iDRAC 8/7 v2.40.40.40 ユーザーズガイド

年 6 月 2017
Rev. A01

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その危険を回避するための方法を説明しています。

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。

目次

1

概要

Integrated Dell Remote Access Controller（iDRAC）は、システム管理者の生産性を高め、Dell サーバー全体の可用性を改善するよう設計されています。iDRAC は、管理者に対してサーバーの問題に関するアラートを送信し、管理者が行うリモート サーバー管理をサポートし、サーバーに物理的にアクセスする必要性を最小限に抑えます。

Lifecycle Controller テクノロジーを搭載した iDRAC 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やワークロードをいつでも利用できるようにします。管理者は、任意の場所からエージェントを使用せずに、Dell サーバーの導入、監視、管理、設定、アップデート、トラブルシューティング、修正を行うことができます。これは、オペレーティング システムまたは Hypervisor の有無や状態にかかわらず実現可能です。

iDRAC および Lifecycle Controller は、次のような製品と連携して IT 業務の簡素化および能率化を図ります。

- Dell Management plug-in for VMware vCenter
- 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

iDRAC には次のタイプが用意されています。

- Basic Management with IPMI（200～500 シリーズのサーバーではデフォルトで使用可能）
- iDRAC Express（600 以上のシリーズのラックまたはタワーサーバー、およびすべてのブレードサーバーではデフォルトで使用可能）
- iDRAC Enterprise（すべてのサーバーモジュールで使用可能）

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

トピック：

iDRAC 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 の詳細に関しては **dell.com/idracmanuals** にある『*Lifecycle Controller ユーザーズガイド*』を、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

iDRAC の主要機能は次のとおりです。

メモ: 一部の機能は、iDRAC Enterprise ライセンスでしか使用できません。ライセンスで使用できる機能については、「ライセンスの管理」を参照してください。

[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なしでのネットワークアダプタとストレージサブシステム（PERC およびダイレクトアタッチトストレージ）のインベントリおよび監視。
- システムインベントリの表示およびエクスポート。
- 温度、電圧、およびイントルージョンなどのセンサー情報の表示。
- CPU 状況、プロセッサ自動スロットル、および予測障害の監視。
- メモリ情報の表示。
- 電力消費の監視および制御。
- SNMPv3 get と alert のサポート。
- 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、iDRAC へのアクセスを提供します。詳細については、**dell.com/support/manuals** にある『Chassis Management Controller ユーザーズガイド』を参照してください。
- ホストオペレーティングシステムで使用可能なネットワークインタフェースを表示します。
- iDRAC Quick Sync 機能とモバイルデバイスを使用して、インベントリおよび監視情報を表示し、基本的な iDRAC 設定を行います。

[導入]

- 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。
- iDRAC 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。
- RACADM および WS-MAN を介した XML プロファイル機能のエクスポートまたはインポートによるサーバー設定の実行。詳細に関しては、『*Lifecycle Controller Remote Services クイックスタートガイド*』を参照してください。
- 仮想アドレス、イニシエータ、およびストレージターゲットの永続性ポリシーを設定します。
- 実行時にシステムに接続されたストレージデバイスをリモートから設定します。
- ストレージデバイスに対して次の手順を実行します。
  - 物理ディスク：物理ディスクのグローバルホットスペアとしての割り当てまたは割り当て解除。
  - 仮想ディスク：
    - 仮想ディスクの作成。
    - 仮想ディスクキャッシュポリシーの編集。
    - 仮想ディスク整合性のチェック。
    - 仮想ディスクの初期化。
    - 仮想ディスクの暗号化。
    - 専用ホットスペアの割り当てまたは割り当て解除。
    - 仮想ディスクの削除。
  - コントローラ：
    - コントローラプロパティの設定。
    - 外部設定のインポートまたは自動インポート。
    - 外部設定のクリア。
    - コントローラ設定のリセット。

        ▪ セキュリティキーの作成または変更。
    ○ PCIe SSD デバイス：
        ▪ サーバー内の PCIe SSD デバイスの正常性のインベントリとリモート監視。
        ▪ PCIe SSD の取り外し準備。
        ▪ データのセキュア消去。
    ○ バックプレーンのモードの設定（統合モードまたは分割モード）。
    ○ コンポーネント LED の点滅または点滅解除。
    ○ デバイス設定の、即時、次回のシステム再起動時、もしくはスケジュールされた時間での適用、または単一ジョブの一部としてバッチ適用する保留中操作としての適用。

[アップデート]

- iDRAC ライセンスの管理。
- BIOS と、Lifecycle Controller によってサポートされるデバイスに対するデバイスファームウェアのアップデート。
- 単一のファームウェアイメージを使用した iDRAC ファームウェアおよび Lifecycle Controller ファームウェアのアップデートまたはロールバック。
- ステージングされたアップデートの管理。
- サーバープロファイルのバックアップおよび復元。
- USB 接続を介した iDRAC インタフェースへのアクセス。
- USB デバイス上のサーバー設定プロファイルを使用した iDRAC の設定。

[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。
- 温度設定の変更によるシステムパフォーマンスと電力消費の最適化。
- OpenManage 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。
- イベントおよび改善された電子メールアラート通知のための電子メールアラート、IPMI アラート、リモートシステムログ、WS Eventing ログ、Redfish イベント、および SNMP トラップ（v1、v2c、および v3）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。
- CPU、メモリ、および I/O モジュールのパフォーマンスインデックスの帯域外監視および通知。
- 吸気口の温度と電力消費量の警告しきい値の設定。
- iDRAC サービスモジュールを使用して次の操作を行います。
    ○ オペレーティングシステム情報の表示。
    ○ Lifecycle Controller ログのオペレーティングシステムログへの複製。
    ○ システムの自動リカバリオプション。
    ○ iDRAC をリモートでハードリセットする
    ○ 帯域内 iDRAC SNMP アラートを有効にする
    ○ ホスト OS を使用して iDRAC にアクセスする（試験的機能）
    ○ Windows Management Instrumentation（WMI）情報の入力。
    ○ SupportAssist コレクションとの統合。これは、iDRAC サービスモジュールバージョン 2.0 以降がインストールされている場合にのみ該当します。詳細については、「SupportAssist コレクションの生成」を参照してください。
    ○ NVMe PCIe SSD の取り外しの準備。詳細については、PCIe SSD の取り外しの準備 、p. 214 を参照して ください。
- 次の方法による SupportAssist コレクションの生成：
    ○ 自動 — OS Collector ツールを自動で呼び出す iDRAC サービスモジュールを使用します。
    ○ 手動 — OS Collector ツールを使用します。

[iDRAC に関するデルのベストプラクティス]

- iDRAC は個別の管理ネットワーク上に置かれることが意図されており、インターネット上に置いたり、インターネットに接続するよう設計されているわけでも、意図されているわけでもありません。そうすることにより、接続されたシステムがセキュリティおよびその他のリスクにさらされる可能性が生じ、デルはそのようなリスクに対して一切の責任を負いません。
- iDRAC を個別の管理サブネットに置くと共に、ユーザーはファイアウォールなどのテクノロジーを使用して管理サブネット / vLAN を分離させ、サブネット /vLAN へのアクセスを承認されたサーバー管理者に限定する必要があります。

[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。iDRAC 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。

- Secure Socket Layer（SSL）証明書用のカスタム署名証明書。
- 署名付きファームウェアアップデート。
- Microsoft Active Directory、汎用 Lightweight Directory Access Protocol（LDAP）ディレクトリサービス、またはローカルで管理されているユーザー ID およびパスワードによるユーザー認証。

- 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。
- iDRAC にローカルで保存されたユーザーアカウントの SNMPv3 認証。これを使用することが推奨されますが、デフォルトで無効になっています。
- ユーザー ID とパスワード設定。
- デフォルトログインパスワードの変更。
- セキュリティ向上のための単方向ハッシュ形式を使用したユーザーパスワードおよび BIOS パスワードの設定。
- FIPS 140-2 レベル 1 の機能。
- TLS 1.2、1.1、および 1.0 のサポート。セキュリティ強化のため、デフォルト設定は TLS 1.1 以上です。
- TLS 1.2 規格を使用して 128 ビットおよび 40 ビット（128 ビットが許容されない国の場合）暗号化をサポートする SMCLP とウェブインタフェース。

  メモ: セキュアな接続を確保するため、デルは TLS 1.1 以上の使用をお勧めします。
- 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。
- iDRAC に接続するクライアントの IP アドレス範囲の限定。
- ラックおよびタワー型サーバーで使用可能の専用ギガビットイーサネットアダプタ（追加のハードウェアが必要となる場合あり）。

本リリースの新機能

- Distributed Management Task Force（DMTF）によって標準化されている RESTful Application Programming Interface（API）である Redfish 1.0.2 に対するサポートを追加。これは、拡張可能でセキュアなシステム管理インタフェースを提供します。IPv6 および VLAN 情報を取得するには、iDRAC サービスモジュール（iSM）をインストールします。
- Redfish インタフェースを使用したサーバ設定プロファイルに対するサポートを追加。
- TLS 1.0 以降、1.1 以降、または 1.2 のみを選択するための TLS 1.0 オプションの無効化に対するサポートを追加。
- FIPS 140-2 レベル 1 の機能。
- OpenDS での LDAP 認証に対するサポートを追加。
- PowerEdge M830 の Amulet カードに対するサポートを追加。
- リモート RACADM、またはウェブインタフェースを使用して開始される一部の設定ジョブ用の LC ログの情報を追加。
- ログインページに Dell Tech Center のリンクを追加。

本ユーザーズガイドの使用方法

本ユーザーズガイドの記載内容は、次を使用したタスクの実行を可能にします。

- iDRAC ウェブインタフェース — ここではタスク関連の情報のみが記載されています。フィールドおよびオプションについては、ウェブインタフェースからアクセスできる『*iDRAC オンラインヘルプ*』を参照してください。
- RACADM — 本書には、使用する必要がある RACADM コマンドまたはオブジェクトが記載されています。詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドライン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 — ここではタスク関連の情報のみが記載されています。フィールドおよびオプションについては、iDRAC 設定 GUI（起動中に <F2> を押し、［システムセットアップメインメニュー］ページで ［iDRAC Settings］ をクリック）で ［ヘルプ］ をクリックするとアクセスできる『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。

対応ウェブブラウザ

iDRAC は、以下のブラウザでサポートされています。

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

サポートされているバージョンのリストについては、**dell.com/idracmanuals** にある『*iDRAC リリースノート*』を参照してください。

ライセンスの管理

iDRAC 機能は、購入済みのライセンス（Basic Management、iDRAC Express、または iDRAC Enterprise）に基づいて利用できます。iDRAC 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、iDRAC 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 や vFlash などの一部の機能では、iDRAC ポートカードが必要となります。これは、200～500 サーバーシリーズではオプションです。

iDRAC 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、iDRAC ウェブインタフェースと RACADM から利用できます。

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。

ライセンスの取得方法

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 — セルフサービスポータルへのリンクは iDRAC から利用可能です。このリンクをクリックして、インターネット上のライセンスセルフサービスポータルを開きます。現在、ライセンスセルフサービスポータルは、サーバーと共に購入されたライセンスの取得に使用することができます。新しいライセンスまたはアップグレードライセンスの購入には、販売担当者かテクニカルサポートにお問い合わせいただく必要があります。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。詳細に関しては、**dell.com/support/manuals** 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。

1 対 1 のライセンス管理には iDRAC、RACADM、WS-MAN、および Lifecycle Controller-Remote Services を使用して、1 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 iDRAC 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 — コンポーネントが不明な場合に、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 iDRAC 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。詳細に関しては、**dell.com/support/manuals** にある『Dell License Manager ユーザーズガイド』を参照してください。

マザーボード交換後のライセンスのインポート

マザーボードを最近交換しており、iDRAC Enterprise ライセンスをローカル（ネットワーク接続なし）で再インストールして専用 NIC をアクティブにする必要がある場合は、Local iDRAC Enterprise License Installation Tool を使用できます。このユーティリティを使用すると、30 日試用版の iDRAC Enterprise ライセンスをインストールし、iDRAC をリセットして共有 NIC から専用 NIC に変更できます。

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	もっと詳しく知る
非システム管理者ログイン	無	無	無	無	有
アクティブなライセンス	有	有	有	有	有
期限切れのライセンス	無	有	有	有	有
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	無	有	有	無	有

メモ: iDRAC ウェブインタフェースの ［ライセンス］ ページで、デバイスを展開してドロップダウンメニューの ［置換］ オプションを表示します。

iDRAC ウェブインタフェースを使用したライセンスの管理

iDRAC 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、『iDRAC 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、［license］ サブコマンドを使用します。詳細に関しては、**dell.com/idracmanuals** にある『iDRAC RACADM コマンドラインインタフェースリファレンスガイド』を参照してください。

iDRAC7 と iDRAC8 のライセンス機能

次の表は、購入したライセンスに基づいて有効化される iDRAC7 および iDRAC8 機能のリストです。

表 2. iDRAC7 と iDRAC8 のライセンス機能

機能	基本管理（iDRAC 7）	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express for Blades	ブレード向け iDRAC8 Express	iDRAC7 Enterprise	iDRAC8 Enterprise
インタフェース / 標準								
IPMI 2.0	有	有	有	有	有	有	有	有
DCMI 1.5	無	有	無	有	無	有	無	有
ウェブベースの GUI	無	有	有	有	有	有	有	有
RACADM コマンドライン（ローカル / リモート）	無	有	有	有	有	有	有	有
Redfish	有	有	有	有	有	有	有	有
SMASH-CLP（SSH 専用）	無	有	有	有	有	有	有	有
Telnet	無	有	有	有	有	有	有	有
SSH	無	有	有	有	有	有	有	有
WS-MAN	有	有	有	有	有	有	有	有
ネットワークタイムプロトコル	無	無	有	有	有	有	有	有
接続性								
共有 NIC（LOM）	有	有	有	有	該当なし	該当なし	有	有
専用 NIC[1]	無	有	無	有	有	有	有	有 [2]
VLAN タグ付け	有	有	有	有	有	有	有	有
IPv4	有	有	有	有	有	有	有	有
IPv6	無	有	有	有	有	有	有	有
DHCP	無	有	無	有	無	有	無	有
ダイナミック DNS	無	有	有	有	有	有	有	有
OS パススルー	無	有	無	有	無	有	無	有
前面パネル USB	無	有	無	有	無	有	無	有
セキュリティ								
役割ベースの権限	有	有	有	有	有	有	有	有
ローカルユーザー	有	有	有	有	有	有	有	有
SSL 暗号化	有	有	有	有	有	有	有	有
IP ブロック	無	無	無	有	無	有	無	有
ディレクトリサービス（AD、LDAP）	無	無	無	無	無	無	有	有
2 要素認証（スマートカード）	無	無	無	無	無	無	有	有
シングルサインオン（kerberos）	無	無	無	有	無	有	有	有
PK 認証（SSH 用）	無	無	無	有	無	有	無	有
リモートプレゼンス								

表 2. iDRAC7 と iDRAC8 のライセンス機能 （続き）

機能	基本管理（iDRAC 7）	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express for Blades	ブレード向け iDRAC8 Express	iDRAC7 Enterprise	iDRAC8 Enterprise
電力制御	有 [4]	有	有	有	有	有	有	有
起動制御	無	有	無	有	無	有	無	有
シリアルオーバー LAN	有	有	有	有	有	有	有	有
仮想メディア	無	無	無	無	有	有	有	有
仮想フォルダ	無	無	無	無	無	無	有	有
リモートファイル共有	無	無	無	無	無	無	有	有
仮想コンソール	無	無	無	無	シングルユーザー	シングルユーザー	有	6 ユーザー
OS への VNC 接続	無	無	無	無	無	無	有	有
品質 / 帯域幅制御	無	無	無	無	無	有	無	有
仮想コンソール連携機能(最大 6 人の同時ユーザー)	無	無	無	無	無	無	無	有
仮想コンソールチャット	無	無	無	無	無	無	有	有
仮想フラッシュパーティション	無	無	無	無	無	無	有	有 [1、2]
電力および温度								
電源喪失後の自動電源オン	無	有	無	有	無	有	無	有
リアルタイム電力メーター	有	有	有	有	有	有	有	有
電力しきい値とアラート（ヘッドルームを含む）	無	無	無	有	無	有	無	有
リアルタイムの電源グラフ	無	無	有	有	有	有	有	有
電力カウンタ履歴	有	無	有	有	有	有	有	有
電力制限	無	無	無	無	無	無	有	有
Power Center 統合	無	無	無	無	無	無	無	有
温度監視	無	有	無	有	無	有	無	有
温度グラフ	無	無	無	有	無	有	無	有
正常性監視								
完全なエージェントフリーの監視	無	有	無	有	無	有	無	有
障害の予測監視	無	有	無	有	無	有	無	有

