDM センサーステータスが表示されます。冗長性が無効な場合は、IDSDM SD1 のみが表示されます。
  - システムの電源がオンになったとき、または iDRAC のリセット後は、当初 IDSDM の冗長性が無効化されています。カードの挿入後にのみ IDSDM SD1 センサーのステータスが表示されます。
  - IDSDM に存在する 2 つの SD カードで IDSDM 冗長性が有効化されている場合、一方の SD カードのステータスが *オンライン* になり、他方のカードのステータスが *オフライン* になります。IDSDM の 2 つの SD カード間で冗長性を復元するには、システムの再起動が必要になります。冗長性の復元後、IDSDM の SD カード両方のステータスが *オンライン* になります。
  - IDSDM に存在する 2 つの SD カード間で冗長性を復元する再構築中は、IDSDM センサーの電源がオフであるため、IDSDM ステータスが表示されません。
  - IDSDM モジュール内の書き込み保護された、または破損した SD カードに対するシステムイベントログ（SEL）は、SD カードを書き込み可能または破損なしの SD カードと取り換えることによってクリアされるまで繰り返されません。
- **温度センサー** — システム基板の吸気口の温度と排気口の温度に関する情報を提供します（ラックおよびタワーにのみ該当）。この温度プローブは、プローブのステータスが事前設定警告と重大なしきい値の範囲内にあるかどうかを示します。
- **電圧センサー** — さまざまなシステムコンポーネントの電圧センサーのステータスと読み取り値を示します。

次の表は、iDRAC7 ウェブインタフェースと RACADM を使用してセンサー情報を表示する方法を示しています。ウェブインタフェースに表示されたプロパティについては、『*iDRAC7 オンラインヘルプ*』の該当するページを参照してください。

表 8. ウェブインタフェースおよび RACADM を使用したセンサー情報

情報を表示するセンサー	ウェブインタフェース使用	RACADM 使用
バッテリ	**概要 → ハードウェア → バッテリ**	**getsensorinfo** コマンドを使用します。 電源装置については、get サブコマンドとともに **System.Power.Supply** コマンドを使用することもできます。 詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。
ファン	**概要 → ハードウェア → ファン**	

情報を表示するセンサー	ウェブインタフェース使用	RACADM 使用
CPU	**概要 → ハードウェア → CPU**	
イントルージョン	**概要 → サーバー → イントルージョン**	
電源装置	**概要 → ハードウェア → 電源装置**	
リムーバブルフラッシュメディア	**概要 → ハードウェア → リムーバブルフラッシュメディア**	
温度	**概要 → サーバー → 電源 / 熱 → 温度**	
電圧	**概要 → サーバー → 電源 / 熱 → 電圧**	

ストレージデバイスのインベントリと監視

iDRAC7 ウェブインタフェースまたは RACADM を使用して、管理下システム内にある次の Comprehensive Embedded Management（CEM）対応ストレージデバイスの正常性をリモートで監視、およびそれらのインベントリを表示することができます。

- バッテリ装備の RAID コントローラ。
- エンクロージャ管理モジュール（EMM）、電源装置、ファンプローブ、および温度プローブ装備のエンクロージャ
- 物理ディスク
- 仮想ディスク

ただし、WS-MAN では、システム内のほとんどのストレージデバイスの情報が表示されます。

iDRAC7 は、H310、H710、H710P、および H810 を含む、PERC 8 シリーズの RAID コントローラに対してインベントリと監視を行います。Comprehensive Embedded Management に対応していないコントローラには、内蔵テープアダプタ（ITA）と SAS 6Gbps HBA があります。

最近のストレージイベントおよびストレージデバイスのトポロジも表示されます。

ストレージイベントに対してアラートと SNMP トラップが生成されます。これらのイベントは、ライフサイクルログに記録されます。

概念情報については、**support.dell.com/manuals** にある『*OpenManage Storage Management ユーザーズガイド*』を参照してください。

ウェブインタフェースを使用したストレージデバイスの監視

ウェブインタフェースを使用してストレージデバイス情報を表示するには、次の手順を実行します。

- **概要 → ストレージ → サマリ** と移動して、ストレージコンポーネントと最近記録されたイベントのサマリを表示します。このページは、30 秒ごとに自動更新されます。
- **概要 → ストレージ → トポロジ** と移動して、物理的に包含されている主要なストレージコンポーネントを階層的に表示します。
- **概要 → ストレージ → 物理ディスク** と移動して、物理ディスク情報を表示します。**物理ディスク** ページが表示されます。
- **概要 → ストレージ → 仮想ディスク** と移動して、仮想ディスク情報を表示します。**仮想ディスク** ページが表示されます。
- **概要 → ストレージ → コントローラ** と移動して、RAID コントローラ情報を表示します。**コントローラ** ページが表示されます。
- **概要 → ストレージ → エンクロージャ** と移動して、エンクロージャ情報を表示します。**エンクロージャ** ページが表示されます。

フィルタを使用して、特定のデバイス情報を表示することもできます。
表示されたプロパティの詳細と、フィルタオプションの使用法については、『*iDRAC7 オンラインヘルプ*』を参照してください。

RACADM を使用したストレージデバイスの監視

ストレージデバイス情報を参照するには、**raid** コマンドを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

ネットワークデバイスのインベントリおよび監視

管理下システム内の次のネットワークデバイスについて、リモートで正常性を監視し、インベントリを表示できます。

- ネットワークインタフェースカード（NIC）
- 統合型ネットワークアダプタ（CNA）
- LAN On Motherboard（LOM）
- ネットワークドーターカード（NDC）
- メザニンカード（ブレードサーバーのみ）

デバイスごとに、次のポート情報とサポートされているパーティションを表示できます。

- リンクステータス
- プロパティ
- 設定および機能
- 受信および送信統計情報

ウェブインタフェースを使用したネットワークデバイスの監視

ウェブインタフェースを使用してネットワークデバイスの情報を表示するには、**概要 → ハードウェア → ネットワークデバイス** と移動します。**ネットワークデバイス** ページが表示されます。表示されるプロパティの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。

メモ: OS ドライバの状態 に動作可能という状態が表示される場合、その表示はオペレーティングシステムドライバの状態または UEFI ドライバの状態を示しています。

RACADM を使用したネットワークデバイスの監視

ネットワークデバイス情報を参照するには、**hwinventory** コマンドと **nicstatistics** コマンドを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。
RACADM または WS-MAN を使用すると、iDRAC7 ウェブインタフェースに表示されるプロパティ以外に、追加のプロパティが表示される場合があります。

FlexAddress メザニンカードのファブリック接続の表示

ブレードサーバーでは、FlexAddress により、管理下サーバーの各ポート接続に、永続的なシャーシ割り当てのワールドワイド名と MAC アドレス（WWN/MAC）を使用できます。
取り付け済みの内蔵 Ethernet ポートやオプションのメザニンカードポートごとに、次の情報を表示できます。

- カードが接続されているファブリック。
- ファブリックのタイプ。
- サーバー割り当て、シャーシ割り当て、またはリモート割り当ての MAC アドレス。

iDRAC7 で Flex Address 情報を表示するには、Chassis Management Controller（CMC）で Flex Address 機能を設定し、有効化します。詳細については、**support.dell.com/manuals** にある『*Dell Chassis Management Controller ユーザーガイド*』を参照してください。FlexAddress 設定を有効化したり無効化すると、既存の仮想コンソールまたは仮想メディアセッションは終了します。

メモ: 管理下システムに電源を投入できなくするようなエラーを防ぐために、各ポートとファブリック接続には正しいタイプのメザニンカードを取り付けることが *必要* です。

FlexAddress 機能は、サーバー割り当ての MAC アドレスをシャーシ割り当ての MAC アドレスに置き換えます。この機能は、ブレード LOM、メザニンカード、および I/O モジュールとともに iDRAC7 に実装されます。iDRAC7 の FlexAddress 機能では、シャーシ内の iDRAC7 に対してスロット固有の MAC アドレスの保存がサポートされます。シャーシ割り当ての MAC アドレスは、CMC の不揮発性メモリに保存され、iDRAC7 の起動時、あるいは CMC の FlexAddress が有効化されたときに、iDRAC7 に送信されます。

CMC がシャーシ割り当ての MAC アドレスを有効化すると、iDRAC7 が次のいずれかのページで **MAC アドレス** を表示します。

- **概要 → サーバー → プロパティ 詳細情報 → iDRAC 情報**。
- **概要 → サーバー → プロパティ WWN/MAC**。
- **概要 → iDRAC 設定 → プロパティ iDRAC 情報 → 現在のネットワーク設定**。
- **概要 → iDRAC 設定 → ネットワーク ネットワーク → ネットワーク設定**。

注意: FlexAddress が有効な状態では、サーバー割り当ての MAC アドレスからシャーシ割り当ての MAC アドレスに切り替えた場合（その逆も同様）、iDRAC7 IP アドレスも変更されます。

iDRAC7 セッションの表示または終了

現在 iDRAC7 にログインしているユーザー数を表示し、ユーザーセッションを終了することができます。

ウェブインタフェースを使用した iDRAC7 セッションの終了

管理権限を持たないユーザーが、iDRAC7 ウェブインタフェースを使用して iDRAC7 セッションを終了するには、iDRAC7 の設定権限が必要です。

iDRAC7 セッションを表示および終了するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → セッション** と移動します。
   セッション ページにはセッション ID、ユーザー名、IP アドレス、およびセッションタイプが表示されます。これらのプロパティの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。
2. セッションを終了するには、**終了** 行で、セッション用のごみ箱 アイコンをクリックします。

RACADM を使用した iDRAC7 セッションの終了

RACADM を使用して iDRAC7 セッションを終了するには、システム管理者権限が必要です。

現在のユーザーセッションを表示するには、**getssninfo** コマンドを使用します。

ユーザーセッションを終了するには、**closessn** コマンドを使用します。

これらのコマンドの詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

6

iDRAC7 通信のセットアップ

次のいずれかのモードを使用して iDRAC7 と通信できます。

- iDRAC7 ウェブインタフェース
- DB9 ケーブルを使用したシリアル接続（RAC シリアルまたは IPMI シリアル） - ラックサーバーまたはタワーサーバーの場合のみ
- IPMI シリアルオーバー LAN
- IPMI Over LAN
- リモート RACADM
- ローカル RACADM
- Remote Services

対応プロトコル、対応コマンド、および前提条件の概要については、次の表を参照してください。

表 9. 通信モード — サマリ

通信のモード	対応プロトコル	対応コマンド	前提条件
iDRAC7 ウェブインタフェース	インターネットプロトコル（https）	-	ウェブサーバー
ヌルモデム DB9 ケーブルを使用したシリアル	シリアルプロトコル	RACADM SMCLP IPMI	iDRAC7 ファームウェアの一部 RAC シリアルまたは IPMI シリアルが有効です。
IPMI シリアルオーバー LAN	インテリジェントプラットフォーム管理バスプロトコル SSH Telnet	IPMI	IPMITool がインストール済みで、IPMI シリアルオーバー LAN が有効です。
IPMI Over LAN	インテリジェントプラットフォーム管理バスプロトコル	IPMI	IPMITool がインストール済みで、IPMI の設定が有効です。
SMCLP	SSH Telnet	SMCLP	iDRAC7 上で SSH または Telnet が有効です。
リモート RACADM	https	リモート RACADM	リモート RACADM がインストール済みで、有効です。
ファームウェア RACADM	SSH Telnet	ファームウェア RACADM	ファームウェア RACADM がインストール済みで、有効です。
ローカル RACADM	IPMI	ローカル RACADM	ローカル RACADM がインストール済みです。
リモートサービス [1]	WS-MAN	WinRM（Windows） OpenWSMAN（Linux）	WinRM（Windows）または OpenWSMAN（Linux）がインストール済みです。

通信のモード	対応プロトコル	対応コマンド	前提条件

[1] 詳細については、**support.dell.com/manuals** にある『*Lifecycle Controller Remote Services ユーザーズガイド*』を参照してください。

関連リンク

DB9 ケーブルを使用したシリアル接続による iDRAC7 との通信
DB9 ケーブル使用時の RAC シリアルとシリアルコンソールの切り替え
IPMI SOL を使用した iDRAC7 との通信
IPMI Over LAN を使用した iDRAC7 との通信
リモート RACADM の有効化または無効化
ローカル RACADM の無効化
管理下システムでの IPMI の有効化
起動中の Linux のシリアルコンソールの設定
サポートされる SSH 暗号化スキーム

DB9 ケーブルを使用したシリアル接続による iDRAC7 との通信

次のいずれかの通信方法を使用して、システム管理の作業をラックサーバーまたはタワーサーバーへのシリアル接続経由で実行できます。

- RAC シリアル
- IPMI シリアル — ダイレクト接続基本モードまたはダイレクト接続ターミナルモード

メモ: ブレードサーバーの場合、シリアル接続はシャーシを介して確立されます。詳細については、**support.dell.com/manuals** にある『*Chassis Management Controller ユーザーズガイド*』を参照してください。

シリアル接続を確立するには、次の手順を実行します。

1. BIOS を設定して、シリアル接続を有効にします。
2. ヌルモデム DB9 ケーブルで管理ステーションをシリアルポートから管理対象システムの外部シリアルコネクタに接続します。
3. 次のいずれかを使用して、管理ステーションのターミナルエミュレーションソフトウェアがシリアル接続用に設定されていることを確認します。
   - Xterm の Linux Minicom
   - Hilgraeve の HyperTerminal Private Edition（バージョン 6.3）

   管理対象システムが起動プロセスのどの段階にあるかに応じて、POST の画面またはオペレーティングシステムの画面が表示されます。これは、Windows の SAC および Linux の Linux テキストモード画面の設定に基づきます。
4. iDRAC7 で RAC シリアル接続または IPMI シリアル接続を有効にします。

関連リンク

BIOS でのシリアル接続の設定
RAC シリアル接続の有効化
IPMI シリアル接続のベーシックモードおよびターミナルモードの有効化

BIOS でのシリアル接続の設定

シリアル接続向けに BIOS を設定するには、次の手順を実行します。

メモ: これは、ラックおよびタワーサーバー上の iDRAC7 にのみ適用されます。

1. システムの電源を入れるか、再起動します。
2. <F2> を押します。
3. **システム BIOS 設定** → **シリアル通信** と移動します。
4. **リモートアクセスデバイス** に **外部シリアルコネクタ** を選択します。
5. **戻る**、**終了** の順にクリックし、**はい** をクリックします。
6. <Esc> を押して **BIOS** に戻ります。

RAC シリアル接続の有効化

BIOS でシリアル接続を有効にした後、iDRAC7 で RAC シリアルを有効にします。

メモ: これは、ラックおよびタワーサーバー上の iDRAC7 にのみ適用されます。

ウェブインタフェースを使用した RAC シリアル接続の有効化

RAC シリアル接続を有効にするには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要** → **iDRAC 設定** → **ネットワーク** → **シリアル** と移動します。
   シリアル ページが表示されます。
2. **RAC シリアル** で、**有効** を選択し、各属性の値を指定します。
3. **適用** をクリックします。
   IPMI シリアル設定が設定されます。

RACADM を使用した RAC シリアル接続の有効化

RAC シリアル接続を有効にするには、次のコマンドを実行します。

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

IPMI シリアル接続のベーシックモードおよびターミナルモードの有効化

iDRAC7 への BIOS の IPMI シリアルルーティングを有効にするには、iDRAC7 で IPMI シリアルを次のいずれかのモードに設定します。

メモ: これは、ラックおよびタワーサーバー上の iDRAC7 にのみ適用されます。

- IPMI ベーシックモード — ベースボード管理ユーティリティ (BMU) に付属する、IPMI シェル (ipmish) などのプログラムアクセス用バイナリインタフェースをサポートします。たとえば、IPMI ベーシックモードで ipmish を使用してシステムイベントログを印刷するには、次のコマンドを実行します。

  ```
  ipmish -com 1 -baud 57600 -flow cts -u root -p calvin sel get
  ```

- IPMI ターミナルモード — シリアルターミナルから送信される ASCII コマンドをサポートします。このモードは、16 進法の ASCII 文字として入力される限られた数のコマンド (電源コントロールを含む) と、raw IPMI コマンドをサポートします。このモードでは、SSH または Telnet を介して iDRAC7 にログインすると、BIOS までのオペレーティングシステム起動順序を表示できます。

関連リンク

BIOS でのシリアル接続の設定
IPMI シリアルターミナルモード用の追加設定

ウェブインタフェースを使用したシリアル接続の有効化

IPMI シリアルを有効にするには、RAC シリアルインタフェースを無効にするようにしてください。

IPMI シリアル設定を設定するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ネットワーク → シリアル** と移動します。
2. **IPMI シリアル** で、各属性の値を指定します。オプションの情報については、『*iDRAC7 オンラインヘルプ*』を参照してください。
3. **適用** をクリックします。

RACADM を使用したシリアル接続 IPMI モードの有効化

IPMI モードを設定するには、次の手順を実行します。

1. RAC シリアルインタフェースを無効にします。
   ```
   racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
   ```
2. 適切な IPMI モードを有効にします。
   ```
   racadm config -g cfgIpmiSerial -o cfgIpmiSerialConnectionMode <0 または 1>
   ```
   ここで、*0* はターミナルモードを示し、*1* は基本モードを示します。

RACADM を使用したシリアル接続 IPMI のシリアル設定の有効化

IPMI シリアルを設定するには、次の手順を実行します。

1. 次のコマンドを使用して、IPMI シリアル接続モードを適切な設定に変更します。
   ```
   racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
   ```
2. コマンド `racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate <ボーレート>` を使用して、IPMI シリアルボーレートを設定します。ここで、<ボーレート> は、9600、19200、57600、または 115200 bps になります。
3. コマンド `racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1` を使用して、IPMI シリアルハードウェアフロー制御を有効にします。
4. コマンド `racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <レベル>` を使用して、IPMI シリアルチャネル最小権限レベルを設定します。ここで、<レベル> は、2（ユーザー）、3（オペレータ）、または 4（管理者）になります。
5. BIOS でシリアル接続を設定するためには、BIOS セットアッププログラムでシリアル MUX（外部シリアルコネクタ）がリモートアクセスデバイスに対して適切に設定されているようにしてください。
   これらのプロパティの詳細については、IPMI 2.0 仕様を参照してください。

IPMI シリアルターミナルモード用の追加設定

本項では、IPMI シリアルターミナルモード用の追加設定について説明します。

ウェブインタフェースを使用した IPMI シリアルターミナルモードに対する追加設定

ターミナルモードを設定するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ネットワーク → シリアル** と移動します。
   シリアル ページが表示されます。
2. IPMI シリアルを有効にします。
3. **ターミナルモード設定** をクリックします。
   ターミナルモード設定 ページが表示されます。
4. 次の値を指定します。
   - 行編集
   - 削除制御
   - エコー制御
   - ハンドシェイク制御

- 新しい行シーケンス
- 新しい行シーケンスの入力

オプションの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。

5. **適用** をクリックします。
   ターミナルモードが設定されます。
6. BIOS でシリアル接続を設定するためには、BIOS セットアッププログラムでシリアル MUX（外部シリアルコネクタ）がリモートアクセスデバイスに対して適切に設定されているようにしてください。

RACADM を使用した IPMI シリアルターミナルモードに対する追加設定

ターミナルモードを設定するには、コマンド `racadm config cfgIpmiSerial` を実行します。

DB9 ケーブル使用時の RAC シリアルとシリアルコンソールの切り替え

iDRAC7 は、ラックおよびタワーサーバーにおいて、RAC シリアルインタフェース通信と、シリアルコンソールの間の切り替えを可能にするエスケープキーシーケンスをサポートします。

シリアルコンソールから RAC シリアルへの切り替え

シリアルコンソールモードのときに RAC シリアルインタフェース通信モードに切り替えるには、次のキーシーケンスを使用してください。

```
<Esc> +<Shift> <9>
```

このキーシーケンスを使用すると、「iDRAC ログイン」プロンプト（iDRAC が RAC シリアルモードに設定されている場合）、またはターミナルコマンドを発行できるシリアル接続モード（iDRAC が IPMI シリアルダイレクト接続ターミナルモードに設定されている場合）に移動します。

RAC シリアルからシリアルコンソールへの切り替え

RAC シリアルインタフェース通信モードのときにシリアルコンソールモードに切り替えるには、次のキーシーケンスを使用します。

```
<Esc> +<Shift> <q>
```

ターミナルモードのときにシリアルコンソールモードに切り替えるには、次のキーシーケンスを使用します。

```
<Esc> +<Shift> <q>
```

シリアルコンソールモードで接続されているときにターミナルモードに戻るには、次のキーシーケンスを使用します。

```
<Esc> +<Shift> <9>
```

IPMI SOL を使用した iDRAC7 との通信

IPMI シリアルオーバー LAN（SOL）は、管理下システムのテキストベースのコンソールシリアルデータを iDRAC7 の専用または共有帯域外 Ethernet 管理ネットワークを介してリダイレクトすることを可能にします。SOL を使用して、次の操作を行えます。

- タイムアウトなしでオペレーティングシステムにリモートアクセスする。
- Windows の Emergency Management Services（EMS）または Special Administrator Console（SAC）、Linux シェルでホストシステムを診断する。
- POST 中サーバーの進捗状況を表示し、BIOS セットアッププログラムを再設定する。

SOL 通信モードを設定するには、次の手順を実行します。

1. シリアル接続のための BIOS を設定します。
2. SOL を使用するように iDRAC7 を設定します。
3. サポートされるプロトコル（SSH、Telnet、IPMItool）を有効にします。

関連リンク

BIOS のシリアル接続用設定
SOL を使用するための iDRAC7 の設定
対応プロトコルの有効化

BIOS のシリアル接続用設定

BIOS をシリアル接続用に設定するには、次の手順を実行します。

メモ: これは、ラックおよびタワーサーバー上の iDRAC7 にのみ適用されます。

1. システムの電源を入れるか、再起動します。
2. <F2> を押します。
3. **システム BIOS 設定** → **シリアル通信** と移動します。
4. 次の値を指定します。
   - シリアル通信 — コンソールリダイレクトでオン。
   - シリアルポートアドレス — COM2。

メモ: シリアルポートアドレス フィールドの **シリアルデバイス 2** も com1 に設定されている限り、**シリアル通信** フィールドを **com1 のシリアルリダイレクトでオン** に設定できます。

   - 外部シリアルコネクタ — シリアルデバイス 2
   - フェイルセーフボーレート — 115200
   - リモートターミナルの種類 — VT100/VT220
   - 起動後のリダイレクト — 有効
5. **次へ** をクリックしてから、**終了** をクリックします。
6. **はい** をクリックして変更を保存します。
7. <Esc> を押して **セットアップユーティリティ** を終了します。

SOL を使用するための iDRAC7 の設定

ウェブインタフェース、RACADM、または iDRAC 設定ユーティリティを使用して、iDRAC7 の SOL 設定を指定できます。

iDRAC7 ウェブインタフェースを使用した SOL を使用するための iDRAC7 の設定

IPMI シリアルオーバー LAN （SOL）を設定するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要** → **iDRAC 設定** → **ネットワーク** → **シリアルオーバー LAN** と移動します。
   シリアルオーバー LAN ページが表示されます。
2. SOL を有効にし、値を指定して、**適用** をクリックします。
   IPMI SOL 設定が設定されます。
3. 文字の蓄積間隔と文字の送信しきい値を設定するには、**詳細設定** を選択します。
   シリアルオーバー LAN 詳細設定 ページが表示されます。

4. 各属性の値を指定し、**適用** をクリックします。
   IPMI SOL の詳細設定が設定されます。これらの値は、パフォーマンスの改善に役立ちます。
   オプションの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。

RACADM を使用した SOL 使用のための iDRAC7 の設定

IPMI シリアルオーバー LAN （SOL）を設定するには、次の手順を実行します。

1. IPMI シリアルオーバー LAN を有効にするには、コマンド `racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1` を実行します。
2. コマンド `racadm config -g cfgIpmiSol o cfgIpmiSolMinPrivilege <レベル>` を使用して、IPMI SOL の最小権限レベルをアップデートします。ここで、<レベル> は 2（ユーザー）、3（オペレータ）、4（システム管理者）です。

メモ: IPMI SOL の最小権限レベルは、IPMI SOL をアクティブにするための最低限の権限を決定します。詳細については、IPMI 2.0 の仕様を参照してください。

3. コマンド `racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <ボーレート>` を使用して、IPMI SOL ボーレートをアップデートします。ここで、<ボーレート> は 9600、19200、57600、または 115200 bps です。

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

4. コマンド `racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <ID> 2` を使用して、各ユーザーに対して SOL を有効にします。ここで、`<ID>` は、ユーザーの固有 ID です。

対応プロトコルの有効化

サポートされるプロトコルは、IPMI、SSH、および Telnet です。

ウェブインタフェースを使用した対応プロトコルの有効化

SSH または Telnet を有効にするには、**概要 → iDRAC 設定 → ネットワーク → サービス** と移動し、SSH または Telnet に対してそれぞれ **有効** を選択します。

IPMI を有効にするには、**概要 → iDRAC 設定 → ネットワーク** と移動し、**IPMI オーバー LAN の有効化** を選択します。**暗号化キー** の値がすべてゼロであることを確認します。そうでない場合は、Backspace キーを押してクリアし、値をヌル文字に変更します。

RACADM を使用したサポート対象プロトコルの有効化

SSH または Telnet を有効にするには、次のコマンドを実行します。

- Telnet - `racadm config -g cfgSerial -o cfgSerialTelnetEnable 1`
- SSH - `racadm config -g cfgSerial -o cfgSerialSshEnable 1`

メモ: SSH ポートを変更するには、コマンド `racadm config -g cfgRacTuning -o cfgRacTuneSshPort <ポート番号>` を実行します。

次のようなツールを使用できます。

- IPMI プロトコルを使用する場合は IPMItool
- SSH または Telnet プロトコルを使用する場合は Putty/OpenSSH

関連リンク

IPMI プロトコルを使用した SOL
SSH または Telnet プロトコルを使用した SOL

IPMI プロトコルを使用した SOL

IPMItool <--> LAN/WAN 接続 <--> iDRAC7

IPMI ベースの SOL ユーティリティと IPMItool は、UDP データグラムを使用してポート 623 に配信される RMCP + を使用します。RMCP+ は、改善された認証、データ整合性チェック、暗号化、および IPMI 2.0 の使用中に複数の種類のペイロードを伝送する機能を提供します。詳細については、**http://ipmitool.sourceforge.net/manpage.html** を参照してください。

RMCP+ は、認証のために 40 文字の 16 進数文字列（文字 0～9、a～f、および A～F）暗号化キーを使用します。デフォルト値は 40 個のゼロから成る文字列です。

iDRAC7 に対する RMCP+ 接続は、暗号化キー（キージェネレータ（KG）キー）を使用して暗号化する必要があります。暗号化キーは、iDRAC7 ウェブインタフェースまたは iDRAC 設定ユーティリティを使用して設定できます。

管理ステーションから IPMItool を使用して SOL セッションを開始するには、次の手順を実行します。

メモ: 必要に応じて、**概要 → iDRAC 設定 → ネットワーク → サービス** と選択して、デフォルトの SOL タイムアウトを変更できます。

1. 『*Dell Systems Management Tools and Documentation*』DVD から IPMITool をインストールします。
   インストール手順については、『*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。
2. コマンドプロンプト（Windows または Linux）で、コマンド `ipmitool -H <iDRAC7 IP アドレス> -I lanplus -U <ログイン名> -P <ログインパスワード> sol activate` を実行して、iDRAC7 から SOL を開始します。
   これにより、管理ステーションが管理対象システムのシリアルポートに接続されます。
3. IPMItool から SOL セッションを終了するには、<~> と <.> を連続して押します。この結果、SOL セッションが終了します。

メモ: SOL セッションが終了しない場合は、iDRAC7 をリセットし、起動が完了するまで最大 2 分間待ちます。

SSH または Telnet プロトコルを使用した SOL

セキュアシェル（SSH）および Telnet は、iDRAC7 へのコマンドライン通信の実行に使用されるネットワークプロトコルです。これらのいずれかのインタフェースを介して、リモートの RACADM コマンドおよび SMCLP コマンドを解析できます。

SSH には、Telnet より優れたセキュリティが備わっています。iDRAC7 では、パスワード認証を伴う SSH バージョン 2 のみをサポートしており、このプロトコルがデフォルトで有効になります。iDRAC7 は最大 2 つの SSH セッションと 2 つの Telnet セッションを同時にサポートします。Telnet はセキュアなプロトコルではないことから、SSH を使用することをお勧めします。Telnet は、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インフラストラクチャがセキュアである場合にのみ使用するようにしてください。

管理ステーションで PuTTY や OpenSSH などの SSH および Telnet ネットワークプロトコルをサポートするオープンソースプログラムを使用して、iDRAC7 に接続します。

メモ: Windows では、VT100 または ANSI ターミナルエミュレータから `OpenSSH` を実行します。Windows コマンドプロンプトで `OpenSSH` を実行しても、フル機能は使用できません（つまり、一部のキーが応答せず、グラフィックが表示されません）。

SSH または Telnet を使用して iDRAC7 と通信する前に、次の操作を行うようにしてください。

1. シリアルコンソールを有効化するよう BIOS を設定。
2. iDRAC7 に SOL を設定。
3. iDRAC7 ウェブインタフェースまたは RACADM を使用して、SSH または Telnet を有効化。
   Telnet（ポート 23）/SSH（ポート 22）クライアント <--> WAN 接続 <--> iDRAC7

iDRAC7 ではシリアルからネットワークへの変換が行われるので、SSH または Telnet プロトコルを使用する IPMI ベースの SOL では追加のユーティリティを必要としません。使用する SSH または Telnet コンソールは、管理下システムのシリアルポートから到着するデータを解釈し、応答することができる必要があります。シリアルポートは通常、ANSI ターミナルまたは VT100/VT220 ターミナルをエミュレートするシェルに接続します。シリアルコンソールは、自動的に SSH または Telnet コンソールにリダイレクトされます。

関連リンク

Windows での PuTTY からの SOL の使用
Linux での OpenSSH または Telnet からの SOL の使用

Windows での PuTTY からの SOL の使用

Windows 管理ステーションで PuTTY から IPMI SOL を開始するには、次の手順を実行します。

メモ: 必要に応じて、**概要 → iDRAC 設定 → ネットワーク → サービス** で、デフォルトの SSH または Telnet タイムアウトを変更できます。

1. iDRAC7 に接続するためのコマンド `putty.exe [-ssh | -telnet] <ログイン名>@<iDRAC7 IP アドレス> <ポート番号>` を実行します。

メモ: ポート番号はオプションです。ポート番号を再割り当てするときにのみ必要です。

2. コマンド `console com2` または `connect` を実行して SOL を開始し、管理下システムを起動します。

   管理ステーションから、SSH または Telnet プロトコルを使用する管理下システムへの SOL セッションが開始されます。iDRAC7 コマンドラインコンソールにアクセスするには、ESC キーシーケンスに従ってください。PuTTY および SOL の接続動作は、次のとおりです。

   - POST 時における PuTTY を介した管理下システムへのアクセス中、PuTTY のファンクションキーおよびキーパッドが次のように設定されます。
     * VT100+ — F2 はパスしますが、F12 はパスできません。
     * ESC[n~ — F12 はパスしますが、F2 はパスできません。
   - Windows では、ホストの再起動直後に Emergency Management System（EMS）コンソールが開かれると、Special Admin Console（SAC）ターミナルが破損するおそれがあります。SOL セッションを終了し、ターミナルを閉じて、別のターミナルを開いてから、同じコマンドで SOL セッションを開始してください。

関連リンク

iDRAC7 コマンドラインコンソールでの SOL セッションの切断

Linux での OpenSSH または Telnet からの SOL の使用

Linux 管理ステーションで OpenSSH または Telnet から SOL を開始するには、次の手順を実行します。

メモ: 必要に応じて、**概要 → iDRAC 設定 → ネットワーク → サービス** と選択して、デフォルトの SSH または Telnet セッションタイムアウトを変更できます。

1. シェルを起動します。
2. 次のコマンドを使用して iDRAC7 に接続します。
   - SSH の場合：ssh <iDRAC7 IP アドレス> -l <ログイン名>
   - Telnet の場合：telnet <iDRAC7 IP アドレス>

メモ: Telnet サービスのポート番号をデフォルト値（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. コマンドプロンプトで次のいずれかのコマンドを入力して、SOL を開始します。

- `connect`
- `console com2`

これにより、iDRAC7 が管理下システムの SOL ポートに接続されます。SOL セッションが確立されると、iDRAC7 コマンドラインコンソールは利用できなくなります。エスケープキーシーケンスに正しく従い、iDRAC7 コマンドラインコンソールを開きます。また、エスケープキーシーケンスは、SOL セッションが接続されるとすぐに画面に表示されます。管理下システムがオフの場合は、SOL セッションの確立にしばらく時間がかかります。

`console -h com2` コマンドは、キーボードからの入力またはシリアルポートからの新しい文字を待つ前にシリアル履歴バッファの内容を表示します。

履歴バッファのデフォルト（および最大）のサイズは 8192 文字です。次のコマンドを使用して、この数値をより小さい値に設定できます。

`racadm config -g cfgSerial -o cfgSerialHistorySize` <数値>

4. SOL セッションを終了してアクティブな SOL セッションを閉じます。

関連リンク

Telnet 仮想コンソールの使用
Telnet セッション用の Backspace キーの設定
iDRAC7 コマンドラインコンソールでの SOL セッションの切断

Telnet 仮想コンソールの使用

BIOS 仮想コンソールが VT100/VT220 エミュレーションに設定されている場合、Microsoft オペレーティングシステム上の一部の Telnet クライアントで BIOS セットアップ画面が適切に表示されないことがあります。この問題が発生した場合は、BIOS コンソールを ANSI モードに変更し、表示をアップデートします。BIOS セットアップメニューでこの手順を実行するには、**仮想コンソール → リモートターミナルの種類 → ANSI** と選択します。

クライアント VT100 エミュレーションウィンドウを設定するときは、リダイレクトされた仮想コンソールを表示するウィンドウまたはアプリケーションを 25 行 x 80 列に設定して、テキストが正しく表示されるようにしてください。この設定を行わないと、一部のテキスト画面が文字化けすることがあります。

Telnet 仮想コンソールを使用するには、次の手順を実行します。

1. **Windows コンポーネントサービス** で **Telnet** を有効化します。
2. コマンド `telnet <IP アドレス>:<ポート番号>` を使用して iDRAC7 に接続します。ここで、`IP` アドレスは、iDRAC7 の IP アドレスであり、ポート番号は Telnet ポート番号です（新しいポートを使用している場合）。

Telnet セッション用の Backspace キーの設定

Telnet クライアントによっては、<Backspace> キーを使用すると予期しない結果を招く場合があります。たとえば、セッションが `^h` をエコーする場合があります。ただし、ほとんどの Microsoft および Linux Telnet クライアントは、<Backspace> キーを使用するように設定できます。

Linux Telnet セッションで <Backspace> キーを使用するように設定するには、コマンドプロンプトを開き、`stty erase ^h` と入力します。プロンプトで、`telnet` と入力します。

Microsoft Telnet クライアントで <Backspace> キーを使用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. 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、`telnet` と入力します。Telnet セッションを実行している場合は、`<Ctrl><]>` を押します。
3. プロンプトで、`set bsasdel` と入力します。

   `Backspace は削除として送信されます` というメッセージが表示されます。

iDRAC7 コマンドラインコンソールでの SOL セッションの切断

SOL セッションを切断するコマンドはユーティリティに基づきます。ユーティリティは、SOL セッションが完全に終了した場合にのみ終了できます。

SOL セッションを切断するには、iDRAC7 コマンドラインコンソールから SOL セッションを終了します。

- SOL リダイレクトを終了するには、<Enter>、<Esc>、および <t> を押します。この結果、SOL セッションが閉じられます。
- Linux 上の Telnet から SOL を終了するには、<Ctrl>+] を押し続けます。Telnet 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。
- ユーティリティで SOL セッションが完全に終了していない場合は、他の SOL セッションを利用できないことがあります。この問題を解決するには、**概要 → iDRAC 設定 → セッション** と選択して ウェブインタフェースでコマンドラインコンソールを終了します。

IPMI Over LAN を使用した iDRAC7 との通信

iDRAC7 で IPMI Over LAN を設定して、すべての外部システムへの LAN チャネルを介した IPMI コマンドを有効または無効にする必要があります。設定が行われない場合、外部システムは IPMI コマンドを使用して iDRAC7 サーバーと通信できません。

ウェブインタフェースを使用した IPMI Over LAN の設定

IPMI Over LAN を設定するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ネットワーク** と移動します。
   ネットワーク ページが表示されます。
2. **IPMI の設定** で、属性の値を指定し、**適用** をクリックします。
   オプションの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。
   IPMI Over LAN が設定されます。

iDRAC 設定ユーティリティを使用した IPMI Over LAN の設定

IPMI Over LAN を設定するには、次の手順を実行します。

1. **iDRAC 設定ユーティリティ** で、**ネットワーク** に移動します。
   iDRAC 設定ネットワーク ページが表示されます。
2. **IPMI の設定** に値を指定します。
   これらのオプションについては、『*iDRAC 設定ユーティリティオンラインヘルプ*』を参照してください。
3. **戻る**、**終了** の順にクリックして、**はい** をクリックします。
   IPMI Over LAN が設定されます。

RACADM を使用した IPMI オーバー LAN の設定

IPMI Over LAN を設定するには、次の手順を実行します。

1. コマンド `racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1` を使用して IPMI Over LAN を有効にします。

メモ: この設定により、IPMI Over LAN インタフェースを使用して実行される IPMI コマンドが決定されます。詳細については、**intel.com** にある IPMI 2.0 仕様を参照してください。

2. コマンド `racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <レベル>` を使用して IPMI チャネル権限を更新します。ここで、<レベル> は、2（ユーザー）、3（オペレータ）、または 4（管理者）のいずれかです。
3. コマンド `racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <キー>` を使用して IPMI LAN チャネル暗号化キー（必要な場合）を設定します。ここで、<キー> は有効な 16 進形式の 20 文字の暗号化キーです。

メモ: iDRAC7 IPMI は、RMCP+ プロトコルをサポートします。詳細については、**intel.com** にある IPMI 2.0 仕様を参照してください。

リモート RACADM の有効化または無効化

iDRAC7 ウェブインタフェースまたは RACADM を使用して、リモート RACADM を有効または無効にできます。最大 5 つのリモート RACADM セッションを並行して実行できます。

ウェブインタフェースを使用したリモート RACADM の有効化または無効化

リモート RACADM を有効または無効にするには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ネットワーク → サービス** と移動します。
   サービス ページが表示されます。
2. **リモート RACADM** で **有効化**、または **無効化** を選択します。
3. **適用** をクリックします。
   この選択に基づいて、リモート RACADM が有効または無効になります。

RACADM を使用したリモート RACADM の有効化または無効化

RACADM リモート機能は、デフォルトで有効になっています。無効になっている場合は、コマンド `racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 1` を入力して有効化します。リモート機能を無効にするには、コマンド `racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0` を入力します。

メモ: これらのコマンドは、ローカルシステムで実行することをお勧めします。

ローカル RACADM の無効化

ローカル RACADM はデフォルトで有効になっています。無効化するには、「ホストシステムで iDRAC7 設定を変更するためのアクセスの無効化」を参照してください。