表 2. iDRAC7 と iDRAC8 のライセンス機能 （続き）

機能	基本管理（iDRAC 7）	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express for Blades	ブレード向け iDRAC8 Express	iDRAC7 Enterprise	iDRAC8 Enterprise
SNMPv1、v2、および v3（トラップおよび取得）	無	有	有	有	有	有	有	有
電子メール警告	無	無	有	有	有	有	有	有
設定可能なしきい値	無	有	無	有	無	有	無	有
ファン監視	無	有	無	有	無	有	無	有
電源装置監視	無	有	有	有	有	有	有	有
メモリ監視	無	有	無	有	無	有	無	有
CPU 監視	無	有	無	有	無	有	無	有
RAID 監視	無	有	無	有	無	有	無	有
NIC 監視	無	有	無	有	無	有	無	有
HD 監視（エンクロージャ）	無	有	無	有	無	有	無	有
帯域外パフォーマンス監視	無	無	無	無	無	無	無	有
アップデート								
リモートでのエージェント不要なアップデート	有[3]	有	有	有	有	有	有	有
組み込みアップデートツール	無	有	無	有	無	有	無	有
リポジトリとの同期（スケジュールされたアップデート）	無	無	無	無	無	無	有	有
自動アップデート	無	無	無	無	無	無	無	有
展開と設定								
組み込み OS 導入ツール	無	有	無	有	無	有	無	有
組み込み設定ツール（iDRAC 設定ユーティリティ）	無	有	無	有	無	有	無	有
組み込み設定ウィザード（Lifecycle Controller ウィザード）	無	有	無	有	無	有	無	有
自動検出	無	有	有	有	有	有	有	有
リモートでの OS 導入	無	無	無	有	無	有	無	有

表 2. iDRAC7 と iDRAC8 のライセンス機能 （続き）

機能	基本管理（iDRAC 7）	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express for Blades	ブレード向け iDRAC8 Express	iDRAC7 Enterprise	iDRAC8 Enterprise
組み込みドライバパック	無	有	無	有	無	有	無	有
完全な設定インベントリ	無	有	無	有	無	有	無	有
インベントリエクスポート	無	有	無	有	無	有	無	有
リモート設定	無	有	有	有	有	有	有	有
ゼロタッチ設定	無	無	無	無	無	無	無	有
システムの廃棄 / 転用	無	有	無	有	無	有	無	有
診断、サービス、およびロギング								
組み込み診断ツール	有	有	有	有	有	有	有	有
部品交換	無	有	有	有	有	有	有	有
サーバー設定のバックアップ	無	無	無	無	無	無	有	有
サーバー設定の復元	無	無	無	無	無	無	有	有
簡単な復元(システム設定）	無	有	無	有	無	有	無	有
正常性 LED/LCD	無	有	無	有	無	有	無	有
Quick Sync(NFC ベゼルが必要）	無	有	無	有	無	該当なし	無	有
iDRAC ダイレクト(前面 USB 管理ポート）	無	有	無	有	無	有	無	有
iDRAC サービスモジュール（iSM）	無	有	有	有	有	有	有	有
組み込みテクニカルサポートレポート	無	有	有	有	有	有	有	有
クラッシュ画面キャプチャ [5]	無	無	有	有	有	有	有	有
クラッシュビデオキャプチャ [5]	無	無	無	無	無	無	有	有
起動キャプチャ	無	無	無	無	無	無	有	有
iDRAC の手動リセット	無	有	無	有	無	有	無	有
仮想 NMI	無	有	無	有	無	有	無	有
OS ウォッチドッグ	無	有	無	有	無	有	無	有

表 2. iDRAC7 と iDRAC8 のライセンス機能 （続き）

機能	基本管理（iDRAC 7）	iDRAC8 Basic	iDRAC7 Express	iDRAC8 Express	iDRAC7 Express for Blades	ブレード向け iDRAC8 Express	iDRAC7 Enterprise	iDRAC8 Enterprise
組み込み正常性レポート	無	有	無	有	無	有	無	有
システムイベントログ	無	有	有	有	有	有	有	有
Lifecycle ログ	無	有	無	有	無	有	無	有
作業メモ	無	有	無	有	無	有	無	有
リモート Syslog	無	無	無	無	無	無	有	有
ライセンス管理	無	有	無	有	無	有	無	有

[1] vFlash SD カードメディアが必要です。

[2] 500 シリーズ以下のラックおよびタワーサーバーでは、この機能を有効にするためにハードウェアカードが必要です。 このハードウェアは追加料金で提供されています。

[3] リモートのエージェントフリーアップデート機能は IPMI を使用する場合にのみ使用可能です。

[4] IPMI を使用する場合にのみ使用可能です。

[5] ターゲットサーバーに OMSA エージェントが必要です。

iDRAC にアクセスするためのインタフェースとプロトコル

次の表は、iDRAC にアクセスするためのインタフェースのリストです。

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. iDRAC にアクセスするためのインタフェースとプロトコル

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 iDRAC 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。
iDRAC ウェブインタフェース	iDRAC ウェブインタフェースを使用して、iDRAC 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します。 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することができます。 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、iDRAC 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 iDRAC 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ために、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

表 3. iDRAC にアクセスするためのインタフェースとプロトコル （続き）

インタフェースまたはプロトコル	説明
	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 iDRAC にログイン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、iDRAC 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、iDRAC 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、iDRAC IP または MAC アドレス、ユーザーによるプログラムが可能な文字列の表示 ● DHCP の設定 ● iDRAC 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、システム識別ボタン 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 ● iDRAC ファームウェアのアップデート ● iDRAC ネットワークの設定 ● iDRAC 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
Lifecycle Controller	iDRAC 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] へと移動します。詳細に関しては、**dell.com/support/idracmanuals** 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 iDRAC にアクセスします。RACADM の詳細に関しては、**dell.com/idracmanuals.** にある『iDRAC RACADM コマンドラインインタフェースリファレンスガイド』を参照してください。SMCLP の詳細に関しては、「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て Telnet コンソールと同じ機能を提供します。SSH サービスはデフォルトでは、iDRAC で有効になっていますが、iDRAC で無効にすることができます。iDRAC は、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。iDRAC の初回起動時に、固有の 1024 ビット RSA ホストキーが生成されます。
IPMITool	IPMITool を使用して、iDRAC 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 の詳細に関しては、**dell.com/idracmanuals** 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。 ⓘ **メモ:** IPMI バージョン 1.5 はサポートされていません。
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。

表 3. iDRAC にアクセスするためのインタフェースとプロトコル （続き）

インタフェースまたはプロトコル	説明
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。iDRAC 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 iDRAC 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。 • **dell.com/idracmanuals.** にある『Lifecycle Controller Remote Services ユーザーズガイド』。 • **dell.com/support/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** • 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/**

iDRAC ポート情報

ファイアウォール経由で iDRAC にリモートでアクセスするには以下のポートが必要です。これらは、接続のために iDRAC がリッスンするデフォルトのポートです。オプションで、ほとんどのポートを変更できます。これを行うには、「サービスの設定」を参照してください。

表 4. iDRAC が接続について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+
161*	snmp
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
5901	VNC VNC 機能が有効になっている場合、ポート 5901 が開きます。
*設定可能なポート	

次の表に、iDRAC がクライアントとして使用するポートを示します。

表 5. iDRAC 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）
123	ネットワークタイムプロトコル（NTP）
3269	グローバルカタログ（GC）用 LDAPS
*設定可能なポート	

その他の必要マニュアル

このガイドに加え、デルサポートサイト（**dell.com/support/manuals**）で入手できる次の文書にもシステム内の iDRAC のセットアップと操作に関する追加情報が記載されています。

- 『*iDRAC オンラインヘルプ*』には、iDRAC 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と、それらの説明が記載されています。このオンラインヘルプには、iDRAC のインストール後にアクセスすることができます。
- 『*iDRAC RACADM コマンドラインインタフェース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 iDRAC 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。
- 『iDRAC RACADM サポートマトリックス』は、特定の iDRAC バージョンに適用可能なサブコマンドおよびオブジェクトのリストを提供します。
- 『*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。
- 『*第 12 世代および第 13 世代 Dell PowerEdge サーバー向け Dell Lifecycle Controller グラフィカルユーザーインタフェースユーザーズガイド*』には、Lifecycle Controller グラフィカルユーザーインタフェース（GUI）の使用に関する情報が記載されています。
- 『*第 12 世代および第 13 世代 Dell PowerEdge サーバー向け Dell Lifecycle Controller Remote Services クイックスタートガイド*』には、Remote Services 機能の概要、Remote Services と Lifecycle Controller API の使用開始方法が記載されており、Dell テックセンター上のさまざまなリソースへの参照が提供されています。
- 『*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説明しています。
- 『*iDRAC サービスモジュールインストールガイド*』では、iDRAC サービスモジュールをインストールするための情報が記載されています。
- 『*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。
- 『*リリースノート*』は、システム、マニュアルへの最新アップデート、または専門知識をお持ちのユーザーや技術者向けの高度な技術資料を提供します。
- 『*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。

- システムに付属している「安全にお使いいただくために」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。
- 『*Getting Started Guide*』(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。
- 『*Owner's Manual*』(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。

関連タスク

デルへのお問い合わせ 、p. 28
Dell EMC サポート サイトからのサポート コンテンツへのアクセス 、p. 28

ソーシャルメディアリファレンス

本製品、ベストプラクティス、およびデルソリューションとサービスの情報についての詳細を知るには、Dell TechCenter などのソーシャルメディアプラットフォームにアクセスすることができます。[www.delltechcenter.com/idrac] の iDRAC wiki ページからは、ブログ、フォーラム、ホワイトペーパー、ハウツービデオなどにアクセスすることができます。

iDRAC およびその他関連ファームウェア文書については、**dell.com/idracmanuals** と **dell.com/esmmanuals** を参照してください。

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. **Dell.com/support** にアクセスします。
2. サポートカテゴリを選択します。
3. ページの下部にある [国 / 地域の選択] ドロップダウンリストで、お住まいの国または地域を確認します。
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。

Dell EMC サポート サイトからのサポート コンテンツへのアクセス

直接リンクを使用して Dell EMC サポート サイトに移動するか、検索エンジンを使用して、一連のシステム管理ツールに関連するサポート コンテンツにアクセスします。

- 直接リンク :
  - Dell EMC エンタープライズ システム管理および Dell EMC リモート エンタープライズ システム管理 : https://www.dell.com/esmmanuals
  - Dell EMC 仮想化ソリューション : https://www.dell.com/SoftwareManuals
  - Dell EMC OpenManage : https://www.dell.com/openmanagemanuals
  - iDRAC : https://www.dell.com/idracmanuals
  - Dell EMC OpenManage Connections エンタープライズ システム管理 : https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - Dell EMC Serviceability Tools : https://www.dell.com/serviceabilitytools
- Dell EMC サポート サイト :
  1. https://www.dell.com/support にアクセスします。
  2. [すべての製品の参照] をクリックします。
  3. [すべての製品] ページで [ソフトウェア] をクリックして、次に必要なリンクをクリックします。

4. 必要な製品をクリックして、必要なバージョンをクリックします。

検索エンジンを使用する場合は、検索ボックスにドキュメントの名前とバージョンを入力します。

2

iDRAC へのログイン

iDRAC には、iDRAC ユーザー、Microsoft Active Directory ユーザー、または Lightweight Directory Access Protocol（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:

- iDRAC へログインするには、iDRAC へのログイン権限が必要です。
- iDRAC GUI は ［戻る］、［進む］、または［更新］ などのブラウザボタンをサポートしていません。

メモ: ユーザー名およびパスワードの推奨文字に関する詳細は、ユーザー名およびパスワードで推奨される文字、p. 126 を参照してください。

関連タスク

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 iDRAC へのログイン、p. 30
スマートカードを使用した iDRAC へのログイン、p. 31
シングルサインオンを使用した iDRAC へのログイン、p. 33
デフォルトログインパスワードの変更、p. 35

トピック：

- 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 iDRAC へのログイン
- スマートカードを使用した iDRAC へのログイン
- シングルサインオンを使用した iDRAC へのログイン
- リモート RACADM を使用した iDRAC へのアクセス
- ローカル RACADM を使用した iDRAC へのアクセス
- ファームウェア RACADM を使用した iDRAC へのアクセス
- SMCLP を使用した iDRAC へのアクセス
- 公開キー認証を使用した iDRAC へのログイン
- 複数の iDRAC セッション
- デフォルトログインパスワードの変更
- デフォルトパスワード警告メッセージの有効化または無効化
- 無効なパスワード資格情報

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 iDRAC へのログイン

ウェブインタフェースを使用して iDRAC にログインする前に、サポートされているウェブブラウザが設定されており、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 以外にも、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。

メモ: OpenDS での LDAP 認証はサポートされています。DH キーは 768 ビットよりも大きい必要があります。

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 iDRAC 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-address]` を入力し、<Enter> キーを押します。

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://[iDRAC-IP-address]:[port-number]` を入力します。ここで、`[iDRAC-IP-address]` は iDRAC IPv4 または IPv6 アドレスであり、`[port-number]` 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、iDRAC 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 iDRAC にログインされます。

   ユーザー設定権限とデフォルトアカウント資格情報でログインする場合に、デフォルトパスワード警告機能が有効になっていると、［ デフォルトパスワード警告 ］ ページが表示され、パスワードを簡単に変更できます。

関連概念

ユーザーアカウントと権限の設定 、p. 126
デフォルトログインパスワードの変更 、p. 35

関連タスク

対応ウェブブラウザの設定 、p. 57

スマートカードを使用した iDRAC へのログイン

スマートカードを使用して iDRAC 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。

関連タスク

スマートカードを使用したローカルユーザーとしての iDRAC へのログイン 、p. 31
スマートカードを使用した Active Directory ユーザーとしての iDRAC へのログイン 、p. 32

スマートカードを使用したローカルユーザーとしての iDRAC 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済み認証局 (CA) の証明書を iDRAC 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

iDRAC 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 iDRAC 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 address]]` を使用して iDRAC ウェブインタフェースにアクセスします。

   [iDRAC ログイン] ページが表示され、スマートカードを挿入するよう求められます。

   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 address]:[port number]` と入力します。ここで、`[IP address]` は iDRAC の IP アドレスであり、`[port number]` 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 iDRAC にログインされました。

   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、iDRAC 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 CRL で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。

関連概念

スマートカードログインの有効化または無効化 、p. 151

関連タスク

ローカルユーザーのための iDRAC スマートカードログインの設定 、p. 149

スマートカードを使用した Active Directory ユーザーとしての iDRAC 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。

- 信頼済み認証局 (CA) 証明書 (CA 署名付き Active Directory 証明書) を iDRAC 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 iDRAC 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 address]` を使用して iDRAC にログインします。
   [iDRAC ログイン] ページが表示され、スマートカードを挿入するよう求められます。

   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 address]:[port number]` と入力します。ここで、`[IP address]` は iDRAC IP アドレスであり、`[[port number]` 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 iDRAC 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。

関連概念

スマートカードログインの有効化または無効化 、p. 151

関連タスク

Active Directory ユーザーのための iDRAC スマートカードログインの設定 、p. 151

シングルサインオンを使用した iDRAC 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、iDRAC にログインできます。

関連概念

Active Directory ユーザーのための iDRAC SSO ログインの設定 、p. 149

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

シングルサインオンを使用して iDRAC 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 iDRAC 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. ウェブブラウザに `https://[FQDN address]` 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 address]:[port number]` を入力します。ここで、`[FQDN address]` は iDRAC FQDN（iDRACdnsname.domain.name）であり、`[port number]` 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、iDRAC 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。

CMC ウェブインタフェースを使用した iDRAC SSO へのログイン

SSO 機能を使用することにより、CMC ウェブインタフェースから iDRAC 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 iDRAC を起動ときの CMC ユーザー権限があります。そのユーザーは、ユーザーアカウントが CMC に存在していても iDRAC にはないという場合でも、CMC から iDRAC を起動できます。

iDRAC 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、iDRAC IP アドレスが変更されている、または iDRAC 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 iDRAC 起動オプションがグレー表示になります。

詳細に関しては、**dell.com/support/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 iDRAC 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 iDRAC にアクセスできます。

詳細に関しては、**dell.com/idracmanuals** にある『iDRAC RACADM コマンドラインインタフェース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 iDRAC の SSL 証明書が保存されていない場合は、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: iDRAC 証明書は、セキュアなセッションを確立するために iDRAC 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。

関連タスク

リモート RACADM を Linux 上で使用するための CA 証明書の検証 、p. 34

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 iDRAC にアップロードします。

ローカル RACADM を使用した iDRAC へのアクセス

ローカル RACADM を使用して iDRAC にアクセスするには、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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 iDRAC へのアクセス

SSH または Telnet インタフェースを使用して、iDRAC にアクセスし、ファームウェア RACADM コマンドを実行できます。詳細に関しては、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

SMCLP を使用した iDRAC へのアクセス

SMCLP は、Telnet または SSH を使用して iDRAC 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 iDRAC へのログイン

パスワードを入力せずに SSH 経由で iDRAC 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。

たとえば、次のとおりです。

［ログイン：］

```
ssh username@<domain>
```

または

```
ssh username@<IP_address>
```

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

[RACADM コマンドの送信：]

```
ssh username@<domain> racadm getversion
```

```
ssh username@<domain> racadm getsel
```

関連概念

SSH の公開キー認証の使用 、p. 123

複数の iDRAC 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 iDRAC セッションのリストを提供します。

表 6. 複数の iDRAC セッション

インタフェース	セッション数
iDRAC ウェブインタフェース	6
リモート RACADM	4
ファームウェア RACADM/SMCLP	SSH - 2 Telnet - 2 シリアル - 1

デフォルトログインパスワードの変更

デフォルトパスワードの変更を許可する警告メッセージは、以下の場合に表示されます。

- ユーザー設定権限で iDRAC にログインする。
- デフォルトパスワード警告機能が有効になっている。
- 現在有効になっているアカウントの資格情報が root/calvin である。

SSH、Telnet、リモート RACADM、またはウェブインタフェースを使用して iDRAC にログインするときは、警告メッセージも表示されます。ウェブインタフェース、SSH、および Telnet の場合は、各セッションに対して単一の警告メッセージが表示されます。リモート RACADM の場合、警告メッセージは各コマンドに対して表示されます。

メモ: ユーザー名およびパスワードの推奨文字に関する詳細は、ユーザー名およびパスワードで推奨される文字、p. 126 を参照してください。

関連タスク

デフォルトパスワード警告メッセージの有効化または無効化、p. 36

ウェブインタフェースを使用したデフォルトログインパスワードの変更

iDRAC ウェブインタフェースにログインするときに、[デフォルトパスワード警告] ページが表示されたら、パスワードを変更できます。これを行うには、次の手順を実行します。

1. [デフォルトパスワードの変更] オプションを選択します。
2. [新しいパスワード] フィールドに、新しいパスワードを入力します。

   メモ: ユーザー名およびパスワードの推奨文字に関する詳細は、ユーザー名およびパスワードで推奨される文字、p. 126 を参照してください。

3. [パスワードの確認] フィールドに、もう一度パスワードを入力します。
4. [続行] をクリックします。新しいパスワードが設定され、iDRAC にログインされます。

メモ: ［続行］は、［新しいパスワード］フィールドと［パスワードの確認］フィールドに入力されたパスワードが一致した場合にのみ有効化されます。

他のフィールドについては、『iDRAC オンラインヘルプ』を参照してください。

RACADM を使用したデフォルトログインパスワードの変更

パスワードを変更するには、次の RACADM コマンドを実行します。

```
racadm set iDRAC.Users.<index>.Password <Password>
```

`<index>` は 1 から 16 までの値で（ユーザーアカウントを示す）、`<password>` は新しいユーザー定義パスワードです。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

メモ: ユーザー名およびパスワードの推奨文字に関する詳細は、ユーザー名およびパスワードで推奨される文字、p. 126 を参照してください。

iDRAC 設定ユーティリティを使用したデフォルトログインパスワードの変更

iDRAC 設定ユーティリティを使用してデフォルトログインパスワードを変更するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、［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. ［パスワードの変更］フィールドに、新しいパスワードを入力します。

   メモ: ユーザー名およびパスワードの推奨文字に関する詳細は、ユーザー名およびパスワードで推奨される文字、p. 126 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。

デフォルトパスワード警告メッセージの有効化または無効化

デフォルトパスワード警告メッセージの表示を有効または無効にすることができます。これを行うには、ユーザー設定権限が必要です。

ウェブインタフェースを使用したデフォルトパスワード警告メッセージの有効化または無効化

iDRAC にログインした後にデフォルトパスワード警告メッセージを有効または無効にするには、次の手順を実行します。

1. ［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. ［デフォルトパスワード警告］セクションで、［有効］を選択し、次に［適用］をクリックして、iDRAC へのログイン時における［デフォルトパスワード警告］ページの表示を有効にします。これを行わない場合は、［無効］を選択します。

   または、この機能が有効になっていて、今後のログインで警告メッセージを表示したくない場合は、［デフォルトパスワード警告］ページで、［今後この警告を表示しない］オプションを選択し、［適用］をクリックします。

RACADM を使用したデフォルトログインパスワードの変更のための警告メッセージの有効化または無効化

RACADM を使用してデフォルトログインパスワードの変更のための警告メッセージの表示を有効にするには、`idrac.tuning.DefaultCredentialWarning` オブジェクトを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

無効なパスワード資格情報

不正なユーザーやサービス拒否（DoS）攻撃に対するセキュリティを提供するため、iDRAC は IP および SNMP トラップ（有効な場合）をブロックする前に次を行います。

- 一連のサインインエラーとアラート
- 連続する不正なログイン試行ごとに時間間隔を増加
- ログエントリ

メモ: サインインエラーとアラート、不正ログインごとの時間間隔の増加、およびログエントリは、ウェブインタフェース、Telnet、SSH、リモート RACADM、WS-MAN、および VMCLI などの iDRAC インタフェースで使用できます。

表 7. 不正なログイン試行時の iDRAC ウェブインタフェースの動作

ログイン試行	ブロック(秒)	エラーログ（USR00034）	GUI 表示メッセージ	SNMP アラート（有効な場合）
最初の不正ログイン	0	無	なし	無
2 回目の不正ログイン	30	有	• `RAC0212: Login failed. Verify that username and password is correct. Login delayed for 30 seconds.` • **再試行** ボタンは 30 秒間無効になります。	有
3 回目の不正ログイン	60	有	• `RAC0212: Login failed. Verify that username and password is correct. Login delayed for 60 seconds.` • **再試行** ボタンは 60 秒間無効になります。	有
それ以降の各不正ログイン	60	有	• `RAC0212: Login failed. Verify that username and password is correct. Login delayed for 60 seconds.` • **再試行** ボタンは 60 秒間無効になります。	有

メモ: 24 時間を過ぎるとカウンタがリセットされ、上記の制限が適用されます。

3

管理下システムと管理ステーションのセットアップ

iDRAC を使用して帯域外システム管理を実行するには、iDRAC 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下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。

iDRAC Express および iDRAC Enterprise の両方とも、デフォルトの静的 IP アドレス状態で出荷されます。ただし、弊社では次の 2 つのオプションも用意しています。

- [プロビジョニングサーバー]— プロビジョニングサーバーがデータセンター環境にインストールされている場合はこのオプションを使用します。プロビジョニングサーバーは、Dell PowerEdge サーバーで、オペレーティングシステムおよびアプリケーションの展開およびアップグレードの管理および自動処理を行います。プロビジョニングサーバーのオプションを有効にすることにより、サーバーは、初回起動時に、プロビジョニングサーバーを検索し、展開やアップグレードプロセスを自動で開始します。
- [DHCP] — DHCP (Dynamic Host Configuration Protocol : 動的ホスト構成プロトコル) サーバーがデータセンター環境にインストールされている場合、または iDRAC 自動設定または OpenManage Essentials Configuration Manager を使用してサーバーのプロビジョニングを自動化する場合には、このオプションを使用します。DHCP サーバーは、IP アドレス、ゲートウェイ、およびサブネットマスクを iDRAC に自動的に割り当てます。

プロビジョニングサーバーまたは DHCP は、サーバーのご注文時に有効にすることができます。いずれの機能においても、有効にするのは無料です。ただし、有効にできるのは 1 つの設定のみです。

関連概念

iDRAC IP アドレスのセットアップ 、p. 38
管理下システムのセットアップ 、p. 50
デバイスファームウェアのアップデート 、p. 62
デバイスファームウェアのロールバック 、p. 71

関連タスク

管理ステーションのセットアップ 、p. 49
対応ウェブブラウザの設定 、p. 57

トピック :

iDRAC IP アドレスのセットアップ

iDRAC との双方向通信を有効にするには、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実行することができます。シャーシの導入後は、シャーシの LCD パネルを使用して iDRAC 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 iDRAC 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実行できます。これには、iDRAC 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、iDRAC ネットワークインタフェースはデフォルトで無効になっています。

iDRAC IP アドレスを設定した後で、次の手順を実行します。

- iDRAC 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してください。
- 次のいずれかのインタフェースで iDRAC にアクセスします。
  - 対応ブラウザ（Internet Explorer、Firefox、Chrome、または Safari）を使用する iDRAC 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［dell.com/support］から入手できる Windows または Linux のデルカスタマイズインストーラが必要）

関連タスク

iDRAC 設定ユーティリティを使用した iDRAC IP のセットアップ、p. 39
CMC ウェブインタフェースを使用した iDRAC IP のセットアップ、p. 42
プロビジョニングサーバーの有効化、p. 43
自動設定を使用したサーバーとサーバコンポーネントの設定、p. 43

iDRAC 設定ユーティリティを使用した iDRAC IP のセットアップ

iDRAC の IP アドレスを設定するには、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. ［戻る］、［終了］、［はい］の順にクリックします。
   ネットワーク情報が保存され、システムが再起動します。

関連タスク

ネットワーク設定、p. 40
共通設定、p. 41
IPv4 設定、p. 41
IPv6 設定、p. 41
IPMI 設定、p. 42
VLAN 設定、p. 42

ネットワーク設定

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。

     このオプションを選択すると、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 ポートとは個別にルーティングします。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ることにより、ホスト LOM または NIC に割り当てられる IP アドレスではなく、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: ブレードサーバーの場合、専用オプションは [シャーシ (専用)] として表示されます。
   - [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 つのすべての LOM オプションを使用することができます。NDC ポート 2 個を備えたブレードサーバーでは 2 つの LOM オプション (LOM1 と LOM2) が使用可能で、NDC ポート 4 個を備えたサーバーでは 4 つのすべての LOM オプションが使用可能です。

   メモ: NDC を 2 個備えたフルハイトサーバーではハードウェア仲裁がサポートされないため、次の bNDC では共有 LOM がサポートされません。
   - Intel 2P X520–k bNDC 10 G
   - Emulex OCM14102–N6–D bNDC 10 Gb
   - Emulex OCm14102-U4-D bNDC 10 Gb
   - Emulex OCm14102-U2-D bNDC 10 Gb
   - QLogic QMD8262–k DP bNDC 10 G
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。

   たとえば、LOM1 がダウンしたときに iDRAC 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]、[フェールオーバーネットワーク] に [LOM2] を選択します。

   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。

   メモ: フェールオーバーは、下記の Emulex rNDC および bNDC における共有 LOM ではサポートされていません。
   - Emulex OCM14104-UX-D rNDC 10 Gbx
   - Emulex OCM14104-U1-D rNDC 10 Gb
   - Emulex OCM14104-N1-D rNDC 10 Gb
   - Emulex OCM14104B-N1-D rNDC 10 Gb
   - Emulex OCM14102-U2-D bNDC 10 Gb
   - Emulex OCM14102-U4-D bNDC 10 Gb
   - Emulex OCM14102-N6-D bNDC 10 Gb

   メモ: Dell PowerEdge FM120x4 および FX2 のサーバーでは、シャーシのスレッド設定で [フェールオーバーネットワーク] がサポートされません。シャーシのスレッド設定の詳細に関しては、**dell.com/idracmanuals** にある『Chassis Management Controller (CMC) ユーザーズガイド』を参照してください。

メモ: PowerEdge FM120x4 サーバーでは、拡張ネットワークアダプタの分離を設定する間、LOM2 がホストシステム上で無効になっており、iDRAC NIC 用に選択されていないことを確認してください。シャーシスレッド設定の詳細に関しては、**dell.com/idracmanuals** にある、『Dell Chassis Management Controller（CMC）ユーザーズガイド』を参照してください。

4. iDRAC 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、iDRAC 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 iDRAC 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。

iDRAC 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 iDRAC に自動的に 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。
   - 静的 IP アドレス
   - 静的ゲートウェイ
   - 静的サブネットマスク
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［静的優先 DNS サーバー］および［静的代替 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、［静的優先 DNS サーバー］と［静的代替 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 iDRAC に対して自動的に IP アドレス、ゲートウェイ、およびサブネッマスクを割り当てるようにするには、［自動設定の有効］下で［有効］オプションを選択します。

   メモ: 静的 IP および DHCP IP の両方を同時に設定することができます。

3. ［静的 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. ［静的プレフィックス長］ボックスに、0～128 の範囲の値を入力します。
5. ［静的ゲートウェイ］ボックスに、ゲートウェイアドレスを入力します。

   メモ: 静的 IP を設定すると、現在の IP アドレス 1 が静的 IP を表示し、IP アドレス 2 が動的 IP を表示します。静的 IP 設定をクリアすると、現在の IP アドレス 1 に動的 IP が表示されます。

6. DHCP を使用している場合は、[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。必要に応じて次の設定を行うことができます。
   - [静的優先 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。
   - [静的代替 DNS サーバー] ボックスに、静的代替 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 設定

VLAN インフラストラクチャ内に iDRAC 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。

メモ: [シャーシ (専用)] として設定されたブレードサーバーでは、VLAN 設定は読み取り専用となり、CMC からしか変更できません。サーバーが共有モードに設定されている場合、VLAN 設定は iDRAC の共有モードで行うことができます。

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。

   メモ: VLAN を有効化した後は、iDRAC IP にしばらくアクセスできません。

CMC ウェブインタフェースを使用した iDRAC IP のセットアップ

CMC ウェブインタフェースを使用して iDRAC 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 iDRAC 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 の導入] 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。詳細に関しては、『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、『iDRAC オンラインヘルプ』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。
   詳細に関しては、**dell.com/support/manuals** にある『Chassis Management Controller ユーザーズガイド』を参照してください。

プロビジョニングサーバーの有効化

プロビジョニングサーバー機能を使用すると、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 iDRAC に提供するため、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。プロビジョニングサーバーの詳細に関しては、**dell.com/idracmanuals** にある『*Lifecycle Controller Remote Services ユーザーズガイド*』を参照してください。

プロビジョニングサーバーは、静的 IP アドレスで動作します。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。

iDRAC 設定ユーティリティまたは Lifecycle Controller を使用してプロビジョニングサーバー機能を有効にできます。Lifecycle Controller の使用方法に関しては、**dell.com/idracmanuals** にある『*Lifecycle Controller ユーザーズガイド*』を参照してください。

プロビジョニングサーバーの機能が工場出荷時のシステム上で有効になっていない場合は、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。プロビジョニングサーバーを有効にする前に必ず、この管理者アカウントを無効にします。Lifecycle Controller でプロビジョニングサーバーの機能が有効になっていると、プロビジョニングサーバーが検知されるまで、すべての iDRAC ユーザーアカウントは無効です。