管理下システムでの IPMI の有効化

管理下システムでは、Dell Open Manage Server Administrator を使用して IPMI を有効または無効にします。詳細については、**support.dell.com\manuals** にある『*Dell Open Manage Server Administrator ユーザーズガイド*』を参照してください。

起動中の Linux のシリアルコンソールの設定

次の手順は Linux GRand Unified Bootloader（GRUB）に固有の手順です。異なるブートローダーを使用する場合は、類似した変更が必要です。

メモ: クライアント VT100 エミュレーションウィンドウを設定するときは、リダイレクトされた仮想コンソールを表示するウィンドウまたはアプリケーションを 25 行 x 80 列に設定して、テキストが正しく表示されるようにしてください。この設定を行わないと、一部のテキスト画面が文字化けすることがあります。

/etc/grub.conf ファイルを次のように編集します。

1. ファイルの全般設定セクションを見つけて、次の内容を追加します。
   ```
   serial --unit=1 --speed=57600 terminal --timeout=10 serial
   ```
2. カーネル行に次の 2 つにオプションを追加します。
   ```
   kernel ..... console=ttyS1,115200n8r console=tty1
   ```
3. GRUB のグラフィカルインタフェースを無効にし、テキストベースのインタフェースを使用します。テキストベースのインタフェースを使用しないと、GRUB 画面が RAC 仮想コンソールで表示されません。グラフィカルインタフェースを無効にするには、splashimage で始まる行をコメントアウトします。

   次の例は、この手順で説明された変更を示したサンプル **/etc/grub.conf** ファイルを示しています。

   ```
   # grub.conf generated by anaconda # Note that you do not have to rerun grub
   after making changes to this file # NOTICE: You do not have a /boot
   partition. This means that all # kernel and initrd paths are relative to /,
   e.g. # root (hd0,0) # kernel /boot/vmlinuz-version ro root=/dev/sda1 #
   initrd /boot/initrd-version.img #boot=/dev/sda default=0 timeout=10
   #splashimage=(hd0,2)/grub/splash.xpm.gz serial --unit=1 --speed=57600
   terminal --timeout=10 serial title Red Hat Linux Advanced Server (2.4.9-e.
   3smp) root (hd0,0) kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1
   hda=ide-scsi console=ttyS0 console=ttyS1,115200n8r initrd /boot/
   initrd-2.4.9-e.3smp.img title Red Hat Linux Advanced Server-up (2.4.9-e.3)
   root (hd0,00) kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s initrd /
   boot/initrd-2.4.9-e.3.im
   ```
4. RAC シリアル接続を介した仮想コンソールセッションを開始するための複数の GRUB オプションを有効にするには、すべてのオプションに次の行を追加します。
   ```
   console=ttyS1,115200n8r console=tty1
   ```
   この例は、最初のオプションに console=ttyS1,57600 を追加した例です。

起動後の仮想コンソールへのログインの有効化

ファイル **/etc/inittab** において、COM2 シリアルポートで agetty を設定する新しい行を追加します。

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

次の例は、新しい行が追加されたサンプルファイルを示しています。

```
#inittab This file describes how the INIT process should set up #the system in
a certain run-level. #Author:Miquel van Smoorenburg #Modified for RHS Linux by
Marc Ewing and Donnie Barnes #Default runlevel. The runlevels used by RHS are:
#0 - halt (Do NOT set initdefault to this) #1 - Single user mode #2 -
Multiuser, without NFS (The same as 3, if you do not have #networking) #3 -
Full multiuser mode #4 - unused #5 - X11 #6 - reboot (Do NOT set initdefault to
this) id:3:initdefault: #System initialization. si::sysinit:/etc/rc.d/
rc.sysinit l0:0:wait:/etc/rc.d/rc 0 l1:1:wait:/etc/rc.d/rc 1 l2:2:wait:/etc/
rc.d/rc 2 l3:3:wait:/etc/rc.d/rc 3 l4:4:wait:/etc/rc.d/rc 4 l5:5:wait:/etc/
rc.d/rc 5 l6:6:wait:/etc/rc.d/rc 6 #Things to run in every runlevel. ud::once:/
sbin/update ud::once:/sbin/update #Trap CTRL-ALT-DELETE ca::ctrlaltdel:/sbin/
shutdown -t3 -r now #When our UPS tells us power has failed, assume we have a
```

```
few #minutes of power left. Schedule a shutdown for 2 minutes from now. #This
does, of course, assume you have power installed and your #UPS is connected and
working correctly. pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System
Shutting Down" #If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

#Run gettys in standard runlevels co:2345:respawn:/sbin/agetty -h -L 57600
ttyS1 ansi 1:2345:respawn:/sbin/mingetty tty1 2:2345:respawn:/sbin/mingetty
tty2 3:2345:respawn:/sbin/mingetty tty3 4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5 6:2345:respawn:/sbin/mingetty tty6 #Run xdm
in runlevel 5 #xdm is now a separate service x:5:respawn:/etc/X11/prefdm -
nodaemon
```

ファイル **/etc/securetty** で、COM2 にシリアル tty の名前を含む新しい行を追加します。

```
ttyS1
```

次の例は、新しい行が追加されたサンプルファイルを示しています。

メモ: IPMI ツールを使用するシリアルコンソールでは、ブレークキーシーケンス（~B）を使用して、Linux **Magic SysRq** キーコマンドを実行します。

```
vc/1 vc/2 vc/3 vc/4 vc/5 vc/6 vc/7 vc/8 vc/9 vc/10 vc/11 tty1 tty2 tty3 tty4
tty5 tty6 tty7 tty8 tty9 tty10 tty11 ttyS1
```

サポートされる SSH 暗号化スキーム

SSH プロトコルを使用して iDRAC7 と通信するため、次の表に示す複数の暗号化スキームがサポートされています。

表 10. SSH 暗号化スキーム

スキームの種類	スキーム
非対称暗号化	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
PKA 認証	公開 - 秘密キーのペア

SSH の公開キー認証の使用

iDRAC7 は、SSH 上での公開キー認証（PKA）をサポートします。これは、ライセンスが必要な機能です。SSH 上での PKA がセットアップされ、適切に使用されると、iDRAC7 へのログインにユーザー名またはパスワードを入力する必要がありません。これは、さまざまな機能を実行する自動化スクリプトを設定する場合に役に立ちます。アップロードされたキーは、RFC 4716 または openssh 形式である必要があります。これ以外の形式である場合は、キーを RFC 4716 または openssh 形式に変換する必要があります。

どのシナリオでも、秘密キーと公開キーのペアを管理ステーションで生成する必要があります。管理ステーションと iDRAC7 間での信頼関係を確立するため、公開キーは iDRAC7 ローカルユーザーにアップロードされ、秘密キーは SSH クライアントによって使用されます。

公開キーと秘密キーのペアは、次を使用して生成できます。

- *PuTTY* キージェネレータアプリケーション（Windows が実行されているクライアント用）
- *ssh-keygen* CLI（Linux が実行されているクライアント用）

注意: 通常、この権限は iDRAC7 の管理者ユーザーグループのメンバーであるユーザーだけのものですが、「カスタム」ユーザーグループのユーザーにもこの権限を割り当てることができます。この権限を持つユーザーは、どのユーザーの設定でも変更できます。これには、任意のユーザーの作成または削除、ユーザーの SSH キー管理などが含まれます。したがって、この権限は慎重に割り当ててください。

注意: SSH キーをアップロード、表示、または削除する能力は、「ユーザーの設定」ユーザー権限に基づきます。この権限は、ユーザーによる他のユーザーの SSH キーの設定を可能にします。この権限は慎重に割り当てる必要があります。

Windows 用の公開キーの生成

PuTTY キージェネレータアプリケーションを使用して基本キーを作成するには、次の手順を実行します。

1. アプリケーションを起動し、生成するキーの種類として SSH-2 RSA または SSH-2 DSA のいずれかを選択します（SSH-1 はサポートされません）。サポートされるキー生成アルゴリズムは RSA と DSA のみです。
2. キーのビット数を入力します。RSA の場合は 768～4096 ビット、DSA の場合は 1024 ビットになります。
3. **生成** をクリックし、指示に従ってマウスポインタをウィンドウ内で移動させます。
   キーが生成されます。
4. キーコメントフィールドを変更できます。
5. キーをセキュアにするためにパスフレーズを入力します。
6. 公開キーと秘密キーを保存します。

Linux 用の公開キーの生成

ssh-keygen アプリケーションを使用してベーシックキーを作成するには、ターミナルウィンドウを開き、シェルプロンプトで `ssh-keygen -t rsa -b 1024 -C testing` と入力します。

ここで、

- `-t` は *dsa* または *rsa* です。
- `-b` は 768～4096 で、ビット暗号化サイズを指定します。
- `-C` を使用すると、公開キーコメントを変更できます。これはオプションです。

メモ: オプションでは大文字と小文字が区別されます。

指示に従ってください。コマンドが実行されたら、公開ファイルをアップロードします。

注意: ssh-keygen を使用して Linux 管理ステーションから生成されたキーは、4716 フォーマットではありません。`ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub` を使用して、キーを 4716 フォーマットに変換してください。キーファイルの権限は変更しないでください。変換は、デフォルトの権限を使用して実行する必要があります。

メモ: iDRAC7 では、キーの ssh-agent フォワード機能はサポートされていません。

SSH キーのアップロード

SSH インタフェース上で使用する公開キーは、1 人のユーザーあたり最大 4 つアップロードできます。公開キーを追加する前に、キーを表示し（キーがセットアップされている場合）、キーが誤って上書きされないようにしてください。

新しい公開キーを追加する場合は、新しいキーが追加されるインデックスに既存のキーが存在しないことを確認します。iDRAC7 は、新しいキーが追加される前に以前のキーが削除されることをチェックしません。新しいキーが追加されると、SSH インタフェースが有効な場合にそのキーが使用可能になります。

ウェブインタフェースを使用した SSH キーのアップロード

SSH キーをアップロードするには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ネットワーク → ユーザー認証 → ローカルユーザー** と移動します。
   ユーザー ページが表示されます。
2. **ユーザー ID** 列で、ユーザー ID 番号をクリックします。
   ユーザーメインメニュー ページが表示されます。
3. **SSH キー設定** で、**SSH キーのアップロード** を選択し、**次へ** をクリックします。
   SSH キーのアップロード ページが表示されます。
4. 次のいずれかの方法で SSH キーをアップロードします。
   - キーファイルをアップロードします。
   - キーファイルの内容をテキストボックスにコピーします。

   詳細については、iDRAC7 オンラインヘルプを参照してください。
5. **適用** をクリックします。

RACADM を使用した SSH キーのアップロード

SSH キーをアップロードするには、次のコマンドを実行します。

メモ: キーのアップロードとコピーを同時に行うことはできません。

- ローカル RACADM の場合：`racadm sshpkauth -i <2〜16> -k <1〜4> -f <ファイル名>`
- Telnet または SSH を使用するリモート RACADM の場合：`racadm sshpkauth -i <2〜16> -k <1〜4> -t <キーテキスト>`

たとえば、ファイルを使用して最初のキースペースの iDRAC7 ユーザー ID 2 に有効なキーをアップロードするには、次のコマンドを実行します。

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

メモ: `-f` オプションは、telnet/ssh/ シリアル RACADM ではサポートされていません。

SSH キーの表示

iDRAC7 にアップロードされたキーを表示できます。

ウェブインタフェースを使用した SSH キーの表示

SSH キーを表示するには、次の手順を実行します。

1. ウェブインタフェースで、**概要 → iDRAC 設定 → ネットワーク → ユーザー認証 → ローカルユーザー** と移動します。
   ユーザー ページが表示されます。
2. **ユーザー ID** 列で、ユーザー ID 番号をクリックします。
   ユーザーメインメニュー ページが表示されます。
3. **SSH キー設定** で、**SSH キーの表示 / 削除** を選択し、**次へ** をクリックします。
   SSH キーの表示 / 削除 ページが、キーの詳細と共に表示されます。

RACADM を使用した SSH キーの表示

SSH キーを表示するには、次のコマンドを実行します。

- 特定のキー — `racadm sshpkauth -i <2〜16> -v -k <1〜4>`
- すべてのキー — `racadm sshpkauth -i <2〜16> -v -k all`

SSH キーの削除

公開キーを削除する前にキーを表示し（キーがセットアップされている場合）、キーが誤って削除されていないことを確認してください。

ウェブインタフェースを使用した SSH キーの削除

SSH キーを削除するには、次の手順を実行します。

1. ウェブインタフェースで、**概要 → iDRAC 設定 → ネットワーク → ユーザー認証 → ローカルユーザー** と移動します。
   ユーザー ページが表示されます。
2. **ユーザー ID** 列で、ユーザー ID をクリックします。
   ユーザーメインメニュー ページが表示されます。
3. **SSH キー設定** で、**SSH キーの表示 / 削除** を選択し、**次へ** をクリックします。
   SSH キーの表示 / 削除 ページに、キーの詳細が表示されます。
4. **削除するキーに対して削除を選択し、適用をクリックします。**
   選択したキーが削除されます。

RACADM を使用した SSH キーの削除

SSH キーを削除するには、次のコマンドを実行します。

- 特定のキー — `racadm sshpkauth -i <2〜16> -d -k <1〜4>`
- すべてのキー — `racadm sshpkauth -i <2〜16> -d -k all`

7

ユーザーアカウントと権限の設定

特定の権限（*ロールベースの権限*）を持つユーザーアカウントをセットアップし、iDRAC7 を使用してシステムを管理したり、システムセキュリティを維持したりできます。デフォルトで、iDRAC7 はローカル管理者アカウントで設定されています。デフォルトユーザー名は *root* で、パスワードは *calvin* です。管理者として、他のユーザーが iDRAC7 にアクセスすることを許可するユーザーアカウントをセットアップできます。

ローカルユーザーをセットアップ、または Microsoft Active Directory や LDAP などのディレクトリサービスを使用してユーザーアカウントをセットアップできます。ディレクトリサービスは、認証されたユーザーアカウントを管理するための一元管理地点を提供します。

iDRAC7 は、関連付けられた権限の一連を持つユーザーへの役割ベースのアクセスをサポートします。役割は、管理者、オペレータ、読み取り専用、またはなしです。これらは、利用可能な最大権限を定義します。

関連リンク

ローカルユーザーの設定
Active Directory ユーザーの設定
汎用 LDAP ユーザーの設定

ローカルユーザーの設定

iDRAC7 では、特定のアクセス権限を持つローカルユーザーを最大 16 人設定できます。iDRAC7 ユーザーを作成する前に、現在のユーザーが存在するかどうかを確認してください。これらのユーザーには、ユーザー名、パスワード、および権限付きの役割を設定できます。ユーザー名とパスワードは、iDRAC7 でセキュア化された任意のインタフェース（つまり、ウェブインタフェース、RACADM、または WS-MAN）を使用して変更できます。

iDRAC7 ウェブインタフェースを使用したローカルユーザーの設定

ローカル iDRAC7 ユーザーを追加し、設定するには、次の手順を実行します。

メモ: iDRAC7 ユーザーを作成するには、ユーザーの設定権限が必要です。

1. iDRAC7 ウェブインタフェースで、**概要** → **iDRAC 設定** → **ユーザー認証** → **ローカルユーザー** と移動します。
   ユーザー ページが表示されます。
2. **ユーザー ID** 列で、ユーザー ID をクリックします。

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、この設定は変更できません。

   ユーザーメインメニュー ページが表示されます。
3. **ユーザーの設定** を選択して、**次へ** をクリックします。
   ユーザー設定 ページが表示されます。
4. ユーザー ID を有効にして、ユーザーのユーザー名、パスワード、およびアクセス権限を指定します。オプションの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。
5. **適用** をクリックします。必要な権限を持つユーザーが作成されます。

RACADM を使用したローカルユーザーの設定

メモ: リモート Linux システム上で RACADM コマンドを実行するには、**root** ユーザーとしてログインする必要があります。

RACADM を使用して単一または複数の iDRAC7 ユーザーを設定できます。

同じ設定を持つ iDRAC7 ユーザーを複数設定する場合は、次の手順のうちいずれかを実行してください。

- 本項の RACADM の例を参考にして、RACADM コマンドのバッチファイルを作成し、各管理下システムでこのバッチファイルを実行します。
- iDRAC7 設定ファイルを作成し、同じ設定ファイルを使用して各管理下システムで **racadm config** サブコマンドを実行します。

新規の iDRAC7 を設定する場合、または **racadm racresetcfg** コマンドを使用した場合、現在のユーザーのみがパスワード `calvin` を持つ `root` となります。**racresetcfg** サブコマンドは iDRAC7 をデフォルト値にリセットされます。

メモ: ユーザーは、経時的に有効化および無効化することができます。その結果、ユーザーは各 iDRAC7 で異なるインデックス番号を持っている場合があります。

ユーザーの存在を確認するには、コマンドプロンプトで次のコマンドを入力します。

```
racadm getconfig -u <ユーザー名>
```

または

各インデックス（1〜16）ごとに、次のコマンドを 1 度ずつ入力します。

```
racadm getconfig -g cfgUserAdmin -i <インデックス>
```

メモ: racadm getconfig -f <*myfile.cfg*> と入力して、iDRAC7 設定パラメータのすべてが含まれる **myfile.cfg** ファイルの表示や編集を行うこともできます。

複数のパラメータとオブジェクト ID が、それぞれの現在の値と共に表示されます。重要な 2 つのオブジェクトは、次のとおりです。

```
# cfgUserAdminIndex=XX

cfgUserAdminUserName=
```

cfgUserAdminUserName オブジェクトに値がない場合、**cfgUserAdminIndex** オブジェクトで示されるインデックス番号を使用できます。名前が「=」の後に表示されている場合、そのインデックスはそのユーザー名によって使用されています。

racadm config サブコマンドを使用してユーザーを手動で有効または無効にする場合は、**-i** オプションでインデックスを指定する*必要があります*。

前例に示されている **cfgUserAdminIndex** オブジェクトに「#」文字が含まれていることに注意してください。これは、読み取り専用オブジェクトであることを示しています。また、**racadm config -f racadm.cfg** コマンドを使用して、任意の数のグループ / オブジェクトを書き込みに指定する場合、インデックスは指定できません。新規ユーザーは最初の使用可能なインデックスに追加されます。この動作は、同じ設定での複数 iDRAC7 の設定におけるより優れた柔軟性を可能にします。

RACADM を使用した iDRAC7 ユーザーの追加

新しいユーザーを RAC 設定に追加するには、次の手順を実行します。

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. 次のユーザー権限を設定します。

- iDRAC7
- LAN
- シリアルポート
- シリアルオーバー LAN

4. ユーザーを有効にします。

例：

次の例では、パスワード「123456」と LOGIN 権限を持つ新しいユーザー名「John」を RAC に追加します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 3 john

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 3 123456

racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminPrivilege 0x00000001

racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminIpmiLanPrivilege 2

racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminIpmiSerialPrivilege 2

racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminSolEnable 1

racadm config -g cfgUserAdmin -i 3 -o cfgUserAdminEnable 1
```

確認するには、次のコマンドのいずれかを使用します。

```
racadm getconfig -u john

racadm getconfig -g cfgUserAdmin -i 3
```

RACADM コマンドの詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

iDRAC7 ユーザーの削除

RACADM を使用する場合、ユーザーは個別に手動で無効化する必要があります。設定ファイルを使用してユーザを削除することはできません。

iDRAC7 ユーザーを削除するためのコマンド構文は、次のとおりです。

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

二重引用符のヌル文字列（""）は、指定したインデックスでユーザー設定を削除して、ユーザー設定をオリジナルの工場出荷時デフォルトにリセットするように iDRAC7 に指示します。

許可を持つ iDRAC7 ユーザーの有効化

特定の管理許可（役割ベースの権限）を持つユーザーを有効にするには、次の手順を実行します。

1. 次のコマンド構文を使用して使用可能なユーザーインデックスを見つけます。
   ```
   racadm getconfig -g cfgUserAdmin -i <インデックス>
   ```
2. 新しいユーザー名とパスワードで次のコマンドを入力します。
   ```
   racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <インデックス> <ユーザー権限ビットマスク値>
   ```

メモ: 特定ユーザー権限用の有効なビットマスク値のリストに関しては、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。デフォルトの権限値は 0 で、ユーザーに有効な権限がないことを示します。

Active Directory ユーザーの設定

会社で Microsoft Active Directory ソフトウェアを使用している場合、iDRAC7 にアクセス権を付与するようにソフトウェアを設定することができます。これにより、ディレクトリサービスの既存ユーザーに iDRAC7 ユーザー権限を追加し、制御することが可能になります。これはライセンスが必要な機能です。

メモ: Active Directory を使用して iDRAC7 ユーザーを認識する機能は、Microsoft Windows 2000、Windows Server 2003 および Windows Server 2008 オペレーティングシステムでサポートされています。

iDRAC7 にログインするために、Active Directory を介してユーザー認証を設定できます。また、管理者が各ユーザーに特定の権限を設定できるようにする、役割ベースの権限を提供することもできます。

iDRAC7 の役割および権限名は、前世代のサーバーから変更されています。役割名は次のとおりです。

表 11. iDRAC7 の役割

前世代	現世代	権限
システム管理者	システム管理者	ログイン、設定、ユーザーの設定、ログ、システム制御、仮想コンソールへのアクセス、仮想メディアへのアクセス、システム操作、デバッグ
パワーユーザー	オペレータ	ログイン、設定、システム制御、仮想コンソールへのアクセス、仮想メディアへのアクセス、システム操作、デバッグ
ゲストユーザー	読み取り専用	ログイン
なし	なし	なし

表 12. iDRAC7 ユーザー権限

前世代	現世代	説明
iDRAC へのログイン	ログイン	ユーザーによる iDRAC へのログインを可能にします。
iDRAC の設定	設定	ユーザーによる iDRAC の設定を可能にします。
ユーザーの設定	ユーザーの設定	ユーザーによる特定のユーザーに対するシステムへのアクセスの許可を可能にします。
ログのクリア	ログ	ユーザーによるシステムイベントログ（SEL）のみのクリアを可能にします。
サーバー制御コマンドの実行	システム制御	ユーザーによる RACADM コマンドの実行を可能にします。
仮想コンソールリダイレクションへのアクセス（ブレードサーバーの場合） 仮想コンソールへのアクセス（ラックおよびタワーサーバーの場合）	仮想コンソールへのアクセス	ユーザーによる仮想コンソールの実行を可能にします。
仮想メディアへのアクセス	仮想メディアへのアクセス	ユーザーによる仮想メディアの実行と使用を可能にします。
テストアラート	システム操作	ユーザーによる特定のユーザーへのテストアラートの送信を可能にします。

前世代	現世代	説明
診断コマンドの実行	デバッグ	ユーザーによる診断コマンドの実行を可能にします。

関連リンク

iDRAC7 の Active Directory 認証を使用するための前提条件
サポートされている Active Directory の認証機構

iDRAC7 の Active Directory 認証を使用するための前提条件

iDRAC7 の Active Directory 認証機能を使用するには、次を確認してください。

- Active Directory インフラストラクチャが展開済み。詳細については、マイクロソフトのウェブサイトを参照してください。
- PKI を Active Directory インフラストラクチャに統合済み。iDRAC7 では、標準の公開キーインフラストラクチャ（PKI）メカニズムを使用して、Active Directory へのセキュアな認証を行います。詳細については、マイクロソフトのウェブサイトを参照してください。
- すべてのドメインコントローラで認証するために、iDRAC7 が接続するすべてのドメインコントローラでセキュアソケットレイヤ（SSL）を有効化済み。

関連リンク

ドメインコントローラでの SSL の有効化

ドメインコントローラでの SSL の有効化

iDRAC7 がユーザーを Active Directory ドメインコントローラで認証するとき、そのドメインコントローラとの SSL セッションが開始されます。このとき、ドメインコントローラは認証局（CA）によって署名された証明書を公開する必要があり、そのルート証明書の iDRAC7 へのアップロードも行われます。iDRAC7 が *任意の* ドメインコントローラ（それがルートドメインコントローラか子ドメインコントローラかにかかわらず）からの認証を受けるには、そのドメインコントローラがドメインの CA によって署名された SSL 対応の証明書を所有している必要があります。

Microsoft Enterprise Root CA を使用してすべてのドメインコントローラを *自動的に* SSL 証明書に割り当てる場合は、次の操作を行う必要があります。

1. 各ドメインコントローラに SSL 証明書をインストールします。
2. ドメインコントローラのルート CA 証明書を iDRAC7 にエクスポートします。
3. iDRAC7 ファームウェア SSL 証明書をインポートします。

関連リンク

各ドメインコントローラの SSL 証明書のインストール
ドメインコントローラのルート CA 証明書の iDRAC7 へのエクスポート
iDRAC7 ファームウェアの SSL 証明書のインポート

各ドメインコントローラの SSL 証明書のインストール

各コントローラに SSL 証明書をインストールするには、次の手順を実行します。

1. **開始** → **管理ツール** → **ドメインセキュリティポリシー** の順にクリックします。
2. **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。
   自動証明書要求セットアップウィザード が表示されます。
3. **次へ** をクリックして、**ドメインコントローラ** を選択します。
4. **次へ**、**終了** の順にクリックします。SSL 証明書がインストールされます。

ドメインコントローラのルート CA 証明書の iDRAC7 へのエクスポート

メモ: Windows 2000 が実行されるシステムの場合、またはスタンドアロン CA を使用している場合の手順は、次の手順とは異なる可能性があります。

ドメインコントローラのルート CA 証明書を iDRAC7 にエクスポートするには、次の手順を実行します。

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. **開始** → **実行** の順にクリックします。
3. mmc と入力して **OK** をクリックします。
4. **コンソール 1**（MMC）ウィンドウで、**ファイル**（Windows 2000 システムでは **コンソール**）をクリックし、**スナップインの追加 / 削除** を選択します。
5. **スナップインの追加と削除** 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** 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、**終了** をクリックして **OK** をクリックします。
9. **コンソール 1** ウィンドウで、**証明書 個人用 証明書** フォルダと移動します。
10. 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。
11. **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、秘密キーはエクスポートしません** を選択します。
12. **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。
13. **次へ** をクリックし、システムのディレクトリに証明書を保存します。
14. 手順 13 で保存した証明書を iDRAC7 にアップロードします。

iDRAC7 ファームウェアの SSL 証明書のインポート

iDRAC7 SSL 証明書は、iDRAC7 ウェブサーバーに使用される証明書と同じものです。すべての iDRAC7 コントローラには、デフォルトの自己署名型証明書が同梱されています。

Active Directory サーバーが SSL セッションの初期化段階でクライアントを認証するように設定されている場合は、iDRAC7 サーバー証明書を Active Directory ドメインコントローラにアップロードする必要があります。この追加手順は、Active Directory が SSL セッションの初期化段階でクライアント認証を実行しない場合は必要ありません。

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

メモ: iDRAC7 ファームウェアの SSL 証明書が CA 署名型であり、その CA の証明書がすでにドメインコントローラの信頼できるルート認証局リストに存在する場合は、本項の手順を実行しないでください。

すべてのドメインコントローラの信頼できる証明書のリストに iDRAC7 ファームウェア SSL 証明書をインポートするには、次の手順を実行します。

1. 次の RACADM コマンドを使用して、iDRAC7 SSL 証明書をダウンロードします。

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

2. 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** と選択します。
3. **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。
4. **次へ** をクリックして SSL 証明書ファイルを参照します。
5. 各ドメインコントローラの **信頼できるルート認証局** に iDRAC7 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** リストに含まれていることを確認してください。認証局がリストにない場合は、お使いのドメインコントローラすべてにその証明書をインストールする必要があります。

6. **次へ** をクリックし、証明書タイプに基づいて証明書ストアを Windows に自動的に選択させるか、希望する証明書ストアを参照します。
7. **終了**、**OK** の順にクリックします。iDRAC7 ファームウェアの SSL 証明書が、すべてのドメインコントローラの信頼できる証明書リストにインポートされました。

サポートされている Active Directory の認証機構

Active Directory を使用して、次の 2 つの方法を使用する iDRAC7 ユーザーアクセスを定義できます。

- Microsoft のデフォルトの Active Directory グループオブジェクトのみを使用する*標準*スキーマソリューション。
- カスタマイズされた Active Directory オブジェクトを持つ*拡張*スキーマソリューション。アクセスコントロールオブジェクトはすべて Active Directory で管理されます。これにより、異なる iDRAC7 上でさまざまな権限レベルを持つユーザーアクセスを設定するための最大限の柔軟性が実現します。

関連リンク

標準スキーマ Active Directory の概要
拡張スキーマ Active Directory の概要

標準スキーマ Active Directory の概要

次の図に示すように、標準スキーマを使用して Active Directory を統合する場合は、Active Directory と iDRAC7 の両方での設定が必要となります。

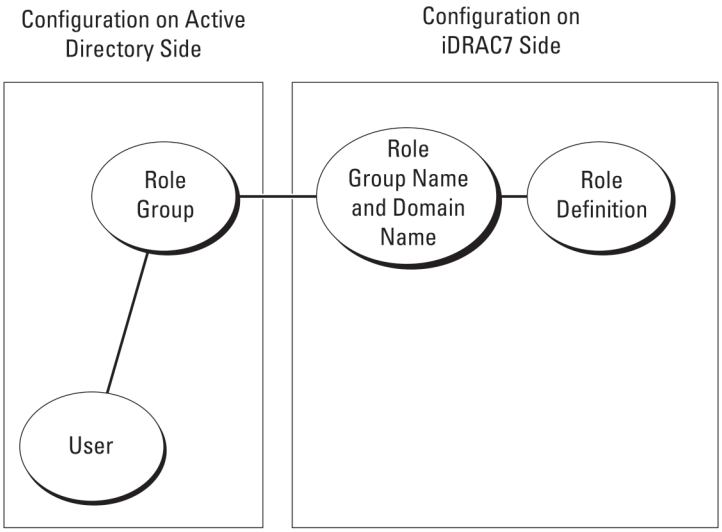

図 1. Active Directory 標準スキーマによる iDRAC7 の設定

標準グループオブジェクトは、Active Directory では役割グループとして使用されます。iDRAC7 アクセスを持つユーザーは、役割グループのメンバーです。このユーザーに特定の iDRAC7 へのアクセスを与えるには、その特定 iDRAC7 に役割グループ名およびドメイン名を設定する必要があります。役割および権限のレベルは、Active Directory ではなく、各 iDRAC7 で定義されます。各 iDRAC7 には最大 5 つまで役割グループを設定できます。表の参照番号は、デフォルトの役割グループの権限を示します。

表 13. デフォルトの役割グループの権限

役割グループ	デフォルトの権限レベル	許可する権限	ビットマスク
役割グループ 1	なし	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、仮想コンソールへのアクセス、仮想メディアへのアクセス、アラートのテスト、診断コマンドの実行。	0x000001ff
役割グループ 2	なし	iDRAC へのログイン、iDRAC の設定、サーバー制御コマンドの実行、仮想コンソールへのアクセス、仮想メディアへのアクセス、アラートのテスト、診断コマンドの実行。	0x000000f9
役割グループ 3	なし	iDRAC へのログイン	0x00000001
役割グループ 4	なし	権限の割り当てなし	0x00000000
役割グループ 5	なし	権限の割り当てなし	0x00000000

メモ: ビットマスク値は、RACADM で標準スキーマを設定する場合に限り使用されます。

シングルドメインとマルチドメインのシナリオの違い

すべてのログインユーザーと役割グループ（ネストされているグループも含む）が同じドメインにある場合、ドメインコントローラのアドレスのみを iDRAC7 で設定する必要があります。このシングルドメインのシナリオでは、すべてのグループの種類がサポートされます。

すべてのログインユーザーと役割グループ、またはネストされているグループのいずれかが複数のドメインにある場合、グローバルカタログサーバーのアドレスを iDRAC7 で設定する必要があります。このマルチドメインのシナリオでは、すべての役割グループとネストされているグループ（もしあれば）の種類は、ユニバーサルグループである必要があります。

標準スキーマ Active Directory の設定

Active Directory のログインアクセスのために iDRAC7 を設定するには、次の手順を実行します。

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。iDRAC7 にアクセスするため、Active Directory ユーザーを Active Directory グループのメンバーとして追加します。
3. iDRAC7 ウェブインタフェースまたは RACADM を使用して、iDRAC7 でのグループ名、ドメイン名、および役割権限を設定します。

関連リンク

iDRAC7 ウェブインタフェースを使用した標準スキーマでの Active Directory の設定
RACADM を使用した標準スキーマの Active Directory の設定

iDRAC7 ウェブインタフェースを使用した標準スキーマでの Active Directory の設定

メモ: さまざまなフィールドについての情報は、『*iDRAC7 オンラインヘルプ*』を参照してください。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ユーザー認証 → ディレクトリサービス → Microsoft Active Directory** と移動します。

Active Directory サマリ ページが表示されます。

2. **Active Directory の設定** をクリックします。
   Active Directory 設定と管理手順 4 の 1 ページが開きます。
3. オプションで、証明書の検証を有効にして、Active Directory（AD）サーバーとの通信を行う際の SSL 接続の開始時に使用される CA 署名付きデジタル証明書をアップロードします。このためには、ドメインコントローラおよびグローバルカタログの FQDN を指定する必要があります。これは、次の手順で行います。従って、ネットワークの設定では DNS が適切に設定されるようにします。
4. **次へ** をクリックします。
   Active Directory 設定と管理手順 4 の 2 ページが開きます。
5. Active Directory を有効にして、Active Directory サーバーとユーザーアカウントの場所の情報を指定します。また、iDRAC7 ログイン時に iDRAC7 が Active Directory からの応答を待機する必要がある時間を指定します。

メモ: 証明書の検証が有効になっている場合、ドメインコントローラサーバーのアドレスおよびグローバルカタログの FQDN を指定します。**概要 → iDRAC 設定 → ネットワーク** で、DNS が正しく設定されていることを確認します。

6. **次へ** をクリックします。**Active Directory 設定と管理手順 4 の 3** ページが開きます。
7. **標準スキーマ** を選択して次へをクリックします。
   Active Directory 設定と管理手順 4 の 4a ページが開きます。
8. Active Directory グローバルカタログサーバーの場所を入力して、ユーザーの認証に使用する権限グループを指定します。
9. **役割グループ** をクリックして、標準スキーマモードのユーザー用に制御認証ポリシーを設定します。
   Active Directory 設定と管理手順 4 の 4b ページが開きます。
10. 権限を指定して、**適用** をクリックします。
    設定が適用され、**Active Directory 設定と管理手順 4 の 4a** ページが開きます。
11. **終了** をクリックします。標準スキーマの Active Directory が設定されます。

RACADM を使用した標準スキーマの Active Directory の設定

RACADM を使用した標準スキーマの iDRAC7 Active Directory を設定するには、次の手順を実行します。

1. racadm コマンドプロンプトで、次のコマンドを実行します。

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 2
racadm config -g cfgStandardSchema -i <インデックス> -o cfgSSADRoleGroupName <役割グループのコモンネーム>
racadm config -g cfgStandardSchema -i <インデックス> -o cfgSSADRoleGroupDomain <完全修飾ドメイン名>
racadm config -g cfgStandardSchema -i <インデックス> -o cfgSSADRoleGroupPrivilege <特定の役割グループパーミッション用のビットマスク値>
```

メモ: 特定の役割グループパーミッション用のビットマスク値については、「デフォルト役割グループの権限」を参照してください。

```
racadm config -g cfgActiveDirectory -o cfgADDomainController1 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
racadm config -g cfgActiveDirectory -o cfgADDomainController2 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
racadm config -g cfgActiveDirectory -o cfgADDomainController3 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
```

メモ: ドメインの FQDN ではなく、ドメインコントローラの FQDN を入力します。たとえば、dell.com ではなく servername.dell.com と入力します。

メモ: 3 つのアドレスのうち少なくとも 1 つを設定する必要があります。iDRAC7 は、正常に接続できるまで、設定された各アドレスに対して 1 つずつ接続を試みます。標準スキーマでは、これらはユーザーアカウントと役割グループが位置するドメインコントローラのアドレスです。

```
racadm config -g cfgActiveDirectory -o cfgGlobal Catalog1 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
```

```
racadm config -g cfgActiveDirectory -o cfgGlobal Catalog2 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
```

```
racadm config -g cfgActiveDirectory -o cfgGlobal Catalog3 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
```

メモ: グローバルカタログサーバーが標準スキーマに必要になるのは、ユーザーアカウントと役割グループが別個のドメイン内にある場合のみです。複数のドメインにある場合は、使用できるのはユニバーサルグループだけです。

メモ: 証明書の検証を有効にしている場合、このフィールドで指定する FQDN または IP アドレスは、ドメインコントローラ証明書のサブジェクトまたはサブジェクト代替名のフィールドの値と一致する必要があります。

SSL ハンドシェイク中の証明書の検証を無効にする場合は、次の RACADM コマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

この場合、認証局（CA）の証明書をアップロードする必要はありません。

SSL ハンドシェイク中に証明書の検証を実施する場合は、次のコマンドを実行します（オプション）。

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

この場合、次の RACADM コマンドを実行して CA 証明書をアップロードする必要があります。

```
racadm sslcertupload -t 0x2 -f <ADS ルート CA 証明書>
```

メモ: 証明書の検証が有効になっている場合、ドメインコントローラサーバーのアドレスおよびグローバルカタログの FQDN を指定します。**概要 → iDRAC 設定 → ネットワーク** で、DNS が正しく設定されていることを確認します。

次の RACADM コマンドの使用はオプションです。

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

2. iDRAC7 上で DHCP が有効化されていて、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. iDRAC7 上で DHCP が無効化されている場合、または手動で DNS IP アドレスを入力する場合は、次の RACADM コマンドを入力します。

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
   ```

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServer1 <プライマリ DNS IP アドレス>
   ```

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

4. ウェブインタフェースにログインするときにユーザー名だけの入力で済むように、ユーザードメインのリストを設定しておく場合は、次のコマンドを入力します。

   ```
   racadm config -g cfgUserDomain -o cfgUserDomainName <ドメインコントローラの完全修飾ドメイン名または IP アドレス> -i <インデックス>
   ```

   1 から 40 のインデックス番号で、最大 40 のユーザードメインを設定できます。

拡張スキーマ Active Directory の概要

拡張スキーマソリューションを使用する場合は、Active Directory スキーマの拡張が必要です。

Active Directory スキーマ拡張

Active Directory データは、*属性*および*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包含できるデータのタイプを決定する規則が含まれます。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。ユーザークラス属性の例としては、ユーザーの名前、名字、電話番号などが挙げられます。特定の要件に独自の固有な*属性*や*クラス*を追加することによって、Active Directory データベースを拡張できます。Dell では、リモート管理認証、および Active Directory を使用した承認をサポートするために必要な変更を取り入れるため、スキーマを拡張しました。

既存の Active Directory スキーマに追加される各*属性*または*クラス*は、固有の ID で定義される必要があります。業界全体で固有の ID を保持するため、マイクロソフトでは Active Directory オブジェクト識別子（OID）のデータベースを維持しており、企業がスキーマに拡張を追加したときに、それらが固有であり、お互いに拮抗しないことを保証できるようにしています。マイクロソフトの Active Directory におけるスキーマの拡張のため、Dell は、ディレクトリサービスに追加される属性およびクラス用に固有の OID、固有の名前拡張子、および固有にリンクされた属性 ID を取得しました。

- 拡張子：`dell`
- ベース OID：`1.2.840.113556.1.8000.1280`
- RAC LinkID の範囲：`12070`～`12079`

iDRAC7 スキーマ拡張の概要

デルでは、*関連*、*デバイス*、および*権限*プロパティを取り入れるために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と、1 つ、または複数の iDRAC7 デバイスとをリンクするために使用されます。このモデルは、複雑な操作をほとんど行うことなく、ネットワーク上のユーザー、iDRAC7 権限、および iDRAC7 デバイスの様々な組み合わせにおける最大の柔軟性をシステム管理者に提供します。

認証および承認のために Active Directory と統合するネットワーク上の物理 iDRAC7 デバイスにはそれぞれ、少なくとも 1 つの関連オブジェクトと 1 つの iDRAC7 デバイスオブジェクトを作成してください。複数の関連オブジェクトを作成でき、各関連オブジェクトは、必要なだけのユーザー、ユーザーグループ、または iDRAC7 デバイスオブジェクトにリンクすることができます。ユーザーおよび iDRAC7 ユーザーグループは、企業内の任意のドメインのメンバーにすることができます。

ただし、各関連オブジェクト（または、ユーザー、ユーザーグループ、あるいは iDRAC7 デバイスオブジェクト）は、1 つの権限オブジェクトにしかリンクすることができません。この例では、システム管理者が、特定の iDRAC7 デバイスで各ユーザーの権限をコントロールすることができます。

iDRAC7 デバイスオブジェクトは、認証および承認のために Active Directory をクエリするための iDRAC7 ファームウェアへのリンクです。iDRAC7 がネットワークに追加されたると、システム管理者は、ユーザーが Active Directory で認証および承認を実行できるように、その Active Directory 名を使用して iDRAC7 とそのデバイスオブジェクトを設定する必要があります。また、ユーザーが認証するために、システム管理者は少なくとも 1 つの関連オブジェクトに iDRAC7 を追加する必要があります。

次の図は、関連オブジェクトによって、認証と許可に必要な接続が提供されていることを示しています。

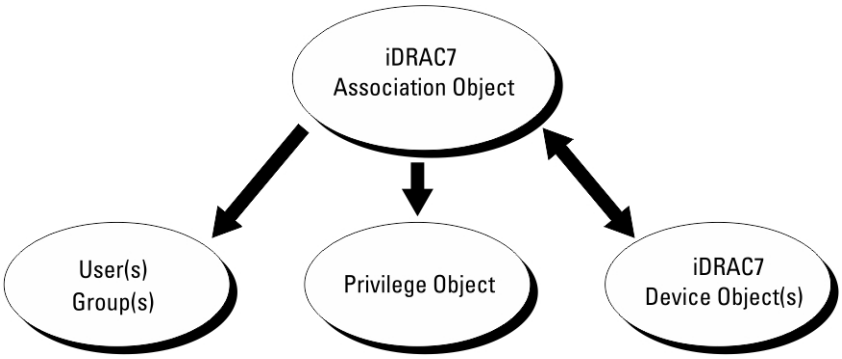

図 2. Active Directory オブジェクトの標準的なセットアップ

関連オブジェクトは、必要に応じて多くも少なくも作成できます。ただし、少なくとも 1 つの関連オブジェクトを作成する必要があり、iDRAC7 との認証および承認用に Active Directory を統合するネットワーク上の iDRAC7 ごとに、1 つの iDRAC7 デバイスオブジェクトが必要です。

関連オブジェクトは、必要な数だけのユーザーおよび / またはグループの他、iDRAC7 デバイスオブジェクトにも対応できます。ただし、関連オブジェクトには、関連オブジェクトにつき 1 つの権限オブジェクトしか含めることができません。関連オブジェクトは、iDRAC7 デバイスに対して権限を持つユーザーを連結します。

ADUC MMC スナップインへの Dell 拡張では、同じドメインの権限オブジェクトと iDRAC7 オブジェクトのみを関連オブジェクトに関連付けることができます。Dell 拡張で、他のドメインのグループまたは iDRAC7 オブジェクトを関連オブジェクトの製品メンバーとして追加することはできません。

別のドメインからユニバーサルグループを追加するときは、ユニバーサルスコープを持つ関連オブジェクトを作成します。Dell Schema Extender ユーティリティによって作成される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、他のドメインのユニバーサルグループとは連携しません。

任意のドメインのユーザー、ユーザーグループ、またはネストされたユーザーグループを関連オブジェクトに追加できます。拡張スキーマソリューションは、Microsoft Active Directory によって許可されている複数のドメイン間でのすべてのユーザーグループタイプおよびユーザーグループネストをサポートします。

拡張スキーマを使用した権限の蓄積

拡張スキーマ認証のメカニズムは、異なる関連オブジェクトを介して同じユーザーに関連付けられた異なる権限オブジェクトからの権限の蓄積をサポートします。言い換えれば、拡張スキーマ認証は権限を蓄積して、このユーザーに関連付けられている異なる権限オブジェクトに対応する、割り当てられたすべての権限のスーパーセットを同じユーザーに許可します。

次の図は、拡張スキーマを使用して権限を蓄積する例を示しています。

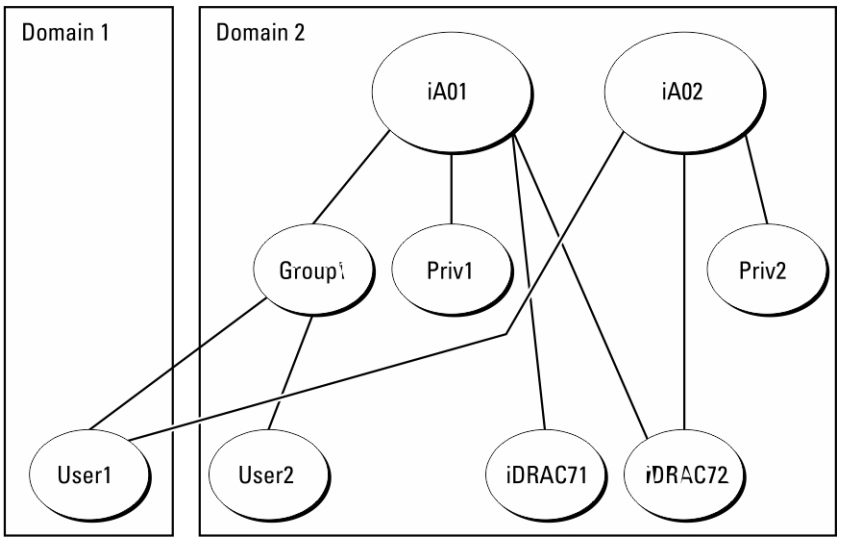

図 3. ユーザーの権限の蓄積

この図は、A01 と A02 の 2 つの関連オブジェクトを示しています。ユーザー 1 は、両方の関連オブジェクトを介して iDRAC72 に関連付けられています。

拡張スキーマ認証は、このユーザーに関連付けられている異なる権限オブジェクトに割り当てられた権限を考慮し、可能な限り最大の権限セットを同じユーザーに許可するために権限を蓄積します。

この例では、ユーザー 1 は iDRAC72 に対する Priv1 権限と Priv2 権限の両方を所有しており、iDRAC71 に対しては Priv1 権限のみを所有しています。ユーザー 2 は iDRAC71 と iDRAC72 の両方に対して Priv1 権限を所有しています。さらに、この図は、ユーザー 1 が異なるドメインに属すことができ、グループのメンバーになり得ることを示しています。

拡張スキーマ Active Directory の設定

Active Directory を設定して iDRAC7 にアクセスするには、次の手順を実行します。

1. Active Directory スキーマを拡張します。
2. Active Directory ユーザーとコンピュータスナップインを拡張します。
3. Active Directory に iDRAC7 ユーザーと権限を追加します。
4. iDRAC7 ウェブインタフェースまたは RACADM を使用して、iDRAC7 Active Directory のプロパティを設定します。

関連リンク

拡張スキーマ Active Directory の概要
Active Directory ユーザーとコンピュータスナップインへの Dell 拡張のインストール
Active Directory への iDRAC7 ユーザーと権限の追加
iDRAC7 ウェブインタフェースを使用した拡張スキーマの Active Directory の設定
RACADM を使用した拡張スキーマの Active Directory の設定

Active Directory スキーマの拡張

Active Directory スキーマを拡張すると、Active Directory スキーマに Dell の組織単位、スキーマクラスと属性、および権限例と関連オブジェクトが追加されます。スキーマを拡張する前に、ドメインフォレストのスキーママスタ Flexible Single Master Operation（FSMO）役割所有者におけるスキーマ管理者権限を所持していることを確認してください。

メモ: この製品は前の世代の RAC 製品とは異なることから、このスキーマ拡張を使用するようにしてください。以前のスキーマは、本製品では機能しません。

メモ: 新規スキーマを拡張しても、前のバージョンの製品には何ら影響しません。

スキーマは、次のいずれかの方法を使用して拡張できます

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

LDIF スクリプトファイルを使用すると、Dell の組織単位はスキーマに追加されません。

LDIF ファイルと Dell Schema Extender はそれぞれ『*Dell Systems Management Tools and Documentation*』DVD の次のディレクトリに収録されています。

- **DVD ドライブ**:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools \Remote_Management_Advanced\LDIF_Files
- <**DVD ドライブ**>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools \Remote_Management_Advanced\Schema Extender

LDIF ファイルを使用するには、**LDIF_Files** ディレクトリにある readme の説明を参照してください。

Schema Extender または LDIF ファイルは、任意の場所にコピーして実行することができます。

Dell Schema Extender の使用

注意: Dell Schema Extender では、SchemaExtenderOem.ini ファイルを使用します。Dell Schema Extender ユーティリティが正常に機能することを確認するため、このファイルの名前は変更しないでください。

1. **ようこそ** 画面で、**次へ** をクリックします。
2. 警告を読み、理解した上で、もう一度 **次へ** をクリックします。
3. **現在のログイン資格情報を使用** を選択するか、スキーマ管理者権限でユーザー名とパスワードを入力します。
4. Dell Schema Extender を実行するには、**次へ** をクリックします。
5. **終了** をクリックします。

   スキーマが拡張されました。スキーマの拡張を確認するには、MMC および Active Directory スキーマスナップインを使用してクラスと属性（「クラスと属性」）が存在することを確認します。MMC と Active Directory スキーマスナップインの使用に関する詳細については、マイクロソフトのマニュアルを参照してください。

クラスと属性

表 14. Active Directory スキーマに追加されたクラスのクラス定義

クラス名	割り当てられたオブジェクト識別番号（OID）
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	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 15. dellRacDevice クラス

OID	1.2.840.113556.1.8000.1280.1.7.1.1
説明	Dell iDRAC7 デバイスを表します。Active Directory では、iDRAC7 は delliDRACDevice として設定される必要があります。この設定によって、iDRAC から Active Directory に Lightweight Directory Access Protocol（LDAP）クエリを送信できるようになります。
クラスタイプ	構造体クラス
SuperClasses	dellProduct
属性	dellSchemaVersion dellRacType

表 16. delliDRACAssociationObject クラス

OID	1.2.840.113556.1.8000.1280.1.7.1.2
説明	Dell 関連オブジェクトを表します。関連オブジェクトは、ユーザーとデバイス間の連結を可能にします。
クラスタイプ	構造体クラス
SuperClasses	グループ
属性	dellProductMembers dellPrivilegeMember

表 17. dellRAC4Privileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.3
説明	iDRAC7 の権限（許可権限）を定義します。
クラスタイプ	補助クラス
SuperClasses	なし
属性	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

表 18. dellPrivileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.4
説明	デルの権限（許可権限）のコンテナクラスとして使用されます。
クラスタイプ	構造体クラス
SuperClasses	ユーザー

OID	1.2.840.113556.1.8000.1280.1.1.1.4
属性	dellRAC4Privileges

表 19. 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。
クラスタイプ	構造体クラス
SuperClasses	コンピュータ
属性	dellAssociationMembers

表 20. Active Directory スキーマに追加された属性のリスト

属性名 / 説明	割り当てられた OID/ 構文オブジェクト識別子	単一値
dellPrivilegeMember この属性に属する dellPrivilege オブジェクトのリスト。	1.2.840.113556.1.8000.1280.1.1.2.1 識別名（LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12）	FALSE
dellProductMembers この役割に属する dellRacDevice オブジェクトと DelliDRACDevice オブジェクトのリスト。この属性は、dellAssociationMembers バックワードリンクへのフォワードリンクです。 リンク ID：12070	1.2.840.113556.1.8000.1280.1.1.2.2 識別名（LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12）	FALSE
dellIsLoginUser ユーザーにデバイスへのログイン権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.3 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsCardConfigAdmin ユーザーにデバイスのカード設定権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.4 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsUserConfigAdmin ユーザーにデバイスのユーザー設定権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.5 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsLogClearAdmin ユーザーにデバイスのログクリア権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.6 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsServerResetUser ユーザーにデバイスのサーバーリセット権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.7 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsConsoleRedirectUser ユーザーにデバイスの仮想コンソール権限がある場合は 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

属性名 / 説明	割り当てられた OID/ 構文オブジェクト識別子	単一値
dellIsTestAlertUser ユーザーにデバイスのテストアラートユーザー権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.10 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsDebugCommandAdmin ユーザーにデバイスのデバッグコマンド管理権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.11 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellSchemaVersion スキーマのアップデートに現在のスキーマバージョンが使用されます。	1.2.840.113556.1.8000.1280.1.1.2.12 大文字小文字を区別しない文字列（LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905）	TRUE
dellRacType この属性は delliDRACDevice 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 大文字小文字を区別しない文字列（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 にリンクされた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、システム管理者が iDRAC デバイス、ユーザーとユーザーグループ、iDRAC 関連付け、および iDRAC 権限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 Tools and Documentation*』DVD を使用してシステム管理ソフトウェアをインストールする場合、インストール手順の実行中に **Active Directory ユーザーとコンピュータスナップイン** オプションを選択して、スナップインを拡張できます。システム管理ソフトウェアのインストールに関する追加手順については、『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。64 ビットの Windows オペレーティングシステムの場合、スナップインのインストーラは次の場所にあります。

<DVD ドライブ>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64

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、マイクロソフトのマニュアルを参照してください。

Active Directory への iDRAC7 ユーザーと権限の追加

Dell 拡張 Active Directory ユーザーとコンピュータスナップインを使用して、デバイスオブジェクト、関連オブジェクト、および権限オブジェクトを作成することにより、iDRAC7 ユーザーおよび権限を追加できます。各オブジェクトを追加するには、次の操作を行います。

- iDRAC デバイスオブジェクトの作成
- 権限オブジェクトの作成
- 関連オブジェクトの作成
- 関連オブジェクトへのオブジェクトの追加

関連リンク

関連オブジェクトへのオブジェクトの追加
iDRAC7 デバイスオブジェクトの作成
権限オブジェクトの作成
関連オブジェクトの作成

iDRAC7 デバイスオブジェクトの作成

iDRAC7 デバイスオブジェクトを作成するには、次の手順を実行します。

1. MMC **コンソールルート** ウィンドウでコンテナを右クリックします。
2. **新規** → **Dell リモート管理オブジェクトの詳細設定** 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、iDRAC7 ウェブインタフェースを使用して Active Directory のプロパティを設定した際に入力した iDRAC7 の名前と同じである必要があります。
4. iDRAC **デバイスオブジェクト** を選択し、OK をクリックします。

権限オブジェクトの作成

権限オブジェクトを作成するには、次の手順を実行します。

メモ: 権限オブジェクトは、関係のある関連オブジェクトと同じドメイン内に作成する必要があります。

1. **コンソールルート**（MMC）ウィンドウで、コンテナを右クリックします。
2. **新規** → **Dell リモート管理オブジェクトの詳細設定** を選択します。
   新規オブジェクト ウィンドウが表示されます。
3. 新しいオブジェクトの名前を入力します。
4. **権限オブジェクト** を選択し、OK をクリックします。
5. 作成した権限オブジェクトを右クリックして **プロパティ** を選択します。
6. **リモート管理権限** タブをクリックして、ユーザーまたはグループに対する権限を設定します。

関連オブジェクトの作成

関連オブジェクトを作成するには、次の手順を実行します。

メモ: iDRAC7 の関連オブジェクトはグループから派生し、その範囲はドメインローカルに設定されています。

1. **コンソールルート**（MMC）ウィンドウで、コンテナを右クリックします。
2. **新規** → **Dell リモート管理オブジェクト詳細設定** と選択します。
   この **新規オブジェクト** ウィンドウが表示されます。
3. 新規オブジェクトの名前を入力し、**関連オブジェクト** を選択します。
4. **関連オブジェクト** の範囲を選択し、OK をクリックします。
5. 認証済みユーザーに、作成された関連オブジェクトにアクセスするためのアクセス権限を提供します。

関連リンク

関連オブジェクトのユーザーアクセス権限の付与

関連オブジェクトのユーザーアクセス権限の付与

認証されたユーザーに、作成された関連オブジェクトへのアクセス権限を提供するには、次の手順を実行します。

1. **管理ツール** → **ADSI 編集** と移動します。**ADSI 編集** ウィンドウが表示されます。
2. 右ペインで、作成された関連オブジェクトに移動して右クリックし、**プロパティ** を選択します。

3. **セキュリティ** タブで **追加** をクリックします。
4. `Authenticated Users` と入力し、**名前の確認**、**OK** の順にクリックします。認証されたユーザーが **グループとユーザー名** のリストに追加されます。
5. **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 ウィンドウを使用して、ユーザーまたはユーザーグループ、権限オブジェクト、iDRAC7 デバイスまたは iDRAC7 デバイスグループを関連付けることができます。

ユーザーおよび iDRAC7 デバイスのグループを追加できます。

関連リンク

ユーザーまたはユーザーグループの追加
権限の追加
iDRAC7 デバイスまたは iDRAC7 デバイスグループの追加

ユーザーまたはユーザーグループの追加

ユーザーまたはユーザーグループを追加するには、次の手順を実行します。

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。

権限の追加

権限を追加するには、次の手順を実行します。

権限オブジェクト タブをクリックして、iDRAC7 デバイスに対して認証を行うときにユーザーまたはユーザーグループの権限を定義する関連に、権限オブジェクトを追加します。関連オブジェクトに追加できる権限オブジェクトは、1 つだけです。

1. **権限オブジェクト** タブを選択し、**追加** をクリックします。
2. 権限オブジェクト名を入力し、**OK** をクリックします。
3. **権限オブジェクト** タブをクリックして、iDRAC7 デバイスに対して認証を行うときにユーザーまたはユーザーグループの権限を定義する関連に、権限オブジェクトを追加します。関連オブジェクトに追加できる権限オブジェクトは、1 つだけです。

iDRAC7 デバイスまたは iDRAC7 デバイスグループの追加

iDRAC7 デバイスまたは iDRAC7 デバイスグループを追加するには、次の手順を実行します。

1. **製品** タブを選択して **追加** をクリックします。
2. iDRAC6 デバイスまたは iDRAC6 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。
4. **プロパティ** タブをクリックして、定義されたユーザーまたはユーザーグループが利用可能なネットワークに接続している iDRAC7 デバイスを 1 つ追加します。関連オブジェクトには複数のデバイスを追加できます。

iDRAC7 ウェブインタフェースを使用した拡張スキーマの Active Directory の設定

ウェブインタフェースを使用して Active Directory を拡張スキーマで設定するには、次の手順を実行します。

メモ: 各種フィールドについては、『*iDRAC7 オンラインヘルプ*』を参照してください。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ユーザー認証 → ディレクトリサービス → Microsoft Active Directory** と移動します。

Active Directory サマリページが表示されます。

2. **Active Directory の設定** をクリックします。
   Active Directory 設定と管理手順 4 の 1 ページが開きます。
3. オプションで証明書検証を有効にして、Active Directory（AD）サーバーと通信するときに SSL 接続開始時に使用した CA 署名付きデジタル証明書をアップロードします。
4. **次へ** をクリックします。
   Active Directory 設定と管理手順 4 の 2 ページが開きます。
5. Active Directory（AD）サーバーの場所情報およびユーザーアカウントを指定します。また、ログイン処理に AD からの応答を iDRAC7 が待つ必要がある時間を指定します。

メモ: 証明書の検証が有効な場合、ドメインコントローラサーバーのアドレスおよび FQDN を指定します。DNS が正しく設定されていることを **概要 → iDRAC 設定 → ネットワーク** で確認してください。

6. **次へ** をクリックします。**Active Directory 設定と管理手順 4 の 3** ページが開きます。
7. **拡張スキーマ** を選択して、**次へ** をクリックします。
   Active Directory 設定と管理手順 4 の 4 ページが開きます。
8. Active Directory（AD）にある iDRAC7 デバイスオブジェクトの名前と場所を入力して、**終了** をクリックします。
   拡張スキーマモード用の Active Directory 設定が設定されます。

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

RACADM を使用した拡張スキーマの Active Directory を設定するには、次の手順を実行します。

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 cfgADRacName <RAC 共通名>
racadm config -g cfgActiveDirectory -o cfgADRacDomain <完全修飾 rac ドメイン名>
racadm config -g cfgActiveDirectory -o cfgADDomainController1 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
racadm config -g cfgActiveDirectory -o cfgADDomainController2 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
racadm config -g cfgActiveDirectory -o cfgADDomainController3 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
```

メモ: 3 つのアドレスのうち少なくとも 1 つを設定する必要があります。iDRAC7 は、正常に接続できるまで、設定された各アドレスに対して 1 つずつ接続を試みます。拡張スキーマでは、これらはこの iDRAC7 デバイスが位置するドメインコントローラの FQDN または IP アドレスです。

SSL ハンドシェイク中の証明書の検証を無効にする場合は、次のコマンドを実行します（オプション）。

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

メモ: この場合、CA 証明書をアップロードする必要はありません。

SSL ハンドシェイク中に証明書の検証を実施する場合は、次のコマンドを実行します（オプション）。

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

この場合、CA 証明書をアップロードする必要があります。

```
racadm sslcertupload -t 0x2 -f <ADS ルート CA 証明書>
```

メモ: 証明書の検証が有効な場合、ドメインコントローラサーバーのアドレスおよび FQDN を指定します。DNS が正しく設定されていることを **概要 → iDRAC 設定 → ネットワーク** で確認してください。

次の RACADM コマンドの使用はオプションです。

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

2. iDRAC7 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。
3. iDRAC7 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. iDRAC7 ウェブインタフェースにログインするときにユーザー名の入力だけで済むように、ユーザードメインのリストを設定しておく場合は、次のコマンドを入力します。

```
racadm config -g cfgUserDomain -o cfgUserDomainName <ドメインコントローラの完全修飾ドメイン名または IP アドレス> -i <インデックス>
```

1 から 40 のインデックス番号で、最大 40 のユーザードメインを設定できます。

5. 拡張スキーマの Active Directory 設定を完了するには、**<Enter>** キーを押します。

Active Directory 設定のテスト

設定が正しいかどうかを検証、または Active Directory ログインに失敗した場合の問題を診断するために、Active Directory 設定をテストすることができます。

iDRAC7 ウェブインタフェースを使用した Active Directory 設定のテスト

Active Directory 設定をテストするには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ユーザー認証 → ディレクトリサービス → Microsoft Active Directory** と移動します。
   Active Directory 概要ページが表示されます。
2. **設定のテスト** をクリックします。
3. テストユーザーの名前（例：**username@domain.com**）およびパスワードを入力して、**テストの開始** をクリックします。詳細なテスト結果およびテストログが表示されます。
   いずれかの手順にエラーが発生した場合は、テストログで詳細を確認し、問題と解決策を特定します。

メモ: 証明書検証を有効化がチェックされた状態で Active Directory 設定をテストする場合、iDRAC7 では、Active Directory サーバーが IP アドレスではなく FQDN で識別されている必要があります。Active Directory サーバーが IP アドレスで識別されていると、iDRAC7 が Active Directory サーバーと通信できないため、証明書の検証に失敗します。

RACADM を使用した Active Directory の設定のテスト

Active Directory の設定をテストするには、`testfeature` コマンドを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

汎用 LDAP ユーザーの設定

iDRAC7 は Lightweight Directory Access Protocol（LDAP）ベースの認証をサポートするための汎用ソリューションを提供します。この機能は、ディレクトリサービス上のどのスキーマ拡張にも必要です。

iDRAC7 LDAP の実装を汎用にするため、ユーザーのグループ化に異なるディレクトリサービス間の共通性を利用し、その後ユーザーグループ関係をマップします。ディレクトリサービス特有の処置はスキーマです。

例えば、それらにはグループ、ユーザー、およびユーザーとグループ間のリンクに異なる属性名がある場合があります。これらの処置は、iDRAC7 に設定できます。

メモ: スマートカードベースの 2 要素認証（TFA）とシングルサインオン（SSO）ログインは、汎用 LDAP ディレクトリサービスではサポートされません。

関連リンク

iDRAC7 のウェブベースインタフェースを使用した汎用 LDAP ディレクトリサービスの設定
RACADM を使用した汎用 LDAP ディレクトリサービスの設定

iDRAC7 のウェブベースインタフェースを使用した汎用 LDAP ディレクトリサービスの設定

ウェブインタフェースを使用して汎用 LDAP ディレクトリサービスを設定するには、次の手順を実行します。

メモ: 各種フィールドについては、『*iDRAC7 オンラインヘルプ*』を参照してください。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ユーザー認証 → ディレクトリサービス → 汎用 LDAP ディレクトリサービス** と移動します。
   汎用 LDAP 設定と管理 ページには、現在の汎用 LDAP 設定が表示されます。
2. **汎用 LDAP の設定** をクリックします。
3. オプションで証明書検証を有効にして、汎用 LDAP サーバーと通信するときに SSL 接続開始時に使用したデジタル証明書をアップロードします。

メモ: 本リリースでは、非 SSL ポートベースの LDAP バインドはサポートされていません。サポートされるのは LDAP Over SSL のみです。

4. **次へ** をクリックします。
   汎用 LDAP 設定と管理手順 3 の 2 ページが表示されます。
5. 汎用 LDAP 認証を有効にして、汎用 LDAP サーバーとユーザーアカウントの場所情報を指定します。

メモ: 証明書の検証を有効にした場合は、LDAP サーバーの FQDN を指定し、**概要 → iDRAC 設定 → ネットワーク** で DNS が正しく設定されたことを確認します。

メモ: このリリースでは、ネストされたグループはサポートされません。ファームウェアは、ユーザー DN に一致するグループのダイレクトメンバーを検索します。また、サポートされるドメインは 1 つだけです。クロスドメインはサポートされません。

6. **次へ** をクリックします。
   汎用 LDAP 設定と管理手順 3 の 3a ページが表示されます。
7. **役割グループ** をクリックします。
   汎用 LDAP 設定と管理手順 3 の 3b ページが表示されます。
8. グループ識別名とそのグループに関連付けられた権限を指定し、**適用** をクリックします。

メモ: Novell eDirectory を使用していて、グループ DN 名に #（ハッシュ）、"（二重引用符）、;（セミコロン）、>（より大きい）、,（カンマ）、または <（より小さい）などの文字を使用した場合は、それらの文字をエスケープする必要があります。

役割グループの設定が保存されます。**汎用 LDAP 設定および管理手順 3 の 3a** ページに、役割グループ設定が表示されます。

9. 追加の役割グループを設定する場合は、手順 7 と 8 を繰り替えします。
10. **終了** をクリックします。汎用 LDAP ディレクトリサービスが設定されました。

RACADM を使用した汎用 LDAP ディレクトリサービスの設定

LDAP ディレクトリサービスを設定するには、**cfgLdap** および **cfgLdapRoleGroup** RACADM グループ内のオブジェクトを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

LDAP ディレクトリサービス設定のテスト

LDAP ディレクトリサービス設定をテストして、設定に誤りがないかどうかを確認したり、障害のある LDAP ログインの問題を診断することができます。

iDRAC7 ウェブインターフェースを使用した LDAP ディレクトリサービスの設定のテスト

LDAP ディレクトリサービスの設定をテストするには、次の手順を実行します。

1. iDRAC7 ウェブインターフェースで、**概要 → iDRAC 設定 → ユーザー認証 → ディレクトリサービス → 汎用 LDAP ディレクトリサービス** と移動します。

   汎用 LDAP 設定と管理 ページには、現在の汎用 LDAP 設定が表示されます。
2. **設定のテスト** をクリックします。
3. LDAP 設定のテストのために選択されたディレクトリユーザーのユーザー名とパスワードを入力します。形式は、使用されている*ユーザーログインの属性*によって異なります。そして、入力されるユーザー名は選択された属性の値と一致する必要があります。

メモ: 証明書の検証を有効にする がチェックされた状態で LDAP 設定をテストする場合、iDRAC7 では LDAP サーバーが IP アドレスではなく FQDN で識別されている必要があります。LDAP サーバーが IP アドレスで識別されていると、iDRAC7 が LDAP サーバーと通信することができないため、証明書の検証に失敗します。

メモ: 汎用 LDAP が有効になっている場合、iDRAC7 はまずディレクトリユーザーとしてユーザーのログインを試みます。ログインに失敗した場合、ローカルユーザーの検索が有効になります。

テスト結果およびテストログが表示されます。

RACADM を使用した LDAP ディレクトリサービス設定のテスト

LDAP ディレクトリサービス設定をテストするには、`testfeature` コマンドを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

8

シングルサインオンまたはスマートカードログインのための iDRAC7 の設定

本項では、スマートカードログイン（ローカルユーザーおよび Active Directory ユーザー向け）とシングルサインオン（SSO）ログイン（Active Directory ユーザー向け）用に iDRAC7 を設定するための情報を記載します。SSO とスマートカードログインは、ライセンスが必要な機能です。

iDRAC7 は、スマートカードおよび SSO ログインをサポートするために、ケルベロスベースの Active Directory 認証をサポートします。ケルベロスについては、マイクロソフトのウェブサイトを参照してください。

関連リンク

Active Directory ユーザーのための iDRAC7 SSO ログインの設定
ローカルユーザー用の iDRAC7 スマートカードログインの設定
Active Directory ユーザーのための iDRAC7 スマートカードログインの設定

Active Directory シングルサインオンまたはスマートカードログインの前提条件

Active Directory ベースの SSO またはスマートカードログインの前提条件は、次のとおりです。

- iDRAC7 の時刻と Active Directory ドメインコントローラの時刻を同期してください。そうしないと、iDRAC7 でのケルベロス認証に失敗します。iDRAC の時刻（UTC）からドメインコントローラの時刻のオフセット値は分単位です（たとえば、中部タイムゾーンの場合は -360）。許容される最大時間差は 5 分です。サーバーの時刻とドメインコントローラの時刻を同期した後は、iDRAC7 を **リセット（再起動）** してください。

  次の RACADM タイムゾーンオフセットコマンドを使用して時刻を同期することもできます。

  ```
  racadm config -g cfgRacTuning -o
  cfgRacTuneTimeZoneOffset <オフセット値>
  ```

  夏時間の実施中は、次のコマンドを使用します。

  ```
  cfgRacTuneDaylightOffset <オフセット値>
  ```

  詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。
- iDRAC7 を Active Directory のルートドメインにコンピュータとして登録します。
- ktpass ツールを使用して、keytab ファイルを生成します。
- 拡張スキーマに対してシングルサインオンを有効にするには、keytab ユーザーの **委任** タブで **任意のサービスへの委任についてこのユーザーを信頼する（ケルベロスのみ）** オプションを選択するようにしてください。このタブは、ktpass ユーティリティを使用して keytab ファイルを作成した後でのみ使用できます。
- SSO ログインが有効になるようにブラウザを設定します。
- Active Directory オブジェクトを作成し、必要な権限を与えます。
- SSO 用に、iDRAC7 が存在するサブネットのための DNS サーバーでリバースルックアップゾーンを設定します。

メモ: ホスト名が DNS リバースルックアップに一致しない場合は、ケルベロス認証に失敗します。

関連リンク

iDRAC7 の Active Directory ルートドメインへのコンピュータとしての登録

Active Directory ルートドメインに iDRAC7 を登録するには、次の手順を実行します。

1. **概要 → iDRAC 設定 → ネットワーク → ネットワーク** とクリックします。
   ネットワーク ページが表示されます。
2. 有効な **優先 / 代替 DNS サーバー** の IP アドレスを指定します。この値は、ルートドメインの一部である有効な DNS サーバーの IP アドレスです。
3. **iDRAC の DNS への登録** を選択します。
4. 有効な **DNS ドメイン名** を入力します。
5. ネットワーク DNS の設定が Active Directory の DNS 情報と一致することを確認します。
   オプションの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。

Kerberos Keytab ファイルの生成

SSO およびスマートカードログイン認証をサポートするために、iDRAC7 は Windows Kerberos ネットワーク上の Kerberos 化されたサービスとして、自らを有効にする設定をサポートします。iDRAC7 での Kerberos 設定では、Windows Server Active Directory で、Windows Server 以外の Kerberos サービスをセキュリティプリンシパルとして設定する手順と同じ手順を実行します。

ktpass ツール（サーバーインストール CD / DVD の一部として Microsoft から入手できます）を使用して、ユーザーアカウントにバインドするサービスプリンシパル名（SPN）を作成し、信頼情報を MIT 形式の Kerberos *keytab* ファイルにエクスポートします。これにより、外部ユーザーやシステムとキー配布センター（KDC）の間の信頼関係が有効になります。keytab ファイルには暗号キーが含まれており、サーバーと KDC の間での情報の暗号化に使用されます。ktpass ツールによって、Kerberos 認証をサポートする UNIX ベースのサービスは Windows Server Kerberos KDC サービスが提供する相互運用性機能を利用できるようになります。**ktpass** ユーティリティの詳細については、マイクロソフトの Web サイト **technet.microsoft.com/en-us/library/cc779157(WS.10).aspx** を参照してください。

keytab ファイルを生成する前に、`ktpass` コマンドの **-mapuser** オプションと使用する Active Directory ユーザーアカウントを作成する必要があります。さらに、このアカウントは、生成した keytab ファイルをアップロードする iDRAC7 DNS 名と同じ名前にする必要があります。

ktpass ツールを使用して keytab ファイルを生成するには、次の手順を実行します。

1. *ktpass* ユーティリティを、Active Directory 内のユーザーアカウントに iDRAC7 をマップするドメインコントローラ（Active Directory サーバー）上で実行します。
2. 次の ktpass コマンドを使用して、Kerberos keytab ファイルを作成します。

```
C:\> ktpass.exe -princ HTTP/idrac7name.domainname.com@DOMAINNAME.COM -
mapuser DOMAINNAME\username -mapOp set -crypto DES-CBC-MD5 -ptype
KRB5_NT_PRINCIPAL -pass [パスワード] +DesOnly -out c:\krbkeytab
```

   暗号化タイプは、DES-CBC-MD5 です。プリンシパルタイプは、KRB5_NT_PRINCIPAL です。サービスプリンシパル名がマップされているユーザーアカウントのプロパティは、このアカウントプロパティを有効にするために、DES 暗号化タイプを使用する必要があります。

メモ: iDRAC7name および **サービスプリンシパル名** には小文字を使用します。ドメイン名には、例に示されているように大文字を使用します。

3. 次のコマンドを実行します。
   ```
   C:\>setspn -a HTTP/iDRAC7name.domainname.com username
   ```
   keytab ファイルが生成されます。

メモ: keytab ファイルが作成される iDRAC7 ユーザーに問題がある場合は、新しいユーザーと新しい keytab ファイルを作成します。最初に作成されたファイルと同じ keytab ファイルが再度実行されると、正しく設定されません。

Active Directory オブジェクトの作成と権限の付与

Active Directory 拡張スキーマベースの SSO ログイン用に、次の手順を実行します。

1. Active Directory サーバーで、デバイスオブジェクト、権限オブジェクト、および関連オブジェクトを作成します。
2. 作成された権限オブジェクトにアクセス権限を設定します。一部のセキュリティチェックを省略できることから、管理者権限を付与しないことを推奨します。
3. 関連オブジェクトを使用して、デバイスオブジェクトと権限オブジェクトを関連付けます。
4. デバイスオブジェクトに先行 SSO ユーザー（ログインユーザー）を追加します。
5. 作成した関連オブジェクトにアクセスするためのアクセス権を、*認証済みユーザー*に与えます。

関連リンク

Active Directory への iDRAC7 ユーザーと権限の追加

Active Directory SSO を有効にするためのブラウザ設定

本項では、Active Directory SSO を有効にするための Internet Explorer および Firefox のブラウザ設定について説明します。

Active Directory SSO を有効にするための Internet Explorer の設定

Internet Explorer のブラウザ設定を行うには、次の手順を実行します。

1. Internet Explorer で、**ローカルイントラネット** に移動して **サイト** をクリックします。
2. 次のオプションのみを選択します。
   - 他のゾーンにリストされていないすべてのローカル（イントラネット）サイトを含める。
   - プロキシサーバーをバイパスするすべてのサイトを含める。
3. **詳細設定** をクリックします。
4. SSO 設定の一部である iDRAC7 インスタンスに使用される関連ドメイン名をすべて追加します（たとえば、**myhost.example.com**）。
5. **閉じる** をクリックして **OK** を 2 回クリックします。

Active Directory SSO を有効にするための Firefox の設定

Firefox 用のブラウザ設定を行うには、次の手順を実行します。

1. Firefox アドレスバーに `about:config` と入力します。
2. **フィルタ** で `network.negotiate` と入力します。
3. network.negotiate-auth.trusted-uris に iDRAC7 の名前を追加します（コンマ区切りのリストを使用）。
4. network.negotiate-auth.delegation-uris に iDRAC7 の名前を追加します（コンマ区切りのリストを使用）。

Active Directory ユーザーのための iDRAC7 SSO ログインの設定

iDRAC7 を Active Directory SSO ログイン用に設定する前に、すべての前提条件を満たしていることを確認してください。

Active Directory に基づいたユーザーアカウントをセットアップすると、Active Directory SSO 用に iDRAC7 を設定できます。

関連リンク

Active Directory シングルサインオンまたはスマートカードログインの前提条件
iDRAC7 ウェブインタフェースを使用した標準スキーマでの Active Directory の設定
RACADM を使用した標準スキーマの Active Directory の設定
iDRAC7 ウェブインタフェースを使用した拡張スキーマの Active Directory の設定
RACADM を使用した拡張スキーマの Active Directory の設定

ウェブインタフェースを使用した Active Directory ユーザーのための iDRAC7 SSO ログインの設定

Active Directory SSO ログイン用に iDRAC7 を設定するには、次の手順を実行します。

メモ: オプションの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。

1. iDRAC7 DNS 名が iDRAC7 完全修飾ドメイン名に一致するかどうかを確認します。これには、iDRAC7 ウェブインタフェースで **概要** → **iDRAC 設定** → **ネットワーク** → **ネットワーク** と移動し、**DNS ドメイン名** プロパティを調べます。
2. 標準スキーマまたは拡張スキーマに基づいてユーザーアカウントをセットアップするために Active Directory を設定する間、次の 2 つの追加手順を実行して SSO を設定します。
   - **Active Directory の設定と管理手順 4 の 1** ページで keytab ファイルをアップロードします。
   - **Active Directory の設定と管理手順 4 の 2** ページで **シングルサインオンの有効化** オプションを選択します。

RACADM を使用した Active Directory ユーザー用の iDRAC7 SSO ログインの設定

SSO を有効にするには、Active Directory の設定中に実行する手順への追加として、次のコマンドを実行します。