次の手順で、iDRAC 設定ユーティリティを使用してプロビジョニングサーバーを有効にします。

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。

自動設定を使用したサーバーとサーバコンポーネントの設定

自動設定機能は、1 回の操作でサーバのすべてのコンポーネントを設定およびプロビジョニングします。コンポーネントには BIOS、iDRAC、PERC が含まれます。自動設定は、設定可能なすべてのパラメータを含むサーバ設定プロファイル (SCP) の XML ファイルを自動的にインポートします。IP アドレスを割り当てる DHCP サーバも、SCP ファイルへのアクセスの詳細を提供します。

SCP ファイルは、ゴールド設定サーバを設定することで作成されます。この設定は、DHCP サーバおよび設定中サーバの iDRAC によって、アクセス可能な共有の CIFS または NFS ネットワークロケーションにエクスポートされます。SCP ファイル名は、ターゲットサーバのサービスタグまたはモデル番号に基づくものか、または一般的な名前を付けます。DHCP サーバは DHCP サーバオプションを使用して SCP ファイル名 (オプション)、SCP ファイルの場所、およびファイルの場所にアクセスするためのユーザー資格情報を指定します。

iDRAC が自動設定用に設定されている DHCP サーバから IP アドレスを取得するとき、iDRAC はサーバのデバイスを設定するために SCP を使用します。自動設定は、iDRAC が、DHCP サーバから IP アドレスを取得するまで呼び出されません。iDRAC が応答や IP アドレスを DHCP サーバから取得しない場合、自動設定は呼び出されません。

メモ:

- 自動設定を有効化することができるのは、[DHCPv4] および、[IPv 4 を有効にする] オプションが有効化されている場合のみです。
- 自動設定および自動検出機能は、相互に排他的です。 自動設定が機能するには自動検出を無効します。
- サーバが自動設定動作を実行した後、自動設定機能は無効になります。自動設定の有効化に関する詳細については、RACADM を使用した自動設定の有効化 、p. 48 を参照してください。

DHCP サーバプール内のすべての Dell PowerEdge サーバが同じモデルタイプと番号の場合、単一の SCP ファイル（config.xml）が必要です。config.xml はデフォルトの SCP ファイル名です。

個別のサーバーサービスタグまたはサーバーモデルがマップされた、異なる設定ファイルが必要なサーバーは、個別に設定することができます。特定の要件を備えた異なる複数のサーバーがある環境では、異なる SCP ファイル名を使用して各サーバーまたはサーバーのタイプを識別できます。例えば、PowerEdge R730 と PowerEdge R530 の 2 つのモデルのサーバーを設定する場合は、2 つの SCP ファイル、R730-config.xml と R530-config.xml を使用します。

メモ: iDRAC バージョン 2.20.20.20 以降が搭載されたシステムで、ファイル名パラメータが DHCP オプション 60 に存在しない場合は、iDRAC サーバ設定エージェントがサーバのサービスタグ、モデル番号、またはデフォルトのファイル名の config.xml を使用して設定ファイル名を自動生成します。

iDRAC サーバ設定エージェントは、次の順にルールを使用して、ファイル共有上のどの SCP ファイルを各 iDRAC に適用するかを決定します。

1. DHCP オプション 60 で指定したファイル名。
2. <ServiceTag>-config.xml - DHCP オプション 60 でファイル名が指定されていない場合は、システムのサービスタグを使用して、システムの SCP ファイルを個別に識別します。例：CDVH7R1-config.xml
3. <Model number>-config.xml - オプション 60 のファイル名が指定されておらず、<Service Tag>-config.xml ファイルが見つからない場合は、使用する SCP ファイル名のベースにシステムのモデル番号を使用します。例：R520-config.xml
4. config.xml - オプション 60 のファイル名、サービスタグベースのファイル、およびモデル番号ベースのファイルが使用できない場合は、デフォルトの config.xml ファイルを使用します。

メモ: これらのファイルがネットワーク共有上にない場合、見つからなかったファイルのためのサーバー設定プロファイルのインポートジョブが失敗としてマークされます。

関連概念

自動設定シーケンス 、p. 44
DHCP オプション 、p. 44

関連タスク

iDRAC ウェブインタフェースを使用した自動設定の有効化 、p. 47
RACADM を使用した自動設定の有効化 、p. 48

自動設定シーケンス

1. Dell サーバーの属性を設定する SCP ファイルを作成または変更します。
2. DHCP サーバーおよび DHCP サーバーから割り当てられた IP アドレスであるすべての Dell サーバーからアクセス可能な共有の場所に、SCP ファイルを置きます。
3. DHCP サーバーで「ベンダーオプション 43」のフィールドに SCP ファイルの場所を指定します。
4. iDRAC は IP アドレス取得の一部として、ベンダークラス識別子 iDRAC をアドバタイズします（オプション 60）。
5. DHCP サーバーは、ベンダーのクラスを dhcpd.conf ファイル内のベンダーのオプションと一致させ、SCP ファイルの場所および SCP ファイル名（指定されている場合）を iDRAC に送信します。
6. iDRAC は、SCP ファイルを処理し、ファイル内にリストされたすべての属性を設定します。

DHCP オプション

DHCPv4 では、グローバルに定義された多数のパラメータを DHCP クライアントにパスすることができます。各パラメータは、DHCP オプションと呼ばれています。各オプションは、1 バイトのサイズのオプションタグで識別されます。0 と 255 のオプションタグはそれぞれパディングとオプションの終了用に予約されています。他のすべての値はオプションの定義に使用できます。

DHCP オプション 43 は、DHCP サーバーから DHCP クライアントに情報を送信するために使用します。このオプションは、テキスト文字列として定義されます。このテキスト文字列は、XML ファイル名、共有の場所、およびこの場所にアクセスするための資格情報の値として設定します。例えば次のようになります。

```
option myname code 43 = text;
subnet 192. 168.0.0 netmask 255.255.255.0 {
# default gateway
        option routers 192.168.0.1;
    option subnet-mask 255.255.255.0;
    option nis-domain  "domain.org";
```

```
    option domain-name "domain.org";
    option domain-name-servers 192.168.1.1;
    option time-offset -18000; #Eastern Standard Time
    option vendor-class-identifier "iDRAC";
    set vendor-string = option vendor-class-identifier;
    option myname "-f system_config.xml -i 192.168.0.130 -u user -p password -n cifs -s 2 -d
0 -t 500";
```

ここで、-i は、リモートファイル共有の場所、-f は、文字列内のファイル名とリモートファイル共有への資格情報を示します。

DHCP Option 60 は DHCP クライアントと特定のベンダーを識別し、関連付けます。クライアントのベンダー ID を元に動作するよう設定されている DHCP サーバーには、オプション 60 とオプション 43 を設定してください。Dell PowerEdge サーバーでは、iDRAC はそれ自身をベンダー ID「*iDRAC*」で識別します。したがって、新しい「ベンダークラス」を追加し、その下に「コード 60」の「範囲のオプション」を作成した後で、DHCP サーバーで新規範囲のオプションを有効にする必要があります。

関連タスク

Windows でのオプション 43 の設定 、p. 45
Windows でのオプション 60 の設定 、p. 45
Linux でのオプション 43 およびオプション 60 の設定 、p. 46

Windows でのオプション 43 の設定

Windows でオプション 43 を設定するには、次の手順を実行します。

1. DHCP サーバーで、[スタート] > [管理ツール] > [DHCP] の順に移動して、DHCP サーバー管理ツールを開きます。
2. サーバーを検索して、下のすべての項目を展開します。
3. [範囲のオプション] を右クリックして、[オプションの設定] を選択します。
   [範囲のオプション] ダイログボックスが表示されます。
4. 下にスクロールして、[043 ベンダー固有の情報] を選択します。
5. [データ入力] フィールドで [ASCII] 下の場所をクリックして、XML 設定ファイルが含まれている共有の場所のあるサーバーの IP アドレスを入力します。
   値は、[ASCII] 下に入力すると表示されますが、左側にバイナリとしても表示されます。
6. **OK** をクリックして設定を保存します。

Windows でのオプション 60 の設定

Windows でオプション 60 を設定するには、次の手順を実行します。

1. DHCP サーバーで、[スタート] > [管理ツール] > [DHCP] の順に進み、DHCP サーバー管理ツールを開きます。
2. サーバーを検索し、その下の項目を展開します。
3. [IPv4] を右クリックして、[ベンダークラスの定義] を選択します。
4. [追加] をクリックします。
   次のフィールドで構成されるダイアログボックスが表示されます。
   - [表示名]
   - [説明 :]
   - [ID : バイナリ : ASCII :]
5. [表示名 :] フィールドで、`iDRAC` と入力します。
6. [説明 :] フィールドで、`Vendor Class` と入力します。
7. [ASCII :] セクションをクリックして、`iDRAC` を入力します。
8. [OK]、[終了] の順にクリックします。
9. DHCP ウィンドウで [IPv4] を右クリックし、[事前定義されたオプションの設定] を選択します。
10. [オプションクラス] ドロップダウンメニューから [iDRAC] (手順 4 で作成済み) を選択し、[追加] をクリックします。
11. [オプションタイプ] ダイアログボックスで、次の情報を入力します。
    - [名前] - `iDRAC`
    - [データタイプ] - 文字列
    - [コード] — 060
    - [説明] - デルのベンダークラス識別子
12. [OK] をクリックして、[DHCP] ウィンドウに戻ります。

13. サーバー名下のすべての項目を展開し、［ スコープオプション ］ を右クリックして、［ オプションの設定 ］ を選択します。
14. ［ 詳細設定 ］ タブをクリックします。
15. ［ ベンダークラス ］ ドロップダウンメニューから ［ iDRAC ］ を選択します。`060 iDRAC` が、［ 使用可能なオプション ］ の列に表示されます。
16. ［ 060 iDRAC ］ オプションを選択します。
17. DHCP 提供の標準 IP アドレスと共に、iDRAC に送信する必要がある文字列の値を入力します。文字列の値は、正しい SCP ファイルをインポートするために役立ちます。

    オプションの ［ データ入力、文字列の値 ］ 設定については、次の文字オプションと値のあるテキストパラメータを使用します。

    - Filename (-f) — これはエクスポートされたサーバー構成プロファイルの XML ファイルの名前を示します。このファイル名の指定は、iDRAC バージョン 2.20.20.20 以降では任意です。

      メモ: ファイルの命名規則の詳細に関しては、「自動設定を使用したサーバーとサーバーコンポーネントの設定」を参照してください。
    - Sharename (-n) — ネットワーク共有の名前を示します。
    - ShareType (-s) - 共有タイプを示します。0 は NFS を示し、2 は CIFS を示します。
    - IPAddress (-i) - ファイル共有の IP アドレスを示します。

      メモ: Sharename (-n)、共有タイプ (-s) および IP アドレス (-i) は、渡されなければならない必要な属性です。
    - Username (-u) — ネットワーク共有へのアクセスにユーザー名が必要なことを示します。この情報は、CIFS にのみ必要です。
    - Password (-p) — ネットワーク共有へのアクセスにパスワードが必要なことを示します。この情報は、CIFS にのみ必要です。
    - ShutdownType (-d) — シャットダウンのモードを示します。0 は正常なシャットダウン、1 はシャットダウンの強制を示します。

      メモ: デフォルト設定は 0 です。
    - TimeToWait (-t) — ホスト システムがシャットダウンするまでの待機時間を示します。デフォルト設定は 300 です。
    - EndHostPowerState (-e) — ホストの電源状態を示します。0 はオフを、1 はオンを示します。デフォルトでは 1 に設定されています。

      メモ: ShutdownType (-d)、TimeToWait (-t)、および EndHostPowerState (-e) は、オプションの属性です。

    メモ: Windows を実行している DHCP サーバーにおける、バージョン 2.20.20.20 より前の iDRAC を搭載したオペレーティングシステムでは、(-f) の前にスペースを必ず追加してください。

    NFS: -f system_config.xml -i 192.168.1.101 -n /nfs_share -s 0 -d 1
    CIFS: -f system_config.xml -i 192.168.1.101 -n cifs_share -s 2 -u <*USERNAME*> -p <*PASSWORD*> -d 1 -t 400

Linux でのオプション 43 およびオプション 60 の設定

`/etc/dhcpd.conf` ファイルをアップデートします。オプションの設定手順は、Windows の場合とほぼ同じです。

1. この DHCP サーバーが割り当てることができるアドレスのブロックまたはプールを確保しておきます。
2. オプション 43 を設定し、名前のベンダークラス識別子をオプション 60 に使用します。

```
option myname code 43 = text;
subnet 192.168.0.0 netmask 255.255.0.0  {
#default gateway
    option routers              192.168.0.1;
    option subnet-mask          255.255.255.0;
    option nis-domain          "domain.org";
    option domain-name          "domain.org";
    option domain-name-servers      192.168.1.1;
    option time-offset          -18000;     # Eastern Standard Time
    option vendor-class-identifier "iDRAC";
  set vendor-string = option vendor-class-identifier;
  option myname "-f system_config.xml -i 192.168.0.130 -u user -p password -n cifs -s 2 -d 0 -t 500";
    range dynamic-bootp 192.168.0.128 192.168.0.254;
    default-lease-time 21600;
    max-lease-time 43200;
        }
}
```

ベンダークラス識別子文字列に渡す必要がある必須およびオプションのパラメータは次のとおりです。

- Filename（-f）— エクスポートされたサーバー構成プロファイルの XML ファイルの名前を示します。ファイル名の指定は、iDRAC バージョン 2.20.20.20 以降では任意です。

  メモ: ファイルの命名規則の詳細に関しては、「自動設定を使用したサーバーとサーバーコンポーネントの設定」を参照してください。
- Sharename（-n）— ネットワーク共有の名前を示します。
- ShareType（-s）- 共有タイプを示します。0 は NFS を示し、2 は CIFS を示します。
- IPAddress（-i）- ファイル共有の IP アドレスを示します。

  メモ: Sharename（-n）、共有タイプ（-s）および IP アドレス（-i）は、渡されなければならない必要な属性です。
- Username（-u）— ネットワーク共有へのアクセスにユーザー名が必要なことを示します。この情報は、CIFS にのみ必要です。
- Password（-p）— ネットワーク共有へのアクセスにパスワードが必要なことを示します。この情報は、CIFS にのみ必要です。

  メモ: Linux NFS および CIFS 共有の例：
  - **NFS:** -f system_config.xml -i 192.168.0.130 -n /nfs -s 0 -d 0 -t 500
  - **CIFS:** -f system_config.xml -i 192.168.0.130 -n sambashare/config_files -s 2 -u user -p password -d 1 -t 400

  NFS ネットワーク共有に NFS2 または NFS3 を使用していることを確認してください
- ShutdownType（-d）— シャットダウンのモードを示します。0 は正常なシャットダウン、1 はシャットダウンの強制を示します。

  メモ: デフォルト設定は 0 です。
- TimeToWait（-t）— ホストシステムがシャットダウンするまでの待機時間を示します。デフォルト設定は 300 です。
- EndHostPowerState（-e）— ホストの電源状態を示します。0 はオフを、1 はオンを示します。デフォルトでは 1 に設定されています。

  メモ: ShutdownType（-d）、TimeToWait（-t）、および EndHostPowerState（-e）は、オプションの属性です。

次の例は、dhcpd.conf ファイルからの静的 DHCP 予約の例です。

```
host my_host {
hardware ethernet b8:2a:72:fb:e6:56;
  fixed-address 192.168.0.211;
option host-name "my_host";
option myname " -f r630_raid.xml -i 192.168.0.1 -n /nfs -s 0 -d 0 -t 300";
}
```

メモ: `dhcpd.conf` ファイルを編集した後、変更を適用するために必ず dhcpd サービスを再起動してください。

自動設定を有効にする前の前提条件

自動設定機能を有効にする前に、次の各項目が既に設定されていることを確認します。

- サポートされているネットワーク共有（NFS または CIFS）は、iDRAC および DHCP サーバーと同じサブネットで使用可能です。ネットワーク共有をテストし、アクセス可能なこと、およびファイアウォールとユーザー権限が正しく設定されていることを確認します。
- サーバー設定プロファイルはネットワーク共有にエクスポートされます。また、XML ファイルに必要な変更が完了していることを確認し、自動設定処理が開始されたときに正しい設定を適用できるようにします。
- iDRAC がサーバーを呼び出して自動設定機能を初期化するのに対して必要に応じて DHCP サーバーは設定され、DHCP 構成がアップデートされます。

iDRAC ウェブインタフェースを使用した自動設定の有効化

DHCPv4 および IPv 4 を有効にするオプションが有効で、自動検出が無効になっていることを確認します。

自動設定を有効化するには、次の手順を実行します。

1. iDRAC のウェブインタフェースで、[概要] > [iDRAC 設定] > [ネットワーク] へと移動します。
   [ネットワーク] ページが表示されます。
2. [自動設定] セクションで、[DHCP プロビジョニングを有効にする] ドロップダウンメニューから次のいずれかのオプションを選択します。