```
racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
```

ローカルユーザー用の iDRAC7 スマートカードログインの設定

スマートカードログインできるように iDRAC7 ローカルユーザーを設定するには、次の手順を実行します。

1. スマートカードユーザー証明書および信頼できる CA 証明書を iDRAC7 にアップロードします。
2. スマートカードログインを有効にします。

関連リンク

証明書の取得
スマートカードユーザー証明書のアップロード
スマートカードログインの有効化または無効化

スマートカードユーザー証明書のアップロード

ユーザー証明書をアップロードする前に、スマートカードベンダーからのユーザー証明書が Base64 フォーマットでエクスポートされていることを確認してください。

関連リンク

証明書の取得

ウェブインタフェースを使用したスマートカードユーザー証明書のアップロード

スマートカードユーザー証明書をアップロードするには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ネットワーク → ユーザー認証 → ローカルユーザー** と移動します。
   ユーザー ページが表示されます。
2. **ユーザー ID** 列で、ユーザー ID 番号をクリックします。
   ユーザーメインメニュー ページが表示されます。
3. **スマートカード設定** で、**ユーザー証明書のアップロード** を選択し、**次へ** をクリックします。
   ユーザー証明書のアップロード ページが表示されます。
4. Base64 ユーザー証明書を参照して選択し、**適用** をクリックします。

RACADM を使用したスマートカードユーザー証明書のアップロード

スマートカードユーザー証明書をアップロードするには、**usercertupload** オブジェクトを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

スマートカード用の信頼できる CA 証明書のアップロード

CA 証明書をアップロードする前に、CA 署名付きの証明書があることを確認してください。

関連リンク

証明書の取得

ウェブインタフェースを使用したスマートカード用の信頼できる CA 証明書のアップロード

スマートカードログイン用の信頼できる CA 証明書をアップロードするには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ネットワーク → ユーザー認証 → ローカルユーザー** と移動します。
   ユーザー ページが表示されます。
2. **ユーザー ID** 列で、ユーザー ID 番号をクリックします。
   ユーザーメインメニュー ページが表示されます。
3. **スマートカード設定** で、**信頼できる CA 証明書のアップロード** を選択し、**次へ** をクリックします。
   信頼できる CA 証明書のアップロード ページが表示されます。
4. 信頼できる CA 証明書を参照して選択し、**適用** をクリックします。

RACADM を使用したスマートカード用の信頼できる CA 証明書のアップロード

スマートカードログイン用に信頼できる CA 証明書をアップロードするには、**usercertupload** オブジェクトを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

Active Directory ユーザーのための iDRAC7 スマートカードログインの設定

Active Directory ユーザー用の iDRAC7 スマートカードログインを設定する前に、必要な前提条件を満たしていることを確認します。

スマートカードログインのために iDRAC7 に設定するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、標準スキーマまたは拡張スキーマに基づいたユーザーアカウントをセットアップするために Active Directory を設定している際に、**Active Directory の設定と管理手順 4 の 1** ページ上で、次の作業を実行します。
   - 証明書の検証を有効にします。
   - 信頼できる CA 署名付き証明書をアップロードします。
   - keytab ファイルをアップロードします。
2. スマートカードログインを有効にします。オプションの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。

関連リンク

スマートカードログインの有効化または無効化
証明書の取得
Kerberos Keytab ファイルの生成
iDRAC7 ウェブインタフェースを使用した標準スキーマでの Active Directory の設定
RACADM を使用した標準スキーマの Active Directory の設定
iDRAC7 ウェブインタフェースを使用した拡張スキーマの Active Directory の設定
RACADM を使用した拡張スキーマの Active Directory の設定

スマートカードログインの有効化または無効化

iDRAC7 に対するスマートカードログインを有効化または無効化にする前に、次を確認してください。

- iDRAC7 の設定許可を持っていること。
- 適切な証明書での iDRAC7 ローカルユーザー設定または Active Directory ユーザー設定が完了していること。

メモ: スマートカードログインが有効になっている場合、SSH、Telnet、IPMI Over LAN、シリアルオーバー LAN、およびリモート RACADM は無効になります。また、スマートカードログインを無効にすると、インタフェースは自動で有効にはなりません。

関連リンク

証明書の取得
Active Directory ユーザーのための iDRAC7 スマートカードログインの設定
ローカルユーザー用の iDRAC7 スマートカードログインの設定

ウェブインタフェースを使用したスマートカードログインの有効化または無効化

スマートカードログオン機能を有効化または無効化するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ユーザー認証 → スマートカード** と移動します。**スマートカード** ページが表示されます。
2. **スマートカードログオンの設定** ドロップダウンメニューから、**有効** を選択してスマートカードログオンを有効化するか、**リモート RACADM で有効化** を選択します。それ以外の場合は、**無効** を選択します。

   オプションの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。

3. **適用** をクリックして設定を適用します。
   以降の iDRAC7 ウェブインタフェースを使用したログオン試行では、スマートカードログインが要求されます。

RACADM を使用したスマートカードログインの有効化または無効化

スマートカードログインを有効にするには、**cfgSmartCardLogonEnable** オブジェクトと **cfgSmartCardCRLEnable** オブジェクトを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

iDRAC 設定ユーティリティを使用したスマートカードログインの有効化または無効化

スマートカードログオン機能を有効化または無効化するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**スマートカード** に移動します。
   iDRAC 設定のスマートカード ページが表示されます。
2. スマートカードログオンを有効化する場合は、**有効** を選択します。それ以外の場合は、**無効** を選択します。オプションの詳細については、『*iDRAC 設定ユーティリティオンラインヘルプ*』を参照してください。
3. **戻る**、**終了** の順にクリックし、**はい** をクリックします。
   選択に従って、スマートカードログオン機能が有効化または無効化されます。

9

アラートを送信するための iDRAC7 の設定

管理下システムで発生する特定のイベントに対してアラートと処置を設定できます。システムコンポーネントのステータスが事前定義の条件を上回るとイベントが発生します。イベントがイベントフィルタと一致したとき、そのフィルタがアラート（電子メール、SNMP トラップ、または IPMI アラート）を生成するように設定されていると、アラートが 1 つ、または複数の設定済み宛先に送信されます。さらに、同じイベントフィルタが処置（システムの再起動、電源の入れ直し、電源オフなど）を実行するようにも設定されていた場合は、その処置が実行されます。処置は、イベントにつき 1 つだけ設定できます。

アラートを送信するように iDRAC7 を設定するには、次の手順を実行します。

1. アラートを有効化します。
2. オプションで、アラートをカテゴリまたは重要度でフィルタリングできます。
3. 電子メールアラート、IPMI アラート、または SNMP トラップ設定を行います。
4. 次のようなイベントの警告とアクションを有効にします。
   - 設定済み宛先に電子メールアラート、IPMI アラート、または SNMP トラップを送信する。
   - 管理下システムの再起動、電源オフ、またはパワーサイクルを実行する。

関連リンク

アラートの有効化または無効化
アラートのフィルタ
イベントアラートの設定
電子メールアラート、SNMP トラップ、または IPMI トラップ設定の設定
アラートメッセージ ID

アラートの有効化または無効化

設定された宛先にアラートを送信する、またはイベント処置を実行するには、グローバルアラートオプションを有効化する必要があります。このプロパティは、設定された個々のアラートまたはイベント処置よりも優先されます。

関連リンク

アラートのフィルタ
電子メールアラート、SNMP トラップ、または IPMI トラップ設定の設定

ウェブインタフェースを使用したアラートの有効化または無効化

アラートの生成を有効化または無効化するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → アラート** と進みます。**アラート** ページが表示されます。
2. **アラート** セクションで次の操作を行います。
   - アラートの生成を有効化、またはイベント処置を実行するには、**有効** を選択します。
   - アラートの生成を無効化、またはイベント処置を無効化するには、**無効** を選択します。
3. **適用** をクリックして設定を保存します。

RACADM を使用したアラートの有効化または無効化

アラートの生成またはイベント処置を有効化または無効化するには、次のコマンドを入力します。

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

iDRAC 設定ユーティリティを使用したアラートの有効化または無効化

アラートの生成またはイベント処置を有効化または無効化するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**アラート** に進みます。
   iDRAC 設定アラート ページが表示されます。
2. **プラットフォームイベント** で、**有効** を選択してアラート生成またはイベントアクションを有効にします。または、**無効** を選択します。オプションの詳細については、『*iDRAC 設定ユーティリティオンラインヘルプ*』を参照してください。
3. **戻る**、**終了** の順にクリックし、**はい** をクリックします。
   アラートが設定されます。

アラートのフィルタ

カテゴリ及び重要度に基づいてアラートをフィルタすることができます。

関連リンク

アラートの有効化または無効化
電子メールアラート、SNMP トラップ、または IPMI トラップ設定の設定

iDRAC7 ウェブインタフェースを使用したアラートのフィルタ

カテゴリ及び重要度に基づいてアラートをフィルタするには、次の手順を実行します。

メモ: 読み取り専用権限を持つユーザーであっても、アラートのフィルタは可能です。

1. iDRAC7 ウェブインタフェースで **概要** → **サーバー** → **アラート** の順に選択します。**アラート** ページが表示されます。
2. **アラートフィルタ** セクションで、次のカテゴリから 1 つまたは複数選択します。
   - システムの正常性
   - ストレージ
   - 設定
   - 監査
   - アップデート
   - ワークノート
3. 次の重要度から 1 つまたは複数を選択します。
   - 情報
   - 警告
   - 重要
4. **適用** をクリックします。
   選択したカテゴリおよび重要度に基づいて、**アラート結果** セクションに結果が表示されます。

RACADM を使用したアラートのフィルタ

アラートをフィルタするには、**eventfilters** コマンドを使用します。詳細に関しては、**support.jp.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

イベントアラートの設定

電子メールアラート、IPMI アラート、SNMP トラップなどのイベントアラートが設定した宛先に送信されるように設定することができます。

関連リンク

アラートの有効化または無効化
電子メールアラート、SNMP トラップ、または IPMI トラップ設定の設定
アラートのフィルタ

ウェブインタフェースを使用したイベントアラートの設定

ウェブインタフェースを使用してイベントアラートを設定するには、次の手順を実行します。

1. 電子メールアラート、IPMI アラート、および SNMP トラップを設定したことを確認します。
2. **概要** → **サーバー** → **アラート** と進みます。
   アラート ページが表示されます。
3. **アラート結果** で、必要なイベントに対して次のアラートの 1 つまたはすべてを選択します。
   - 電子メールアラート
   - SNMP トラップ
   - IPMI アラート
4. **適用** をクリックします。
   設定が保存されます。
5. **アラート** セクションで **有効** オプションを選択して、設定した宛先にアラートを送信します。

RACADM を使用したイベントアラートの設定

イベントアラートを設定するには、**eventfilters** コマンドを使用します。詳細に関しては、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

イベント処置の設定

システムで、再起動、パワーサイクル、電源オフ、または処置なしなどのイベント処置を設定できます。

関連リンク

アラートのフィルタ
アラートの有効化または無効化

ウェブインタフェースを使用したイベントアクションの設定

イベントアクションを設定するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → アラート** の順に選択します。**アラート** ページが表示されます。
2. **アラートの結果** の **処置** ドロップダウンメニューから、各イベントに対する処置を選択します。
   - 再起動
   - パワーサイクル
   - 電源オフ
   - 処置なし
3. **適用** をクリックします。
   設定が保存されます。

RACADM を使用したイベントアクションの設定

イベントアクションを設定するには、**cfgIpmiPefAction** オブジェクトまたは **eventfilters** コマンドを使用します。詳細に関しては、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

電子メールアラート、SNMP トラップ、または IPMI トラップ設定の設定

管理ステーションは、Simple Network Management Protocol（SNMP）および Intelligent Platform Management Interface（IPMI）トラップを使用して、iDRAC7 からデータを受信します。多数のノードを含むシステムの場合、発生し得るすべての状態について各 iDRAC7 をポーリングするのは効率的ではない場合があります。たとえば、イベントトラップはノード間の負荷分散や、認証が失敗した場合のアラート送信で、管理ステーションを援助します。

IPv4 および IPv6 アラートの宛先設定、電子メール設定、SMTP サーバー設定を行い、これらの設定をテストすることができます。

電子メール、SNMP、または IPMI トラップを設定する前に、次を確認します。

- RAC の設定許可を持っている。
- イベントフィルタを設定した。

関連リンク

IP アラート宛先の設定
電子メールアラートの設定

IP アラート宛先の設定

IPMI アラートまたは SNMP トラップを受信する IPv6 または IPv4 アドレスを設定できます。

ウェブインタフェースを使用した IP アラート宛先の設定

ウェブインタフェースを使用して IPv4 または IPv6 アラート宛先を設定するには、次の手順を実行します。

1. **概要 → サーバー → アラート → SNMP と電子メールの設定** と移動します。
2. **状態** オプションを選択して、トラップを受信する IP アドレスを有効にし、IPv4 および IPv6 の IP アドレスを入力します。最大で 4 個の IPv4 宛先アドレスと 4 個の IPv6 宛先アドレスを指定できます。このオプションの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。
3. iDRAC7 SNMP コミュニティ文字列を入力します。このオプションの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。

メモ: このコミュニティ文字列の値は、iDRAC7 から送信された Simple Network Management Protocol（SNMP）アラートトラップで使用されるコミュニティ文字列を示します。宛先のコミュニティ文字列が iDRAC7 コミュニティ文字列と同じであることを確認してください。デフォルト値は Public です。

4. IP アドレスが IPMI トラップまたは SNMP トラップを受信しているかどうかをテストするには、**IPMI トラップのテスト** と **SNMP トラップのテスト** でそれぞれ **送信** をクリックします。
5. **適用** をクリックします。アラート宛先が設定されます。

RACADM を使用した IP アラート宛先の設定

トラップアラートを設定するには、次の手順を実行します。

1. トラップを有効にするには、次の手順を実行します。
   - IPv4 アドレスの場合：

     ```
     racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i (インデックス) (0|1)
     ```
   - IPv6 アドレスの場合：

     ```
     racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6AlertEnable -i (インデックス) (0|1)
     ```

     （インデックス）は宛先インデックスです。0 は トラップを無効にし、1 はトラップを有効にします。
     たとえば、トラップをインデックス 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
     ```
2. トラップの宛先アドレスを設定するには、次の手順を実行します。

   ```
   racadm config -g cfgIpmiPetIpv6 -o cfgIpmiPetIpv6AlertDestIPAddr -i [インデックス] [IP アドレス]
   ```

   [インデックス] はトラップの宛先インデックスであり、[IP アドレス] はプラットフォームイベントアラートを受信するシステムの宛先 IP アドレスです。
3. 次の手順を実行して、SNMP コミュニティ名文字列を設定します。

   ```
   racadm config -g cfgIpmiLan -o cfgIpmiPetCommunityName [名前]
   ```

   ここで [名前] は SNMP コミュニティ名です。
4. 必要に応じてトラップをテストするには、次の手順を実行します。

   ```
   racadm testtrap -i [インデックス]
   ```

   ここで [インデックス] は、テストするトラップの宛先インデックスです。

   詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

iDRAC 設定ユーティリティを使用した IP アラート宛先の設定

iDRAC 設定ユーティリティを使用すると、IPv4 アラート宛先だけを設定できます。IPv4 アラート宛先を設定するには、次の手順を実行します。

1. **iDRAC 設定ユーティリティ** で **アラート** に進みます。
   iDRAC 設定アラート ページが表示されます。
2. **トラップ設定** で、トラップを受信する IP アドレスを有効にし、IPv4 宛先アドレスを入力します。最大 4 個の IPv4 アドレスを指定できます。
3. コミュニティ文字列名を入力します。
   オプションについては、『*iDRAC 設定ユーティリティオンラインヘルプ*』を参照してください。
4. 戻る、終了、はい の順にクリックします。

IPv4 アラート宛先が設定されます。

電子メールアラートの設定

電子メールアラートを受信する電子メールアドレスを設定できます。また、SMTP サーバーアドレスも設定できます。

メモ: メールサーバーが Microsoft Exchange Server 2007 である場合、iDRAC7 から 電子メールアラートを受信するには、そのメールサーバー用に iDRAC7 ドメイン名が設定されていることを確認してください。

メモ: 電子メールアラートは IPv4 および IPv6 アドレスの両方をサポートします。IPv6 を使用する場合には、DRAC DNS ドメイン名を指定する必要があります。

関連リンク

SMTP 電子メールサーバーアドレス設定の設定

ウェブインタフェースを使用した電子メールアラート設定の設定

ウェブインタフェースを使用して E-メールアラート設定を設定するには、次の手順を実行します。

1. **概要 → サーバー → アラート → SNMP と電子メールの設定** と移動します。
2. **状態** オプションを選択して、アラートを受け取る電子メールアドレスを有効にし、有効な電子メールアドレスを入力します。オプションの詳細については、『*iDRAC7 のオンラインヘルプ*』を参照してください。
3. **電子メールのテスト** で **送信** をクリックして、指定された電子メールアラートの設定をテストします。
4. **適用** をクリックします。

RACADM を使用した電子メールアラート設定の設定

電子メールアラート設定を行うには、次の手順を実行します。

1. 電子メールアラートを有効にする：

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i [インデックス] [0|1]
   ```

   [インデックス] は 電子メール送信先のインデックスで、0 は電子メールアラートを無効に、1 は電子メールアラートを有効にします。

   電子メール送信先のインデックスは、1～4 の値が可能です。たとえば、電子メールをインデックス 4 で有効にするには、次のコマンドを入力します。

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

2. 電子メール設定を行う：

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 <E-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アラートを受け取る送信先の電子メールアドレスです。

3. カスタムメッセージを設定する：

   ```
   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のインデックスで、[カスタムメッセージ] はカスタマイズされたメッセージです。

4. 指定された電子メールアラートをテストする（必要な場合）：

   ```
   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のインデックスです。

詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

SMTP 電子メールサーバーアドレス設定の設定

電子メールアラートを指定の宛先に送信するためには、SMTP サーバーアドレスを設定する必要があります。

iDRAC7 ウェブインタフェースを使用した SMTP 電子メールサーバーアドレス設定の設定

SMTP サーバーアドレスを設定するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → アラート → SNMP と電子メールの設定** と移動します。
2. **認証の有効化** オプションを選択し、ユーザー名とパスワード（SMTP サーバーへのアクセス権を持つユーザー）を指定し、設定で使用される有効な IP アドレスまたは SMTP サーバーの完全修飾ドメイン名（FQDN）を入力します。

   オプションの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。
3. **適用** をクリックします。

   SMTP が設定されます。

RACADM を使用した SMTP 電子メールサーバーアドレスの設定

SMTP 電子メールサーバーを設定するには、次のコマンドを実行します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr <SMTP 電子メールサーバーの IP アドレス>
```

アラートメッセージ ID

次の表に、アラートに対して表示されるメッセージ ID の一覧を示します。

表 21. アラートメッセージ ID

メッセージ ID	説明
AMP	アンペア数
ASR	自動システムリセット
BAR	バックアップ / 復元
BAT	バッテリイベント
BIOS	BIOS 管理
BOOT	起動コントロール
CBL	ケーブル
CPU	プロセッサ
CPUA	プロセッサ不在
CTL	ストレージコントローラ
DH	証明書管理
DIS	自動検出
ENC	ストレージエンクロージャ
FAN	ファンイベント
FSD	デバッグ
HWC	ハードウェア設定

メッセージ ID	説明
IPA	DRAC IP 変更
ITR	イントルージョン
JCP	ジョブ制御
LC	Lifecycle Controller
LIC	ライセンス
LNK	リンクステータス
LOG	ログイベント
MEM	メモリ
NDR	NIC OS ドライバ
NIC	NIC 設定
OSD	オペレーティングシステムの導入
OSE	OS イベント
PCI	PCI デバイス
PDR	物理ディスク
PR	部品交換
PST	BIOS POST
PSU	電源装置
PSUA	PSU 不在
PWR	電力消費
RAC	RAC イベント
RDU	冗長性
RED	FW ダウンロード
RFL	IDSDM メディア
RFLA	IDSDM 不在
RFM	FlexAddress SD
RRDU	IDSDM の冗長性
RSI	リモートサービス
SEC	セキュリティイベント
SEL	システムイベントログ
SRD	ソフトウェア RAID
SSD	PCIe SSD
STOR	ストレージ
SUP	FW アップデートジョブ
SWC	ソフトウェア設定
SWU	ソフトウェアの変更
SYS	システム情報
TMP	温度

メッセージ ID	説明
TST	テストアラート
UEFI	UEFI イベント
USR	ユーザー追跡
VDR	仮想ディスク
VF	vFlash SD カード
VFL	vFlash イベント
VFLA	vFlash 不在
VLT	電圧
VME	仮想メディア
VRM	仮想コンソール
WRK	作業メモ

10

ログの管理

iDRAC7 は、システム、ストレージデバイス、ネットワークデバイス、ファームウェアのアップデート、設定変更、ライセンスメッセージなどに関連するイベントが含まれたライフサイクルログを提供します。ただし、システムイベントは、システムイベントログ（SEL）と呼ばれる別のログとしても使用できます。ライフサイクルログは、iDRAC7 ウェブインタフェース、RACADM、および WS-MAN インタフェースからアクセスすることが可能です。

ライフサイクルログのサイズが 800 KB に達すると、ログは圧縮され、アーカイブされます。表示できるのはアーカイブ化されていないログのみです。また、アーカイブされていないログには、フィルタを適用したり、コメントを追加したりできます。アーカイブされたログを表示するには、ライフサイクルログ全体をシステム上の場所にエクスポートする必要があります。

関連リンク

システムイベントログの表示
ライフサイクルログの表示
作業メモの追加
リモートシステムロギングの設定

システムイベントログの表示

管理下システムでシステムイベントが発生すると、そのイベントはシステムイベントログ（SEL）に記録されます。LC ログにも、同じ SEL エントリが提供されます。

ウェブインタフェースを使用したシステムイベントログの表示

SEL を表示するには、iDRAC7 ウェブインタフェースで、**概要 → サーバー → ログ** タブの順に移動します。

システムイベントログ ページには、ログされた各イベントのシステム正常性インジケータ、タイムスタンプ、および説明が表示されます。詳細に関しては、『*iDRAC7 オンラインヘルプ*』を参照してください。

名前を付けて保存 をクリックして、**SEL** を希望する場所に保存します。

メモ: Internet Explorer を使用しており、保存中に問題が発生した場合は、マイクロソフトのサポートサイト **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するようにしてください。

RACADM を使用したシステムイベントログの表示

SEL を表示するには、次のコマンドを使用します。

```
racadm getsel <オプション>
```

引数の指定がない場合は、ログ全体が表示されます。

SEL エントリの数を表示するには、次のコマンドを使用します。

```
racadm getsel -i
```

詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

ライフサイクルログの表示

ライフサイクルコントローラログでは、管理下システムに取り付けられたコンポーネントに関する変更履歴が提供されます。次に関するイベントのログが提供されます。

- ストレージデバイス
- システムイベント
- ネットワークデバイス
- 設定
- 監査
- アップデート
- 作業メモ

カテゴリおよび重要度に基づいたログのフィルタ、表示、エクスポート、ログイベントへの作業メモの追加を実行できます。

関連リンク

ライフサイクルログのフィルタ
ライフサイクルログ結果のエクスポート
ライフサイクルログへのコメントの追加

ウェブインタフェースを使用したライフサイクルログの表示

ライフサイクルログを表示するには、**概要** → **サーバー** → **ログ** → **ライフサイクルログ** とクリックします。**ライフサイクルログ** ページが表示されます。オプションの詳細に関しては、『*iDRAC7 オンラインヘルプ*』を参照してください。

ライフサイクルログのフィルタ

ログは、カテゴリ、重要度、キーワード、または期間に基づいてフィルタすることができます。

ライフサイクルログをフィルタするには、次の手順を実行します。

1. **ライフサイクルログ** ページの **ログフィルタ** セクションで、次の操作のいずれか、またはすべてを実行します。
   - ドロップダウンリストから **ログタイプ** を選択します。
   - **ステータスレベル** ドロップダウンリストから重要度を選択します。
   - キーワードを入力します。
   - 期限を指定します。
2. **適用** をクリックします。

   ログ結果 にフィルタされたログエントリが表示されます。

ライフサイクルログ結果のエクスポート

ライフサイクルログ結果をエクスポートするには、**ライフサイクルログ** ページの **ログ結果** セクションで、**エクスポート** をクリックします。ログエントリを XML フォーマットで希望する場所に保存できるダイアログボックスが表示されます。

ライフサイクルログへのコメントの追加

ライフサイクルログにコメントを追加するには、次の手順を実行します。

1. **ライフサイクルログ** ページで、必要なログエントリの + アイコンをクリックします。

メッセージ ID の詳細が表示されます。

2. **コメント** ボックスに、ログエントリに対するコメントを入力します。
   コメントが **コメント** ボックスに表示されます。

RACADM を使用したライフサイクルログの表示

ライフサイクルログを表示するには、`lclog` コマンドを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

作業メモの追加

iDRAC7 にログインする各ユーザーは、作業メモを追加でき、これはイベントとしてライフサイクルログに保存されます。作業メモを追加するには iDRAC7 ログ権限が必要です。それぞれの新しい作業メモで最大 255 文字がサポートされます。

メモ: 作業メモは削除できません。

作業メモを追加するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → プロパティ → サマリ** と移動します。
   システムサマリ ページが表示されます。
2. **作業メモ** の下で、空のテキストボックスにテキストを入力します。

メモ: 特殊文字を使いすぎないことが推奨されます。

3. **追加** をクリックします。
   作業メモがログに追加されます。詳細に関しては、『*iDRAC7 オンラインヘルプ*』を参照してください。

リモートシステムロギングの設定

ライフサイクルログをリモートシステムに送信できます。これを行う前に、次を確認してください。

- iDRAC7 とリモートシステム間がネットワーク接続されている。
- リモートシステムと iDRAC7 が同じネットワーク上にある。

ウェブインタフェースを使用したリモートシステムロギングの設定

リモート Syslog サーバーを設定するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → ログ → 設定** と移動します。
   リモート Syslog 設定 ページが表示されます。
2. リモート Syslog を有効化して、サーバーアドレスおよびポート番号を指定します。このオプションの詳細に関しては、『*iDRAC7 オンラインヘルプ*』を参照してください。
3. **適用** をクリックします。
   設定が保存されます。ライフサイクルログに書き込まれるすべてのログは、設定されたリモートサーバーにも同時に書き込まれます。

RACADM を使用したリモートシステムロギングの設定

リモート Syslog サーバーを設定するには、次の RACADM オブジェクトを使用します。

- cfgRhostsSyslogEnable
- cfgRhostsSyslogPort
- cfgRhostsSyslogServer1
- cfgRhostsSyslogServer2
- cfgRhostsSyslogServer3

詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

11

電源の監視と管理

iDRAC7 を使用して、管理下システムの電源要件の監視および管理ができます。これは、システムの電力消費量を適切に分配および制御することによって、システムの停電を防ぎます。

主な機能は次のとおりです。

- **電源監視** — 管理下システムの電源ステータス、電力測定の履歴、現在の平均、ピークなどの表示。
- **電力制限** — 最小および最大の潜在電力消費量の表示を含む、管理下システムの電力制限を表示および設定します。これはライセンスが必要な機能です。
- **電源制御** — 管理下システムでの電源制御操作（電源オン、電源オフ、システムリセット、パワーサイクル、および正常なシャットダウンなど）をリモートに実行できます。
- PSU オプション — 冗長性ポリシー、ホットスペア、およびパワーファクタ補正などの電源装置オプションを設定します。

関連リンク

電源の監視
電源コントロール操作の実行
電力制限
電源装置オプションの設定
電源ボタンの有効化または無効化

電源の監視

iDRAC7 は、システム内の電力消費量を継続的に監視し、次の電源に関する値を表示します。

- 電力消費量の警告しきい値および重要しきい値
- 累積電力、ピーク電力、およびピークアンペアの値
- 直近 1 時間、昨日、または先週の電力消費量
- 平均、最小、最大の電力消費量
- 過去のピーク値およびピーク時のタイムスタンプ
- ピーク時のヘッドルーム値および瞬間的ヘッドルーム値（ラックおよびタワーサーバーの場合）

ウェブインタフェースを使用した電源の監視

電源の監視情報を表示するには、iDRAC7 ウェブインタフェースで、**概要 → サーバー → 電源 / 熱 → 電源監視** と移動します。**電源監視ページ** が表示されます。詳細に関しては、『*iDRAC7 のオンラインヘルプ*』を参照してください。

RACADM を使用した電源の監視

電源監視情報を表示するには、**get** コマンドで **System.Power** グループオブジェクトを使用するか、**getconfig** コマンドで **cfgServerPower** オブジェクトを使用します。詳細に関しては、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

電源コントロール操作の実行

iDRAC7 では、ウェブインタフェースまたは RACADM を使用して、電源の投入、電源の切断、リセット、正常なシャットダウン、マスク不能割り込み（NMI）、またはパワーサイクルをリモートで実行できます。

Lifecycle Controller Remote Service または WS-Management を使用してこれらの操作を実行することもできます。詳細については、**support.dell.com/manuals** にある『*Lifecycle Controller Remote Services ユーザーズガイド*』および **delltechcenter.com** にある『*Dell 電源状態管理*』プロファイルマニュアルを参照してください。

ウェブインタフェースを使用した電源コントロール操作の実行

電源コントロール操作を実行するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → 電源 / 熱 → 電源コントロール → 電源設定** と移動します。**電源コントロール** ページが表示されます。
2. 必要な電源コントロール操作を選択します。
   - システムの電源を入れる
   - システムの電源を切る
   - NMI（マスク不能割り込み）
   - 正常なシャットダウン
   - システムのリセット（ウォームブート）
   - システムのパワーサイクル（コールドブート）
3. **適用** をクリックします。詳細は、『*iDRAC7 オンラインヘルプ*』を参照してください。

RACADM を使用した電源コントロール操作の実行

電源操作を実行するには、**serveraction** コマンドを使用します。詳細に関しては、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

電力制限

高負荷のシステムがデータセンターに示す AC および DC 電力消費量の範囲を対象とする電力しきい値の限界を表示することができます。これはライセンスが必要な機能です。

ブレードサーバーの電力制限

ブレードサーバーに電源投入される前に、iDRAC7 は CMC に電源要件を提示します。これはブレードが消費する可能性のある実際の電力よりも高く、限られたハードウェアのインベントリ情報に基づいて計算されるものです。サーバーが起動された後は、サーバーによる実際の電力消費量に基づき、それよりも低い電力範囲を要求する場合があります。電力消費量が徐々に増え、サーバーが割り当ての最大限度に近い電力を消費している場合、iDRAC7 は最大潜在電力消費量の増加を要求する場合があり、これによりパワーエンベロープが増加します。iDRAC7 は、CMC に対する最大潜在電力消費量要求だけを増加します。消費が減少しても、iDRAC7 は最小潜在電力を減少させる要求は行いません。iDRAC7 は、電力消費量が CMC によって割り当てられた電力を超える場合、より多くの電力を要求し続けます。

その後、システムに電源が投入されて初期化され、iDRAC7 は、実際のブレードの構成に基づき、新しい電源要件を計算します。 CMC が新しい電力要求の割り当てに失敗した場合でも、ブレードは電源オンのままです。

CMC は優先順位の低いサーバーの未使用電力を取り戻し、その電力を優先順位の高いインフラストラクチャモジュールやサーバーに割り当てます。

十分な電力が割り当てられていない場合は、ブレードサーバーの電源はオンになりません。ブレードに十分な電力が割り当てられている場合、iDRAC7 はシステムに電源を投入します。

電力制限ポリシーの表示と設定

電力制限ポリシーを有効にすると、システムに対するユーザー定義の電力制限が施行されます。電力制限ポリシーを有効にしない場合は、デフォルトで実装されたハードウェアの電源保護ポリシーが使用されます。この電源保護ポリシーは、ユーザー定義のポリシーの影響を受けません。システムパフォーマンスは、電力消費量が指定されたしきい値付近に維持されるよう、動的に調整されます。

実際の電力消費量は、軽い負荷では少なかったり、パフォーマンス調整が完了するまでに一時的にしきい値を超える場合があります。たとえば、あるシステム設定では、最大電力消費は 700 W であり、最小電力消費量は 500 W ですが、電力バジェットしきい値を指定して有効にし、現在の 650 W から 525 W に減少させることができます。これ以降、システムのパフォーマンスは、動的に調整され、電力消費量がユーザー指定のしきい値である 525 W を超えないように維持されます。

電力制限値が推奨される最小しきい値よりも低く設定されると、iDRAC7 は要求された電力制限を維持できないことがあります。

この値は、ワット、BTU/時、または推奨される電力上限に対する割合（%）で指定できます。

BTU/ 時間で電力制限しきい値を設定する場合、ワットへの変換は、最も近い整数値に四捨五入されます。ワットから BTU/ 時間にもどして電力制限しきい値読み取る時も、その変換は同様の方法で四捨五入されます。この結果、書き込み値と読み取り値は、名目上異なる場合があります。たとえば、600 BTU/ 時に設定されたしきい値が読み戻されると、601 BTU/ 時になります。

ウェブインタフェースを使用した電力制限ポリシーの設定

電力ポリシーを表示し、設定するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → 電源 / 熱 → 電源設定 → 電源設定** と移動します。**電源設定** ページが表示されます。

   電源設定 ページが表示されます。現在の電力ポリシー制限が **現在アクティブな電力制限ポリシー** セクションに表示されます。
2. **iDRAC 電力制限ポリシー** で **有効** を選択します。
3. **ユーザー定義の制限値** セクションに、ワット、BTU/ 時、または推奨システム制限値の最大 % で電力最大制限値を入力します。
4. **適用** をクリックして値を適用します。

RACADM を使用した電力制限ポリシーの設定

現在の電力制限値を表示および設定するには、次の手順を実行します。

- 次のオブジェクトを **config** サブコマンドと共に使用します。
  - cfgServerPowerCapWatts
  - cfgServerPowerCapBTUhr
  - cfgServerPowerCapPercent
  - cfgServerPowerCapEnable
- 次のオブジェクトを **set** サブコマンドと共に使用します。
  - System.Power.Cap.Enable
  - System.Power.Cap.Watts
  - System.Power.Cap.Btuhr

– System.Power.Cap.Percent

詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

iDRAC 設定ユーティリティを使用した電力制限ポリシーの設定

電力ポリシーを表示し、設定するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**電源設定** に移動します。
   iDRAC 設定の電源設定 ページが表示されます。
2. **iDRAC 電力制限ポリシー** を有効にするには、**有効** を選択します。それ以外の場合は、**無効** を選択します。
3. 推奨されている設定を使用するか、**ユーザー定義の制限値** で必要な制限値を入力します。
   オプションの詳細については、『*iDRAC 設定ユーティリティオンラインヘルプ*』を参照してください。
4. **戻る**、**終了** の順にクリックし、**はい** をクリックします。
   電力制限値が設定されます。

電源装置オプションの設定

冗長性ポリシー、ホットスペア、およびパワーファクタ補正などの電源装置オプションを設定できます。

ホットスペアは、冗長電源装置（PSU）を設定して、サーバーの負荷に応じて電源をオフする PSU の機能です。これにより、残りの PSU はより高い負荷および効率で動作できます。これには、この機能をサポートする PSU が必要で、必要なときに迅速に電源オンできます。

2 台の PSU システムでは、プライマリ PSU（オンである必要あり）を設定する必要があります。4 台の PSU システムでは、オンである必要のある PSU のペア（1+1 または 2+2）を設定する必要があります。

ホットスペアが有効になると、負荷に基づいて PSU をアクティブ化、またはスリープモードにすることができます。

パワーファクタは、実際の電力消費量と見掛け上の電力の比です。パワーファクタ補正が無効になっている場合、サーバーの電源をオフにすると、電力消費量は減少します。デフォルトで、システムを電源オンにするとき、パワーファクタ補正が有効です。

ウェブインタフェースを使用した電源装置オプションの設定

電源装置オプションを設定するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → 電源 / 熱 → 電源設定 → 電源設定** と移動します。
   電源設定 ページが表示されます。
2. **電源装置オプション** で、必要なオプションを選択します。詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。
3. **適用** をクリックします。電源装置オプションが設定されます。

RACADM を使用した電源装置オプションの設定

電源装置オプションを設定するには、次のオブジェクトと共に **set** サブコマンドを使用します。

- System.Power.RedundancyPolicy
- System.Power.Hotspare.Enable
- System.Power.Hotspare.PrimaryPSU
- System.Power.PFC.Enable

詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

iDRAC 設定ユーティリティを使用した電源装置オプションの設定

電源装置オプションを設定するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**電源設定** に進みます。
   iDRAC 設定の電源設定 ページが表示されます。
2. 電源装置オプション で次の操作を行います。
   - 電源装置の冗長性を有効化または無効化する。
   - ホットスペアを有効化または無効化する。
   - プライマリ電源装置を設定する。
   - パワーファクタ補正を有効化または無効化する。オプションの詳細については、『*iDRAC 設定ユーティリティオンラインヘルプ*』を参照してください。
3. **戻る**、**終了** の順にクリックし、**はい** をクリックします。
   電源装置オプションが設定されます。

電源ボタンの有効化または無効化

管理下システムの電源ボタンを有効化または無効化するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**セキュリティ設定** に移動します。
   iDRAC 設定のセキュリティ設定 ページが表示されます。
2. 電源ボタンを有効にするには、**有効** を選択します。それ以外の場合は、**無効** を選択します。
3. **戻る**、**終了** の順にクリックし、**はい** をクリックします。設定が保存されます。

12

仮想コンソールの設定と使用

リモートシステムの管理には、仮想コンソールを使用でき、管理ステーションのキーボード、ビデオ、マウスを使用して、管理下システムの対応するデバイスを制御します。これは、ラックおよびタワーサーバーでは、ライセンスが必要な機能です。ブレードサーバーでは、デフォルトで使用できます。

主な機能は次のとおりです。

- 最大 4 つの仮想コンソールセッションが同時にサポートされます。すべてのセッションに対して、同じ管理下サーバーコンソールが同時に表示されます。
- 仮想コンソールは、Java または ActiveX プラグインを使用して、サポートされるウェブブラウザで起動できます。管理ステーションが Windows 以外のオペレーティングシステムで実行されている場合は、Java ビューアを使用する必要があります。
- 仮想コンソール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。
- 単一の管理ステーションから、1 つ、または複数の管理下システムに対する複数の仮想コンソールセッションを同時に開くことができます。
- 同じプラグインを使用して、管理ステーションから管理下サーバーに対する 2 つのコンソールセッションを開くことはできません。
- 2 人目のユーザーが仮想コンソールセッションを要求すると、最初のユーザーが通知を受け、アクセスを拒否する、読み取り専用アクセスを許可する、または完全な共有アクセスを許可するオプションが提供されます。2 人目のユーザーには、別のユーザーが制御権を持っていると通知されます。最初のユーザーは 30 秒以内に応答する必要があり、応答しないと、デフォルト設定に基づいて 2 人目のユーザーにアクセスが付与されます。2 つのセッションが同時にアクティブな場合、最初のユーザーには、2 人目のセッションがアクティブであることを示すメッセージが画面の右上隅に表示されます。最初のユーザーまたは 2 人目のユーザーのどちらも管理者権限を持っていない場合、最初のユーザーのセッションを終了すると、2 人目のセッションも自動的に終了されます。

関連リンク

仮想コンソールを使用するためのウェブブラウザの設定
仮想コンソールの設定
仮想コンソールの起動

対応画面解像度とリフレッシュレート

次の表に、管理下サーバーで実行されている仮想コンソールセッションに対してサポートされている画面解像度と対応するリフレッシュレートを示します。

表 22. 対応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

モニターの画面解像度は 1280x1024 ピクセル以上に設定することをお勧めします。

メモ: アクティブな仮想コンソールセッションが存在し、低解像度のモニタが仮想コンソールに接続されている場合、ローカルコンソールでサーバーが選択されると、サーバーコンソールの解像度がリセットされる場合があります。システムが Linux オペレーティングシステムを実行している場合、ローカルモニターで X11 コンソールを表示できないことがあります。iDRAC7 仮想コンソールで <Ctrl><Alt><F1> を押して、Linux をテキストコンソールに切り換えます。

仮想コンソールを使用するためのウェブブラウザの設定

管理ステーションで仮想コンソールを使用するには、次の手順を実行します。

1. サポートされているバージョンの Internet Explorer（Windows）または Mozilla Firefox（Windows または Linux）がインストールされていることを確認します。

   Windows および Linux オペレーティングシステムでサポートされているブラウザのバージョンの詳細に関しては、readme を参照してください。
2. ActiveX または Java プラグインを使用するようにウェブブラウザを設定します。

   ActiveX ビューアは、Internet Explorer だけでサポートされています。Java ビューアは、すべてのブラウザでサポートされています。
3. 仮想コンソールおよび仮想メディアが Java プラグインを使用するように設定されている場合、Internet Explorer で *セキュリティ強化モード* を無効にします。無効にできない場合は、iDRAC7 で仮想コンソールが ActiveX プラグインを使用するように設定します。IE で ActiveX コントロールを有効にし、iDRAC7 のウェブ URL をイントラネットのセキュリティゾーンに追加、その後このゾーンのセキュリティレベルを *中低* に設定して、仮想コンソールおよび仮想メディアが適切に機能するようにします。

メモ: Windows Server オペレーティングシステムの場合、**コントロールパネル → 管理ツールサーバーマネージャ → Internet Explorer セキュリティ強化の構成** ウィンドウで IE セキュリティ強化の構成にアクセスできます。このウィンドウでは、必要な権限も設定できます。

4. 管理下システムでルート証明書をインポートして、証明書の検証を求めるポップアップが表示されないようにします。
5. **compat-libstdc++-33-3.2.3-61** 関連パッケージをインストールします。

メモ: Windows では、「compat-libstdc++-33-3.2.3-61」関連パッケージが .NET フレームワークパッケージまたはオペレーティングシステムパッケージに含まれている場合があります。

関連リンク

Java プラグインを使用するためのウェブブラウザの設定
ActiveX プラグインを使用するための IE の設定
管理ステーションへの CA 証明書のインポート

Java プラグインを使用するためのウェブブラウザの設定

Firefox または IE を使用しており、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。

メモ: 64 ビットのオペーティングシステムでは 32 ビットまたは 64 ビットの JRE バージョン、32 ビットのオペーティングシステムでは 32 ビットの JRE バージョンをインストールします。

Java プラグインを使用するために IE を設定するには、次の手順を実行します。

- Internet Explorer でファイルダウンロード時の自動プロンプトを無効化します。
- Internet Explorer で *セキュリティ強化モード* を無効化します。

関連リンク

仮想コンソールの設定

ActiveX プラグインを使用するための IE の設定

ActiveX プラグインは、Internet Explorer 以外では使用できません。

ActiveX プラグインを使用するために IE を設定するには、次の手順を実行します。

1. ブラウザのキャッシュをクリアします。
2. iDRAC7 IP またはホスト名を **信頼済みサイト** リストに追加します。
3. カスタム設定を **中低** にリセットするか、設定を変更して署名済みの ActiveX プラグインのインストールを許可します。
4. ブラウザが暗号化されたコンテンツをダウンロードし、サードパーティ製のブラウザ拡張を有効にできるようにします。この操作を実行するには、**ツール → インターネットオプション → 詳細設定** と移動し、**暗号化されたページをディスクに保存しない** オプションをクリアして、**サードパーティブラウザ拡張を有効化** オプションを選択します。

メモ: サードパーティのブラウザ拡張を有効にする設定を反映させるために、Internet Explorer を再起動します。

5. **ツール → インターネットオプション → セキュリティ** と進み、アプリケーションを実行するゾーンを選択します。
6. **カスタムレベル** をクリックします。**セキュリティ設定** ウィンドウで、次の手順を実行します。
   - **ActiveX コントロールに対して自動的にダイアログを表示** に対して **有効** を選択します。
   - **署名済み ActiveX コントロールのダウンロード** に対して **プロンプト** を選択します。
   - **ActiveX コントロールとプラグインの実行** に対して **有効** または **プロンプト** を選択します。
   - **スクリプトを実行しても安全だとマークされた ActiveX コントロールのスクリプトの実行** に対して **有効** または **プロンプト** を選択します。
7. **OK** をクリックして、**セキュリティ設定** ウィンドウを閉じます。
8. **OK** をクリックして、**インターネットオプション** ウィンドウを閉じます。

メモ: ActiveX コントロールをインストールする前に、Internet Explorer がセキュリティ警告を表示する場合があります。ActiveX コントロールのインストール手順を完了するには、Internet Explorer でセキュリティ警告が表示されたときに ActiveX コントロールのインストールに同意します。

関連リンク

ブラウザキャッシュのクリア

Windows Vista 以降の Microsoft オペレーティングシステム用の追加設定

Windows Vista 以降の Microsoft オペレーティングシステム用の追加設定

Windows Vista 以降のオペレーティングシステムの Internet Explorer ブラウザには、*保護モード*と呼ばれる追加のセキュリティ機能があります。

*保護モード*付きの Internet Explorer ブラウザで ActiveX アプリケーションを起動して実行するには、次の手順を実行します。

1. IE を管理者として実行します。
2. **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** の順に選択します。
3. 信頼済みサイトゾーンに対して **保護モードを有効にする** オプションが選択されていないことを確認してください。または、イントラネットゾーンのサイトに iDRAC7 アドレスを追加することもできます。イントラネットゾーンと信頼済みサイトゾーンのサイトについては、保護モードはデフォルトでオフになっています。
4. **サイト** をクリックします。
5. **この Web サイトをゾーンに追加する** フィールドに iDRAC7 のアドレスを追加し、**追加** をクリックします。

6. **閉じる** をクリックして、**OK** をクリックします。
7. 設定を有効にするために、ブラウザを閉じてから再起動します。

ブラウザキャッシュのクリア

仮想コンソールの操作中に問題（範囲外エラーや同期問題など）が発生した場合は、ブラウザのキャッシュをクリアして、システムに格納されている可能性のある古いバージョンのビューアを削除してから再試行してください。

メモ: ブラウザのキャッシュをクリアするには、管理者権限が必要です。

IE7 での以前の ActiveX バージョンのクリア

IE7 の以前のバージョンの Active-X ビューアをクリアするには、次の手順を実行します。

1. Video Viewer と Internet Explorer ブラウザを閉じます。
2. Internet Explorer ブラウザを再度開き、**Internet Explorer → ツール → アドオンの管理** と移動して、**アドオンの有効化または無効化** をクリックします。**アドオンの管理** ウィンドウが表示されます。
3. **表示** ドロップダウンメニューから **Internet Explorer で使用されたアドオン** を選択します。
4. *Video Viewer* アドオンを削除します。

IE8 での以前の ActiveX バージョンのクリア

IE8 の以前のバージョンの Active-X ビューアをクリアするには、次の手順を実行します。

1. Video Viewer と Internet Explorer ブラウザを閉じます。
2. Internet Explorer ブラウザを再度開き、**Internet Explorer → ツール → アドオンの管理** と移動して、**アドオンの有効化または無効化** をクリックします。**アドオンの管理** ウィンドウが表示されます。
3. **表示** ドロップダウンメニューから **すべてのアドオン** を選択します。
4. *Video Viewer* アドオンを選択し、**詳細情報** リンクをクリックします。
5. **詳細情報** ウィンドウから **削除** を選択します。
6. **詳細情報** と **アドオンの管理** ウィンドウを閉じます。

古い Java バージョンのクリア

Windows または Linux で古いバージョンの Java ビューアをクリアするには、次の手順に従います。

1. コマンドプロンプトで、`javaws-viewer` または `javaws-uninstalll` を実行します。
   Java キャッシュ ビューアが表示されます。
2. *iDRAC7 仮想コンソールクライアント*という項目を削除します。

管理ステーションへの CA 証明書のインポート

仮想コンソールまたは仮想メディアの起動時には、証明書の検証を求めるプロンプトが表示されます。カスタムウェブサーバー証明書がある場合は、Java または ActiveX の信頼できる証明書ストアに CA 証書をインポートすることによって、これらのプロンプトが表示されないようにすることができます。

関連リンク

Java の信頼できる証明書ストアへの CA 証明書のインポート
ActiveX の信頼できる証明書ストアへの CA 証明書のインポート

Java の信頼できる証明書ストアへの CA 証明書のインポート

Java の信頼できる証明書ストアに CA 証明書をインポートするには、次の手順を実行します。

1. **Java コントロールパネル** を起動します。
2. **セキュリティ** タブをクリックしてから、**証明書** をクリックします。
   証明書 ダイアログボックスが表示されます。
3. 証明書タイプのドロップダウンメニューで、**信頼できる証明書** を選択します。
4. **インポート** をクリックして参照し、CA 証明書（Base64 エンコード形式）を選択してから **開く** をクリックします。
   選択した証明書が、Java Web Start の信頼できる証明書ストアにインポートされます。
5. **閉じる**をクリックしてから **OK** をクリックします。**Java コントロールパネル** ウィンドウが閉じます。

ActiveX の信頼できる証明書ストアへの CA 証明書のインポート

Secure Hash Algorithm（SHA）を使用した証明書のハッシュを作成するには、OpenSSL コマンドラインツールを使用する必要があります。OpenSSL ツール 1.0.x 以降は デフォルトで SHA を使用することから、OpenSSL ツール 1.0.x 以降の使用が推奨されます。CA 証明書は、Base64 エンコード PEM フォーマットである必要があります。それぞれの CA 証明書をインポートするのは 1 回のみのプロセスです。

CA 証明書を ActiveX の信頼できる証明書ストアへインポートするには、次の手順を実行します。

1. OpenSSL コマンドプロンプトを開きます。
2. コマンド `openssl x509 -in （CA 証明書の名前） -noout -hash` を使用して、管理ステーションで現在使用中の CA 証明書で 8 バイトのハッシュを実行します。
   出力ファイルが生成されます。たとえば、CA 証明書ファイルの名前が **cacert.pem** である場合は、コマンドは次のようになります。
   ```
   openssl x509 -in cacert.pem -noout -hash
   ```
   「431db322」に類似した出力が生成されます。
3. CA ファイルの名前を出力ファイル名に変更し、「.0」という拡張子を付加します。例：431db322.0
4. 名前を変更した CA 証明書をホームディレクトリにコピーします。例：**C:\Documents and Settings\<ユーザー> directory**

仮想コンソールの設定

仮想コンソールを設定する前に、管理ステーションが設定されていることを確認します。

仮想コンソールは、iDRAC7 ウェブインタフェースまたは RACADM コマンドラインインタフェースを使用して設定できます。

関連リンク

仮想コンソールを使用するためのウェブブラウザの設定
仮想コンソールの起動

ウェブインタフェースを使用した仮想コンソールの設定

iDRAC7 ウェブインタフェースを使用して仮想コンソールを設定するには、次の手順を実行します。

1. **概要 → サーバー → コンソール** と移動します。**仮想コンソール** ページが表示されます。
2. 仮想コンソールを有効にし、必要な値を指定します。オプションについては、『*iDRAC7 オンラインヘルプ*』を参照してください。
3. **適用** をクリックします。仮想コンソールが設定されます。

RACADM を使用した仮想コンソールの設定

仮想コンソールを設定するには、次のオブジェクトを使用します。

- cfgRACTuneConRedirEnable
- cfgRACTuneConRedirPort
- cfgRACTuneConRedirEncryptEnable
- cfgRacTunePluginType
- cfgRacTuneVirtualConsoleAuthorizeMultipleSessions

これらのオブジェクトの詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

仮想コンソールのプレビュー

仮想コンソールを起動する前に、**システム → プロパティ → システムサマリ** ページで仮想コンソールの状態をプレビューできます。**仮想コンソールプレビュー** セクションに、仮想コンソールの状態を示すイメージが表示されます。イメージは 30 秒ごとに更新されます。これはライセンスが必要な機能です。

メモ: 仮想コンソールイメージは、仮想コンソールを有効にしている場合にのみ表示できます。

仮想コンソールの起動

仮想コンソールは、iDRAC7 ウェブインタフェースまたは URL を使用して起動できます。

メモ: 管理下システムのウェブブラウザから仮想コンソールセッションを起動しないでください。

仮想コンソールを起動する前に、次のことを確認します。

- 管理者権限がある。
- ウェブブラウザが Java または ActiveX プラグインを使用するよう設定されている。
- 最低限のネットワーク帯域幅（1 MB/ 秒）が利用可能。

32 ビット版または 64 ビット版 IE ブラウザを使用して仮想コンソールを起動する場合は、各ブラウザで必要なプラグイン（Java または ActiveX）が利用可能になります。インターネットオプション設定は両方のブラウザで共通です。

Java プラグインを使用して仮想コンソールを起動すると、Java コンパイルエラーが発生することがあります。この問題を解決するには、**Java コントロールパネル → 一般 → ネットワーク設定** に移動し、**直接接続** を選択します。

仮想コンソールが ActiveX プラグインを使用するよう設定された場合は、当初仮想コンソールが起動しないことがあります。これは、低速のネットワーク接続が原因であり、一時資格情報（仮想コンソールが接続するために使用するもの）のタイムアウトは 2 分間です。ActiveX クライアントプラグインのダウンロード時間はこの時間を超えることがあります。プラグインが正常にダウンロードされたあとで、仮想コンソールを通常どおりに起動できます。

ActiveX プラグインがインストールされた IE8 を使用して仮想コンソールを初めて起動する場合、「証明書エラー：ナビゲーションはブロックされました」というメッセージが表示されることがあります。**セキュリティ警告** ウィンドウで、**このサイトの閲覧を続行する** をクリックし、**インストール** をクリックして ActiveX コントロールをインストールします。仮想コンソールセッションが起動されます。

関連リンク

URL を使用した仮想コンソールの起動
Java プラグインを使用するためのウェブブラウザの設定
ActiveX プラグインを使用するための IE の設定
ウェブインタフェースを使用した仮想コンソールの起動
マウスポインタの同期

ウェブインタフェースを使用した仮想コンソールの起動

仮想コンソールは、次の方法で起動できます。

- **概要 → サーバー → コンソール** と移動します。**仮想コンソール** ページが表示されます。**仮想コンソールの起動** をクリックします。**仮想コンソールビューア** が起動します。
- **概要 → サーバー → プロパティ** と移動します。**システムサマリ** ページが表示されます。**仮想コンソールプレビュー** セクションで **起動** をクリックします。**仮想コンソールビューア** が起動します。

仮想コンソールビューア には、リモートシステムのデスクトップが表示されます。このビューアを使用して、お使いの管理ステーションからリモートシステムのマウスおよびキーボード機能を制御できます。

このアプリケーションの起動後に、複数のメッセージボックスが表示される場合があります。不正ユーザーがこのアプリケーションにアクセスしないようにするため、3 分以内にこのメッセージボックスを処理してください。処理しない場合、アプリケーションの再起動を求めるプロンプトが表示されます。

ビューアの起動中に 1 つ、または複数のセキュリティアラートウィンドウが表示される場合には、はいをクリックして続行します。

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。1 つは管理下サーバーのマウスポインタで、もう 1 つは自身の管理ステーションのマウスポインタです。カーソルが同期しない場合は、仮想コンソールビューアの **ツール** で **シングルカーソル** を選択します。

Windows Vista 管理ステーションから仮想コンソールを起動すると、仮想コンソールの再起動を求めるメッセージが表示される場合があります。このメッセージが表示されないようにするには、次の場所に適切なタイムアウト値を設定します。

- **コントロールパネル → 電源オプション → 省電力 → 詳細設定 → ハードディスク → 次の時間が経過後ハードディスクの電源を切る <タイムアウト時間>**
- **コントロールパネル → 電源オプション → 高パフォーマンス → 詳細設定 → ハードディスク → 次の時間が経過後ハードディスクの電源を切る <タイムアウト時間>**

URL を使用した仮想コンソールの起動

URL を使用して仮想コンソールを起動するには、次の手順を実行します。

1. サポートされるウェブブラウザを開き、アドレスボックスに URL **https://iDRAC7_ip/console** を小文字で入力します。
2. ログイン設定に基づいて、対応する **ログイン** ページが表示されます。
   - シングルサインオンが無効になっていて、ローカル、Active Directory、LDAP、またはスマートカードログインが有効になっている場合は、対応する **ログイン** ページが表示されます。
   - シングルサインオンが有効になっている場合は、**仮想コンソールビューア**が起動し、**仮想コンソール** ページがバックグラウンドに表示されます。

メモ: Internet Explorer は、ローカル、Active Directory、LDAP、スマートカード（SC）、およびシングルサインオン（SSO）ログインをサポートします。Firefox は、Windows ベースのオペレーティングシステムではローカル、Active Directory、および SSO ログインをサポートし、Linux ベースのオペレーティングシステムではローカル、Active Directory、および LDAP ログインをサポートします。

メモ: 仮想コンソールへのアクセス権限はないが仮想メディアへのアクセス権限があるという場合は、この URL を使用すると仮想コンソールの代わりに仮想メディアが起動します。

仮想コンソールビューアの使用

仮想コンソールビューアでは、マウスの同期、チャットオプション、キーボードマクロ、電源処置、仮想メディアへのアクセスなど、さまざまな制御が可能です。詳細は、『*iDRAC7 オンラインヘルプ*』を参照してください。

メモ: リモートサーバーの電源がオフになっている場合は、「信号なし」のメッセージが表示されます。

仮想コンソールビューアのタイトルバーには、管理ステーションから接続する先の iDRAC7 の DNS 名または IP アドレスが表示されます。iDRAC7 に DNS 名がない場合は、IP アドレスが表示されます。フォーマットは次のとおりです。

- ラックおよびタワーサーバーの場合：
  `<DNS 名 / IPv6 アドレス / IPv4 アドレス>, <モデル>, User: <ユーザー名>, <fps>`
- ブレードサーバーの場合：
  `<DNS 名 / IPv6 アドレス / IPv4 アドレス>, <モデル>, <スロット番号>、User: <ユーザー名>, <fps>`

場合によっては、仮想コンソールビューアに表示されるビデオの品質が低くなることがあります。これは、仮想コンソールセッションの開始時に 1 ～ 2 個のビデオフレームが失われる結果となるネットワーク接続が遅さが原因です。すべてのビデオフレームを伝送して今後のビデオ品質を改善するには、次のいずれかを実行します。

- **システムサマリ** ページの **仮想コンソールプレビュー** セクションで、**更新** をクリックします。
- **仮想コンソールビューア** の **パフォーマンス** タブで、スライダを **最高ビデオ品質** に設定します。

マウスポインタの同期

仮想コンソールを介して管理下システムに接続すると、管理下ステムのマウスの加速度が管理ステーションのマウスポインタと同期されず、ビューアのウィンドウに 2 つのマウスポインタが表示される場合があります。

Red Hat Enterprise Linux または Novell SUSE Linux を使用している場合には、仮想コンソールビューアを起動する前に Linux のマウスモードを設定します。オペレーティングシステムのデフォルトマウス設定が仮想コンソールビューアにおけるマウス矢印の制御に使用されます。

2 つのマウスカーソルがクライアントの仮想コンソールビューアに表示される場合、サーバーのオペレーティングシステムが相対位置をサポートしていることを示します。これは、Linux オペレーティングシステムまたは Lifecycle Controller によくある問題で、サーバーのマウス加速設定が仮想コンソールクライアントのマウス加速設定と異なる場合に、マウスが 2 つになります。この問題を解決するには、（仮想コンソールビューアの）**ツール** メニューで **シングルカーソル** を選択するか、管理下システムのマウス加速度を管理ステーションに一致させます。シングルカーソルモードを終了するには、<F9> を押します。

メモ: Windows オペレーティングシステムを実行している管理下システムは絶対位置をサポートしているため、これは適用されません。

仮想コンソールを使用して最新の Linux ディストリビューションのオペレーティングシステムをインストールした管理下システムに接続する場合、マウスの同期化の問題が発生することがあります。これは、GNOME デスクトップの予測可能ポインタ加速機能が原因である可能性があります。iDRAC7 仮想コンソールでの正しいマウス同期化には、この機能を無効にする必要があります。予測可能ポインタ加速機能を無効にするには、**/etc/X11/xorg.conf** ファイルのマウスセクションに次を追加します。