- ［一回のみ有効］ – DHCP サーバーによって参照される XML ファイルを使用して、コンポーネントを一回だけ設定します。この後、自動設定は無効になります。
- ［リセット後一回のみ有効］ – iDRAC のリセット後、DHCP サーバーによって参照される XML ファイルを使用してコンポーネントを 1 回だけ設定します。この後、自動設定は無効になります。
- ［無効化］ — 自動設定機能を無効にします。

3. 設定を適用するには、［適用］ をクリックします。
   ネットワークページが自動的に更新されます。

RACADM を使用した自動設定の有効化

RACADM を使用して自動設定機能を有効にするには、`iDRAC.NIC.AutoConfig` オブジェクトを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

自動設定機能の詳細に関しては、**delltechcenter.com/idrac** にあるホワイトペーパー、『*Zero-Touch Bare Metal Server Provisioning using Dell iDRAC with Lifecycle Controller Auto Config*』(Dell iDRAC を使用した、Lifecycle Controller の自動設定でのゼロタッチベアメタルサーバープロビジョニング) を参照してください。

セキュリティ向上のためのハッシュパスワードの使用

バージョン 2.*xx.xx.xx* 搭載の PowerEdge サーバーでは、一方向ハッシュ形式を使用してユーザーパスワードと BIOS パスワードを設定できます。ユーザー認証メカニズムは影響を受けず (SNMPv3 と IPMI を除く)、パスワードをプレーンテキスト形式で指定できます。

新しいパスワードハッシュ機能により次のことが可能になります。

- 独自の SHA256 ハッシュを生成して iDRAC ユーザーパスワードと BIOS パスワードを設定できます。これにより、サーバー構成プロファイル、RACADM、および WSMAN で SHA256 の値を指定できます。SHA256 パスワードの値を提供する場合は、SNMPv3 と IPMI を介して認証することはできません。
- 現在のプレーンテキストメカニズムを使用して、すべての iDRAC ユーザーアカウントと BIOS パスワードを含むテンプレートサーバーをセットアップすることができます。サーバーのセットアップ後、パスワードハッシュ値と共にサーバー設定プロファイルをエクスポートすることができます。エクスポートには SNMPv3 認証に必要なハッシュ値が含まれます。このプロファイルのインポートによって、ハッシュ化されたパスワード値を設定されたユーザーに対する IPMI 認証が失われ、F2 IDRAC インタフェースにユーザーアカウントが無効であると表示されることになります。
- iDRAC GUI などののその他のインターフェイスにはユーザーアカウントが有効であると表示されます。

メモ: デル第 12 世代 PowerEdge サーバーをバージョン 2.xx.xx.xx から 1.xx.xx にダウングレードするときは、サーバーがハッシュ認証で設定されていると、パスワードがデフォルトに設定されていない限り、いずれのインタフェースにもログインできません。

SHA 256 を使用して、ソルトあり、またはソルトなしでハッシュパスワードを生成することができます。

ハッシュパスワードを含め、エクスポートするにはサーバー制御権限が必要です。

すべてのアカウントへのアクセスが失われた場合は、iDRAC 設定ユーティリティまたはローカル RACADM を使用し、iDRAC のデフォルトタスクへのリセットを実行します。

iDRAC のユーザーアカウントのパスワードが SHA256 パスワードハッシュのみで設定され、その他のハッシュ (SHA1v3Key または MD5v3Key) を使用していない場合、SNMP v3 を介した認証は使用できません。

RACADM を使用したハッシュパスワード

ハッシュパスワードを設定するには、`set` コマンドで次のオブジェクトを使用します。

- iDRAC.Users.SHA256Password
- iDRAC.Users.SHA256PasswordSalt

エクスポートされたサーバー構成プロファイルにハッシュパスワードを含めるには、次のコマンドを使用します。

```
racadm get -f <file name> -l <NFS / CIFS share> -u <username> -p <password>  -t <filetype> --
includePH
```

関連するハッシュが設定された場合は、ソルト属性を設定する必要があります。

メモ: この属性は、INI 設定ファイルには適用されません。

サーバー構成プロファイルのハッシュパスワード

新しいハッシュパスワードは、サーバー構成プロファイルでオプションでエクスポートできます。

サーバー構成プロファイルをインポートする場合は、既存のパスワード属性または新しいパスワードハッシュ属性をコメント解除できます。その両方がコメント解除されると、エラーが生成され、パスワードが設定されません。コメントされた属性は、インポート時に適用されません。

SNMPv3 および IPMI 認証なしでのハッシュパスワードの生成

SNMPv3 および IPMI 認証なしでハッシュパスワードを生成するには、次の手順を実行します。

1. iDRAC ユーザーアカウントの場合は、SHA256 を使用してパスワードをソルト化する必要があります。

   パスワードをソルト化する場合は、16 バイトのバイナリ文字列が付加されます。ソルトの長さは 16 バイトである必要があります（提供される場合）。
2. インポートされたサーバー構成プロファイル、RACADM コマンド、または WSMAN でハッシュ値とソルトを提供します。
3. パスワードの設定後に、通常のプレーンテキストパスワードは機能しますが、パスワードがハッシュでアップデートされた iDRAC ユーザーアカウントに対して SNMP v3 および IPMI 認証が失敗します。

管理ステーションのセットアップ

管理ステーションは、iDRAC 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、リリースノートを参照してください。
2. 対応ウェブブラウザ（Internet Explorer、Firefox、Chrome、または Safari）をインストールして設定します。
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 iDRAC 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、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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

関連概念

VMCLI ユーティリティのインストールと使用、p. 241

関連タスク

対応ウェブブラウザの設定、p. 57

iDRAC へのリモートアクセス

管理ステーションから iDRAC 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 iDRAC 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。管理下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関しては、**dell.com/support/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 — iDRAC NIC を専用または LOM1 に設定し、管理ステーションが iDRAC と同じネットワークに存在することを確認します。

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、iDRAC 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。

関連概念

仮想コンソールの起動 、p. 226

関連タスク

ネットワーク設定 、p. 40

管理下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 の詳細に関しては、**dell.com/support/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。

関連タスク

ローカル管理者アカウント設定の変更 、p. 50

ローカル管理者アカウント設定の変更

iDRAC IP アドレスを設定した後で、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 [パスワードの変更] 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

iDRAC 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を指定するには、次の手順を実行します。

1. iDRAC 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、『iDRAC 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 iDRAC 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、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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

サーバーを冷却するために必要な電力は、システム電力全体におけるかなりの電力量の誘因となり得ます。温度制御はファン速度およびシステム電源管理を介したシステム冷却のアクティブ管理で、システムの消費電力、通気、およびシステムのノイズ出力を最小化しながら、システムの信頼性を確保します。温度制限設定を調整して、システムパフォーマンスおよび 1 ワットあたりのパフォーマンス要件のために最適化することができます。

iDRAC 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、以下の温度設定を変更することができます。

- パフォーマンスのための最適化
- 最小電力のための最適化
- 最大排気温度の設定
- ファンオフセットによる必要に応じた通気の増加
- 最小ファン速度の増加による通気の増加

iDRAC ウェブインタフェースを使用したサーマル設定の変更

温度設定を変更するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、[概要] > [ハードウェア] > [ファン] > [セットアップ] に移動します。
   [ファンのセットアップ] ページが表示されます。
2. 以下を指定します。
   - [温度プロファイル] - 温度プロファイルを選択します。
     - [デフォルト温度プロファイル設定] - 温度アルゴリズムが [システム BIOS] > [システム BIOS 設定システムプロファイル設定] ページで定義されたものと同じシステムプロファイル設定を使用することを示します。

     これはデフォルトで [デフォルト温度プロファイル設定] に設定されています。BIOS プロファイルに依存しないカスタムアルゴリズムを選択することもできます。これには、次のオプションがあります。
     - [最大パフォーマンス (パフォーマンス最適化)] :
       - メモリまたは CPU スロットルの確率を削減。
       - ターボモードのアクティブ化の確率を増加。
       - 一般に、アイドル負荷および応力負荷ではファン速度が上昇。
     - [最小電力 (1 ワットあたりのパフォーマンス最適化)] :
       - 最適なファン電力状態に基づいて、最小のシステム消費電力のために最適化。
       - 一般に、アイドル負荷および応力負荷ではファン速度が減少。

     メモ: [最大パフォーマンス] または [最小電力] を選択すると、[システム BIOS] > [システム BIOS 設定.システムプロファイル設定] ページのシステムプロファイル設定に関連付けられている温度設定が上書きされます。
   - [最大排気温度制限] - ドロップダウンメニューから最大排気温度を選択します。この値はシステムに基づいて表示されます。

     デフォルト値は [デフォルト、70°C (158°F)] です。

     このオプションを使用すると、排気温度が選択した排気温度制限を超過しないように、システムのファン速度を変更させることが可能になります。この機能はシステム負荷およびシステム冷却能力に依存するため、すべてのシステム稼動条件下で常に保証されるとは限りません。

- [ファン速度オフセット] - このオプションを選択することにより、サーバーに冷却機能を追加することができます。ハードウェア (たとえば新規 PCIe カードなど) を追加した場合、冷却が追加で必要になることがあります。ファン速度オフセットにより、ファン速度がオフセット % 値に従って、温度制御アルゴリズムによって計算されたベースラインファン速度を超過する速度に上昇します。可能な値は次のとおりです。
  - [低ファン速度] - ファン速度を緩やかなファン速度まで上昇させます。
  - [中ファン速度] - ファン速度を中程度近くまで上昇させます。
  - [高ファン速度] - ファンの速度を最大速度近くまで上昇させます。
  - [ファン最大速] - ファンの速度を最大速度まで上昇させます。
  - [オフ] - ファン速度オフセットはオフに設定されます。これはデフォルト値です。オフに設定されると、パーセントは表示されません。デフォルトのファン速度はオフセットなしで適用されます。それとは異なり、最大設定の場合は、すべてのファンが最大速度で稼働します。

  ファン速度オフセットは動的で、システムに基づきます。各オフセットのファン速度上昇率 (%) は、各オプションの横に表示されます。

  ファン速度オフセットは、すべてのファンの速度を同じ割合で上昇させます。ファン速度は、個々のコンポーネントの冷却の必要性に応じてオフセット速度を超える速度に上昇する場合があります。全体的なシステム電力消費量の上昇が予測されます。

  ファン速度オフセットでは、システムファン速度を 4 つの段階で上昇させることができます。これらの 4 段階は、サーバーシステムファンの標準的なベースライン速度と最大速度の間で均等に分割されています。一部のハードウェア構成ではベースラインファン速度が高くなるため、最大オフセット以外のオフセット値で最大速度を達成することになります。

  最も一般的な使用シナリオは、非標準の PCIe アダプタの冷却です。ただし、この機能は、他の目的のためにシステムの冷却機能を向上させるために使用することもできます。

- [最小ファン速度 (PWM 単位)(最大速度の %)] - ファン速度を調整する場合はこのオプションを選択します。他のカスタムファン速度オプションの場合に必要なファン速度に到達しないときは、高いベースラインシステムファン速度を設定するか、システム速度を増加させることができます。
  - [デフォルト] - デフォルト値によって決定されます。最小ファン速度を、システム冷却アルゴリズムによって決定されたデフォルト値に設定します。
  - [カスタム] - 割合値 (%) を入力します。

  最小ファン速度 (PWM) の許容範囲は、システム設定に基づいて変化します。最初の値がアイドル時の速度であり、2 番目の値は、設定最大速度です (システム設定に 100 % 基づかないことがあります)。

  システムファンは、システムの温度要件に基いてこの速度より高い速度で稼働できますが、定義された最小速度よりも低い速度で稼働することはできません。たとえば、最小ファン速度を 35 % で設定すると、ファン速度は 35 % PWM よりも低くなりません。

  メモ: 0 % PWM は、ファンはオフ状態であることを示しません。これは、ファンが実現可能な最小ファン速度です。

  この設定は保持されます。つまり、設定され、適用されると、システム再起動、パワーサイクル、iDRAC アップデート、または BIOS アップデートのときにデフォルトの設定に自動的に変更されません。一部の Dell サーバーでは、これらのカスタムユーザー冷却オプションの一部またはすべてがサポートされることがあります。これらのオプションがサポートされない場合、オプションは表示されないか、またはカスタム値を指定することができません。

3. 設定を適用するには、[適用] をクリックします。

   次のメッセージが表示されます。

   ```
   It is recommended to reboot the system when a thermal profile change has been made. This is
   to ensure all power and thermal settings are activated.
   ```

   [後で再起動] または [今すぐ再起動] をクリックします。

   メモ: 設定を反映にするには、システムを再起動する必要があります。

RACADM を使用した温度設定の変更

温度設定を変更するには、次の表に示されたように、**system.thermalsettings** グループ内のオブジェクトを **set** コマンドで使用します。

表 8. 温度設定

表 8. 温度設定 （続き）

オブジェクト	説明	使用状況	例

AirExhaustTemp	最大排気温度制限を設定することができます。	次の値のいずれかに設定します（システムに基づく）。
		● 0 — 40°C を示します。
		● 1 — 45°C を示します。
		● 2 — 50°C を示します。
		● 3 — 55°C を示します。
		● 4 — 60°C を示します。
		● 255 - 70 °C を示します(デフォルト)。
			システムで既存の設定を確認するには、次のコマンドを実行します。
			`racadm get system.thermalsettings.AirExhaustTemp`
			出力は次のとおりです。
			`AirExhaustTemp=70`
			この出力は、システムが排気温度を 70 °C に制限するよう設定されていることを示します。
			排気温度制限を 60 °C に設定するには、次のコマンドを実行します。
			`racadm set system.thermalsettings.AirExhaustTemp 4`
			出力は次のとおりです。
			`Object value modified successfully.`
			システムで特定の排気温度制限がサポートされない場合は、次のコマンドを実行します。
			`racadm set system.thermalsettings.AirExhaustTemp 0`
			次のエラーメッセージが表示されます。
			`ERROR: RAC947: Invalid object value specified.`
			オブジェクトの種類に応じた値を指定します。
			詳細については、RACADM のヘルプを参照してください。
			デフォルト値に制限を設定するには、次のコマンドを実行します。
			`racadm set system.thermalsettings.AirExhaustTemp 255`

FanSpeedHighOffsetVal	● この変数を取得すると、高速ファン速度オフセット設定用のファン速度オフセッ	0～100 の値	`racadm get system.thermalsettings`

表 8. 温度設定 （続き）

オブジェクト	説明	使用状況	例

	ト値（%PWM）が読み取られます。
	● この値は、システムによって異なります。
	● `FanSpeedOffset` オブジェクトを使用してインデックス値 1 でこの値を設定します。
			`FanSpeedHighOffsetVal`
			たとえば「66」などの数値が返されます。この値は、次のコマンドを使用したときに、ベースラインファン速度上に高速ファン速度オフセット（66% PWM）が適用されることを意味します。
			`racadm set system.thermalsettings FanSpeedOffset 1`

`FanSpeedLowOffsetVal`	● この変数を取得すると、低速ファン速度オフセット設定用のファン速度オフセット値（%PWM）が読み取られます。
	● この値は、システムによって異なります。
	● `FanSpeedOffset` オブジェクトを使用してインデックス値 0 でこの値を設定します。
		0～100 の値	`racadm get system.thermalsettings FanSpeedLowOffsetVal`
			これにより、「23」などの値が返されます。これは、次のコマンドを使用したときに、ベースラインファン速度上に低速ファン速度オフセット（23 % PWM）が適用されることを意味します。
			`racadm set system.thermalsettings FanSpeedOffset 0`