```
Option "AccelerationScheme" "lightweight".
```

同期の問題が解決されない場合は、**<ユーザーのホーム>/.gconf/desktop/gnome/peripherals/mouse/%gconf.xml** ファイルで、さらに次の変更を行います。

motion_threshold および motion_acceleration の値を -1 に変更します。

GNOME デスクトップでマウス加速をオフにした場合、**ツール → セッションオプション → マウス** と移動します。**マウスアクセラレーション** タブで **なし** を選択します。

管理下サーバーコンソールへの排他的アクセスについては、ローカルコンソールを無効にし、**仮想コンソール** ページで **最大セッション数** を 1 に設定する必要があります。

仮想コンソールを介してすべてのキーストロークを渡す

すべてのキーストロークをサーバーに渡すオプションを有効にし、仮想コンソールビューアを介して管理ステーションから管理下システムにすべてのキーストロークとキーの組み合わせを送信することができます。無効になっている場合は、仮想コンソールセッションが実行されている管理ステーションに、すべてのキーの組み合わせが送信されます。

すべてのキーストロークをサーバーに渡す機能の動作は、次の条件に応じて異なります。

- 起動される仮想コンソールセッションに基づくプラグインタイプ（Java または ActiveX）。
- 管理ステーションおよび管理下システムで実行されているオペレーティングシステム。管理ステーションのオペレーティングシステムにとって意味のあるキーの組み合わせは、管理下システムに渡されません。
- 仮想コンソールビューアモード — ウィンドウ表示または全画面表示。

  全画面モードでは、すべてのキーストロークをサーバーに渡す機能がデフォルトで有効になっています。

  ウィンドウモードでは、仮想コンソールビューアが表示されてアクティブになっている場合にのみ、キーが渡されます。

  全画面モードからウィンドウモードに変更すると、すべてのキーを渡す機能の以前の状態が再開されます。

関連リンク

Windows オペレーティングシステム上で動作する Java ベースの仮想コンソールセッション
Linux オペレーティングシステム上で動作する Java ベースの仮想コンソールセッション
Windows オペレーティングシステム上で動作する ActiveX ベースの仮想コンソールセッション

Windows オペレーティングシステム上で動作する Java ベースの仮想コンソールセッション

- Ctrl+Alt+Del キーは、管理対象システムに送信されませんが、常に管理ステーションによって解釈されます。
- すべてのキーストロークをサーバーに渡す機能が有効な場合、次のキーは管理下システムに送信されません。
  - ブラウザの戻るキー
  - ブラウザの進むキー
  - ブラウザの更新キー
  - ブラウザの停止キー
  - ブラウザの検索キー
  - ブラウザのお気に入りキー
  - ブラウザの開始およびホームキー
  - 音量をミュートするキー
  - 音量を下げるキー
  - 音量を上げるキー
  - 次のトラックキー
  - 前のトラックキー
  - メディアの停止キー

- メディアの再生 / 一時停止キー
- メールの起動キー
- メディアの選択キー
- アプリケーション 1 の起動キー
- アプリケーション 2 の起動キー

- 個々のキー（異なるキーの組み合わせではなく、単一のキーストローク）はすべて、常に管理下システムに送信されます。これには、すべてのファンクションキー、Shift、Alt、Ctrl、および Menu キーが含まれます。これらの一部のキーは、管理ステーションと管理下システムの両方に影響を与えます。たとえば、管理ステーションと管理対象システムで Windows オペレーティングシステムが実行され、すべてのキーを渡す機能が無効な場合は、**スタート** メニューを開くために Windows キーを押すと、管理ステーションと管理下システムの両方で **スタート** メニューが開きます。ただし、すべてのキーを渡す機能が有効な場合、**スタート** メニューは管理対象システムでのみ開き、管理ステーションでは開きません。
- すべてのキーを渡す機能が無効な場合、動作は押されたキーの組み合わせと、管理ステーション上のオペレーティングシステムによって解釈された特別な組み合わせによって異なります。

Linux オペレーティングシステム上で動作する Java ベースの仮想コンソールセッション

Windows オペレーティングシステムについて記載されている動作は、次の例外を除き、Linux オペレーティングシステムにも適用されます。

- すべてのキーストロークをサーバーに渡す機能を有効にすると、<Ctrl+Alt+Del> が管理下システムのオペレーティングシステムに渡されます。
- マジック SysRq キーは、Linux カーネルによって認識されるキーの組み合わせです。管理ステーションまたは管理下システムのオペレーティングシステムがフリーズし、システムを回復する必要がある場合に便利です。次のいずれかの方法を使用して、Linux オペレーティングシステムのマジック SysRq キーを有効にできます。

  - **/etc/sysctl.conf** にエントリを追加する
  - echo "1" > /proc/sys/kernel/sysrq
- すべてのキーストロークをサーバーに渡す機能を有効にすると、マジック SysRq キーが管理下システムのオペレーティングシステムに送信されます。オペレーティングシステムをリセット（つまり、アンマウントまたは同期なしで再起動）するキーシーケンスの動作は、管理ステーションでマジック SysRq が有効になっているか無効になっているかによって異なります。

  - 管理ステーションで SysRq が有効になっている場合は、システムの状態に関わらず、<Ctrl+Alt+SysRq+b> または <Alt+SysRq+b> によって管理ステーションがリセットされます。
  - 管理ステーションで SysRq が無効になっている場合は、<Ctrl+Alt+SysRq+b> または <Alt+SysRq+b> キーによって管理下システムのオペレーティングシステムがリセットされます。
  - その他の SysRq キーの組み合わせ（<Alt+SysRq+k>、<Ctrl+Alt+SysRq+m> など）は、管理ステーションで SysRq キーが有効になっているかどうかに関わらず、管理下システムに渡されます。

Windows オペレーティングシステム上で動作する ActiveX ベースの仮想コンソールセッション

Windows オペレーティングシステムで動作する ActiveX ベースの仮想コンソールセッションの すべてのキーストロークをサーバーに渡す機能の動作は、Windows 管理ステーションで実行されている Java ベースの仮想コンソールセッションで説明された動作に似ていますが、次の例外があります。

- すべてのキーを渡すが無効な場合、F1 を押すと、管理ステーションと管理下システムの両方でアプリケーションのヘルプが起動し、次のメッセージが表示されます。
  仮想コンソールページのヘルプをクリックして、オンラインヘルプを表示します
- メディアキーを明示的にブロックすることはできません。
- <Alt + Space>、<Ctrl + Alt + +>、<Ctrl + Alt + -> は管理下システムに送信されず、管理ステーション上のオペレーティングシステムによって解釈されます。

13

仮想メディアの管理

仮想メディアを使用すると、管理対象サーバーは管理ステーション上のメディアデバイスや、ネットワーク共有上の ISO CD/DVD イメージに、それらが管理対象サーバーにあるかのようにアクセスできます。

仮想メディア機能を使用すると、次の操作を実行できます。

- リモートシステムに接続されたメディアにネットワークを介してリモートアクセス
- アプリケーションのインストール
- ドライバの更新
- 管理下システムへのオペレーティングシステムのインストール

これは、ラックおよびタワーサーバーでは、ライセンスが必要な機能です。ブレードサーバーでは、デフォルトで使用できます。

主な機能は次のとおりです。

- 仮想メディアは、仮想オプティカルドライブ（CD/DVD）、フロッピードライブ（USB ベースのドライブを含む）、および USB フラッシュドライブをサポートします。
- 管理下システムには、管理ステーション上のフロッピー、USB フラッシュドライブ、またはキーのいずれかと 1 つのオプティカルドライブを接続できます。サポートされるフロッピードライブには、フロッピーイメージまたは 1 つの利用可能なフロッピードライブが含まれます。サポートされるオプティカルドライブには、最大 1 つの利用可能なオプティカルドライブまたは 1 つの ISO イメージファイルが含まれます。

  次の図は、一般的な仮想メディアのセットアップを示しています。
- 仮想マシンから iDRAC7 の仮想フロッピーメディアにアクセスすることはできません。
- 接続された仮想メディアは、管理下システム上の物理デバイスをエミュレートします。
- Windows ベースの管理下システムでは、仮想メディアドライブは接続され、ドライブ文字が設定された場合に自動マウントされます。
- いくつかの設定がある Linux ベースの管理下システムでは、仮想メディアドライブは自動マウントされません。仮想メディアドライブを手動でマウントするには、mount コマンドを使用します。
- 管理下システムからのすべての仮想ドライブアクセス要求は、ネットワークを介して管理ステーションに送信されます。
- 仮想デバイスは、管理下システムで 2 つのドライブとして表示されます（ドライブにはメディアが取り付けられません）。
- 2 つの管理下システム間で管理ステーションの CD/DVD ドライブ（読み取り専用）を共有できますが、USB メディアを共有することはできません。
- 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。
- LOM または NIC フェイルオーバーが発生した場合は、仮想メディアセッションを切断できません。

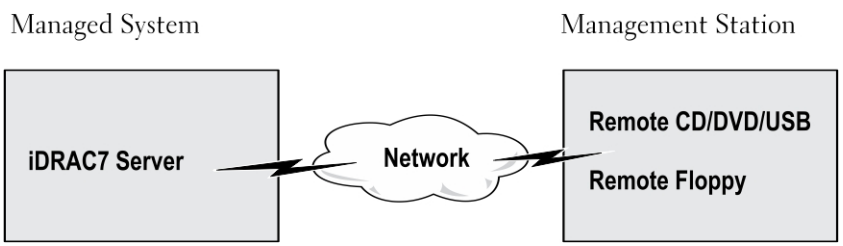

図 4. 仮想メディアのセットアップ

サポートされているドライブとデバイス

次の表では、仮想メディアでサポートされているドライブをリストします。

表 23. サポートされているドライブとデバイス

ドライブ	サポートされているストレージメディア
仮想光学ドライブ	• レガシー 1.44 フロッピードライブ（1.44 フロッピーディスケット） • CD-ROM • DVD • CD-RW • コンビネーションドライブ（CD-ROM メディア）
仮想フロッピードライブ	• ISO9660 フォーマットの CD-ROM/DVD イメージファイル • ISO9660 フォーマットのフロッピーイメージファイル
USB フラッシュドライブ	• CD-ROM メディアのある USB CD-ROM ドライブ • ISO9660 フォーマットの USB キーイメージ

仮想メディアの設定

仮想メディアを設定する前に、ウェブブラウザが Java または ActiveX プラグインを使用するように設定されていることを確認してください。

関連リンク

仮想コンソールを使用するためのウェブブラウザの設定

iDRAC7 ウェブインタフェースを使用した仮想メディアの設定

仮想メディアを設定するには、次の手順を実行します。

注意: 仮想メディアセッションの実行中には、iDRAC7 をリセットしないでください。リセットした場合、データ損失など望ましくない結果が生じることがあります。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → 連結されたメディア** と移動します。
2. 必要な設定を指定します。詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。
3. **適用** をクリックして設定を保存します。

RACADM を使用した仮想メディアの設定

仮想メディアを設定するには、**cfgRacVirtual** グループのオブジェクトを使用します。詳細に関しては、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

iDRAC 設定ユーティリティを使用した仮想メディアの設定

iDRAC 設定ユーティリティを使用すると、仮想メディアの連結、連結解除、自動連結を行うことがきます。この手順は次のとおりです。

1. iDRAC 設定ユーティリティで、**仮想メディア** に移動します。
   iDRAC 設定の仮想メディア ページが表示されます。
2. 要件に基づいて、**連結解除**、**連結**、または **自動連結** を選択します。これらのオプションの詳細については、『*iDRAC 設定ユーティリティオンラインヘルプ*』を参照してください。
3. **戻る**、**終了** の順にクリックし、**はい** をクリックします。
   アラートが設定されます。

連結されたメディアの状態とシステムの応答

次の表は、連結されたメディアの設定に基づいたシステム応答について説明しています。

表 24. 連結されたメディアの状態とシステムの応答

連結されたメディアの状態	システム応答
分離	イメージをシステムにマップできません。
連結	メディアは、**クライアントビュー** が閉じられている場合であってもマップされます。
自動連結	メディアは、**クライアントビュー** が開いている場合にはマップされ、**クライアントビュー** が閉じている場合にはマップ解除されます。

仮想メディアへのアクセス

仮想メディアには、仮想コンソールを使用しても使用しなくてもアクセスできます。仮想メディアにアクセスする前に、ウェブブラウザを設定するようにしてください。

関連リンク

仮想コンソールを使用するためのウェブブラウザの設定
仮想メディアの設定

仮想コンソールを使用した仮想メディアの起動

仮想コンソールを介して仮想メディアを起動する前に、次を確認してください。

- 仮想コンソールが有効になっている。
- システムが空のドライブを表示するように設定されている。これを行うには、Windows エクスプローラで **フォルダオプション** に移動し、**空のドライブはコンピュータフォルダに表示しない** オプションのチェックを外して **OK** をクリックします。

仮想コンソールを使用して仮想メディアにアクセスするには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → コンソール** の順に選択します。
   仮想コンソール ページが表示されます。
2. **仮想コンソールの起動** をクリックします。
   仮想コンソールビューア が起動します。

メモ: Linux の場合、仮想コンソールにアクセスするためのデフォルトのプラグインタイプは Java です。Windows の場合、Java を使用して仮想コンソールにアクセスするには、**.jnlp** ファイルを開いて仮想コンソールを起動します。

3. **仮想メディア → 仮想メディアの起動** の順にクリックします。
   マッピングに使用できるデバイスのリストした仮想メディアの **クライアントビュー** ウィンドウが表示されます。

メモ: 仮想メディアにアクセスしている間は、**仮想コンソールビューア** ウィンドウがアクティブな状態である必要があります。

関連リンク

仮想コンソールを使用するためのウェブブラウザの設定
仮想メディアの設定

仮想コンソールを使用しない仮想メディアの起動

仮想コンソール が無効になっているときに仮想メディアを起動する前に、次を確認してください。

- 仮想メディアが*連結*状態である。
- システムが空のドライブを表示するように設定されている。これを行うには、Windows エクスプローラで **フォルダオプション** に移動し、**空のドライブはコンピュータフォルダに表示しない** オプションのチェックを外して **OK** をクリックします。

仮想コンソールが無効になっている場合に仮想メディアを起動するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → コンソール** の順に選択します。
   仮想コンソール ページが表示されます。
2. **仮想コンソールの起動** をクリックします。
   次のメッセージが表示されます。
   仮想コンソールが無効化されました。仮想メディアリダイレクトの使用を続行しますか?
3. **OK** をクリックして仮想メディアに連結します。
   マッピングに使用できるデバイスのリストした仮想メディアの **クライアントビュー** ウィンドウが表示されます。

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 セキュリティ強化が設定されている Windows オペレーティングシステムクライアントでは、仮想メディアが正常に機能しないことがあります。この問題を解決するには、マイクロソフトの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。

関連リンク

仮想メディアの設定

仮想メディアイメージの追加

仮想メディアイメージを追加するには、仮想メディア **クライアントビュー** ウィンドウで、次の手順を実行します。

- イメージを追加するには、**イメージの追加** をクリックして、次に管理ステーション、または管理下システムの C: ドライブからイメージファイルを選択します。
  ISO またはフロッピーイメージが使用可能なデバイスのリストに追加されます。

- ISO およびフロッピーイメージとしてフォルダを追加するには、**イメージとしてフォルダを追加** をクリックします。この機能は、リモートフォルダのメディアイメージを作成して、USB に接続されたデバイスとしてサーバーのオペレーティングシステムにマウントします。
  メディアは接続されて、情報が **クライアントビュー** ウィンドウでアップデートされます。

  フォルダがイメージとして追加されると、**.iso** ファイルがこの機能を使用する管理ステーションのデスクトップに作成されます。この **.iso** ファイルが移動または削除されると、仮想メディアの **クライアントビュー** ウィンドウにあるこのフォルダに対応するエントリは動作しません。このため、*追加されたフォルダ*の使用中に **.iso** ファイルを移動したり、削除したりすることは推奨されません。ただし、**.iso** ファイルは、最初に関連するエントリが選択解除され、エントリを削除するための **イメージの削除** を使用して削除された後で、削除できます。

仮想メディアイメージの削除

イメージを削除するには、仮想メディアの **クライアントビュー** ウィンドウで、必要なマップ済みイメージを選択し、**イメージの削除** をクリックします。
クライアントビュー ウィンドウのデバイスリストから、選択したイメージが削除されます。

仮想デバイスの詳細情報の表示

仮想デバイス詳細情報を表示するには、仮想メディアの **クライアントビュー** ウィンドウで **詳細情報** をクリックします。利用可能な仮想デバイスと各デバイスに対する読み取り / 書き込みの動作が記載された **詳細情報** セクションが表示されます。

USB のリセット

USB デバイスをリセットするには、次の手順を実行します。

1. 仮想メディアの **クライアントビュー** ウィンドウで、**詳細情報** をクリックし、**USB のリセット** をクリックします。
   USB 接続をリセットすると、仮想メディア、キーボード、マウスを含むターゲットデバイスへのすべての入力に影響を与える可能性があることを警告するメッセージが表示されます。
2. **はい** をクリックします。
   USB がリセットされます。

メモ: iDRAC7 ウェブインタフェースセッションからログアウトしても、iDRAC7 仮想メディアは終了しません。

仮想ドライブのマッピング

仮想ドライブをマップするには、次の手順を実行します。

メモ: ActiveX ベースの仮想メディアを使用する場合、オペレーティングシステム DVD または（管理ステーションに接続されている）USB フラッシュドライブをマップするための管理者権限が必要です。ドライブをマップするには、IE を管理者として起動するか、iDRAC7 の IP アドレスを信頼済みサイトのリストに追加します。

1. 別のメディアソースにマップする前に、既存のマップ済みドライブを分離します。
2. 仮想メディアの **クライアントビュー** ウィンドウで、イメージまたはイメージがあるフォルダを追加します。

3. **マップ済み** 列で、必要なイメージがあるドライブに関連するチェックボックスを選択します。書き込み可能デバイスを読み取り専用としてマップするには、マップするの前に、デバイスの **読み取り専用** オプションを選択します。
   デバイスが管理下システムにマップされます。

関連リンク

マッピング用の正しい仮想ドライブの表示
仮想メディアイメージの追加

マッピング用の正しい仮想ドライブの表示

Linux ベースの管理ステーションでは、仮想メディアの **クライアント** ウィンドウに、管理ステーションの一部ではないリムーバブルディスクやフロッピーディスクが表示されることがあります。正しい仮想ドライブをマッピングに使用できるようにするには、接続されている SATA ハードディスクドライブのポート設定を有効にする必要があります。これを行うには、次の手順を実行します。

1. 管理ステーションのオペレーティングシステムを再起動します。POST 中に、<F2> または <F12> を押してセットアップユーティリティを起動します。
2. **SATA の設定** に進みます。ポートの詳細が表示されます。
3. 実際に存在し、ハードディスクドライブに接続されているポートを有効にします。
4. 仮想メディアの **クライアント** ウィンドウにアクセスします。マップできる正しいドライブが表示されます。

関連リンク

仮想ドライブのマッピング

仮想ドライブのマッピング解除

仮想ドライブのマッピングを解除するには、次の手順を実行します。

1. 仮想メディアの **クライアントビュー** ウィンドウの **マップ済み** 列で、仮想ドライブのチェックボックスをオフにします。
   仮想ドライブが管理対象システムからマップ解除されます。
2. **仮想メディア** セッションを終了するには、**終了** をクリックします。
   仮想メディアの **クライアントビュー** ウィンドウが閉じられます。

BIOS を介した起動順序の設定

システム BIOS 設定ユーティリティを使用すると、管理下システムが仮想光学ドライブまたは仮想フロッピードライブから起動するように設定できます。

メモ: 接続中に仮想メディアを変更すると、システムの起動順序が停止する可能性があります。

管理下システムが起動できるようにするには、次の手順を実行します。

1. 管理下システムを起動します。
2. <F2> を押して、**セットアップユーティリティ** ページを開きます。
3. **システム BIOS 設定 → 起動設定 → BIOS 起動設定 → 起動順序** と移動します。
   ポップアップウィンドウに、仮想光デバイス と仮想フロッピードライブのリストがその他の標準起動デバイスと共に表示されます。
4. 仮想デバイスが有効であり、起動可能なメディアの 1 番目のデバイスとして表示されていることを確認します。必要に応じて、画面の指示に従って起動順序を変更します。
5. **OK** をクリックして **システム BIOS 設定** ページに戻り、**終了** をクリックします。

6. **はい** をクリックして変更内容を保存し、終了します。

   管理下システムが再起動します。

   管理化システムは、起動順序に基づいて起動可能なデバイスからの起動を試みます。仮想デバイスが連結されており、起動可能なメディアが存在する場合、システムは仮想デバイスから起動します。それ以外の場合、起動可能なメディアのない物理デバイスと同様に、システムは仮想デバイスを認識しません。

仮想メディアの一回限りの起動の有効化

リモート仮想メディアデバイスを連結した後の起動時に、起動順序を 1 回限り変更できます。

一回限りの起動オプションを有効にする前に、次を確認してください。

- *ユーザーの設定*権限がある。
- 仮想メディアのオプションを使用して、ローカルまたは仮想ドライブ（CD/DVD、フロッピー、または USB フラッシュデバイス）をブータブルメディアまたはイメージにマップする。
- 起動順序に仮想ドライブが表示されるように、仮想メディアが *連結*状態になっている。

一回限りの起動オプションを有効にし、仮想メディアから管理下システムを起動するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → 連結されたメディア** と移動します。
2. **仮想メディア** で **一回限りの起動の有効化** を選択し、**適用** をクリックします。
3. 管理下システムの電源を入れ、**<F2>** を押して **iDRAC 設定** を起動します。
4. リモート仮想メディアデバイスから起動するように、起動順序を変更します。
5. サーバーを再起動します。

   管理下システムが 1 回だけ仮想メディアから起動します。

関連リンク

仮想ドライブのマッピング
仮想メディアの設定

14

VMCLI ユーティリティのインストールと使用

仮想メディアコマンドラインインタフェース（VMCLI）ユーティリティは、管理ステーションから管理下システム上の iDRAC7 に仮想メディア機能を提供するインタフェースです。このユーティリティを使用すると、ネットワーク内の複数のリモートシステムでオペレーティングシステムを展開するため、イメージファイル、物理ドライブなどの仮想メディア機能にアクセスすることができます。

メモ: VMCLI ユーティリティを実行できるのは、管理ステーションのみです。

VMCLI ユーティリティは次の機能をサポートします。

- 仮想メディアを介したアクセスが可能なリムーバブルデバイスまたはイメージの管理
- iDRAC7 ファームウェアの **1 回限りの起動** オプションが有効な時のセッションの自動終了
- Secure Socket Layer（SSL）を使用した iDRAC7 へのセキュアな通信
- 次の時点までの VMCLI コマンドの実行：
  - 接続が自動的に終了。
  - オペレーティングシステムがプロセスを終了。

メモ: Windows でプロセスを終了させるには、タスクマネージャを使用します。

VMCLI のインストール

VMCLI ユーティリティは、『*Dell Systems Management Tools and Documentation*』DVD に収録されています。

VMCLI ユーティリティをインストールするには、次の手順を実行します。

1. 管理ステーションの DVD ドライブに『*Dell Systems Management Tools and Documentation*』DVD を挿入します。
2. 画面上の指示に従って DRAC ツールをインストールします。
3. 正常なインストール後に、**install\Dell\SysMgt\rac5** フォルダをチェックして **vmcli.exe** が存在することを確認します。同様に、UNIX の場合は、該当するパスをチェックします。

   VMCLI ユーティリティがシステムにインストールされます。

VMCLI ユーティリティの実行

- オペレーティングシステムが特定の権限やグループメンバーシップを必要とする場合は、VMCLI コマンドを実行するためにも同様の権限が必要です。
- Windows システムでは、非管理者は VMCLI ユーティリティを実行するために**パワーユーザー**権限が必要です。
- Linux システムでは、iDRAC7 にアクセスし、VMCLI ユーティリティを実行して、ユーザーコマンドをログに記録するため、非管理者は VMCLI コマンドの先頭に `sudo` を指定する必要があります。ただし、VMCLI 管理者グループのユーザーを追加または編集するには、`visudo` コマンドを使用してください。

VMCLI 構文

VMCLI インタフェースは、Windows システムでも Linux システムでも同じです。VMCLI 構文は次のとおりです。

VMCLI [パラメータ] [オペレーティングシステムのシェルオプション]

例：vmcli -r iDRAC7 IP アドレス:iDRAC7 SSL ポート

このパラメータは、VMCLI による指定したサーバーへの接続、iDRAC7 へのアクセス、指定した仮想メディアへのマップを可能にします。

メモ: VMCLI 構文では大文字と小文字が区別されます。

セキュリティ確保のため、次の VMCLI パラメータを使用することをお勧めします。

- vmcli -i — VMCLI を開始するためのインタラクティブな方法を有効にします。これにより、別のユーザーがプロセスを確認する際にユーザー名とパスワードが表示されないようになります。
- vmcli -r <iDRAC7 IP アドレス[:iDRAC7 SSL ポート]> -S -u <iDRAC7 ユーザー名> -p <iDRAC7 ユーザーパスワード> -c {<デバイス名 > | <イメージファイル >} — iDRAC7 CA 証明書が有効かどうかを示します。証明書が有効でない場合は、このコマンドの実行時に警告メッセージが表示されますが、コマンドは正常に実行され、VMCLI セッションが確立されます。VMCLI パラメータの詳細については、『*VMCLI ヘルプ*』または『*VMCLI マニュアルページ*』を参照してください。

関連リンク

仮想メディアにアクセスするための VMCLI コマンド
VMCLI オペレーティングシステムのシェルオプション

仮想メディアにアクセスするための VMCLI コマンド

次の表に、さまざまな仮想メディアへのアクセスに必要な VMCLI コマンドを示します。

表 25. VMCLI コマンド

仮想メディア	コマンド
フロッピードライブ	vmcli -r [RAC IP またはホスト名] -u [iDRAC7 ユーザー名] -p [iDRAC7 ユーザーパスワード] -f [デバイス名]
起動可能なフロッピーまたは USB キーイメージ	vmcli -r [iDRAC7 IP アドレス] [iDRAC7 ユーザー名] -p [iDRAC7 パスワード] -f [フロッピー.img]
-f オプションを使用した CD ドライブ	vmcli -r [iDRAC7 IP アドレス] -u [iDRAC7 ユーザー名] -p [iDRAC7 パスワード] -f [デバイス名]|[イメージファイル]-f [cdrom - dev]
起動可能な CD/DVD イメージ	vmcli -r [iDRAC7 IP アドレス] -u [iDRAC7 ユーザー名] -p [iDRAC7 パスワード] -c [DVD.img]

ファイルが書き込み禁止になっていない場合、仮想メディアがイメージファイルに書き込みを行う場合があります。仮想メディアがメディアに書き込みを行わないことを確実にするには、次の手順を実行します。

- 上書きされないようにする必要があるフロッピーイメージファイルを書き込み禁止にするように、オペレーティングシステムを設定します。

- デバイスの書き込み禁止機能を使用します。

読み取り専用のイメージファイルを仮想化するとき、複数セッションで同じイメージメディアを同時に使用できます。

物理ドライブを仮想化すると、その物理ドライブには一度に 1 つのセッションしかアクセスできなくなります。

VMCLI オペレーティングシステムのシェルオプション

VMCLI では、シェルオプションを使用して次のオペレーティングシステム機能を有効にします。

- stderr/stdout redirection — 表示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、指定したファイルが VMCLI ユーティリティの表示出力で上書きされます。

メモ: VMCLI ユーティリティは標準入力（stdin）からは読み取りを行いません。したがって、stdin リダイレクトは不要です。

- バックグラウンド実行 — デフォルトで、VMCLI ユーティリティはフォアグラウンドで実行されます。ユーティリティをバックグラウンドで実行するには、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します。
  たとえば、Linux オペレーティングシステムでは、コマンドの直後にアンパサンド文字（&）を指定すると、プログラムが新しいバックグラウンドプロセスとして生成されます。この技法は、VMCLI コマンドで新しいプロセスが開始された後でもスクリプトを続行できるため、スクリプトプログラム用に便利です（これ以外では、VMCLI 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）。

  複数の VMCLI セッションが開始された場合、プロセスのリストと終了にはオペレーティングシステム固有の機能を使用してください。

15

vFlash SD カードの管理

vFlash SD カードは、管理下システムの vFlash SD カードスロットに差し込む Secure Digital（SD）カードです。最大 16GB の容量のカードを使用することができます。カードの挿入後、パーティションの作成や管理をするには、vFlash サービスを有効にする必要があります。

システムの vFlash SD カードスロットにカードがない場合は、**概要 → サーバー → vFlash** の iDRAC7 ウェブインタフェースに次のエラーメッセージが表示されます。

SD カードが検知されませんでした。256 MB 以上のサイズの SD カードを挿入してください。

メモ: iDRAC7 vFlash カードスロットには、vFlash 対応の SD カードのみを挿入するようにしてください。非対応の SD カードを挿入した場合、カードの初期化時に「*SD カードの初期化中にエラーが発生しました*」というメッセージが表示されます。

主な機能は次のとおりです。

- ストレージ容量を提供し、USB デバイスをエミュレートします。
- 最大 16 個のパーティションを作成します。これらのパーティションは連結されると、選択したエミュレーションモードに応じて、フロッピードライブ、ハードディスクドライブ、または CD/DVD ドライブとしてシステムに表示されます。
- 対応ファイルシステムタイプでパーティションを作成します。フロッピー用に **.img** フォーマット、CD/DVD 用に **.iso** フォーマット、およびハードディスクエミュレーションタイプ用には **.iso** および **.img** フォーマットの両方をサポートします。
- 起動可能な USB デバイスを作成します。
- エミュレートされた USB デバイスから一度だけ起動します。

メモ: vFlash ライセンスが vFlash 動作中に期限切れになる可能性も考えられますが、期限が切れても、進行中の vFlash 動作は正常に完了します。

vFlash SD カードの設定

vFlash を設定する前に、vFlash SD カードがシステムに取り付けられていることを確認します。システムへのカードの取り付け方法、および取り外し方法の詳細に関しては、**support.dell.com/manuals** にあるシステムの『*ハードウェアオーナーズマニュアル*』を参照してください。

メモ: vFlash 機能の有効と無効を切り替えたり、カードを初期化したりするには、iDRAC7 の設定許可が必要です。

関連リンク

vFlash SD カードプロパティの表示
VFlash 機能の有効化または無効化
vFlash SD カードの初期化

vFlash SD カードプロパティの表示

vFlash 機能が有効になると、iDRAC7 ウェブインタフェースまたは RACADM を使用して SD カードのプロパティを表示できます。

ウェブインタフェースを使用した vFlash SD カードプロパティの表示

vFlash SD カードのプロパティを表示するには、iDRAC7 ウェブインタフェースで **概要 → サーバー → vFlash** と移動します。**SD カードプロパティ** ページが表示されます。表示されたプロパティの詳細に関しては、『*iDRAC7 オンラインヘルプ*』を参照してください。

RACADM を使用した vFlash SD カードプロパティの表示

RACADM を使用して vFlash SD カードのプロパティを表示するには、次の手順を実行します。

1. システムに対する telnet、SSH、またはシリアルコンソールを開き、ログインします。
2. `racadm getconfig -g cfgvFlashSD` コマンドを入力します。
   次の読み取り専用プロパティが表示されます。
   - cfgVFlashSDSize
   - cfgVFlashSDLicensed
   - cfgVFlashSDAvailableSize
   - cfgVFlashSDHealth
   - cfgVFlashSDEnable
   - cfgVFlashSDWriteProtect
   - cfgVFlashSDInitialized

iDRAC 設定ユーティリティを使用した vFlash SD カードプロパティの表示

vFlash SD カードのプロパティを表示するには、**iDRAC 設定ユーティリティ** で **vFlash メディア** に移動します。**iDRAC 設定の vFlash メディア** ページにプロパティが表示されます。表示されるプロパティの詳細に関しては、『*iDRAC 設定ユーティリティオンラインヘルプ*』を参照してください。

VFlash 機能の有効化または無効化

パーティション管理を実行するには、vFlash 機能を有効にする必要があります。

ウェブインタフェースを使用した vFlash 機能の有効化または無効化

vFlash 機能を有効化または無効化するには、次の手順を実行します。

1. iDRAC7 ウェブ インタフェースで、**概要 → サーバー → vFlash** と移動します。
   SD カードプロパティ ページが表示されます。
2. **vFLASH 有効** オプションを選択、またはクリアして、vFlash 機能を有効または無効にします。vFlash パーティションが連結されている場合は vFlash を無効にすることができず、エラーメッセージが表示されます。

メモ: vFlash 機能が無効な場合、SD カードのプロパティは表示されません。

3. **適用** をクリックします。選択に基づいて vFlash 機能が有効または無効になります。

RACADM を使用した vFlash 機能の有効化または無効化

RACADM を使用して vFlash 機能を有効化または無効化するには、次の手順を実行します。

1. システムに対する telnet、SSH、またはシリアルコンソールを開き、ログインします。
2. 次のコマンドを入力します。
   - vFlash を有効にするには、次のコマンドを入力します。
     `racadm config -g cfgvFlashsd -o cfgvflashSDEnable 1`

– vFlash を無効にするには、次のコマンドを入力します。
```
racadm config -g cfgvFlashsd -o cfgvflashSDEnable 0
```

メモ: RACADM コマンドは、vFlash SD カードが存在する場合に限り機能します。カードが存在しない場合は、*エラー：SD カードが存在しません*というメッセージが表示されます。

iDRAC 設定ユーティリティを使用した vFlash 機能の有効化または無効化

vFlash 機能を有効または無効にするには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**vFlash メディア** に移動します。
   iDRAC 設定の vFlash メディア ページが表示されます。
2. **有効** を選択して vFlash 機能を有効にするか、**無効** を選択して vFlash 機能を無効にします。
3. **戻る**、**終了** の順にクリックし、**はい** をクリックします。
   選択に基づいて、vFlash 機能が有効または無効になります。

vFlash SD カードの初期化

初期化操作は SD カードを再フォーマットし、カード上の初期 vFlash システム情報を設定します。

ウェブインタフェースを使用した vFlash SD カードの初期化

vFlash SD カードを初期化するには、次の手順を実行します。

1. iDRAC7 ウェブ インタフェースで、**概要 → サーバー → vFlash** と移動します。
   SD カードのプロパティ ページが表示されます。
2. **vFLASH** を有効にし、**初期化** をクリックします。
   既存のすべての内容が削除され、カードが新しい vFlash システム情報で再フォーマットされます。
   いずれかの vFlash パーティションが連結されている場合、初期化は失敗し、エラーメッセージが表示されます。

RACADM を使用した vFlash SD カードの初期化

RACADM を使用して vFlash SD カードを初期化するには、次の手順を実行します。

1. システムに対する telnet、SSH、またはシリアルコンソールを開き、ログインします。
2. `racadm vflashsd initialize` コマンドを入力します。
   既存のパーティションはすべて削除され、カードが再フォーマットされます。

iDRAC 設定ユーティリティを使用した vFlash SD カードの初期化

iDRAC 設定ユーティリティを使用して vFlash SD カードを初期化するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**vFlash メディア** に移動します。
   iDRAC 設定の vFlash メディア ページが表示されます。
2. **vFlash の初期化** をクリックします。
3. **はい** をクリックします。初期化が開始されます。
4. **戻る** をクリックし、同じ **iDRAC 設定の vFlash メディア** ページに移動して、成功を示すメッセージを確認します。
   既存のすべての内容が削除され、カードが新しい vFlash システム情報で再フォーマットされます。

RACADM を使用した最後のステータスの取得

vFlash SD カードに送信された最後の初期化コマンドのステータスを取得するには、次の手順を実行します。

1. システムに対する Telnet、SSH、またはシリアルコンソールを開き、ログインします。
2. コマンド `racadm vFlashsd status` を入力します。
   SD カードに送信されたコマンドのステータスが表示されます。
3. すべての vflash パーティションの最後のステータスを取得するには、コマンド `racadm vflashpartition status -a` を使用します。
4. 特定のパーティションの最後のステータスを取得するには、コマンド `racadm vflashpartition status -i (index)` を使用します。

メモ: iDRAC7 がリセットされると、前回のパーティション操作のステータスが失われます。

vFlash パーティションの管理

iDRAC7 ウェブインタフェースまたは RACADM を使用して、次の操作を実行できます。

メモ: システム管理者は、vFlash パーティション上のすべての操作を実行できます。管理者ではない場合は、パーティションの作成、削除、フォーマット、連結、分離、または内容コピーには **仮想メディアへのアクセス** 権限を持つ必要があります。

- 空のパーティションの作成
- イメージファイルを使ったパーティションの作成
- パーティションのフォーマット
- 使用可能なパーティションの表示
- パーティションの変更
- パーティションの連結または分離
- 既存のパーティションの削除
- パーティション内容のダウンロード
- パーティションからの起動

メモ: WS-MAN、iDRAC 設定ユーティリティ、または RACADM などのアプリケーションが vFlash を使用しているときに、vFlash ページで任意のオプションをクリックする場合、または GUI の他のページに移動する場合、iDRAC7 は次のメッセージを表示する可能性があります。`vFlash は現在別のプロセスで使用中です。しばらくしてから再試行してください。`

フォーマット、パーティションの連結などの進行中の vFlash 動作が他にない場合、vFlash は高速パーティション作成を実行できます。このため、他の個々のパーティションの動作を実行する前に、まずすべてのパーティションを作成することを推奨します。

空のパーティションの作成

システムに連結されている空のパーティションは、空の USB フラッシュドライブと似ています。vFlash SD カード上には空のパーティションを作成でき、*フロッピー*または*ハードディスク*タイプのパーティションを作成できます。パーティションタイプ CD は、イメージを使ったパーティションの作成中にのみサポートされます。

空のパーティションを作成する前に、次を確認してください。

- **仮想メディアへのアクセス** 権限を持っている。
- カードが初期化されている。

- カードが書き込み禁止になっていない。
- カード上で初期化が実行されていない。

ウェブインタフェースを使用した空のパーティションの作成

空の vFlash パーティションを作成するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → vFlash → 空のパーティションの作成** と移動します。

   空のパーティションの作成 ページが表示されます。

2. 必要な情報を指定して、**適用** をクリックします。オプションの詳細に関しては、『*iDRAC7 オンラインヘルプ*』を参照してください。

   新しい未フォーマットの空のパーティションが作成されます。これはデフォルトで読み取り専用です。進行状況の割合を示すページが表示されます。次の場合にエラーメッセージが表示されます。

   - カードが書き込み禁止になっている。
   - ラベル名が既存のパーティションのラベルに一致する。
   - パーティションサイズとして非整数値が入力された、入力値がカード上で利用可能な容量を超えている、または 4 GB を超えている。
   - カード上で初期化が実行中。

RACADM を使用した空のパーティションの作成

20 MB の空のパーティションを作成するには、次の手順を実行します。

1. システムに対する telnet、SSH、またはシリアルコンソールを開き、ログインします。
2. `racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s 20` コマンドを入力します。

   20 MB の空のパーティションが FAT16 形式で作成されます。デフォルトでは、空のパーティションは読み取り / 書き込みパーティションとして作成されます。

イメージファイルを使用したパーティションの作成

イメージファイル（**.img** または **.iso** 形式で入手可能）を使用して、vFlash SD カードで新しいパーティションを作成できます。パーティションは、フロッピー（**.img**）、ハードディスク（**.img** または **.iso**）、または CD（**.iso**）エミュレーションタイプです。作成されたパーティションサイズは、イメージファイルのサイズに等しくなります。

イメージファイルからパーティションを作成する前に、次を確認してください。

- 仮想メディアへのアクセス権限がある。
- カードが初期化されている。
- カードが書き込み禁止になっていない。
- カード上で初期化が実行されていない。
- イメージタイプとエミュレーションタイプが一致する。

メモ: アップロードされたイメージとエミュレーションタイプは一致する必要があります。iDRAC7 が不適切なイメージタイプのデバイスをエミュレートする場合は問題があります。たとえば、ISO イメージを使用してパーティションを作成し、ハードディスクがエミュレーションタイプとして指定された場合、BIOS はこのイメージから起動できません。

- イメージファイルのサイズは、カード上の使用可能容量以下です。
- サポートされている最大パーティションサイズは 4 GB なので、イメージファイルのサイズは 4 GB 以下になります。ただし、ウェブブラウザを使用してパーティションを作成する場合のイメージファイルサイズは、2 GB 未満である必要があります。

ウェブインタフェースを使用したイメージファイルからのパーティションの作成

イメージファイルから vFlash パーティションを作成するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → vFlash → イメージから作成** と移動します。
   イメージファイルからのパーティションの作成 ページが表示されます。
2. 必要な情報を入力して、**適用** をクリックします。オプションの詳細に関しては、『*iDRAC7 オンラインヘルプ*』を参照してください。
   新しいパーティションが作成されます。CD エミュレーションタイプには、読み取り専用パーティションが作成されます。フロッピーまたはハードディスクエミュレーションタイプには、読み取り / 書き込みパーティションが作成されます。次の場合には、エラーメッセージが表示されます。
   - カードが書き込み禁止になっている。
   - ラベル名が既存のパーティションのラベルに一致する。
   - イメージファイルのサイズが 4GB を超えるか、カード上の空き容量を超えている。
   - イメージファイルが存在しないか、イメージファイルの拡張子が .img または .iso.でない。
   - カード上で初期化がすでに実行中である。

RACADM を使用したイメージファイルからのパーティションの作成

RACADM を使用してイメージファイルからパーティションを作成するには、次の手順を実行します。

1. システムに対する telnet、SSH、またはシリアルコンソールを開き、ログインします。
2. `racadm vflashpartition create -i 1 -o drive1 -e HDD -t image -l //myserver/sharedfolder/foo.iso -u root -p mypassword` コマンドを入力します。
   新しいパーティションが作成されます。デフォルトでは、作成されるパーティションは読み取り専用です。このコマンドでは、イメージファイル名拡張子の大文字と小文字が区別されます。ファイル名の拡張子が大文字の場合（たとえば、FOO.iso ではなく、FOO.ISO）、コマンドは構文エラーを返します。

メモ: この機能は ローカル RACADM ではサポートされていません。

メモ: CFS または NFS IPv6 有効ネットワーク共有に配置されたイメージファイルからの vFlash パーティションの作成はサポートされていません。

パーティションのフォーマット

ファイルシステムのタイプに基づいて、vFlash SD カード上の既存のパーティションをフォーマットできます。サポートされているファイルシステムタイプは、EXT2、EXT3、FAT16、および FAT32 です。フォーマットできるのは、タイプがハードディスクまたはフロッピーのパーティションのみで、CD タイプはフォーマットできません。読み取り専用パーティションもフォーマットできません。
イメージファイルからパーティションを作成する前に、次を確認してください。

- **仮想メディアへのアクセス** 権限がある。
- カードが初期化されている。
- カードが書き込み禁止になっていない。
- カード上で初期化が実行中ではない。

vFlash パーティションをフォーマットするには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → vFlash → フォーマット** と移動します。
   パーティションのフォーマット ページが表示されます。
2. 必要な情報を入力し、**適用** をクリックします。

オプションの詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。

そのパーティション上のすべてのデータが消去されることを警告するメッセージが表示されます。

3. **OK** をクリックします。
   選択したパーティションが指定したファイルシステムタイプにフォーマットされます。次の場合には、エラーメッセージが表示されます。
   - カードが書き込み禁止になっている。
   - カード上で初期化がすでに実行中である。

使用可能なパーティションの表示

使用可能なパーティションのリストを表示するため、vFlash 機能が有効化されていることを確認します。

ウェブインタフェースを使用した使用可能なパーティションの表示

iDRAC7 ウェブインタフェースで使用可能な vFlash パーティションを表示するには、**概要 → サーバー → vFlash → 管理** と移動します。**パーティションの管理** ページが表示され、使用可能なパーティションと各パーティションの関連情報が一覧表示されます。パーティションの詳細に関しては、『*iDRAC7 オンラインヘルプ*』を参照してください。

RACADM を使用した使用可能なパーティションの表示

RACADM を使用して使用可能なパーティションおよびそのプロパティを表示するには、次の手順を実行してください。

1. システムに対する Telnet、SSH、またはシリアルコンソールを開き、ログインします。
2. 次のコマンドを入力します。
   - すべての既存パーティションおよびそのプロパティを一覧表示する場合
     ```
     racadm vflashpartition list
     ```
   - パーティション 1 上での動作状態を取得する場合
     ```
     racadm vflashpartition status -i 1
     ```
   - すべての既存パーティションの状態を取得する場合
     ```
     racadm vflashpartition status -a
     ```

メモ: -a オプションは、ステータス処置と併用する場合に限り有効です。

パーティションの変更

読み取り専用パーティションを読み取り / 書き込みパーティションに変更したり、その逆を行うことができます。パーティションを変更する前に、次を確認してください。

- vFlash 機能が有効である。
- **仮想メディアへのアクセス** 権限がある。

メモ: デフォルトでは、読み取り専用パーティションが作成されます。

ウェブインタフェースを使用したパーティションの変更

パーティションを変更するには、次の手順を実行します。

1. DRAC7 ウェブインタフェースで、**概要 → サーバー → vFlash → 管理** と移動します。

パーティションの管理 ページが表示されます。

2. **読み取り専用** 列で、次の操作を行います。
   - パーティションのチェックボックスを選択し、**適用** をクリックして読み取り専用に変更します。
   - パーティションのチェックボックスのチェックを外し、**適用** をクリックして読み取り / 書き込みに変更します。
     選択内容に応じて、パーティションは読み取り専用または読み取り / 書き込みに変更されます。

メモ: パーティションが CD タイプの場合、状態は読み取り専用です。この状態を読み取り / 書き込みに変更することはできません。パーティションが連結されている場合、チェックボックスはグレー表示になっています。

RACADM を使用したパーティションの変更

カード上の使用可能なパーティションとそれらのプロパティを表示するには、次の手順を実行します。

1. システムに対する Telnet、SSH、またはシリアルコンソールを開き、ログインします。
2. 次のコマンドを入力します。
   - 読み取り専用パーティションを読み取り / 書き込みに変更：
     ```
     racadm config -g cfgvflashpartition -i 1 -o
     cfgvflashPartitionAccessType 1
     ```
   - 読み取り / 書き込みパーティションを読み取り専用に変更：
     ```
     racadm config -g cfgvflashpartition -i 1 -o
     cfgvflashPartitionAccessType 0
     ```

パーティションの連結または分離

1 つ、または複数のパーティションを連結すると、これらのパーティションはオペレーティングシステムおよび BIOS によって USB 大容量ストレージデバイスとして表示されます。複数のパーティションを割り当てられたインデックスに基づいて連結すると、オペレーティングシステムおよび BIOS の起動順序メニューに昇順で一覧表示されます。

パーティションを分離すると、オペレーティングシステムおよび BIOS の起動順序メニューには表示されません。

パーティションを連結または分離すると、管理下システムの USB バスがリセットされます。これは vFlash を使用するアプリケーションに影響を及ぼし、iDRAC7 仮想メディアセッションを切断します。

パーティションを連結または分離する前に、次を確認してください。

- vFlash 機能が有効になっている。
- カード上で初期化がすでに実行開始されていない。
- **仮想メディアへのアクセス** 権限を持っている。

ウェブインタフェースを使用したパーティションの連結または分離

パーティションを連結または分離するには、次の手順を実行します。

1. DRAC7 ウェブインタフェースで、**概要 → サーバー → vFlash → 管理** と移動します。
   パーティションの管理 ページが表示されます。
2. **連結** 列で、次の操作を行います。
   - パーティションのチェックボックスを選択し、**適用** をクリックしてパーティションを連結します。
   - パーティションのチェックボックスのチェックを外し、**適用** をクリックしてパーティションを分離します。

パーティションは選択に基づいて連結または分離されます。

RACADM を使用したパーティションの連結または分離

パーティションを連結または分離するには、次の手順を実行します。

1. システムに対する Telnet、SSH、またはシリアルコンソールを開き、ログインします。
2. 次のコマンドを入力します。
   - パーティションを連結：
     ```
     racadm config -g cfgvflashpartition -i 1 -o
     cfgvflashPartitionAttachState 1
     ```
   - パーティションを分離：
     ```
     racadm config -g cfgvflashpartition -i 1 -o
     cfgvflashPartitionAttachState 0
     ```

連結されたパーティションに対するオペレーティングシステムの動作

Windows および Linux オペレーティングシステムの場合は、次のように動作します。

- オペレーティングシステムは連結されたパーティションを制御し、ドライブ文字を割り当てます。
- 読み取り専用パーティションは、オペレーティングシステムでは読み取り専用ドライブとなります。
- オペレーティングシステムは連結されたパーティションのファイルシステムをサポートしている必要があります。そうでない場合、オペレーティングシステムからパーティションの内容の読み取りや変更を行うことはできません。たとえば、Windows 環境では、Linux 固有のパーティションタイプ EXT2 を読み取ることはできません。また、Linux 環境では、Windows 固有のパーティションタイプ NTFS を読み取ることはできません。
- vFlash パーティションのラベルは、エミュレートされた USB デバイス上のファイルシステムのボリューム名とは異なります。エミュレートされた USB デバイスのボリューム名はオペレーティングシステムから変更できますが、iDRAC7 で保存されているパーティションラベル名は変更されません。

既存のパーティションの削除

既存のパーティションを削除する前に、次を確認してください。

- vFlash 機能が有効になっている。
- カードが書き込み禁止になっていない。
- パーティションが連結されていない。
- カード上で初期化が実行中ではない。

ウェブインタフェースを使用した既存のパーティションの削除

既存のパーティションを削除するには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → vFlash → 管理** と移動します。
   パーティションの管理 ページが表示されます。
2. **削除** 行で、削除するパーティションの削除アイコンをクリックします。
   この処置を実行すると、パーティションが恒久的に削除されることを示すメッセージが表示されます。
3. **OK** をクリックします。
   パーティションが削除されます。

RACADM を使用した既存のパーティションの削除

パーティションを削除するには、次の手順を実行します。

1. システムに対する Telnet、SSH、またはシリアルコンソールを開き、ログインします。
2. 次のコマンドを入力します。
   - パーティションを削除：
     `racadm vflashpartition delete -i 1`
   - すべてのパーティションを削除するには、vFlash SD カードを再初期化します。

パーティション内容のダウンロード

.img または **.iso** 形式の vFlash パーティションの内容は、次の場所にダウンロードできます。

- 管理下システム（iDRAC7 を操作するシステム）
- 管理ステーションにマップされているネットワーク上の場所

パーティションの内容をダウンロードする前に、次を確認してください。

- 仮想メディアへのアクセス権限がある。
- vFlash 機能が有効である。
- カード上で初期化が実行されていない。
- 読み取り / 書き込みパーティションが連結されていない。

vFlash パーティションの内容をダウンロードするには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → vFlash → ダウンロード** と移動します。
   パーティションのダウンロード ページが表示されます。
2. **ラベル** ドロップダウンメニューでダウンロードするパーティションを選択し、**ダウンロード** をクリックします。

メモ: すべての既存のパーティション（連結されたパーティションは除く）がリストに表示されます。最初のパーティションがデフォルトで選択されています。

3. ファイルの保存場所を指定します。
   選択したパーティションの内容が指定した場所にダウンロードされます。

メモ: フォルダの場所が指定された場合に限り、パーティションラベルがファイル名として使用されます。また、CD およびハードディスクタイプのパーティションには **.iso** 拡張子、フロッピーおよびハードディスクタイプのパーティションんには **.img** 拡張子が使用されます。

パーティションからの起動

連結された vFlash パーティションを次回起動時の起動デバイスとして設定できます。
パーティションを起動する前に、次を確認してください。

- vFlash パーティションに、デバイスから起動するための起動可能なイメージ（**.img** 形式または **.iso** 形式）が含まれている。
- vFlash 機能が有効である。
- 仮想メディアへのアクセス権限がある。

ウェブインタフェースを使用したパーティションからの起動

vFlash パーティション を最初の起動デバイスとして設定するには、「最初の起動デバイスの設定」を参照してください。

メモ: 連結された vFlash パーティションが **最初の起動デバイス** ドロップダウンメニューのリストに表示されていない場合は、BIOS が最新バージョンにアップデートされていることを確認します。

RACADM を使用したパーティションからの起動

vFlash パーティションを 1 番目の起動デバイスとして設定するには、`cfgServerInfo` を使用します。詳細に関しては、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

メモ: このコマンドを実行すると、vFlash パーティションラベルが、1 回限りの起動に自動的に設定されます（`cfgserverBootOnce` が `1` に設定されます）。1 回限りの起動は、1 度だけパーティションからデバイスを起動し、起動順序を永続的に 1 番にしておくわけではありません。

16

SMCLP の使用

Server Management Command Line Protocol（SMCLP）仕様は、CLI ベースのシステム管理を可能にします。SMCLP は標準文字単位のストリームを介して管理コマンドを送信するためのプロトコルを定義します。このプロトコルでは、人間指向型コマンドセットを使用して Common Information Model Object Manager（CIMOM）にアクセスします。SMCLP は、複数のプラットフォームにわたるシステム管理を合理化するための Distributed Management Task Force（DMTF）SMASH イニシアチブのサブコンポーネントです。SMCLP 仕様には、管理下エレメントアドレス指定仕様や、SMCLP マッピング仕様に対する多数のプロファイルとともに、さまざまな管理タスク実行のための標準動詞とターゲットについて記述されています。

メモ: ここでは、ユーザーに Systems Management Architecture for Server Hardware（SMASH）イニシアチブおよび SMWG SMCLP 仕様についての知識があることを前提としています。

SM-CLP は、複数のプラットフォームにわたるサーバー管理を合理化するための Distributed Management Task Force（DMTF）SMASH イニシアチブのサブコンポーネントです。SM-CLP 仕様は、管理下エレメントアドレス指定仕様や、SM-CLP マッピング仕様に対する多数のプロファイルとともに、さまざまな管理タスク実行のための標準バーブとターゲットについて説明しています。

SMCLP は iDRAC7 コントローラのファームウェアからホストされ、Telnet、SSH、およびシリアルベースのインタフェースをサポートしています。iDRAC7 SMCLP インタフェースは、DMTF が提供する SMCLP 仕様バージョン 1.0 に基づいています。

メモ: プロファイル、拡張、および MOF に関する情報は **delltechcenter.com** から、DMTF に関する全情報は **dmtf.org/standards/profiles/** から入手可能です。

SM-CLP コマンドは、ローカル RACADM コマンドのサブセットを実装します。これらのコマンドは管理ステーション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 などの明確に定義された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および管理ツールとの統合を容易にします。

SMCLP を使用したシステム管理機能

iDRAC7 SMCLP では次の操作が可能です。

- サーバー電源の管理 — システムのオン、シャットダウン、再起動
- システムイベントログ（SEL）の管理 — SEL レコードの表示やクリア
- iDRAC7 ユーザーアカウントの管理
- システムプロパティの表示

SMCLP コマンドの実行

SMCLP コマンドは、SSH または Telnet インタフェースを使用して実行できます。SSH または Telnet インタフェースを開いて、管理者として iDRAC7 にログインします。SMCLP プロンプト（admin ->）が表示されます。

SMCLP プロンプト：

- yx1x ブレードサーバーは -$ を使用します。
- yx1x ラックおよびタワーサーバーは、admin-> を使用します。
- yx2x ブレード、ラック、およびタワーサーバーは、admin-> を使用します。

y は、M（ブレードサーバーの場合）、R（ラックサーバーの場合）、および T（タワーサーバーの場合）など英数字であり、x は数字です。これは、Dell PowerEdge サーバーの世代を示します。

メモ: -$ を使用したスクリプトでは、これらを yx1x システムに使用できますが、yx2x システム以降は、ブレード、ラック、およびタワーサーバーに admin-> を使用した一つのスクリプトを使用できます。

iDRAC7 SMCLP 構文

iDRAC7 SMCLP は、動詞とターゲットの概念を使用し、CLI 経由でシステム管理機能を提供します。動詞は、実行する動作を示し、ターゲットは、その動作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。

SMCLP コマンドライン構文：

<動詞> [<オプション>] [<ターゲット>] [<プロパティ>]

次の表は、動詞とその定義が示されています。

表 26. SMCLP 動詞

動詞	定義
cd	シェルを使用して MAP を移動します
set	プロパティを特定の値に設定します
help	特定のターゲットのヘルプを表示します
reset	ターゲットをリセットします
show	ターゲットのプロパティ、動詞、サブターゲットを表示します
start	ターゲットをオンにします
stop	ターゲットをシャットダウンします
exit	SMCLP シェルセッションを終了します
version	ターゲットのバージョン属性を表示します
load	バイナリイメージを URL から指定されたターゲットアドレスに移動します

次の表は、ターゲットのリストが示されています。

表 27. SMCLP ターゲット

ターゲット	定義
admin1	管理ドメイン
admin1/profiles1	iDRAC7 内の登録済みプロファイル
admin1/hdwr1	ハードウェア
admin1/system1	管理下システムターゲット
admin1/system1/capabilities1	管理下システム SMASH 収集機能
admin1/system1/capabilities1/pwrcap1	管理下システムの電力活用機能
admin1/system1/capabilities1/elecap1	管理下システムターゲット機能
admin1/system1/logs1	レコードログ収集ターゲット

ターゲット	定義
admin1/system1/logs1/log1	システムイベントログ（SEL）のレコードエントリ
admin1/system1/logs1/log1/record*	管理下システムの SEL レコードの個々のインスタンス
admin1/system1/settings1	管理下システム SMASH 収集機能
admin1/system1/capacities1	管理下システム機能 SMASH 収集
admin1/system1/consoles1	管理下システムコンソール SMASH 収集
admin1/system1/sp1	サービスプロセッサ
admin1/system1/sp1/timesvc1	サービスプロセッサ時間サービス
admin1/system1/sp1/capabilities1	サービスプロセッサ機能 SMASH 収集
admin1/system1/sp1/capabilities1/clpcap1	CLP サービス機能
admin1/system1/sp1/capabilities1/pwrmgtcap1	システムの電源状態管理サービス機能
admin1/system1/sp1/capabilities1/acctmgtcap*	アカウント管理サービス機能
admin1/system1/sp1/capabilities1/rolemgtcap*	ローカル役割ベースの管理機能
admin1/system1/sp1/capabilities/PwrutilmgtCap1	電力活用管理機能
admin1/system1/sp1/capabilities1/elecap1	認証機能
admin1/system1/sp1/settings1	サービスプロセッサ設定収集
admin1/system1/sp1/settings1/clpsetting1	CLP サービス設定データ
admin1/system1/sp1/clpsvc1	CLP サービスプロトコルサービス
admin1/system1/sp1/clpsvc1/clpendpt*	CLP サービスプロトコルエンドポイント
admin1/system1/sp1/clpsvc1/tcpendpt*	CLP サービスプロトコル TCP　エンドポイント
admin1/system1/sp1/jobq1	CLP サービスプロトコルジョブキュー
admin1/system1/sp1/jobq1/job*	CLP サービスプロトコルジョブ
admin1/system1/sp1/pwrmgtsvc1	電源状態管理サービス
admin1/system1/sp1/account1-16	ローカルユーザーアカウント
admin1/sysetm1/sp1/account1-16/identity1	ローカルユーザー識別アカウント

ターゲット	定義
admin1/sysetm1/sp1/account1-16/identity2	IPMI 識別（LAN）アカウント
admin1/sysetm1/sp1/account1-16/identity3	IPMI 識別（シリアル）アカウント
admin1/sysetm1/sp1/account1-16/identity4	CLP 識別アカウント
admin1/system1/sp1/acctsvc1	ローカルユーザーアカウント管理サービス
admin1/system1/sp1/acctsvc2	IPMI アカウント管理サービス
admin1/system1/sp1/acctsvc3	CLP アカウント管理サービス
admin1/system1/sp1/rolesvc1	ローカル役割ベース認証（RBA）サービス
admin1/system1/sp1/rolesvc1/Role1-16	ローカル役割
admin1/system1/sp1/rolesvc1/Role1-16/privilege1	ローカル役割権限
admin1/system1/sp1/rolesvc2	IPMI RBA サービス
admin1/system1/sp1/rolesvc2/Role1-3	IPMI 役割
admin1/system1/sp1/rolesvc2/Role4	IPMI シリアルオーバー LAN（SOL）役割
admin1/system1/sp1/rolesvc3	CLP RBA サービス
admin1/system1/sp1/rolesvc3/Role1-3	CLP 役割
admin1/system1/sp1/rolesvc3/Role1-3/privilege1	CLP 役割権限

関連リンク

SMCLP コマンドの実行
使用例

MAP アドレス領域のナビゲーション

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領域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。これは、iDRAC7 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 動詞を使用してルートから移動します。

メモ: スラッシュ（/）およびバックスラッシュ（\）は、SM-CLP アドレスパスで互換性があります。ただし、コマンドラインの末尾にバックスラッシュを置くと、コマンドが次のラインまで続くことになり、コマンドの解析時に無視されます。

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 /admin1/system1/logs1/log1/record3
```

ターゲットなしで cd 動詞を入力し、アドレス領域内の現在の場所を検索します。省略形 .. と . の機能は Windows および Linux の場合と同様で、.. は親レベルを示し、. は現在のレベルを示します。

Show 動詞の使用

ターゲットの詳細を確認するには、show 動詞を使用します。この動詞は、ターゲットのプロパティ、サブターゲット、関連性、およびその場所で許可されている SM-CLP 動詞のリストを表示します。

-display オプションの使用

show -display オプションでは、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、アソシエーション、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およびターゲットのみを表示するには、次のコマンドを使用します。

```
show -display properties,targets
```

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=(ユーザー ID,名前) /admin1/system1/sp1/account1
```

1 つのプロパティのみを表示する場合は、括弧を省略できます。

-level オプションの使用

show -level オプションは、指定されたターゲットよりも下の追加レベルで show を実行します。アドレス領域内のすべてのターゲットとプロパティを参照するには、-l all オプションを使用します。

-output オプションの使用

-output オプションは、4 つの SM-CLP 動詞出力フォーマット（**テキスト**、**clpcsv**、**キーワード**、**clpxml**）のうち、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** であり、最も読み取りやすい出力です。**clpcsv** フォーマットは、スプレッドシートプログラムへのロードに最適な、コンマ区切り値フォーマットです。**キーワード** フォーマットは、1 行あたり 1 つのキーワード = 値のペアとして情報を出力します。**clpxml** フォーマットは、**response** XML 要素を含む XML ドキュメントです。DMTF は、**clpcsv** フォーマットと **clpxml** フォーマットを指定しています。これらの仕様は、DMTF ウエブサイト（**dmtf.org**）で確認できます。

次の例は、SEL の内容を XML で出力する方法を示しています。

```
show -l all -output format=clpxml /admin1/system1/logs1/log1
```

使用例

本項では、SMCLP の使用事例のシナリオについて説明します。

- サーバーの電源管理
- SEL 管理
- MAP ターゲットのナビゲーション

サーバーの電源管理

次の例は、SMCLP を使用して管理下システムで電源管理操作を実行する方法を示しています。

SMCLP コマンドプロンプトで、次のコマンドを入力します。

- サーバーの電源をオフにする：

stop /system1
次のメッセージが表示されます。
システム 1 が正常に停止されました

- サーバーの電源をオンにする：
  start /system1
  次のメッセージが表示されます。
  システム 1 が正常に起動されました
- サーバーを再起動する：
  reset /system1
  次のメッセージが表示されます。
  システム 1 が正常にリセットされました

SEL 管理

次の例は、SM-CLP を使用して、管理下システムで SEL 関連の操作を実行する方法を示しています。SMCLP コマンドプロンプトで、次のコマンドを入力します。

- SEL を表示する場合
  show/system1/logs1/log1
  次の出力が表示されます。
  /システム 1/ログ 1/ログ 1
  ターゲット：
  レコード 1
  レコード 2
  レコード 3
  レコード 4
  レコード 5
  プロパティ:
  インスタンス ID = IPMI:BMC1 SEL ログ
  レコード最大数 = 512
  現在のレコード数 = 5
  名前 = IPMI SEL
  有効化された状態 = 2
  動作状態 = 2
  正常性状態 = 2
  キャプション = IPMI SEL
  説明 = IPMI SEL
  エレメント名 = IPMI SEL
  コマンド:
  cd
  表示
  ヘルプ
  終了

バージョン

- SEL レコードを表示する場合
  show/system1/logs1/log1
  次の出力が表示されます。
  /システム 1/ログ 1/ログ 1

  プロパティ:
  ログ作成クラス名= CIM_RecordLog
  作成クラス名= CIM_LogRecord
  ログ名= IPMI SEL
  レコード ID= 1
  メッセージタイムスタンプ= 20050620100512.000000-000
  説明= FAN 7 RPM: ファンセンサー、障害検出
  エレメント名 = IPMI SEL レコード

  コマンド:
  cd
  表示
  ヘルプ
  終了
  バージョン
- SEL をクリアする場合
  delete /system1/logs1/log1/record*
  次の出力が表示されます。
  すべてのレコードが正常に削除されました

MAP ターゲットナビゲーション

次の例は、cd 動詞を使用して MAP をナビゲートする方法を示します。すべての例で、最初のデフォルトターゲットは / であると想定されます。

SMCLP コマンドプロンプトで、次のコマンドを入力します。

- システムターゲットまで移動して再起動：
  cd system1 reset The current default target is /.
- SEL ターゲットまで移動してログレコードを表示：
  cd system1
  cd logs1/log1
  show
- 現在のターゲットを表示：
  type cd .
- 1 つ上のレベルに移動：
  type cd ..
- 終了：
  exit

17

オペレーティングシステムの展開

管理下システムへのオペレーティングシステムの展開には、次のいずれかのユーティリティを使用できます。

- 仮想メディアコマンドラインインタフェース（CLI）
- 仮想メディアコンソール
- リモートファイル共有

関連リンク

VMCLI を使用したオペレーティングシステムの導入
リモートファイル共有を使用したオペレーティングシステムの展開
仮想メディアを使用したオペレーティングシステムの展開

VMCLI を使用したオペレーティングシステムの導入

vmdeploy スクリプトを使用してオペレーティングシステムを導入する前に、次を確認してください。

- VMCLI ユーティリティが管理ステーションにインストールされている。
- iDRAC7 の **ユーザーの設定** 権限および **仮想メディアへのアクセス** 権限がそのユーザーで有効になっている。
- IPMItool が管理ステーションにインストールされている。

メモ: IPMItool は、管理下システムまたは管理ステーションのいずれかで IPv6 が設定されている場合は機能しません。

- ターゲットリモートシステムに iDRAC7 が設定されている。
- イメージファイルからシステムを起動できる。
- iDRAC7 で IPMI Over LAN が有効になっている。
- ネットワーク共有に、ドライバおよびオペレーティングシステムのブータブルイメージファイルが **.img** または **.iso** などの業界標準のフォーマットで含まれている。

メモ: イメージファイルの作成中は、標準のネットワークベースのインストール手順に従います。また展開イメージを読み取り専用としてマークして、各ターゲットシステムが同じ展開手順から起動し、実行することを確実にします。

- 仮想メディアのステータスが連結状態である。
- **vmdeploy** スクリプトが管理ステーションにインストールされている。VMCLI に含まれている vmdeploy サンプルスクリプトを確認してください。スクリプトには、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方法が記述されています。内部的には VMCLI と IPMItool が使用されます。

メモ: vmdeploy スクリプトはインストール中、ディレクトリに存在する一部のサポートファイルに依存します。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してください。IPMItool ユーティリティがインストールされていない場合は、他のファイルとともにユーティリティもコピーしてください。

ターゲットリモートシステムにオペレーティングシステムを展開するには、次の手順を実行します。

1. ターゲットリモートシステムの iDRAC7 IPv4 アドレスを、**ip.txt** テキストファイルにリストします。1 行に 1 つの IPv4 アドレスをリストします。
2. 起動可能なオペレーティングシステム CD または DVD を管理ステーションのドライブに挿入します。
3. コマンドプロンプトを管理者権限で開き、**vmdeploy** スクリプトを実行します。

```
vmdeploy.bat -r <iDRAC7 IP アドレスまたはファイル> -u <iDRAC7 ユーザー> -p
<iDRAC7 ユーザーパスワード> [ -f {<フロッピーイメージ> | <デバイス名>} | -c {<デバイ
ス名>|<イメージファイル>} ] [-i <デバイス ID>]
```

メモ: IPv6 では IPMItool がサポートされないため、vmdeploy は IPv6 をサポートしていません。

メモ: vmdeploy スクリプトは -r オプションを vmcli -r オプションとは少し異なる形で処理します。-r オプションの引数が既存のファイルの名前である場合、スクリプトは指定されたファイルから iDRAC7 IPv4 または IPv6 アドレスを読み取り、各行で 1 回ずつ VMCLI ユーティリティを実行します。-r オプションの引数がファイル名でない場合は、単独の iDRAC7 アドレスになります。この場合、-r は VMCLI ユーティリティの説明どおりに機能します。

次の表に、vmdeploy コマンドのパラメータを示します。

表 28. vmdeploy コマンドのパラメータ

パラメータ	説明
<iDRAC7 ユーザー>	iDRAC7 ユーザー名。これには次の属性が必要です。 – 有効なユーザー名 – iDRAC7 仮想メディアユーザー権限 iDRAC7 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。
<iDRAC7 IP | ファイル>	iDRAC7 IP アドレス、または iDRAC7 IP アドレスを含むファイル。
<iDRAC7 ユーザーパスワード> または <iDRAC7 パスワード>	iDRAC7 ユーザーのパスワード。 iDRAC7 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。
-c {<デバイス名> | <イメージファイル>}	オペレーティングシステムのインストール CD または DVD の ISO9660 イメージへのパス。
<フロッピーデバイス>	オペレーティングシステムのインストール CD、DVD、またはフロッピーが挿入されているデバイスへのパス。
<フロッピーイメージ>	有効なフロッピーイメージへのパス。
<デバイス ID>	1 回限りの起動を行うデバイスの ID。

関連リンク

仮想メディアの設定
iDRAC7 の設定

リモートファイル共有を使用したオペレーティングシステムの展開

リモートファイル共有を使用してオペレーティングシステムを展開する前に、次を確認してください。

- 起動順序に仮想ドライブが表示されるように、仮想メディアが **連結** 状態になっている。
- iDRAC7 の **ユーザーの設定** 権限および **仮想メディアへのアクセス** 権限がそのユーザーで有効になっている。
- リモートファイル共有が有効になっている。
- ネットワーク共有に、ドライバおよびオペレーティングシステムのブータブルイメージファイルが **.img** または **.iso** などの業界標準のフォーマットで含まれている。

メモ: イメージファイルの作成中は、標準のネットワークベースのインストール手順に従います。また展開イメージを読み取り専用としてマークして、各ターゲットシステムが同じ展開手順から起動し、実行することを確実にします。

リモートファイル共有を使用してオペレーティングシステムを展開するには、次の手順を実行します。

1. ISO または IMG イメージファイルを NFS または CIFS を使用して管理下システムにマウントします。
2. **概要 → セットアップ → 最初の起動デバイス** に移動します。
3. **最初の起動デバイス** ドロップダウンメニューで起動順序を **リモートファイル共有** に設定します。
4. **一回限りの起動** オプションを選択して、次のインスタンスについてのみ、管理下システムがイメージファイルを使って再起動するようにします。
5. **適用** をクリックします。
6. 管理下システムを再起動し、画面の指示に従って展開を完了します。

関連リンク

仮想メディアの設定
最初の起動デバイスの設定
リモートファイル共有の管理

リモートファイル共有の管理

リモートファイル共有（RFS）機能を使用すると、ネットワーク共有上にある ISO または IMG イメージファイルを設定し、NFS または CIFS を使ってそれを CD または DVD としてマウントすることにより、管理下サーバーのオペレーティングシステムから仮想ドライブとして使用できるようにすることができます。これはライセンスが必要な機能です。

メモ: IPv4 アドレスは、CIFS と NFS の両方でサポートされています。IPv6 アドレスは、CIFS でのみサポートされています。

リモートファイル共有では、イメージファイルフォーマット **.img** と **.iso** のみがサポートされます。**.img** ファイルは仮想フロッピーとしてリダイレクトされ、**.iso** ファイルは仮想 CDROM としてリダイレクトされます。

RFS のマウントを行うには、仮想メディアの権限が必要です。

メモ: 管理下システムで ESXi が実行されていて、リモートファイル共有を使用してフロッピーイメージ（**.img**）をマウントした場合、ESXi オペレーティングシステムでは連結されたフロッピーイメージを使用できません。

RFS の接続ステータスは iDRAC7 ログで提供されます。連結が完了すると、RFS マウントされた仮想ドライブは、iDRAC7 からログアウトしても切断されません。iDRAC7 がリセットされた場合、またはネットワーク接続が切断された場合は、RFS 接続が終了します。RFS 接続を終了するために、CMC および iDRAC7 でウェブインタフェースおよびコマンドラインオプションも使用できます。CMC からの RFS 接続は、iDRAC7 の既存の RFS マウントに常に優先します。

メモ: iDRAC7 VFlash 機能と RFS には、関連性がありません。

ウェブインタフェースを使用したリモートファイル共有の設定

リモートファイル共有を有効にするには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → 連結されたメディア** と移動します。
   連結されたメディア ページが表示されます。
2. **リモートファイル共有** で、連結または自動連結を選択して、ユーザー名、パスワード、およびイメージファイルのパスを指定します。詳細に関しては、『*iDRAC7 オンラインヘルプ*』を参照してください。
3. **適用** をクリックして、**接続** をクリックします。

接続が確立され、**接続ステータス** に接続済みと表示されます。

メモ: リモートファイル共有を設定した場合でも、セキュリティ上の理由から、ウェブインタフェースはユーザー資格情報を表示しません。

Linux ディストリビューションでは、この機能にランレベル init 3 での実行時における手動での mount コマンドの入力が必要な場合があります。コマンドの構文は、次のとおりです。

```
mount /dev/OS_specific_device / user_defined_mount_point
```

user_defined_mount_point は、他の mount コマンドの場合と同様に、マウント用に選択したディレクトリです。

RHEL の場合、CD デバイス（**.iso** 仮想デバイス）は /dev/scd0 で、フロッピーデバイス（**.img** 仮想デバイス）は /dev/sdc です。

SLES の場合、CD デバイスは /dev/sr0 で、フロッピーデバイスは is /dev/sdc です。正しいデバイスが使用されていることを確認するには（SLES または RHEL のいずれかの場合）、仮想デバイスの接続時に、Linux OS ですぐに次のコマンドを実行します。

```
tail /var/log/messages | grep SCSI
```

このコマンドを入力すると、デバイスを識別するテキスト（たとえば、SCSI device sdc）が表示されます。この手順は、ランレベル init 3 での Linux ディストリビューションの使用時の仮想メディアにも適用されます。デフォルトで、仮想メディアは init 3 では自動マウントされません。

RACADM を使用したリモートファイル共有の設定

RACADM を使用してリモートファイル共有を設定するには、次のコマンドを使用します。

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

オプションは、次のとおりです。

-c：イメージを連結

-d：イメージを分離

-u <ユーザー名>：ネットワーク共有にアクセスするユーザー名

-p <パスワード>：ネットワーク共有にアクセスするためのパスワード

-l <イメージの場所>：ネットワーク共有上のイメージの場所（場所を二重引用符で囲む）

-s：現在のステータスを表示

メモ: ユーザー名、パスワード、イメージの場所には、英数字と特殊文字を含むすべての文字（ただし、'（一重引用符）、"（二重引用符）、,（コンマ）、<（小なり記号）、>（大なり記号）は除く）を使用できます。

仮想メディアを使用したオペレーティングシステムの展開

仮想メディアを使用してオペレーティングシステムを展開する前に、次を確認してください。

- 起動順序に仮想ドライブが表示されるように、仮想メディアが *連結* 状態になっている。
- 仮想メディアが *自動連結* モードの場合、システムを起動する前に仮想メディアアプリケーションを起動する必要がある。
- ネットワーク共有に、ドライバおよびオペレーティングシステムのブータブルイメージファイルが **.img** または **.iso** などの業界標準のフォーマットで含まれている。

仮想メディアを使用してオペレーティングシステムを展開するには、次の手順を実行します。

1. 次の手順のいずれか 1 つを実行します。

- オペレーティングシステムのインストール CD または DVD を管理ステーションの CD ドライブまたは DVD ドライブに挿入します。
- オペレーティングシステムのイメージを連結します。

2. マップするために必要なイメージが保存されている管理ステーションのドライブを選択します。
3. 次のいずれか 1 つの方法を使用して、必要なデバイスから起動します。
   - iDRAC7 ウェブインタフェースを使用して、**仮想フロッピー**または**仮想 CD/DVD/ISO** から 1 回限りの起動を行うように起動順序を設定します。
   - 起動時に <F2> を押して、**セットアップユーティリティ → システム BIOS 設定** から起動順序を設定します
4. 管理下システムを再起動し、画面の指示に従って展開を完了します。

関連リンク

仮想メディアの設定
最初の起動デバイスの設定
iDRAC7 の設定

複数のディスクからのオペレーティングシステムのインストール

1. 既存の CD/DVD のマップを解除します。
2. リモート光学ドライブに次の CD/DVD を挿入します。
3. CD/DVD ドライブを再マップします。

SD カードの内蔵オペレーティングシステムの展開

SD カード上の内蔵ハイパーバイザをインストールするには、次の手順を実行します。

1. システムの内蔵デュアル SD モジュール（IDSDM）スロットに 2 枚の SD カードを挿入します。
2. BIOS で SD モジュールと冗長性（必要な場合）を有効にします。
3. 起動中に <F11> を押して、ドライブの 1 つで SD カードが使用可能かどうかを検証します。
4. 内蔵されたオペレーティングシステムを展開し、オペレーティングシステムのインストール手順に従います。

関連リンク

IDSDM について
BIOS での SD モジュールと冗長性の有効化

BIOS での SD モジュールと冗長性の有効化

BIOS で SD モジュールおよび冗長性を有効にするには、次の手順を実行します。

1. 起動中に <F2> を押します。
2. **セットアップユーティリティ → システム BIOS 設定 → 内蔵デバイス** と移動します。
3. **内蔵 USB ポート** を **オン** に設定します。これを **オフ** に設定した場合、IDSDM を起動デバイスとして使用できません。
4. 冗長性が必要でない場合は（単独の SD カード）、**内蔵 SD カードポート** を **オン** に設定し、**内蔵 SD カードの冗長性** を **無効** に設定します。
5. 冗長性が必要な場合は（2 枚の SD カード）、**内蔵 SD カードポート** を **オン** に設定し、**内蔵 SD カードの冗長性** を **ミラー** に設定します。
6. **戻る** をクリックして、**終了** をクリックします。

7. **はい** をクリックして設定を保存し、<Esc> を押して**セットアップユーティリティ**を終了します。

IDSDM について

内蔵デュアル SD モジュール（IDSDM）は、適切なプラットフォームのみで使用できます。IDSDM は、1 枚目の SD カードの内容をミラーリングする別の SD カードを使用して、ハイパーバイザ SD カードに冗長性を提供します。

2 枚の SD カードのどちらでもマスターにすることができます。たとえば、2 枚の新しい SD カードが IDSDM に装着されている場合、SD1 はアクティブ（マスター）カードであり、SD2 はスタンバイカードです。データは両方のカードに書き込まれますが、データの読み取りは SD1 から行われます。SD1 に障害が発生するか、取り外されたときには、常に SD2 が自動的にアクティブ（マスター）カードになります。

iDRAC7 ウェブインタフェースまたは RACADM を使用して、IDSDM のステータス、正常性、および可用性を表示できます。SD カードの冗長性ステータスおよびエラーイベントは SEL にログされ、前面パネルに表示されます。アラートが有効に設定されている場合は、PET アラートが生成されます。

関連リンク

センサー情報の表示

18

iDRAC7 を使用した管理下システムのトラブルシューティング

次を使用して、リモートの管理下システムの診断およびトラブルシューティングができます。

- 診断コンソール
- POST コード
- 起動キャプチャビデオおよびクラッシュキャプチャビデオ
- 前回のシステムクラッシュ画面
- システムイベントログ
- ライフサイクルログ
- 前面パネルステータス
- 問題の兆候
- システムの正常性

関連リンク

診断コンソールの使用
Post コードの表示
起動キャプチャとクラッシュキャプチャのビデオの表示
ログの表示
前回のシステムクラッシュ画面の表示
前面パネルステータスの表示
ハードウェア問題の兆候
システム正常性の表示

診断コンソールの使用

iDRAC7 では、Microsoft Windows または Linux ベースのシステムに含まれるツールと似たネットワーク診断ツールの標準セットが提供されます。ネットワークデバッグツールは、iDRAC7 ウェブインタフェースを使用してアクセスできます。

診断コンソールにアクセスするには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → トラブルシューティング → 診断** と移動します。
2. **コマンド** テキストボックスにコマンドを入力し、**送信** をクリックします。コマンドの詳細に関しては、『*iDRAC7 オンラインヘルプ*』を参照してください。

   結果は同じページに表示されます。

Post コードの表示

Post コードは、システム BIOS からの進行状況インジケータであり、パワーオンリセットからの起動シーケンスのさまざまな段階を示します。また、システムの起動に関するすべてのエラーを診断することも可能になります。**Post コード** ページには、オペレーティングシステムを起動する直前の Post コードが表示されます。

Post コードを表示するには、**概要 → サーバー → トラブルシューティング → Post コード** と移動します。

POST コード ページには、システムの正常性インジケータ、16 進数コード、およびコードの説明が表示されます。

起動キャプチャとクラッシュキャプチャのビデオの表示

次のビデオ記録を表示できます。

- 最後の 3 回の起動サイクル — 起動サイクルビデオでは、起動サイクルで発生した一連のイベントがログに記録されます。起動サイクルビデオは、最新の記録から順に並べられます。
- 最後のクラッシュビデオ — クラッシュビデオでは、障害に至った一連のイベントがログに記録されます。

これはライセンスが必要な機能です。

iDRAC7 は起動時に 50 フレームを記録します。起動画面の再生は、1 フレーム / 秒の速度で実行されます。ビデオは RAM に保存されており、リセットによって削除されるため、iDRAC7 をリセットすると起動キャプチャのビデオは利用できなくなります。

メモ: 起動キャプチャおよびクラッシュキャプチャのビデオを再生するには、仮想コンソールへのアクセス権限または管理者権限が必要です。

起動キャプチャ 画面を表示するには、**概要 → サーバー → トラブルシューティング → ビデオキャプチャ** の順にクリックします。

ビデオキャプチャ 画面にビデオ記録が表示されます。詳細は、『*iDRAC7 オンラインヘルプ*』を参照してください。

ログの表示

システムイベントログ（SEL）およびライフサイクルログを表示できます。詳細は、「システムイベントログの表示」および「ライフサイクルログの表示」を参照してください。

前回のシステムクラッシュ画面の表示

前回のクラッシュ画面機能は、最新のシステムクラッシュのスクリーンショットをキャプチャして保存し、iDRAC7 で表示します。これは、ライセンスが必要な機能です。

前回のクラッシュ画面を表示するには、次の手順を実行します。

1. 前回のシステムクラッシュ画面機能が有効になっていることを確認します。
2. iDRAC7 ウェブインタフェースで、**概要 → サーバー → トラブルシューティング → 前回のクラッシュ画面** と移動します。

   前回のクラッシュ画面 ページに、管理下システムの前回のクラッシュ画面が表示されます。

   前回のクラッシュ画面を削除するには、**クリア** をクリックします。

関連リンク

前回のクラッシュ画面の有効化

前面パネルステータスの表示

管理下システムの前面パネルには、システム内の次のコンポーネントのステータス概要が表示されます。

- バッテリ
- ファン
- イントルージョン
- 電源装置

- リムーバブルフラッシュメディア
- 温度
- 電圧

管理下システムの前面パネルの次のステータスを表示できます。

- ラックおよびタワーサーバーの場合：LCD 前面パネルおよびシステム ID LED ステータス、または LED 前面パネルおよびシステム ID LED ステータス
- ブレードサーバーの場合：システム ID LED のみ

システムの前面パネル LCD ステータスの表示

該当するラックサーバーおよびタワーサーバーの LCD 前面パネルステータスを表示するには、iDRAC7 ウェブインタフェースで、**概要 → ハードウェア → 前面パネル** と移動します。**前面パネル** ページが表示されます。

前面パネルライブフィード セクションには、LCD 前面パネルに現在表示されているメッセージのライブフィードが表示されます。システムが正常に動作していると（LCD 前面パネルでは青色の点灯で示されます）、**エラーを非表示にする** および **エラーを再表示する** の両方がグレー表示されます。エラーの表示と非表示は、ラックサーバーおよびタワーサーバーでのみ実行可能です。

RACADM を使用して LCD 前面パネルステータスを表示するには、`System.LCD` グループに属するオブジェクトを使用します。詳細については、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

関連リンク

LCD の設定

システムの前面パネル LED ステータスの表示

現在のシステム ID LED ステータスを表示するには、iDRAC7 ウェブインタフェースで、**概要 → ハードウェア → 前面パネル** と移動します。**前面パネルライブフィード** セクションには現在の前面パネルのステータスが表示されます。

- 青色の点灯 — 管理下システムにエラーはありません。
- 青色の点滅 — （管理下システムでのエラーの有無に関係なく）識別モードが有効です。
- 橙色の点灯 — 管理下システムはフェイルセーフモードです。
- 橙色の点滅 — 管理下システムでエラーが発生しています。

システムが正常に稼働していると（LED 前面パネルの青色の正常性アイコンで示されます）、**エラーを非表示にする** および **エラーを表示する** の両方がグレー表示されます。ラックサーバーおよびタワーサーバーについてのみエラーの表示または再表示が可能です。

RACADM を使用してシステム ID LED ステータスを表示するには、**getled** コマンドを使用します。詳細に関しては、**support.dell.com/manuals** にある『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

関連リンク

システム ID LED の設定

ハードウェア問題の兆候

ハードウェア関連の問題には次のものがあります。

- 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
- ハードディスクドライブの不具合
- USB メディアエラー
- 物理的損傷

問題に基づいて、次の方法で問題を修正します。

- モジュールまたはコンポーネントを装着し直して、システムを再起動
- ブレードサーバーの場合は、モジュールをシャーシ内の異なるベイに挿入
- ハードディスクドライブまたは USB フラッシュドライブを交換
- 電源およびネットワークケーブルを再接続 / 交換

問題が解決しない場合は、『*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に関する特定のトラブルシューティングを参照してください。

△ **注意: 製品マニュアルで許可されている、またはオンライン / 電話サービスやサポートチームにより指示されたトラブルシューティングや簡単な修理のみを行うようにしてください。デルが許可していない修理による損傷は、保証の対象にはなりません。製品に同梱の安全にお使いいただくための注意をお読みになり、指示に従ってください。**

システム正常性の表示

iDRAC7 および CMC（ブレードサーバーの場合）ウェブインタフェースには、次のアイテムのステータスが表示されます。

- バッテリ
- ファン
- イントルージョン
- 電源装置
- リムーバブルフラッシュメディア
- 温度
- 電圧
- CPU

iDRAC7 ウェブインタフェースで、**概要 → サーバー → システムサマリ → サーバー正常性** セクション、と移動します。

CPU の状態を表示するには、**概要 → ハードウェア → CPU** と進みます。

システム正常性インジケータは次のとおりです。

-  — 通常のステータスを示します。
-  — 警告ステータスを示します。
-  — 障害ステータス
-  — 不明ステータスを示します。

コンポーネントの詳細を表示するには、**サーバー正常性** セクションで任意のコンポーネント名をクリックします。

サーバーステータス画面でのエラーメッセージの確認

橙色 LED が点滅し、特定のサーバーにエラーが発生した場合、LCD のメインサーバーステータス画面に、エラーがあるサーバーがオレンジ色でハイライト表示されます。LCD ナビゲーションボタンを使用してエラー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。LCD パネルに表示されるエラーメッセージのリストについては、サーバーのオーナーズマニュアルを参照してください。

iDRAC7 の再起動

サーバーの電源を切らずに、iDRAC7 のハード再起動あるいはソフト再起動を実行できます。

- ハード再起動 — サーバーで、LED ボタンを 15 秒間押し続けます。
- ソフト再起動 — iDRAC7 ウェブインタフェースまたは RACADM を使用します。

iDRAC7 ウェブインタフェースを使用した iDRAC7 のリセット

iDRAC7 をリセットするには、iDRAC7 ウェブインタフェースで次のいずれかを実行します。

- **概要** → **サーバー** → **サマリ** と進みます。**クイック起動タスク** で、**iDRAC のリセット** をクリックします。
- **概要** → **サーバー** → **トラブルシューティング** → **診断** と進みます。**iDRAC のリセット** をクリックします。

RACADM を使用した iDRAC7 のリセット

iDRAC7 を再起動するには、**racreset** コマンドを使用します。詳細に関しては、**support.dell.com/manuals** にある『*iDRAC7 および CMC 向け RACADM リファレンスガイド*』を参照してください。

工場出荷時のデフォルト設定への iDRAC7 のリセット

工場出荷時のデフォルト設定への iDRAC7 のリセットは、iDRAC 設定ユーティリティを使用するか、ファームウェアのアップデートを実行中に **設定を保存する** オプションの選択を解除することによって実行できます。

iDRAC 設定ユーティリティを使用して iDRAC7 を工場出荷時のデフォルト値にリセットするには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**iDRAC 設定のデフォルトへのリセット** を選択します。
   iDRAC 設定のデフォルトへのリセット ページが表示されます。
2. **はい** をクリックします。iDRAC のリセットが開始されます。
3. **戻る** をクリックして、同じ **iDRAC 設定のデフォルトへのリセット** ページに移動し、リセットの成功を示すメッセージを確認します。

19

よくあるお問い合わせ

本項では、次に関するよくあるお問い合わせをリストします。

システムイベントログ

Internet Explorer で iDRAC7 ウェブインタフェースを使用する場合、名前を付けて保存 オプションを使用して SEL が保存されないのはなぜですか。

これは、ブラウザ設定が原因です。この問題を解決するには、次の手順を実行してください。

1. Internet Explorer で、**ツール → インターネット オプション → セキュリティ** と移動し、ダウンロードするゾーンを選択します。

   たとえば、iDRAC7 デバイスがローカルイントラネット上にある場合は、**ローカルイントラネット** を選択して **レベルのカスタマイズ...** をクリックします。
2. **セキュリティ設定** ウィンドウの **ダウンロード** で、次のオプションが有効になっていることを確認します。
   - ファイルのダウンロード時に自動的にダイアログを表示（このオプションを使用できる場合）
   - ファイルのダウンロード

注意: iDRAC7 へのアクセスに使用されるコンピュータの安全性を確実にするため、その他 で アプリケーションと安全でないファイルの起動 オプションは有効にしないでください。

ネットワークセキュリティ

iDRAC7 ウェブインタフェースへのアクセス中に、認証局（CA）で発行された SSL 証明書が信頼できないことを示すセキュリティ警告が表示されます。

iDRAC7 にはデフォルトの iDRAC7 サーバー証明書が含まれており、ウェブベースのインタフェースおよびリモート RACADM を介したアクセス中のネットワークセキュリティを確保します。この証明書は、信頼できる CA によって発行されたものではありません。この問題を解決するには、信頼できる CA（たとえば、Microsoft 認証局、Thawte、または Verisign）によって発行された iDRAC7 サーバー証明書をアップロードします。

DNS サーバーが iDRAC7 を登録しないのはどうしてですか?

一部の DNS サーバーは、最大 31 文字の iDRAC7 名しか登録しません。

iDRAC7 ウェブベースインタフェースにアクセスすると、SSL 証明書のホスト名が iDRAC7 ホスト名と一致しないことを示すセキュリティ警告が表示されます。

iDRAC7 にはデフォルトの iDRAC7 サーバー証明書が含まれており、ウェブベースのインタフェースおよびリモート RACADM を介したアクセス中のネットワークセキュリティを確保します。この証明書が使用される場合、iDRAC7 に発行されたデフォルトの証明書が iDRAC7 ホスト名（たとえば、IP アドレス）に一致しないため、ウェブブラウザにセキュリティ警告が表示されます。

この問題を解決するには、その IP アドレスまたは iDRAC7 ホスト名に対して発行された iDRAC7 サーバー証明書をアップロードします。証明書の発行に使用された CSR の生成時には、CSR のコモンネームと iDRAC7 IP アドレス（証明書が IP に対して発行された場合）または DNS iDRAC7 の登録名（証明書が iDRAC7 登録名に対して発行された場合）を一致させます。

CSR が DNS iDRAC7 の登録名と一致することを確実にするには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → iDRAC 設定 → ネットワーク** と移動します。**ネットワーク** ページが表示されます。
2. **共通設定** セクションで次の手順を実行します。
   - **iDRAC の DNS への登録** オプションを選択します
   - **DNS iDRAC 名** フィールドに iDRAC7 名を入力します。
3. **Apply**（適用） をクリックします。

Active Directory

Active Directory へのログインに失敗しました。どのように解決すればよいですか?

問題を診断するには、**Active Directory の設定と管理** ページで **設定のテスト** をクリックします。テスト結果を確認して問題を解決します。テストユーザーが認証手順に合格するまで、設定を変更して、テストを実施します。

一般的には、次を確認します。

- ログイン時には、NetBIOS 名ではなく、適切なユーザードメイン名を使用します。ローカル iDRAC7 ユーザーアカウントが設定されている場合は、ローカル資格情報を使用して iDRAC7 にログインします。ログイン後は、次を確認します。
  - **Active Directory 設定と管理** ページで **Active Directory の有効化** オプションがオンになっている。
  - **iDRAC7 ネットワーク設定** ページで DNS が正しく設定されている。
  - 証明書の検証が有効の場合、正しい Active Directory のルート CA 証明書が iDRAC7 にアップロードされている。
  - 拡張スキーマを使用している場合、iDRAC 名および iDRAC ドメイン名が Active Directory の環境設定に一致する。
  - 標準スキーマを使用している場合、グループ名とグループドメイン名が Active Directory 設定に一致する。
- ドメインコントローラの SSL 証明書で、iDRAC7 の日付が証明書の有効期間内であることを確認します。

証明書の検証が有効の場合でも、Active Directory へのログインに失敗します。テスト結果には、次のエラーメッセージが表示されます。このエラーが発生するのはなぜですか? どのように解決すればよいですか?

エラー：LDAP サーバーにアクセスできません、エラー：14090086：SSL ルーチン：SSL3_GET_SERVER_CERTIFICATE：証明書の検証が失敗しました：正しい認証局（CA）の証明書が iDRAC7 にアップロードされていることを確認してください。また、iDRAC7 の日付が証明書の有効期間内であること、および iDRAC7 で設定されたドメインコントローラアドレスがディレクトリサーバー証明書のサブジェクトと一致することも確認してください。

証明書の検証が有効の場合、iDRAC7 がディレクトリ サーバーとの SSL 接続を確立すると、iDRAC7 はアップロードされた CA 証明書を使用してディレクトリサーバー証明書を検証します。証明書の検証に失敗する主な理由は次のとおりです。

- iDRAC7 の日付がサーバー証明書または CA 証明書の有効期間内ではない。iDRAC7 の日付と証明書の有効期間を確認してください。
- iDRAC7 で設定されたドメインコントローラアドレスがディレクトリサーバー証明書のサブジェクトまたはサブジェクト代替名と一致しない。IP アドレスを使用している場合は、次の質問をご覧ください。FQDN を使用している場合は、ドメインではなく、ドメインコントローラの FQDN を使用していることを確認します。たとえば、**example.com** ではなく、**servername.example.com** を使用します。

IP アドレスをドメインコントローラアドレスとして使用しても証明書の検証に失敗します。どのように解決すればよいですか?

ドメインコントローラ証明書のサブジェクトフィールドまたはサブジェクト代替名フィールドを確認します。通常、Active Directory は、ドメインコントローラ証明書のサブジェクトフィールドまたはサブジェクト代替名フィールドには、ドメインコントローラの IP アドレスではなく、ホスト名を使用します。これを解決するには、次の手順のいずれかを実行します。

- サーバー証明書のサブジェクトまたはサブジェクト代替名と一致するように、iDRAC7 でドメインコントローラのホスト名（FQDN）を *ドメインコントローラアドレス*として設定します。
- iDRAC7 で設定された IP アドレスと一致する IP アドレスをサブジェクトフィールドまたはサブジェクト代替名フィールドで使用するようにサーバー証明書を再発行します。
- SSL ハンドシェイク中の証明書の検証なしでドメインコントローラを信頼することを選択した場合は、証明書の検証を無効にします。

複数ドメイン環境で拡張スキーマを使用している場合は、ドメインコントローラアドレスをどのように設定しますか?

このアドレスは、iDRAC7 オブジェクトが属するドメイン用のドメインコントローラのホスト名（FQDN）または IP アドレスである必要があります。

グローバルカタログアドレスを設定するのはいつですか?

標準スキーマを使用しており、ユーザーおよび役割グループが異なるドメインに属する場合は、グローバルカタログアドレスが必要です。この場合、ユニバーサルグループのみを使用できます。

標準スキーマを使用し、すべてのユーザーおよび役割グループが同じドメインに属する場合は、グローバルカタログアドレスは必要はありません。

拡張スキーマを使用している場合、グローバルカタログアドレスは使用されません。

標準スキーマクエリの仕組みを教えてください。

iDRAC7 は、まず設定されたドメインコントローラアドレスに接続し、ユーザーおよび役割グループがそのドメインにある場合は、権限が保存されます。

グローバルコントローラアドレスが設定されている場合、iDRAC7 はグローバルカタログのクエリを続行します。グローバルカタログから追加の権限が検出された場合、これらの権限は蓄積されます。

iDRAC7 は、常に LDAP over SSL を使用しますか?

はい。すべての転送は、安全なポート 636 および 3269 の両方またはいずれか一方を使用して行われます。テスト設定では、iDRAC7 は問題を分離するためだけに LDAP 接続を行います。安全ではない接続で LDAP バインドを実行することはありません。

iDRAC7 で、証明書の検証がデフォルトで有効になっているのはなぜですか?

iDRAC7 は、iDRAC7 が接続するドメインコントローラの ID を保護するために強力なセキュリティを施行します。証明書の検証なしでは、ハッカーがドメインコントローラを偽造し、SSL 接続を乗っ取ることが可能になります。証明書の検証を行わずにセキュリティ境界内のすべてのドメインコントローラを信頼することを選択する場合、これはウェブインタフェースまたは RACADM から証明書の検証を無効にできます。

iDRAC7 は NetBIOS 名をサポートしていますか?

このリリースでは、サポートされていません。

Active Directory のシングルサインオンまたはスマートカードログインを使用して iDRAC7 にログインするのに最大 4 分かかるのはなぜですか?

通常、Active Directory のシングルサインオンまたはスマートカードログインにかかる時間は 10 秒未満ですが、優先 DNS サーバーおよび代替 DNS サーバーを指定しており、優先 DNS サーバーで障害が発生すると、ログインに最大 4 分かかる場合があります。DNS サーバーがダウンしている場合は、DNS タイムアウトが発生します。iDRAC7 は、代替 DNS を使用してユーザーをログインします。

Active Directory は、Windows Server 2008 の Active Directory に属するドメイン用に設定されています。ドメインには子ドメイン、つまりサブドメインが存在し、ユーザーおよびグループは同じ子ドメインに属します。ユーザーは、このドメインのメンバーです。子ドメインに属するユーザーを使用して iDRAC7 にログインしようとすると、Active Directory のシングルサインオンログインが失敗します。

これは、誤ったグループタイプが原因です。Active Directory サーバーには 2 種類のグループタイプがあります。

- セキュリティ — セキュリティグループでは、ユーザーとコンピュータによる共有リソースへのアクセスの管理や、グループポリシー設定のフィルタが可能です。
- 配布 — 配布グループは、電子メール配布リストとして使用することだけが目的です。

グループタイプは、常にセキュリティにするようにしてください。配布グループはグループポリシー設定のフィルタに使用しますが、オブジェクトへの許可の割り当てに使用することはできません。

シングルサインオン

Windows Server 2008 R2 x64 で SSO ログインが失敗します。これを解決するには、どのような設定が必要ですか?

1. ドメインコントローラとドメインポリシーに対して **technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** を実行します。
2. DES-CBC-MD5 暗号スイートを使用するようにコンピュータを設定します。
   これらの設定は、クライアントコンピュータ、またはお使いの環境内のサービスとアプリケーションとの互換性に影響を与える場合があります。Kerberos ポリシー設定に許可される暗号化タイプは、**コンピュータ設定 → セキュリティ設定 → ローカルポリシー → セキュリティオプション** にあります。
3. ドメインクライアントに、アップデート済みの GPO があることを確認してください。
4. コマンドラインで `gpupdate /force` と入力し、古いキータブを `klist purge` コマンドで削除します。
5. GPO を更新したら、新しいキータブを作成します。
6. キータブを iDRAC7 にアップロードします。

これで、SSO を使用して iDRAC7 にログインできます。

Windows 7 と Windows Server 2008 R2 の Active Directory ユーザーで SSO ログインが失敗するのはなぜですか?

Windows 7 と Windows Server 2008 R2 の暗号化タイプを有効にする必要があります。暗号化タイプの有効化には、次の手順を実行します。

1. システム管理者としてログインするか、管理者権限を持つユーザーとしてログインします。
2. **スタート** から **gpedit.msc** を実行します。**ローカルグループポリシーエディタ** ウィンドウが表示されます。
3. **ローカルコンピュータ設定 → Windows 設定 → セキュリティ設定 → ローカルポリシー → セキュリティオプション** と移動します。
4. **ネットワークセキュリティ : kerberos に許可される暗号化方式の設定** を右クリックして、**プロパティ** を選択します。
5. すべてのオプションを有効にします。

6. **OK** をクリックします。これで、SSO を使用して iDRAC7 にログインできます。

拡張スキーマでは、次の追加設定を行います。

1. **ローカルグループポリシーエディタ** ウィンドウで、**ローカルコンピュータ設定 → Windows 設定 → セキュリティ設定 → ローカルポリシー → セキュリティオプション** と移動します。
2. **ネットワークセキュリティ：NTLM の制限：リモートサーバーへの発信 NTLM トラフィック** を右クリックして **プロパティ** を選択します。
3. **すべて許可** を選択し、**OK** をクリックしてから、**ローカルグループポリシーエディタ** ウィンドウを閉じます。
4. **スタート** から cmd を実行します。コマンドプロンプトウィンドウが表示されます。
5. `gpupdate /force` コマンドを実行します。グループポリシーがアップデートされます。コマンドプロンプトウィンドウを閉じます。
6. **スタート** から regedit を実行します。**レジストリエディタ** ウィンドウが表示されます。
7. **HKEY_LOCAL_MACHINE → System → CurrentControlSet → Control → LSA** と移動します。
8. 右ペインで、**新規 → DWORD（32 ビット）値** を右クリックして選択します。
9. 新しいキーを **SuppressExtendedProtection** と名付けます。
10. **SuppressExtendedProtection** を右クリックして、**変更** をクリックします。
11. **値データ** フィールドに **1** を入力して **OK** をクリックします。
12. **レジストリエディタ** ウィンドウを閉じます。これで、SSO を使用して iDRAC7 にログインできます。

iDRAC7 用に SSO を有効にし、Internet Explorer を使って iDRAC7 にログインすると、SSO が失敗し、ユーザー名とパスワードの入力を求められます。どのように解決すればよいですか?

iDRAC7 の IP アドレスが **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** のリストに表示されていることを確認してください。リストに表示されていない場合は、SSO が失敗し、ユーザー名とパスワードの入力を求められます。**キャンセル** をクリックして、先に進んでください。

スマートカードログイン

Active Directory スマートカードログインを使用して iDRAC7 にログインするには最大 4 分かかります。

通常の Active Directory スマートカードログインにかかる時間は 10 秒未満ですが、**ネットワーク** ページで優先 DNS サーバーおよび代替 DNS サーバーを指定しており、優先 DNS サーバーで障害が発生すると、ログインに最大 4 分かかる場合があります。DNS サーバーがダウンしている場合は、DNS タイムアウトが発生します。iDRAC7 は、代替 DNS を使用してユーザーをログインします。

ActiveX プラグインがスマートカードリーダーを検出しません。

スマートカードが Microsoft Windows オペレーティングシステムでサポートされていることを確認します。Windows は、限られた数のスマートカード暗号化サービスプロバイダ（CSP）しかサポートしません。

一般的に、スマートカード CSP が特定のクライアントに存在するかどうかを確認するには、Windows のログオン（Ctrl-Alt-Del）画面でスマートカードをリーダーに挿入して、Windows がスマートカードを検出し、PIN ダイアログボックスを表示するかどうかをチェックします。

間違ったスマートカード PIN です。

間違った PIN での試行回数が多すぎたためにスマートカードがロックされていないかをチェックします。このような場合は、組織のスマートカード発行者に問い合わせて、新しいスマートカードを取得してください。

仮想コンソール

iDRAC7 ウェブインタフェースからログアウトしても、仮想コンソールがアクティブです。これは正常な動作ですか?

はい。仮想コンソールビューアウィンドウを閉じて、対応するセッションからログアウトしてください。

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。

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 iDRAC7 が受信すると、ビデオはすぐにオンになります。

ローカルユーザーもビデオをオフにしたり、オンしたりできますか?

ローカルコンソールを無効にすると、ローカルユーザーがビデオをオフにしたり、オンにしたり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なりますか?

いいえ。

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。

iDRAC7 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?

iDRAC7 設定権限を持っているすべてのユーザーが、ローカルコンソールをオンにしたり、オフにしたりできます。

ローカルサーバービデオの現在のステータスは、どのように取得しますか?

ステータスは、仮想コンソールページに表示されます。

`cfgRacTuneLocalServerVideo` オブジェクトのステータスを表示するには、RACADM コマンドの `racadm getconfig -g cfgRacTuning` を使用します。

または、Telnet、SSH、またはリモートセッションから次の RACADM コマンドを使用します。