`FanSpeedMaxOffsetVal`	● この変数を取得すると、最速ファン速度オフセット設定用のファン速度オフセット値（%PWM）が読み取られます。
	● この値は、システムによって異なります。
	● `FanSpeedOffset` を使用してインデックス値 3 でこの値を設定します。
		0～100 の値	`racadm get system.thermalsettings FanSpeedMaxOffsetVal`
			これにより、「100」などの値が返されます。これは、次のコマンドを使用したときに、最速ファン速度オフセット（フルスピードのこと、100% PWM）が適用されることを意味します。通常、このオフセットはファン速度がフルスピードまで上昇する原因となります。
			`racadm set system.thermalsettings FanSpeedOffset 3`

`FanSpeedMediumOffsetVal`	● この変数を取得すると、中速ファン速度オフセット設定用のファン速度オフセット値（%PWM）が読み取られます。 ● この値は、システムによって異なります。	0～100 の値	`racadm get system.thermalsettings FanSpeedMediumOffsetVal` これにより、「47」などの値が返されます。これは、次のコマン

表 8. 温度設定 （続き）

オブジェクト	説明	使用状況	例
	● FanSpeedOffset オブジェクトを使用してインデックス値 2 でこの値を設定します。		ドを使用したときに、ベースラインファン速度上に中速ファン速度オフセット（47 % PWM）が適用されることを意味します。 `racadm set system.thermalsettings FanSpeedOffset 2`

FanSpeedOffset	● get コマンドでこのオブジェクトを使用すると、既存のファン速度オフセット値が表示されます。
	● set コマンドでこのオブジェクトを使用すると、必要なファン速度オフセット値を設定することができます。
	● このインデックス値により、適用されるオフセットが決定され、FanSpeedLowOffsetVal、FanSpeedMaxOffsetVal、FanSpeedHighOffsetVal、および FanSpeedMediumOffsetVal オブジェクト（以前に定義済み）が、オフセットが適用される値になります。
		値は次のとおりです。
		● 0 - 低速ファン速度
		● 1 - 高速ファン速度
		● 2 - 中速ファン速度
		● 3 - 最大ファン速度
		● 255 - なし
			既存の設定を表示するには、次のコマンドを実行します。
			`racadm get system.thermalsettings.FanSpeedOffset`
			ファン速度オフセットを高い値（FanSpeedHighOffsetVal で定義済み）に設定するには、次のコマンドを実行します。
			`racadm set system.thermalsettings.FanSpeedOffset 1`

MFSMaximumLimit	MFS の最大制限の読み取り	1～100 の値	MinimumFanSpeed オプションを使用して設定できる最大値を表示するには、次のコマンドを実行します。 `racadm get system.thermalsettings.MFSMaximumLimit`
MFSMinimumLimit	MFS の最低制限の読み取り	0～MFSMaximumLimit の値 デフォルト値は 255 です（なしを意味します）。	MinimumFanSpeed オプションを使用して設定できる最小値を表示するには、次のコマンドを実行します。 `racadm get system.thermalsettings.MFSMinimumLimit`
MinimumFanSpeed	● システムが稼働するために必要な最小ファン速度を設定できます。 ● ファン速度のベースライン（フロアー）が定義され、定義されたこのファン速度値よりも低い速度でファンが	MFSMinimumLimit～MFSMaximumLimit の値 get コマンドが 255 を報告した場合は、ユーザーが設定したオフセットが適用されていないことを意味します。	システムの最小速度が 45% PWM（45 は MFSMinimumLimit～MFSMaximumLimit の値である必要があります）よりも低く

表 8. 温度設定

オブジェクト	説明	使用状況	例
	稼働できるようになります。 ● この値はファン速度の %PWM 値です。		ならないようにするには、次のコマンドを実行します。 `racadm set system.thermalsettings.MinimumFanSpeed 45`

`ThermalProfile`	● 温度ベースアルゴリズムを指定することができます。
	● 必要に応じて、プロファイルに関連付けられた温度動作のシステムプロファイルを設定できます。
		値は次のとおりです。
		● 0 - 自動
		● 1 - 最大パフォーマンス
		● 2 - 最小電力
			既存の温度プロファイル設定を表示するには、次のコマンドを実行します。
			`racadm get system.thermalsettings.ThermalProfile`
			温度プロファイルを最大パフォーマンスに設定するには、次のコマンドを実行します。
			`racadm set system.thermalsettings.ThermalProfile 1`

`ThirdPartyPCIFanResponse`	● サードパーティ PCI カード用サーマルオーバーライド。 ● 検出されたサードパーティ PCI カードのデフォルトのシステムファンの応答を、無効または有効にすることができます。 ● サードパーティ PCI カードのメッセージ ID PCI3018 を Lifecycle Controller ログに表示することで、カードの存在を確認することができます。	値は次のとおりです。 ● 1 — 有効 ● 0 — 無効 **メモ:** デフォルト値は 1 です。	検出されたサードパーティ PCI カードのデフォルトのファン速度応答設定を無効にするには： `racadm set system.thermalsettings.ThirdPartyPCIFanResponse 0`

iDRAC 設定ユーティリティを使用したサーマル設定の変更

サーマル設定を変更するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、［ サーマル ］ に移動します。
   ［ iDRAC 設定 サーマル ］ ページが表示されます。
2. 以下を指定します。
   - サーマルプロファイル
   - 最大排気温度制限
   - ファン速度オフセット
   - 最小ファン速度

   フィールドの詳細については、「ウェブインタフェースを使用したサーマル設定の変更」を参照してください。

   この設定は保持されます。つまり、設定され、適用されると、システム再起動、パワーサイクル、iDRAC アップデート、または BIOS アップデートのときにデフォルトの設定に自動的に変更されません。一部の Dell サーバーでは、これらのカスタムユーザー冷却オプションの一部またはすべてがサポートされることがあります。これらのオプションがサポートされない場合、オプションは表示されないか、またはカスタム値を指定することができません。

3. ［ 戻る ］、［ 終了 ］ の順にクリックし、［ はい ］ をクリックします。
   サーマルが設定されました。

対応ウェブブラウザの設定

メモ: 対応ブラウザとバージョンの詳細については、**dell.com/idracmanuals** にある『リリースノート』を参照してください。

iDRAC ウェブインタフェースのほとんどの機能は、デフォルト設定でこれらのブラウザを使用してアクセスできます。一部の機能は、動作させるためにいくつかの設定を変更する必要があります。これらの設定には、ポップアップブロッカーの無効化、Java、ActiveX、または HTML5 プラグインサポートの有効化などが含まれます。

プロキシサーバー経由でインターネットに接続している管理ステーションから iDRAC 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します。

メモ: Internet Explorer または Firefox を使用して iDRAC ウェブインタフェースにアクセスする場合は、このセクションで説明されているように特定の設定を行う必要がある場合があります。デフォルト設定で他の対応ブラウザを使用することができます。

関連概念

ウェブインタフェースのローカライズバージョンの表示、p. 62

関連タスク

信頼済みサイトリストへの iDRAC IP の追加、p. 57
Firefox のホワイトリスト機能の無効化、p. 58

Internet Explorer の設定

本項には、iDRAC ウェブインタフェースにアクセスしてすべての機能を使用できるようにするための Internet Explorer（IE）の設定に関する詳細を記載しています。設定には次のようなものがあります。

- セキュリティ設定のリセット
- 信頼済みサイトへの iDRAC IP の追加
- Active Directory SSO を有効にするための IE の設定

Internet Explorer のセキュリティ設定のリセット

Internet Explorer（IE）設定が Microsoft 推奨のデフォルト設定に設定されていることを確認し、このセクションで説明されているように設定をカスタマイズしてください。

1. 管理者として、または管理者アカウントを使用して IE を開きます。
2. ［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］または［ローカルイントラネット］をクリックします。
3. ［カスタムレベル］をクリックして［Medium-Low］を選択し、［リセット］をクリックします。［OK］をクリックして確認します。

信頼済みサイトリストへの iDRAC IP の追加

iDRAC ウェブインタフェースにアクセスしたときに、リストに IP アドレスがないと iDRAC IP アドレスを信頼済みドメインのリストに追加するように求められます。 完了したら、［更新］をクリックするか、またはウェブブラウザを再度立ち上げて iDRAC ウェブインタフェースへの接続を確立します。IP を追加するように求められない場合は、IP を信頼済みサイトのリストへ手動で追加することをお勧めします。

メモ: ブラウザに信頼されていない証明書で iDRAC ウェブインタフェースに接続すると、ブラウザの最初の証明書エラー警告を受け入れた後、再表示される場合があります。

信頼済みサイトリストに iDRAC 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］の順にクリックします。
2. ［この Web サイトをゾーンに追加する］に、iDRAC 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。

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 iDRAC 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。

Mozilla Firefox の設定

このセクションは、iDRAC ウェブインタフェースにアクセスして、すべての機能を使用できるようにする Firefox の設定に関する詳細を記載しています。設定には以下が含まれます。

- ホワイトリスト機能の無効化
- Active Directory SSO を有効にするための Firefox の設定

Firefox のホワイトリスト機能の無効化

Firefox には、プラグインをホストする個別サイトそれぞれのために、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。有効な場合は、ホワイトリスト機能を使用するために、アクセスする各 iDRAC の仮想コンソールビューアーをインストールする必要があります。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。

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 にドメイン名を追加します (コンマ区切りのリストを使用)。
4. network.negotiate-auth.delegation-uris にドメイン名を追加します (コンマ区切りのリストを使用)。

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. 対応バージョンのブラウザ (Internet Explorer (Windows)、Mozilla Firefox (Windows または Linux)、Google Chrome、Safari) がインストールされていることを確認します。

   対応ブラウザバージョンの詳細に関しては、**dell.com/idracmanuals** にある『リリースノート』を参照してください。
2. Internet Explorer を使用するには、IE を [管理者として実行] に設定します。
3. ActiveX、Java、または HTML5 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 のみでサポートされています。HTML5 または 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。

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。

6. MAC オペレーティングシステムを使用している場合は、[ユニバーサルアクセス] ウィンドウ内の [補助装置にアクセスできるようにする] オプションを選択します。

   詳細に関しては、MAC オペレーティングシステムのマニュアルを参照してください。

関連概念

HTML5 ベースのプラグインを使用するための Internet Explorer の設定 、p. 59
Java プラグインを使用するためのウェブブラウザの設定 、p. 59
ActiveX プラグインを使用するための IE の設定 、p. 60
管理ステーションへの CA 証明書のインポート 、p. 61

HTML5 ベースのプラグインを使用するための Internet Explorer の設定

HTML5 仮想コンソールと仮想メディア API は HTML5 テクノロジーを使用することで作成されます。HTML5 テクノロジーの利点は次の通りです。

- クライアントワークステーションへのインストールが必要ない。
- 互換性はブラウザに基づいており、オペレーティングシステムまたはインストールされているコンポーネントに基づいていない。
- ほとんどのデスクトップとモバイルプラットフォームとの互換性がある。
- 素早く導入でき、クライアントはウェブページの一部としてダウンロードされる。

HTML5 ベースの仮想コンソールと仮想メディアアプリケーションを起動して実行する前に Internet Explorer (IE) を設定する必要があります。ブラウザ設定を行うには、次の手順を実行します。

1. ポップアップブロッカーを無効にします。これを行うには、[ツール] > [インターネットオプション] > [プライバシー] をクリックし、[ポップアップブロックを有効にする] チェックボックスのチェックを外します。
2. HTML5 仮想コンソールを次のいずれかの方法で起動します。
   - IE で [ツール] > [互換表示設定] をクリックし、[イントラネットサイトを互換表示で表示する] チェックボックスのチェックを外します。
   - IPv6 アドレスを使用した IE では、次のように Ipv6 アドレスを変更します。

     ```
     https://[fe80::d267:e5ff:fef4:2fe9]/ to https://fe80--d267-e5ff-fef4-2fe9.ipv6-literal.net/
     ```

   - IPv6 アドレスを使用した IE での Direct HTML5 仮想コンソールでは、次のように IPv6 アドレスを変更します。

     ```
     https://[fe80::d267:e5ff:fef4:2fe9]/console to https://fe80--d267-e5ff-fef4-2fe9.ipv6-literal.net/console
     ```

3. IE でタイトルバーの情報を表示するには、[コントロールパネル] > [デスクトップのカスタマイズ] > [個人設定] > [Windows クラシック] と移動します。

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。

関連概念

仮想コンソールの設定 、p. 226

ActiveX プラグインを使用するための IE の設定

開始する前に IE ブラウザを設定し、ActiveX ベースの仮想コンソールと仮想メディアアプリケーションを実行する必要があります。ActiveX アプリケーションは、iDRAC サーバーからの署名付き CAB ファイルとして提供されます。プラグインのタイプが仮想コンソールで Native-ActiveX タイプに設定されている場合、仮想コンソールを開始しようとすると、CAB ファイルがクライアントシステムにダウンロードされ、ActiveX ベースの仮想コンソールが開始されます。Internet Explorer には、これらの ActiveX ベースアプリケーションをダウンロード、インストール、および実行するための設定が必要です。

Internet Explorer は、64 ビットブラウザで 32 ビットバージョンと 64 ビットバージョンの両方を使用できます。任意のバージョンを使用できますが、プラグインを 64 ビットブラウザにインストールした場合に、32 ビットブラウザでビューアを実行するには、プラグインを再インストールする必要があります。

メモ: ActiveX プラグインは、Internet Explorer 以外では使用できません。

メモ: Internet Explorer 9 が搭載された システム で ActiveX プラグインを使用するには、Internet Explorer を設定する前に、Internet Explorer で、または Windows Server のオペレーティングシステムのサーバー管理で、セキュリティ強化モードを必ず無効にしてください。

Windows 2003、Windows XP、Windows Vista、Windows 7、および Windows 2008 の ActiveX アプリケーションについて、ActiveX プラグインを使用するには、次の Internet Explorer 設定を行います。

1. ブラウザのキャッシュをクリアします。
2. iDRAC 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］ へと進み、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: Internet Explorer 11 を搭載したシステムでは、［ツール］ > ［ 互換表示設定］ をクリックして iDRAC IP を追加するようにしてください。

   メモ:

   - Internet Explorer のさまざまなバージョンは、［インターネットオプション］ を共有します。したがって、サーバーを一つのブラウザの*信頼済みサイト*のリストに追加した後、別のブラウザも同じ設定を使用することになります。
   - 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。

関連概念

ブラウザキャッシュのクリア 、p. 61
Windows Vista 以降の Microsoft オペレーティングシステム用の追加設定 、p. 61

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 iDRAC 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. [このウェブサイトをゾーンに追加する] フィールドに iDRAC 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。

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-uninstall` を実行します。
   [Java キャッシュ] ビューアが表示されます。
2. iDRAC 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 の信頼済み証明書ストアに 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。

関連概念

Java の信頼済み証明書ストアへの CA 証明書のインポート 、p. 61
ActiveX の信頼済み証明書ストアへの CA 証明書のインポート 、p. 61

Java の信頼済み証明書ストアへの CA 証明書のインポート

Java の信頼済み証明書ストアに 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、[信頼済み証明書] 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 の信頼済み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 の信頼済み証明書ストアへの 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 の信頼済み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 (name of CA cert) -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**

ウェブインタフェースのローカライズバージョンの表示

iDRAC 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。

iDRAC ウェブインタフェースは、対応言語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、iDRAC 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、iDRAC 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。

デバイスファームウェアのアップデート

iDRAC では、Lifecycle Controller アップデートを使用することによって iDRAC、BIOS、および以下のようなすべてのデバイスファームウェアをアップデートできます。

- Fibre Channel (FC) カード
- 診断
- オペレーティングシステムドライバパック
- ネットワークインタフェースカード (NIC)
- RAID コントローラ
- 電源装置ユニット (PSU)
- NVMe PCIe デバイス
- SAS/SATA ハードドライブ
- 内部および外部エンクロージャのバックプレーンアップデート
- OS コレクタ

注意: PSU ファームウェアのアップデートは、システム設定と PSU モデルによって数分かかる場合があります。PSU の損傷を避けるため、PSU ファームウェアのアップデート中に、アップデートプロセスを中断したりシステムの電源を入れたりしないでください。