```
racadm -r (iDRAC IP) -u -p getconfig -g cfgRacTuning
```

このステータスは、仮想コンソール OSCAR ディスプレイにも表示されます。ローカルコンソールが有効の場合、サーバー名の横に緑色のステータスが表示されます。無効の場合には、黄色の丸が表示され、iDRAC7 によってローカルコンソールがロックされていることが示されます。

システム画面の一番下が仮想コンソールウィンドウに表示されないのはなぜですか?

管理ステーションのモニターの解像度が 1280 x 1024 に設定されていることを確認してください。

Linux オペレーティングシステムで仮想コンソールビューアウィンドウが文字化けするのはなぜですか?

Linux でコンソールビューアを使用するには、UTF-8 文字セットが必要です。お使いのロケールを確認し、必要に応じて文字セットをリセットします。

ライフサイクルコントローラの Linux テストコンソールでマウスが同期しないのはなぜですか?

仮想コンソールでは USB マウスドライバが必要ですが、USB マウスドライバは X-Window オペレーティングシステムでのみ使用できます。仮想コンソールビューアで、次の手順のいずれかを実行します。

- **ツール → セッションオプション → マウス** タブと移動します。**マウス加速度** で **Linux** を選択します。
- **ツール** メニューで **シングルカーソル** オプションを選択します。

仮想コンソールビューアウィンドウでマウスポインタを同期させるには、どうすればよいですか?

仮想コンソールセッションを開始する前に、オペレーティングシステムに対して正しいマウスが選択されていることを確認します。

iDRAC7 仮想コンソールクライアントで、iDRAC7 仮想コンソールメニューの **ツール** にある **シングルカーソル** オプションが選択されていることを確認します。デフォルトは、2 カーソルモードです。

仮想コンソールから Microsoft オペレーティングシステムをリモートでインストールしている間に、キーボードまたはマウスを使用できますか?

いいえ。BIOS で有効に設定された仮想コンソールを使用して、サポートされている Microsoft オペレーティングシステムをシステムにリモートインストールするときは、リモートで **OK** を選択する必要のある EMS 接続メッセージが送信されます。ローカルシステムで **OK** を選択するか、リモートで管理されているサーバーを再起動し、再インストールしてから、BIOS で仮想コンソールをオフにする必要があります。

このメッセージは、仮想コンソールが有効に設定されていることをユーザー警告するためにマイクロソフト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ため、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は、常に iDRAC 設定ユーティリティで仮想コンソールをオフにするようにします。

管理ステーションの Num Lock インジケータがリモートサーバーの Num Lock インジケータのステータスを反映しないのはなぜですか?

iDRAC7 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、リモートサーバーの Num Lock の状態と必ずしも一致しません。Num Lock の状態は、管理ステーションの Num Lock の状態に関わらず、リモートセッション接続時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仮想コンソール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?

ローカルシステムから仮想コンソールセッションを設定していますが、これはサポートされていません。

仮想コンソールセッションが進行中であり、ローカルユーザーが管理下サーバーにアクセスすると、最初のユーザーは警告メッセージを受信しますか?

いいえ。ローカルユーザーがシステムにアクセスすると、双方がシステムを制御することになります。

仮想コンソールセッションの実行に必要な帯域幅はどのくらいですか?

良パフォーマンスを得るためには、5 MBPS の接続をお勧めします。最低限のパフォーマンスのためには、1 MBPS の接続が必要です。

管理ステーションで仮想コンソールを実行するために最低限必要なシステム要件は何ですか?

管理ステーションには、Intel Pentium III 500 MHz プロセッサと最低限 256 MB の RAM が必要です。

仮想コンソールビューアウィンドウに信号無しメッセージが表示されることがあるのはなぜですか?

このメッセージが表示される理由としては、iDRAC7 仮想コンソールプラグインがリモートサーバーのデスクトップビデオを受信していないことが考えられます。一般に、この動作はリモートサーバーの電源がオフになっている場合に発生します。時折、リモートサーバーのデスクトップビデオ受信の誤作動が原因でこのメッセージが表示されることもあります。

仮想コンソールビューアウィンドウに範囲外メッセージが表示されることがあるのはなぜですか?

このメッセージが表示される理由としては、ビデオのキャプチャに必要なパラメータが、iDRAC7 がビデオをキャプチャできる範囲を超えていることが考えられます。画面解像度とリフレッシュレートなどのパラメータが高すぎると、範囲外状態を引き起こします。通常、ビデオメモリの容量、または帯域幅によってパラメータの最大範囲が設定されます。

iDRAC7 ウェブインタフェースから仮想コンソールのセッションを開始すると、ActiveX セキュリティポップアップが表示されるのはなぜですか?

iDRAC7 が信頼済みサイトリストに含まれていない可能性があります。仮想コンソール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が表示されないようにするには、クライアントブラウザで iDRAC7 を信頼済みリストに追加します。

1. **ツール** → **インターネットオプション** → **セキュリティ** → **信頼済みリスト** とクリックします。
2. **サイト** をクリックして iDRAC7 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。

4. **カスタムレベル** をクリックします。
5. **セキュリティ設定** ウィンドウの **署名なしの ActiveX Controls のダウンロード** で **プロンプト** を選択します。

仮想コンソールビューアウィンドウに何も表示されないのはなぜですか?

仮想コンソール権限ではなく、仮想メディア権限を持っている場合、ビューアを起動して仮想メディア機能にアクセスすることはできますが、管理下サーバーのコンソールは表示されません。

仮想コンソールを使用しているときに DOS でマウスが同期しないのはなぜですか?

Dell BIOS は、マウスドライバを PS/2 マウスとしてエミュレートします。設計上、PS/2 マウスはマウスポインタに相対位置を使用するので、同期に遅れが生じます。iDRAC7 には USB マウスドライバが装備されているので、絶対位置とマウスポインタの緻密な追跡が可能になります。iDRAC7 が USB マウスの絶対位置を Dell BIOS に渡したとしても、BIOS エミュレーションにより相対位置に変換されるため、この遅れは生じたままとなります。この問題を解決するには、設定画面でマウスモードを USC/Diags に設定します。

仮想コンソールを起動すると、仮想コンソールでのマウスカーソルはアクティブですが、ローカルシステムでのマウスカーソルがアクティブではありません。この原因はなんですか? どのように解決すればよいですか?

これは、**マウスモード** を **USC/Diags** に設定した場合に発生します。ローカルシステムでマウスを使用するには、**Alt + M** ホットキーを押します。仮想コンソールでマウスを使用するには、もう一度 **Alt + M** を押します。

仮想コンソールの起動直後に CMC ウェブインタフェースから iDRAC7 ウェブインタフェースを起動すると、GUI セッションがタイムアウトになるのはなぜですか?

CMC ウェブインタフェースから iDRAC7 に仮想コンソールを起動すると、仮想コンソールを起動するためのポップアップが開きます。このポップアップは、仮想コンソールを開いてしばらくすると閉じます。

管理ステーション上で GUI と仮想コンソールの両方を同じ iDRAC7 システムに起動した場合、ポップアップが閉じる前に GUI が起動されると、iDRAC7 GUI のセッションタイムアウトが発生します。仮想コンソールのポップアップが閉じた後で CMC ウェブインタフェースから iDRAC7 GUI が起動されると、この問題は発生しません。

Linux SysRq キーが Internet Explorer で機能しないのはなぜですか?

Internet Explorer から仮想コンソールを使用する場合は、Linux SysRq キーの動作が異なります。SysRq キーを送信するには、**Ctrl** キーと **Alt** キーを押したまま、**Print Screen** キーを押して放します。Internet Explorer の使用中に、iDRAC7 を介してリモートの Linux サーバーに SysRq キーを送信するには、次の手順を実行します。

1. リモートの Linux サーバーでマジックキー機能を有効にします。Linux 端末でこの機能を有効にするには、次のコマンドを使用できます。
   ```
   echo 1 > /proc/sys/kernel/sysrq
   ```
2. Active X ビューアのキーボードパススルーモードを有効にします。
3. **Ctrl + Alt + Print Screen** を押します。
4. **Print Screen** のみを放します。
5. **Print Screen+Ctrl+Alt** を押します。

メモ: Internet Explorer および Java では、SysRq 機能は現在サポートされていません。

仮想コンソールの下部に「リンクが切断されました」メッセージが表示されるのはなぜですか?

サーバーの再起動中に共有ネットワークポートを使用すると、BIOS がネットワークカードをリセットしている間は iDRAC が切断されます。10 Gb カードでは切断時間が長くなり、接続されているネットワークスイッチでスパニングツリープロトコル（STP）が有効に設定されている場合には、この時間がことのほか長くなります。この場合、サーバーに接続されているスイッチポートの「portfast」を有効にすることをお勧めします。多くの場合、仮想コンソールは自己回復します。

仮想メディア

仮想メディアクライアントの接続が切断することがあるのはなぜですか?

ネットワークのタイムアウトが発生すると、iDRAC7 ファームウェアはサーバーと仮想ドライブ間の接続をドロップし、接続を中断します。

クライアントシステムで CD を変更した場合、新しい CD に自動開始機能が備わっている場合があります。この場合、クライアントシステムが CD 読み取りに時間をかけすぎると、ファームウェアがタイムアウトすることがあり、接続が失われます。接続が失われた場合は、GUI から再接続して、以前の操作を続行してください。

仮想メディアの設定を iDRAC7 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変更した場合、設定変更の適用時に接続しているすべてのメディアが切断されます。

仮想ドライブを再接続するには、仮想メディアの **クライアントビュー** ウィンドウを使用します。

仮想メディアからの Windows オペレーティングシステムのインストールに長時間かかるのはなぜですか?

『*Dell Systems Management Tools and Documentation DVD*』を使用して Windows オペレーティングシステムをインストールしており、ネットワーク接続の速度が遅い場合、ネットワーク遅延が原因で、iDRAC7 ウェブインタフェースへのアクセスに長時間かかることがあります。インストールウィンドウには、インストールの進捗状況が示されません。

仮想デバイスを起動可能なデバイスとして設定するにはどうすればよいですか?

管理下システムで BIOS セットアップにアクセスし、起動メニューに移動します。仮想 CD、仮想フロッピー、または vFlash を探し、必要に応じてデバイスの起動順序を変更します。また、CMOS セットアップの起動順序で「スペースバー」キーを押して、仮想デバイスを起動可能にします。たとえば、CD ドライブから起動するには、CD ドライブを起動順序 1 番目のデバイスに設定します。

起動可能なデバイスとして設定できるメディアのタイプは?

iDRAC7 では、次の起動可能な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する USB キー
- USB キーイメージ

USB キーを起動可能なデバイスにするにはどうすればよいですか?

support.dell.com で Dell Boot Utility を検索してください。

Windows 98 の起動ディスクで起動して、起動ディスクから USB キーにシステムファイルをコピーすることもできます。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
```

ここで x: は起動可能なデバイスとして設定する必要のある USB キーです。

仮想メディアが連結済みであり、リモートフロッピーに接続されていますが、Red Hat Enterprise Linux または SUSE Linux オペレーティングシステムを実行するシステムで仮想フロッピー / 仮想 CD デバイスが見つかりません。どのように解決すればよいですか?

一部の Linux バージョンは、仮想フロッピードライブおよび仮想 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 が仮想フロッピードライブに割り当てるデバイスノードを確認します。仮想フロッピードライブをマウントするには、次の手順を実行します。

1. Linux コマンドプロンプトを開き、次のコマンドを実行します。
   ```
   grep "Virtual Floppy" /var/log/messages
   ```

2. そのメッセージの最後のエントリを確認し、その時刻を書きとめます。
3. Linux のプロンプトで次のコマンドを実行します。
   ```
   grep "hh:mm:ss" /var/log/messages
   ```
   ここで hh:mm:ss は、手順 1 で grep から返されたメッセージのタイムスタンプです。
4. 手順 3 で、grep コマンドの結果を読み、仮想フロッピーに与えられたデバイス名を確認します。
5. 仮想フロッピードライブに連結済みであり、接続されていることを確認します。
6. Linux のプロンプトで次のコマンドを実行します。
   ```
   mount /dev/sdx /mnt/floppy
   ```
   ここで /dev/sdx は手順 4 で確認したデバイス名であり、/mnt/floppy はマウントポイントです。

仮想 CD ドライブをマウントするには、Linux が仮想 CD ドライブに割り当てるデバイスノードを確認します。仮想 CD ドライブをマウントするには、次の手順を実行します。

1. Linux コマンドプロンプトを開き、次のコマンドを実行します。
   ```
   grep "Virtual Floppy" /var/log/messages
   ```
2. そのメッセージの最後のエントリを確認し、その時刻を書きとめます。
3. Linux のプロンプトで次のコマンドを実行します。
   ```
   grep "hh:mm:ss" /var/log/messages
   ```
   ここで hh:mm:ss は、手順 1 で grep から返されたメッセージのタイムスタンプです。
4. 手順 3 で、grep コマンドの結果を読み、*Dell 仮想* CD に与えられたデバイス名を確認します。
5. 仮想 CD ドライブが連結済みであり、接続されていることを確認します。
6. Linux のプロンプトで次のコマンドを実行します。
   ```
   mount /dev/sdx /mnt/CD
   ```
   ここで /dev/sdx は手順 4 で確認したデバイス名であり、/mnt/floppy はマウントポイントです。

iDRAC7 ウェブインタフェースを使用してリモートファームウェアアップデートを実行した後に、サーバーに連結されていた仮想ドライブが削除されるのはなぜですか?

ファームウェアのアップデートにより iDRAC7 がリセットされてリモート接続が中断し、仮想ドライブがアンマウントされました。これらのドライブは、iDRAC7 のリセットが完了すると再表示されます。

USB デバイスの接続後にすべての USB デバイスの接続が解除されるのはなぜですか?

仮想メディアデバイスと vFlash デバイスは複合 USB デバイスとしてホスト USB バスに接続されており、共通の USB ポートを共有しています。いずれかの仮想メディアまたは vFlash USB デバイスがホスト USB バスに対して接続されるか、接続解除されると、すべての仮想メディアおよび vFlash デバイスの接続がホスト USB バスから一時解除され、再び接続されます。ホストオペレーティングシステムが仮想メディアを使用している場合には、1 つ、または複数の仮想メディアまたは vFlash デバイスを連結したり、分離したりしないでください。USB デバイスを使用する前に、必要な USB デバイスすべてを接続することをお勧めします。

USB リセットの機能とは何ですか?

サーバーに接続されているリモートおよびローカル USB デバイスをリセットします。

仮想メディアのパフォーマンスを最大化するにはどうしますか?

仮想メディアのパフォーマンスを最大化するには、仮想コンソールを無効にして仮想メディアを起動するか、次のいずれかの手順を実行します。

- パフォーマンススライダを最大速度に変更します。
- 仮想メディアと仮想コンソールの両方の暗号化を無効にします。

メモ: この場合、管理下サーバーと、仮想メディアおよび仮想コンソール用 iDRAC7 間のデータ転送はセキュア化されません。

- Windows Server オペレーティングシステムを使用している場合は、Windows イベントコレクタという名前の Windows サービスを停止します。この操作を実行するには、**スタート → 管理ツール → サービス** と移動します。**Windows イベントコレクタ** を右クリックし、**停止** をクリックします。

フロッピードライブまたは USB の内容の表示中、仮想メディアを介して同じドライブが連結されると、接続エラーメッセージが表示されます。

仮想フロッピードライブへの同時アクセスは許可されません。ドライブの内容を表示するために使用されるアプリケーションを閉じてから、ドライブの仮想化を試行してください。

仮想フロッピードライブでサポートされているファイルシステムのタイプは?

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。

現在仮想メディアを使用していなくても、仮想メディアを介して DVD/USB に接続しようとするとエラーメッセージが表示されるのはなぜですか?

エラーメッセージは、リモートファイル共有（RFS）機能も使用中である場合に表示されます。一度に使用できるのは、RFS または仮想メディア のうちの 1 つです。両方を使用することはできません。

vFlash SD カード

vFlash SD カードがロックされるのはいつですか?

vFlash SD カードは、操作の進行時中にロックされています。たとえば、初期化操作中にロックされます。

SNMP 認証

「リモートアクセス：SNMP 認証の失敗」というメッセージが表示されるのはなぜですか?

IT Assistant は、検出の一環として、デバイスの get コミュニティ名および set コミュニティの検証を試行します。IT Assistant では、get コミュニティ名は public であり、set コミュニティ名は private です。デフォルトでは、iDRAC7 エージェントの SNMP エージェントコミュニティ名は public です。IT Assistant が set 要求を送信すると、iDRAC7 エージェントは SNMP 認証エラーを生成します。これは、iDRAC7 エージェントが public コミュニティの要求のみを受け入れるからです。

SNMP 認証エラーが生成されないようにするには、iDRAC7 エージェントによって受け入れられるコミュニティ名を入力する必要があります。iDRAC7 では 1 つのコミュニティ名のみが許可されているため、IT Assistant 検出セットアップに同じ get コミュニティ名と set コミュニティ名を使用する必要があります。

ストレージデバイス

システムに接続されているすべてのデバイスに関する情報が表示されず、OpenManage Storage Management では iDRAC7 よりも多くのストレージデバイスが表示されます。なぜですか?

iDRAC7 では、Comprehensive Embedded Management（CEM）でサポートされるデバイスの情報のみが表示されます。

RACADM

iDRAC7 をリセット（racadm racreset コマンドを使用）した後にコマンドを発行すると、次のメッセージが表示されます。これは何を示していますか?

エラー：指定された IP アドレスで RAC に接続できません。

このメッセージは、別のコマンドを発行する前に、iDRAC7 のリセットの完了を待つ必要があることを示しています。

RACADM コマンドおよびサブコマンドを使用する場合、明瞭ではないエラーがいくつかあります。

RACADM コマンドやサブコマンドを使用するとき、次のようなエラーが 1 つ、または複数発生することがあります。

- ローカル RACADM エラーメッセージ — 構文、入力ミス、名前の誤りなどの問題。
- リモート RACADM エラーメッセージ — IP アドレスの誤り、ユーザー名の誤り、パスワードの誤りなどの問題。

iDRAC7 に対する Ping テスト中、ネットワークモードが専用モードと共有モードの間で切り替えられた場合、Ping に対する応答がありません。

システムの ARP テーブルをクリアしてください。

リモート RACADM が SUSE Linux Enterprise Server（SLES）11 SP1 から iDRAC7 への接続に失敗します。

openssl および libopenssl の公式バージョンがインストールされていることを確認します。次のコマンドを実行して、RPM パッケージをインストールします。

```
rpm -ivh --force <ファイル名>
```

ファイル名 は openssl または libopenssl rpm パッケージファイルです。

例えば、次のとおりです。

```
rpm -ivh --force openssl-0.9.8h-30.22.21.1.x86_64.rpm
```

```
rpm -ivh --force libopenssl0_9_8-0.9.8h-30.22.21.1.x86_64.rpm
```

プロパティを変更すると、リモート RACADM とウェブベースのサービスを使用できなくなるのはなぜですか?

iDRAC7 ウェブサーバーのリセット後は、リモート RACADM サービスとウェブベースのインタフェースが使用できるようになるまでに時間がかかることがあります。

iDRAC7 ウェブサーバーは、次の場合にリセットされます。

- iDRAC7 ウェブユーザーインタフェースを使用してネットワーク設定またはネットワークセキュリティのプロパティが変更された。
- cfgRacTuneHttpsPort プロパティが変更された（`config -f`（config ファイル）が変更された時も含む）。
- racresetcfg コマンドが使用された。
- iDRAC7 がリセットされた。
- 新しい SSL サーバー証明書がアップロードされた。

ローカル RACADM を使用してパーティションを作成した後にこのパーティションを削除しようとするとエラーメッセージが表示されるのはなぜですか?

これは、パーティションの作成操作が進行中であるために発生します。しかし、しばらくするとパーティションが削除され、パーティションが削除されたことを示すメッセージが表示されます。それ以外の場合は、パーティションの作成操作が完了するのを待ってから、パーティションを削除します。

その他

ブレードサーバーの iDRAC IP アドレスを検索するには、どうすればよいですか?

次の方法のいずれかを使用して iDRAC IP アドレスを検索できます。

CMC ウェブインタフェースを使用する：**シャーシ → サーバー → セットアップ → 展開** と移動します。表示される表でサーバーの IP アドレスを確認します。

仮想コンソールを使用する：サーバーを再起動して、POST 実行中に iDRAC IP アドレスを表示します。OSCAR で「Dell CMC」コンソールを選択して、ローカルシリアル接続を介して CMC にログインします。この接続から CMC RACADM コマンドを送信できます。CMC RACADM サブコマンドの一覧表に関しては、『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

ローカル RACADM から、racadm getsysinfo コマンドを使用します。たとえば、次のコマンドを使用します。

```
$ 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
```

LCD を使用する：メインメニューで、サーバー をハイライト表示してチェックボタンを押し、必要なサーバーを選択してチェックボタンを押します。

ブレードサーバーに関連する CMC IP アドレスはどのように検索すればよいですか?

DRAC7 ウェブインタフェースから：**概要 → iDRAC 設定 → CMC** の順にクリックします。**CMC サマリ** ページに CMC IP アドレスが表示されます。

仮想コンソールから：OSCAR で「Dell CMC」コンソールを選択し、ローカル接続を介して CMC にログインします。この接続から CMC RACADM コマンドを送信できます。CMC RACADM サブコマンドの一覧表に関しては、『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』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
```

メモ: リモート RACADM を使用してこの操作を実行することもできます。

ラックおよびタワーサーバーの iDRAC IP アドレスはどのように検索すればよいですか?

iDRAC7 ウェブインタフェースから：**概要 → サーバ → プロパティ → サマリ** と移動します。**システムサマリ** ページに iDRAC7 IP アドレスが表示されます。

ローカル RACADM から：racadm getsysinfo コマンドを使用します。

LCD から：物理サーバーで、LCD パネルナビゲーションボタンを使用して iDRAC7 IP アドレスを表示します。**セットアップビュー → 表示 → iDRAC IP → IPv4** または **IPv6 → IP** と移動します。

OpenManage Server Administrator から：Server Administrator ウェブインタフェースで、**モジュラーエンクロージャ → システム / サーバーモジュール → メインシステムシャーシ / メインシステム → リモートアクセス** と移動します。

iDRAC7 ネットワーク接続が機能しません。

ブレードサーバーの場合：

- 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。
- NIC の設定、IPv4 または IPv6 の設定、および静的または DHCP がネットワークで有効になっていることを確認してください。

ラックおよびタワーサーバーの場合：

- 共有モードでは、レンチ記号が表示される NIC ポートに LAN ケーブルが接続されていることを確認してください。
- 専用モードでは、LAN ケーブルが iDRAC LAN ポートに接続されていることを確認してください。
- お使いのネットワークで NIC 設定、IPv4 または IPv6 設定、および静的または DHCP がネットワークで有効になっていることを確認してください。

ブレードサーバーをシャーシに挿入して電源スイッチを押しましたが、電源がオンになりません。

- iDRAC7 では、サーバーの電源がオンになる前の初期化に最大 2 分かかります。
- CMC 電源バジェットをチェックします。シャーシの電源バジェットを超過した可能性があります。

iDRAC7 の管理者ユーザー名とパスワードを取得するには、どうすればよいですか?

iDRAC7 をデフォルト設定に復元する必要があります。詳細については、「工場出荷時のデフォルト設定への iDRAC7 のリセット」を参照してください。

シャーシ内のシステムのスロット名を変更するには、どうすればよいですか?

1. CMC ウェブインタフェースにログインし、**シャーシ → サーバー → セットアップ** と移動します。
2. お使いのサーバーの行に新しいスロット名を入力して、**適用** をクリックします。

ブレードサーバーの起動中に iDRAC7 が応答しません。

サーバーを取り外し、挿入し直してください。

iDRAC7 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を CMC ウェブインタフェースで確認します。表示されている場合は、「CMC ウェブインタフェースを使用したファームウェアのアップデート」の手順に従います。

問題が解決しない場合は、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、次の状態のいずれかが原因で発生します。

- メモリが取り付けられていない、またはアクセス不可能である。
- CPU が取り付けられていない、またはアクセス不可能である。
- ビデオライザーカードが見つからない、または正しく接続されていない。

または、iDRAC7 ウェブインタフェースを使用するか、サーバーの LCD で、iDRAC7 ログのエラーメッセージを確認します。

20

使用事例シナリオ

本項は、本ガイドの特定の項に移動して、典型的な使用事例のシナリオを実行するために役立ちます。

アクセスできない管理下システムのトラブルシューティング

OpenManage Essentials、デルの管理コンソール、またはローカルのトラップコレクタからのアラートの受け取り後、データセンター内の 5 台のサーバーがオペレーティングシステムまたはサーバーのハングアップなどの問題によってアクセスできなくなります。原因を識別してトラブルシューティングを行い、iDRAC7 を使用してサーバーを再稼働させます。

アクセスできないシステムをトラブルシューティングする前に、次の前提要件が満たされていることを確認します。

- 前回のクラッシュ画面を有効化
- iDRAC7 でアラートを有効化

原因を識別するには、iDRAC ウェブインタフェースで次を確認し、システムへの接続を再確立します。

メモ: iDRAC ウェブインタフェースにアクセスできない場合は、サーバーに移動して LCD パネルにアクセスし、IP アドレスまたはホスト名を記録してから、管理ステーションの iDRAC ウェブインタフェースを使用して次の操作を実行します。

- サーバーの LED ステータス — 橙色に点滅または点灯。
- 前面パネル LCD ステータスまたはエラーメッセージ — 橙色の LCD またはエラーメッセージ。
- 仮想コンソールにオペレーティングシステムイメージが表示されます。イメージが表示されていれば、システムをリセット（ウォームブート）して、再度ログインします。ログインできる場合、問題は解決されています。
- 前回のクラッシュ画面。
- 起動キャプチャのビデオ。
- クラッシュキャプチャのビデオ。
- サーバー正常性ステータス — 問題のあるシステム部品の赤い *x* アイコン。
- ストレージアレイステータス — オフラインまたは故障の可能性のあるアレイ
- システムハードウェアおよびファームウェアに関連する重要なイベントのライフサイクルログ、およびシステムクラッシュ時に記録されたログエントリ。

システム情報の取得およびシステム正常性の評価

システム情報を取得し、システムの正常性を評価するには次の手順を実行します。

- iDRAC7 ウェブインタフェースで、**概要 → サーバー → システムサマリ** と移動してシステム情報を表示し、ページのさまざまなリンクにアクセスしてシステムの正常性を評価します。たとえば、シャーシファンの正常性を確認できます。
- シャーシロケータ LED を設定して、色に基づいてシステムの正常性を評価することも可能です。

アラートのセットアップと電子メールアラートの設定

アラートをセットアップし、電子メールアラートを設定するには、次の手順を実行します。

1. アラートを有効にします。
2. 電子メールアラートを設定し、ポートを確認します。
3. 管理下システムで再起動、電源オフ、またはパワーサイクルを実行します。
4. テストアラートを送信します。

ライフサイクルログとシステムイベントログの表示とエクスポート

ライフサイクルログログおよびシステムイベントログ（SEL）を表示およびエクスポートするには、次の手順を実行します。

1. iDRAC7 ウェブインタフェースで、**概要 → サーバー → ログ** と移動して、SEL を表示します。また **概要 → サーバー → ログ → ライフサイクルログ** と移動してライフサイクルログを表示します。

メモ: SEL はライフサイクルログにも記録されます。フィルタオプションを使用して SEL を表示します。

2. SEL またはライフサイクルログは、XML フォーマットで外部の場所（管理ステーション、USB、ネットワーク共有など）にエクスポートします。その代わりに、リモートシステムログを有効にして、ライフサイクルログに書き込まれるすべてのログが、設定されたリモートサーバーに同時に書き込まれるようにすることもできます。

iDRAC ファームウェアをアップデートするためのインタフェース

iDRAC ファームウェアをアップデートするには、次のインタフェースを使用します。

- iDRAC7 ウェブインタフェース
- RACADM CLI（iDRAC7 および CMC）
- Dell Update Package（DUP）
- CMC ウェブインタフェース
- Lifecycle Controller–Remote Services
- Lifecycle Controller
- Dell Remote Access Configuration Tool（DRACT）

正常なシャットダウンの実行

正常なシャットダウンを実行するには、iDRAC7 ウェブインタフェースで、次のいずれかの場所に移動します。

- **概要 → サーバー → 電源 / 熱 → 電源設定 → 電源制御** と移動します。**電源制御** ページが表示されます。**正常なシャットダウン** を選択し、**適用** をクリックします。
- **概要 → サーバー → 電源 / 熱 → 電源監視** と移動します。**電源管理** ドロップダウンメニューで **正常なシャットダウン** を選択し、**適用** をクリックします。

詳細については、『*iDRAC7 オンラインヘルプ*』を参照してください。

新しい管理者ユーザーアカウントの作成

デフォルトのローカル管理ユーザーアカウントを変更したり、新しい管理者ユーザーアカウントを作成したりすることができます。ローカル管理者ユーザーアカウントを変更するには、「ローカル管理者アカウント設定の変更」を参照してください。
新しい管理者アカウントを作成するには、次の項を参照してください。

- 「ローカルユーザーの設定」
- 「Active Directory ユーザーの設定」
- 「汎用 LDAP ユーザーの設定」

サーバーのリモートコンソールの起動と USB ドライブのマウント

リモートコンソールを起動し、USB ドライブをマウントするには、次の手順を実行します。

1. USB フラッシュドライブ（必要なイメージが含まれたもの）を管理ステーションに接続します。
2. 次の方法のいずれかを使用して、iDRAC7 ウェブインタフェースから仮想コンソールを起動します。
   - **概要** → **サーバー** → **コンソール** と移動し、**仮想コンソールの起動** をクリックします。
   - **概要** → **サーバー** → **プロパティ** と移動し、**仮想コンソールプレビュー** で **起動**をクリックします。

   仮想コンソールビューアが表示されます。
3. **ファイル** メニューで、**仮想メディア** → **仮想メディアの起動** とクリックします。
4. **イメージの追加** をクリックし、USB フラッシュドライブに保存されているイメージを選択します。
   使用可能なドライブのリストにイメージが追加されます。
5. イメージをマップするドライブを選択します。USB フラッシュドライブのイメージが管理下システムにマップされます。

連結された仮想メディアとリモートファイル共有を使用したベアメタル OS のインストール

この操作を実行するには、「リモートファイル共有を使用したオペレーティングシステムの展開」を参照してください。

ラック密度の管理

現在、2 台のサーバーがラックに取り付けられています。さらに 2 台のサーバーを追加するには、ラックに残されている収容量を確認する必要があります。
さらにサーバーを追加するためにラックの収容量を評価するには、次の手順を実行します。

1. サーバーの現在の電力消費量データおよび過去の電力消費量データを表示します。
2. このデータ、電源インフラ、および冷却システムの制限に基づいて、電力制限ポリシーを有効にし、電力制限値を設定します。

メモ: 制限値をピーク値に近い値に設定してから、この制限レベルを使用して、サーバーの追加のためにラックに残っている収容量を判断することをお勧めします。

新しい電子ライセンスのインストール

詳細については、「ライセンス操作」を参照してください。