必要なファームウェアを iDRAC にアップロードする必要があります。アップロードの完了後に、デバイスにインストールされている現在のバージョンのファームウェアと適用中のバージョンが表示されます。アップロード中のファームウェアが有効でない場合、エラーメッセージが表示されます。再起動を必要としないアップデートは即時に適用されます。システム再起動を必要とするアッ

プデートはステージングされ､次のシステム再起動時に実行されるようにコミットされます。すべてのアップデートを実行するために必要なシステム再起動は 1 度のみです。

ファームウェアのアップデート後、[システムインベントリ] ページにアップデートされたファームウェアバージョンが表示され、ログが記録されます。

サポートされているファームウェアイメージファイルの種類は、以下の通りです。

- `.exe` — Windows ベースの Dell Update Package (DUP)
- `.d7` — iDRAC と Lifecycle Controller ファームウェアの両方が含まれています。

`.exe` 拡張子のファイルには、システム制御権限が必要です。リモートファームウェアアップデートのライセンス対象機能、および Lifecycle Controller が有効になっている必要があります。

`.d7` 拡張子のファイルには、設定権限が必要です。

メモ: iDRAC ファームウェアのアップグレード後、NTP を使用して iDRAC 時間をリセットするまで、Lifecycle Controller ログに表示されるタイムスタンプに違いが生じる場合があります。Lifecycle ログは、iDRAC 時間がリセットされるまで BIOS 時間を表示します。

ファームウェアアップデートは、次の方法で実行できます。

- ローカルシステムまたはネットワーク共有からサポートするイメージタイプを 1 つずつアップロード。
- FTP、TFTP、または HTTP サイト、または Windows DUP と対応するカタログファイルを含むネットワークリポジトリに接続。

  Dell Repository Manager を使用して、カスタムリポジトリを作成することができます。 詳細については､『*Dell Repository Manager Data Center ユーザーズガイド*』を参照してください。iDRAC は、 BIOS とシステムにインストールされたファームウェアとの間の差異レポートと、リポジトリで利用可能なアップデートを提供できます。リポジトリに含まれる適用可能なすべてのアップデートはシステムに適用されます。この機能は、iDRAC Enterprise ライセンスで利用できます。
- カタログファイルおよびカスタムリポジトリを使用した定期的な自動ファームウェアアップデートをスケジューリング。

iDRAC ファームウェアのアップデートに使用できる複数のツールとインタフェースがあります。次の表は、iDRAC ファームウェアにのみ適用されます。表には、対応インタフェース、イメージファイルの種類、Lifecycle Controller をファームウェアのアップデートが可能な状態にする必要があるかどうかが記載されています。

表 9. イメージファイルの種類と依存関係

	.D7 イメージ		iDRAC DUP	
インタフェース	対応	LC を有効にする必要がある	対応	LC を有効にする必要がある
BMCFW64.exe ユーティリティ	有	無	無	該当なし
Racadm FW アップデート (旧)	有	無	無	該当なし
Racadm アップデート (新)	有	有	有	有
iDRAC UI	有	有	有	有
WSMAN	有	有	有	有
帯域内 OS DUP	無	該当なし	有	無

次の表は､ファームウェアが特定のコンポーネントに対してアップデートされた場合にシステムの再起動が必要となるかどうかを示しています。

メモ: 複数のファームウェアのアップデートを帯域外の方法で適用する場合、アップデートは不要なシステム再起動の回数を減らすため、最も効率的な順序で行われます。

表 10. ファームウェアアップデート — 対応コンポーネント

コンポーネント名	ファームウェアのロールバックをサポートしていますか (はい、または、いいえ)	帯域外 — システム再起動の必要性	帯域内 — システム再起動の必要性	Lifecycle Controller GUI — 再起動の必要性
診断	無	無	無	無

表 10. ファームウェアアップデート — 対応コンポーネント （続き）

コンポーネント名	ファームウェアのロールバックをサポートしていますか（はい、または、いいえ）	帯域外 — システム再起動の必要性	帯域内 — システム再起動の必要性	Lifecycle Controller GUI — 再起動の必要性
オペレーティングシステムのドライバパック	無	無	無	無
Lifecycle Controller 使用 iDRAC	有	無	**いいえ*	有
BIOS	有	有	有	有
RAID コントローラ	有	有	有	有
バックプレーン	有	有	有	有
エンクロージャ	有	有	無	有
NIC	有	有	有	有
電源装置ユニット	有	有	有	有
CPLD	無	有	有	有
FC カード	有	有	有	有
NVMe PCIe SSD ドライブ（第 13 世代 Dell PowerEdge サーバーのみ）	有	無	無	無
SAS/SATA ハードドライブ	無	有	有	無
CMC（PowerEdge FX2 サーバー）	無	有	有	有
OS コレクタ	無	無	無	無

* は、システムの再起動は不必要であっても、アップデートの適用には iDRAC の再起動が必要であることを示しています。iDRAC 通信と監視は一時的に中断される場合があります。

** iDRAC をバージョン 1.30.30 以降からアップデートする場合、システムの再起動は必要ありません。ただし、1.30.30 より前の iDRAC ファームウェアバージョンには、帯域外インタフェースを使用した適用時にシステムの再起動が必要になります。

メモ: オペレーティングシステム内で行われた設定変更とファームウェアアップデートは、サーバーを再起動するまでインベントリに適切に反映されないことがあります。

アップデートを確認する場合、**使用可能** としてマークされたバージョンが、必ずしも使用可能な最新バージョンであるとは限りません。アップデートをインストールする前に、選択したバージョンが現在インストールされているバージョンより新しいことを確認してください。iDRAC が検出するバージョンを制御する場合は、Dell Repository Manager（DRM）を使用してカスタムリポジトリを作成し、アップデートの確認にそのリポジトリを使用するように iDRAC を設定します。

関連タスク

単一デバイスのファームウェアのアップデート 、p. 65
リポジトリを使用したファームウェアのアップデート 、p. 65
FTP、TFTP、または HTTP を使用したファームウェアのアップデート 、p. 66
RACADM を使用したデバイスファームウェアのアップデート 、p. 67
自動ファームウェアアップデートのスケジュール設定 、p. 67
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 、p. 69
DUP を使用したファームウェアのアップデート 、p. 69
リモート RACADM を使用したファームウェアのアップデート 、p. 69
Lifecycle Controller Remote Services を使用したファームウェアのアップデート 、p. 70

iDRAC 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

ローカルシステム上のファームウェアイメージ、またはネットワーク共有（CIFS または NFS）上のリポジトリや FTP からの使用が可能なファームウェアイメージを使用してデバイスファームウェアをアップデートすることができます。

単一デバイスのファームウェアのアップデート

単一デバイスのアップデート方法を使用してファームウェアのアップデートを行う前に、ローカルシステム上の場所にファームウェアイメージをダウンロードしていることを確認します。

メモ: シングルコンポーネント DUP のファイル名には、空白スペースが無いことを確認してください。

iDRAC ウェブインタフェースを使用して単一デバイスの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. ［概要］ > ［iDRAC 設定］ > ［アップデートとロールバック］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。
2. ［アップデート］タブで、ファイルの場所として［ローカル］を選択します。
3. ［参照］をクリックして、必要なコンポーネントのファームウェアイメージファイルを選択して、［アップロード］をクリックします。
4. アップロードが完了すると、［アップデート詳細］セクションに iDRAC にアップロードされた各ファームウェアファイルとそのステータスが表示されます。

   ファームウェアイメージファイルが有効であり、正常にアップロードされた場合、［内容］列がプラスアイコン（+）をファームウェアイメージファイル名の横に表示します。名前を展開して［デバイス名］、［現在］、および［利用可能なファームウェアバージョン］情報を表示します。
5. 必要なファームウェアファイルを選択し、次のいずれかを実行します。
   - ホストシステムの再起動を必要としないファームウェアのイメージの場合は、［インストール］をクリックします。例えば、iDRAC ファームウェアファイルなどです。
   - ホストシステムの再起動を必要とするファームウェアイメージの場合は、［インストールして再起動］または［次の再起動時にインストール］をクリックします。
   - ファームウェアアップデートをキャンセルするには、［キャンセル］をクリックします。

   ［インストール］、［インストールして再起動］または［次の再起動時にインストール］をクリックすると、`Updating Job Queue` というメッセージが表示されます。
6. ［ジョブキュー］ページを表示するには、［ジョブキュー］をクリックします。このページを使用してステージングされたファームウェアアップデートを表示し管理するか、または［OK］をクリックして現在のページを更新しファームウェアアップデートのステータスを表示します。

   メモ: アップデートを保存せずにページから移動すると、エラーメッセージが表示され、アップロードされたすべての内容が失われます。

関連概念

デバイスファームウェアのアップデート 、p. 62
ステージングされたアップデートの表示と管理 、p. 71

リポジトリを使用したファームウェアのアップデート

Dell Repository Manager（DRM）で iDRAC がアップデートをチェックできるリポジトリを作成できます。DRM はリポジトリの作成に以下を使用します。

- 新しいデルオンラインカタログ
- 使用されている以前のデルカタログ
- ローカルソースリポジトリ
- カスタムリポジトリ

メモ: DRM についての詳細は、**delltechcenter.com/repositorymanager** を参照してください。

メモ: Lifecycle Controller を有効にしてください。また、iDRAC 以外のデバイスのファームウェアをアップデートするサーバ制御権限が必要です。

リポジトリを使用してデバイス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. iDRAC ウェブインタフェースで、[概要] > [iDRAC 設定] > [アップデートとロールバック] 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。
2. [アップデート] タブで [ネットワーク共有] を [ファイルの場所] として選択します。
3. [カタログの場所] セクションで、ネットワーク設定の詳細を入力します。

   ネットワーク共有設定を指定する場合は、ユーザー名とパスワードに特殊記号を使用しないようにするか、特殊文字をパーセントエンコードすることが推奨されます。詳細については、ユーザー名およびパスワードで推奨される文字 、p. 126 を参照してください。

   フィールドについては、『*iDRAC オンラインヘルプ*』を参照してください。
4. [アップデートのチェック] をクリックします。

   この [アップデート詳細] セクションには、現在のファームウェアバージョンとリポジトリ内で使用可能なファームウェアのバージョンの、比較レポートが表示されます。

   メモ: サポートされていない、またはシステムあるいは取り付けられたハードウェアに適用できないアップデートは、比較レポートに含まれません。
5. 必要なアップデートを選択して、次のいずれかを実行します。

   メモ: 使用可能としてマークされたバージョンが、必ずしも使用可能な最新バージョンまたは既にインストールされているバージョンよりも新しいとは限りません。

   - ホストシステムの再起動を必要としないファームウェアイメージの場合は、[インストール] をクリックします。例えば、`.d7` ファームウェアファイルなどです。
   - ホストシステムの再起動を必要とするファームウェアイメージの場合は、[インストールして再起動] または [次の再起動時にインストール] をクリックします。
   - ファームウェアアップデートをキャンセルするには、[キャンセル] をクリックします。

   [インストール]、[インストールして再起動] または [次の再起動時にインストール] をクリックすると、`Updating Job Queue` というメッセージが表示されます。
6. [ジョブキュー] をクリックして、[ジョブキュー] ページを表示します。ここでは、ステージングされたファームウェアアップデートを表示および管理できます。また、[OK] をクリックして現在のページを更新し、ファームウェアアップデートの状態を表示できます。

関連概念

デバイスファームウェアのアップデート 、p. 62
ステージングされたアップデートの表示と管理 、p. 71
自動ファームウェアアップデートのスケジュール設定 、p. 67

FTP、TFTP、または HTTP を使用したファームウェアのアップデート

ファームウェアアップデートの実行に使用するため、FTP、TFTP、または HTTP サーバをセットアップし、iDRAC を設定できます。Windows ベースのアップデートパッケージ（DUP）とカタログファイルを使用できます。

メモ: Lifecycle Controller を有効にしてください。また、iDRAC 以外のデバイスのファームウェアをアップデートするサーバ制御権限が必要です。

1. iDRAC ウェブインタフェースで、[概要] > [iDRAC 設定] > [アップデートとロールバック] 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。
2. [アップデート] タブで、[ファイルの場所] — [FTP]、 [TFTP]、または [HTTP] の希望するオプションを選択します。
3. 表示されたフィールドに必要な詳細を入力します。

   フィールドについては、『iDRAC オンラインヘルプ』を参照してください。
4. [アップデートのチェック] をクリックします。
5. アップロードが完了すると、[アップデートの詳細] セクションに、現在のファームウェアバージョンとリポジトリ内で使用可能なファームウェアのバージョンの、比較レポートが表示されます。

   メモ: サポートされていない、またはシステムあるいは取り付けられたハードウェアに適用できないアップデートは、比較レポートに含まれません。
6. 必要なアップデートを選択して、次のいずれかを実行します。
   - ホストシステムの再起動を必要としないファームウェアイメージの場合は、[インストール] をクリックします。例えば、`.d7` ファームウェアファイルなどです。

- ホストシステムの再起動を必要とするファームウェアイメージの場合は、[インストールして再起動] または [次の再起動時にインストール] をクリックします。
- ファームウェアアップデートをキャンセルするには、[キャンセル] をクリックします。

[インストール]、[インストールして再起動] または [次の再起動時にインストール] をクリックすると、`Updating Job Queue` というメッセージが表示されます。

7. [ジョブキュー] ページを表示するには、[ジョブキュー] をクリックします。このページで、ステージングされたファームウェアアップデートを表示し管理することができます。[OK] をクリックして現在のページを更新しファームウェアアップデートのステータスを表示します。

関連概念

デバイスファームウェアのアップデート 、p. 62
ステージングされたアップデートの表示と管理 、p. 71
自動ファームウェアアップデートのスケジュール設定 、p. 67

RACADM を使用したデバイスファームウェアのアップデート

RACADM を使用してデバイスファームウェアをアップデートするには、`update` のサブコマンドを使用します。詳細に関しては、**dell.com/idracmanuals** にある『iDRAC 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。

例：

- アップデートのリポジトリを使用して比較レポートを生成する場合：

```
racadm update -f catalog.xml -l //192.168.1.1 -u test -p passwd --verifycatalog
```

- `myfile.xml` を使用してカタログファイルから適用可能なすべてのアップデートを実行し、正常な再起動を実行する場合：

```
racadm update -f “myfile.xml” -b “graceful” -l //192.168.1.1 -u test -p passwd
```

- `Catalog.xml` をカタログファイルとして使用して FTP アップデートリポジトリから 適用可能なすべてのアップデートを実行する場合：

```
racadm update -f “Catalog.xml” -t FTP -e 192.168.1.20/Repository/Catalog
```

自動ファームウェアアップデートのスケジュール設定

新規ファームウェアアップデートのチェックを行うための定期的な反復スケジュールを iDRAC 用に作成することができます。スケジュールされた日付と時刻に、iDRAC を指定された送信先に接続し、新しいアップデートがあるかをチェックして、適用可能なすべてのアップデートを適用またはステージングします。リモートサーバで作成されたログファイルには、サーバーアクセスおよびステージングされたファームウェアのアップデートに関する情報が含まれています。

Dell Repository Manager（DRM）を使用してリポジトリを作成し、ファームウェアのアップデートをチェックして実行するために iDRAC を設定してこのリポジトリを使用することをお勧めします。内部リポジトリを使用することで iDRAC に使用できるファームウェアとバージョンを制御することができ、意図しないファームウェアの変更を避けるのに役立ちます。

メモ: DRM についての詳細は、**delltechcenter.com/repositorymanager** を参照してください。

自動アップデートをスケジュールするには iDRAC Enterprise ライセンスが必要です。

自動ファームウェアアップデートは、iDRAC ウェブインタフェースまたは RACADM を使用してスケジュールすることができます。

メモ: IPv6 アドレスは、ファームウェアの自動アップデートのスケジュール向けにサポートされていません。

関連概念

デバイスファームウェアのアップデート 、p. 62
ステージングされたアップデートの表示と管理 、p. 71

ウェブインタフェースを使用したファームウェアの自動アップデートのスケジュール

ウェブインタフェースを使用してファームウェアの自動アップデートをスケジュールするには、次の手順を実行します。

メモ: ジョブがすでにスケジュール済みの場合は、次の自動アップデートジョブのスケジュールを作成しないでください。作成すると、現在のスケジュール済みジョブが上書きされます。

1. iDRAC ウェブインタフェースで、[概要] > [iDRAC 設定] > [アップデートとロールバック] 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。
2. [自動アップデート] タブをクリックします。
3. [自動アップデートの有効化] オプションを選択します。
4. 次のオプションのいずれかを選択して、アップデートのステージ後にシステム再起動が必要かどうかを指定します。
   - [アップデートをスケジュール] — ファームウェアアップデートをステージしても、サーバーは再起動しません。
   - [アップデートをスケジュールしてサーバーを再起動] — ファームウェアアップデートのステージ後のサーバー再起動を有効にします。
5. 次のいずれかを選択して、ファームウェアイメージの場所を指定します。
   - [ネットワーク] — ネットワーク共有 (CIFS または NFS) からのカタログファイルを使用します。ネットワーク共有ロケーションの詳細を入力してください。

     メモ: ネットワーク共有設定を指定する場合は、ユーザー名とパスワードに特殊記号を使用しないようにするか、特殊文字をパーセントエンコードすることが推奨されます。
   - [FTP] - FTP サイトからカタログファイルを使用します。FTP サイトの詳細を入力します。
6. 手順 5 での選択内容に応じて、ネットワーク設定または FTP 設定を入力します。

   フィールドについては、『iDRAC オンラインヘルプ』を参照してください。
7. [アップデート間隔のスケジュール] セクションで、ファームウェアのアップデート動作の開始時刻と頻度 (毎日、毎週、または毎月) を指定します。

   フィールドについては、『iDRAC オンラインヘルプ』を参照してください。
8. [アップデートのスケジュール] をクリックします。

   次にスケジュールされているジョブがジョブキュー内に作成されます。反復ジョブの最初のインスタンスが開始されてから 5 分後、次の期間のジョブが作成されます。

RACADM を使用したファームウェアの自動アップデートのスケジュール

ファームウェアの自動アップデートをスケジュールするには、次の各コマンドを使用します。

- ファームウェアの自動アップデートを有効にする：

```
racadm set lifecycleController.lcattributes.AutoUpdate.Enable 1
```

- ファームウェアの自動アップデートのステータスを表示する：

```
racadm get lifecycleController.lcattributes.AutoUpdate
```

- ファームウェアのアップデートの開始時刻および頻度をスケジュールする：

```
racadm AutoUpdateScheduler create -u username -p password -l <location> [-f
catalogfilename -pu <proxyuser> -pp<proxypassword> -po <proxy port> -pt <proxytype>] -time
< hh:mm> [-dom < 1 - 28,L,'*'> -wom <1-4,L,'*'> -dow <sun-sat,'*'>] -rp <1-366> -a
<applyserverReboot (1-enabled | 0-disabled)>
```

  たとえば、次のとおりです。
  - CIFS 共有を使用してファームウェアを自動アップデートする：

```
racadm AutoUpdateScheduler create -u admin -p pwd -l //1.2.3.4/CIFS-share -f cat.xml -
time 14:30 -wom 1 -dow sun -rp 5 -a 1
```

  - FTP を使用してファームウェアを自動アップデートする：

```
racadm AutoUpdateScheduler create -u admin -p pwd -l ftp.mytest.com -pu puser -pp puser –
po 8080 -pt http -f cat.xml -time 14:30 -wom 1 -dow sun -rp 5 -a 1
```

- 現在のファームウェアのアップデートのスケジュールを表示する：

```
racadm AutoUpdateScheduler view
```

- ファームウェアの自動アップデートを無効にする：

```
racadm set lifecycleController.lcattributes.AutoUpdate.Enable 0
```

- スケジュールの詳細をクリアする：

```
racadm AutoUpdateScheduler clear
```

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 iDRAC 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 iDRAC ファームウェアをアップデートするには、次の手順を実行します。

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］>［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。

関連概念

デバイスファームウェアのアップデート、p. 62
iDRAC 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、p. 65

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 iDRAC 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 iDRAC 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

1. ファームウェアイメージを TFTP または FTP サーバ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：

   - `fwupdate` コマンドの使用：

     ```
     racadm -r <iDRAC IP address> -u <username> -p <password> fwupdate -g -u -a <path>
     ```

     path

     `firmimg.d7` が保存されている TFTP サーバ上の場所です。

   - `update` コマンドの使用：

     ```
     racadm -r <iDRAC IP address> -u <username> -p <password> update –f <filename>
     ```

FTP サーバ：

- `fwupdate` コマンドの使用：

  ```
  racadm -r <iDRAC IP address> -u <username> -p <password> fwupdate -f <ftpserver IP>
  <ftpserver username> <ftpserver password> -d <path>
  ```

  path

  `firmimg.d7` が保存されている FTP サーバ上の場所です。

- `update` コマンドの使用：

  ```
  racadm -r <iDRAC IP address> -u <username> -p <password> update –f <filename>
  ```

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』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アップデート

Lifecycle Controller – Remote Services を使用してファームウェアをアップデートするための情報に関しては、**dell.com/idracmanuals** にある『*Lifecycle Controller Remote Services クイックスタートガイド*』を参照してください。

iDRAC からの CMC ファームウェアのアップデート

PowerEdge FX2/FX2s シャーシでは、iDRAC から Chassis Management Controller、および CMC によるアップデートとサーバーによる共有が可能な任意のコンポーネントに対するファームウェアのアップデートを行うことができます。

アップデートを適用する前に、次の事項を確認してください。

- サーバーに対して CMC による電源投入が許可されていない。
- LCD のあるシャーシが「アップデートが進行中です」のメッセージを表示している。
- LCD のないシャーシが LED の点滅パターンによってアップデート進行中であることを示している。
- アップデート中は、シャーシ処置電源コマンドが無効になっている。

すべてのサーバーをアイドル状態にする必要がある IOM の Programmable System-on-Chip（PSoC）などのコンポーネントのためのアップデートは、次回のシャーシ電源投入時に適用されます。

CMC ファームウェアを iDRAC からアップデートするための CMC 設定

PowerEdge FX2/FX2s シャーシでは、iDRAC から CMC とその共有コンポーネントに対するファームウェアアップデートを実行する前に、次の操作を行います。

1. CMC ウェブインタフェースを起動します。
2. ［シャーシ概要］>［セットアップ］>［一般］と移動します。
3. ［サーバーモードでのシャーシ管理］ドロップダウンメニューで、［管理および監視］を選択して、［適用］をクリックします。

CMC ファームウェアをアップデートするための iDRAC 設定

PowerEdge FX2/FX2s シャーシでは、iDRAC から CMC とその共有コンポーネントに対するファームウェアをアップデートする前に、iDRAC で次の設定を行ってください。

1. iDRAC ウェブインタフェースで、［概要］>［iDRAC 設定］>［アップデートとロールバック］>［設定］と移動します。
   ［Chassis Management Controller ファームウェアアップデート設定］ページが表示されます。
2. ［OS および Lifecycle Controller 経由での CMC アップデートの許可］で［有効］を選択して、iDRAC からの CMC ファームウェアアップデートを有効にします。
3. ［現在の CMC 設定］で、［サーバーモードでのシャーシ管理］オプションに［管理と監視］が表示されていることを確認します。これは、CMC で設定することができます。

ステージングされたアップデートの表示と管理

設定ジョブおよびアップデートジョブなどのスケジューリングされたジョブを表示および管理できます。これは、ライセンスが必要な機能です。次回の再起動時に実行するためにキューに入れられているすべてのジョブは、削除可能です。

関連タスク

デバイスファームウェアのアップデート、p. 62

iDRAC ウェブインタフェースを使用したステージングされたアップデートの表示と管理

iDRAC ウェブインタフェースを使用してスケジュールされたジョブのリストを表示するには、[概要] > [サーバー] > [ジョブキュー] と移動します。[ジョブキュー] ページには、Lifecycle Controller ジョブキュー内のジョブステータスが表示されます。表示されるフィールドについては、『iDRAC オンラインヘルプ』を参照してください。

ジョブを削除するには、ジョブを選択して [削除] をクリックします。ページが更新され、選択したジョブが Lifecycle Controller ジョブキューから削除されます。次の再起動時に実行するためにキューに入れられていたすべてのジョブを削除できます。アクティブなジョブ、つまりステータスが *実行中* または *ダウンロード中* のジョブは削除できません。

ジョブを削除するにはサーバー制御権限が必要です。

RACADM を使用したステージングされたアップデートの表示と管理

RACADM を使用してステージングされたアップデートを表示するには、`jobqueue` のサブコマンドを使用します。詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

デバイスファームウェアのロールバック

iDRAC または Lifecycle Controller がサポートするデバイスのファームウェアは、以前に別のインタフェースを使用してアップグレードが行われた場合であっても、ロールバックすることができます。たとえば、ファームウェアが Lifecycle Controller GUI を使用してアップグレードされた場合でも、iDRAC ウェブインタフェースを使用してファームウェアをロールバックすることができます。また、1 回のシステム再起動で複数のデバイスのファームウェアロールバックを実行できます。

単一の iDRAC および Lifecycle Controller ファームウェアを持つデルの第 13 世代 PowerEdge サーバでは、iDRAC ファームウェアをロールバックすると、Lifecycle Controller ファームウェアもロールバックされます。ただし、ファームウェアバージョンが 2.*xx.xx.xx* の第 12 世代 PowerEdge サーバでは、iDRAC を 1.*xx.xx* などの以前のバージョンにロールバックしても、Lifecycle Controller ファームウェアバージョンはロールバックされません。Lifecycle Controller の以前のバージョンへのロールバックは、iDRAC のロールバック後に行うことをお勧めします。

メモ: ファームウェアバージョン 2.10.10.10 搭載の第 12 世代 PowerEdge サーバでは、iDRAC をロールバックせずに Lifecycle Controller を 1.*xx.xx* にロールバックすることはできません。Lifecycle Controller をロールバックするには、最初に iDRAC を 1.*xx.xx* バージョンにロールバックします。

最新の機能とセキュリティのアップデートを確保するため、ファームウェアを常にアップデートすることをお勧めします。アップデート後に問題が発生した場合、アップデートをロールバックするか、または前のバージョンをインストールする必要がある場合があります。前のバージョンをインストールするには、Lifecycle Controller を使用してアップデートをチェックし、インストールするバージョンを選択します。

次のコンポーネントのファームウェアロールバックを実行することができます。

- Lifecycle Controller 使用 iDRAC
- BIOS
- ネットワークインタフェースカード (NIC)
- 電源装置ユニット (PSU)
- RAID コントローラ
- バックプレーン

メモ: ファームウェアロールバックは、診断、ドライバパック、および CPLD に対して実行することができます。

ファームウェアをロールバックする前に、次を確認してください。

- iDRAC ファームウェアをロールバックするための設定権限がある。
- サーバー制御権限があり、iDRAC 以外のデバイスすべてのファームウェアをロールバックするために Lifecycle Controller が有効化されている。
- NIC モードが ［共有 LOM］ として設定されている場合は、［専用］ に変更する。

ファームウェアは、次のいずれかの方法を使用して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。

- iDRAC ウェブインタフェース
- CMC ウェブインタフェース
- RACADM CLI ー iDRAC および CMC
- Lifecycle Controller GUI
- Lifecycle Controller リモートサービス

関連タスク

iDRAC 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 、p. 72
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 、p. 72
RACADM を使用したファームウェアのロールバック 、p. 73
Lifecycle Controller を使用したファームウェアのロールバック 、p. 73
Lifecycle Controller-Remote Services を使用したファームウェアのロールバック 、p. 73

iDRAC 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

デバイスファームウェアをロールバックするには、以下の手順を行います。

1. iDRAC ウェブインタフェースで、［概要］ > ［iDRAC 設定］ > ［アップデートとロールバック］ > ［ロールバック］ に移動します。
   ［ロールバック］ ページに、ファームウェアのロールバックが可能なデバイスが表示されます。デバイス名、関連付けられているデバイス、現在インストールされているファームウェアバージョン、および使用可能なファームウェアロールバックバージョンを表示することができます。
2. ファームウェアをロールバックする 1 つ、または複数のデバイスを選択します。
3. 選択されたデバイスに基づいて、［インストールして再起動］ または ［次回の再起動時にインストール］ をクリックします。iDRAC のみが選択されている場合は ［インストール］ をクリックします。
   ［インストールして再起動］ または ［次の再起動時にインストール］ をクリックすると、「ジョブキューをアップデート中」というメッセージが表示されます。
4. ［ジョブキュー］ をクリックします。
   ステージングされたファームウェアアップデートを表示および管理することができる ［ジョブキュー］ 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。

   次の場合は、エラー メッセージが表示されます。
   - iDRAC 以外のファームウェアをロールバックするサーバー制御権限、または iDRAC ファームウェアをロールバックするための設定権限がない。
   - ファームウェアロールバックが別のセッションで進行中である。
   - アップデートが実行用にステージされているか、またはすでに実行状況である。

   Lifecycle Controller が無効またはリカバリ状態のときに iDRAC 以外のデバイスのファームウェアロールバックを試行すると、適切な警告メッセージが Lifecycle Controller の有効化手順と共にが表示されます。

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］ をクリックし、「iDRAC 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」の項で説明されているとおりにデバイス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

1. 次の `swinventory` コマンドを使用して、ロールバックのステータスおよび FQDD ををチェックします。

   ```
   racadm swinventory
   ```

   ファームウェアのロールバックを行うデバイスの場合は、`Rollback Versio` が `Available` になっている必要があります。また、FQDD をメモしておきます。

2. 次のコマンドを使用して、デバイスのファームウェアをロールバックします。

   ```
   racadm rollback <FQDD>
   ```

   詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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

この詳細については、**dell.com/idracmanuals** 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

詳細情報に関しては、**dell.com/idracmanuals** にある『*Lifecycle Controller Remote Services クイックスタートガイド*』を参照してください。

iDRAC のリカバリ

iDRAC は、iDRAC を起動できるようにするために、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。

- iDRAC 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。
- ブートローダーは SD カードを検出し、点滅している LED を橙色に点灯して、firmimg.d7 を読み取り、iDRAC を再プログラムし、iDRAC を再起動します。

TFTP サーバーの使用

Trivial File Transfer Protocol（TFTP）サーバーを使用して iDRAC ファームウェアのアップグレードとダウングレード、または証明書のインストールを行うことができます。これは、iDRAC から、または iDRAC へのファイルの転送のために SM-CLP および RACADM コマンドラインインタフェースで使用されます。TFTP サーバーには、iDRAC 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 iDRAC 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 サーバーが実行されていない場合は、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。

サーバープロファイルのバックアップ

BIOS、RAID、NIC、iDRAC、Lifecycle Controller、およびネットワークドーターカード（NDC）などの各種コンポーネント上にインストールされているファームウェアイメージと、これらのコンポーネントの構成設定を含むシステム設定をバックアップすることができます。バックアップ操作には、ハードディスク設定データ、マザーボード、および交換済み部品も含まれます。バックアップにより、vFlash SD カードまたはネットワーク共有（CIFS または NFS）に保存することができる単一のファイルが作成されます。

また、特定の日、週、または月に基づいたファームウェアとサーバー構成の定期的バックアップを有効化およびスケジュールすることもできます。

バックアップ機能はライセンスされており、iDRAC Enterprise ライセンスで使用可能です。

メモ: 第 13 世代サーバーでは、この機能は自動的に有効になります。

バックアップ操作を実行する前に、次のことを確認します。

- Collect System Inventory On Reboot（CSIOR）オプションが有効。CSIOR が無効になっているときにバックアップ操作を行うと、次のメッセージが表示されます。

```
System Inventory with iDRAC may be stale,start CSIOR for updated inventory
```

- vFlash SD カードのバックアップを実行するには、次の手順を行います。
  - vFlash SD カードが挿入され、有効化および初期化されました。
  - VFlash SD カードには、バックアップファイルを保存するための 100 MB 以上の空き容量があります。

バックアップファイルには、サーバープロファイルにインポート操作に使用できる暗号化されたユーザー機密データ、設定情報、およびファームウェアイメージが含まれます。

バックアップイベントが Lifecycle ログに記録されます。

関連概念

サーバープロファイルの自動バックアップのスケジュール、p. 75
サーバプロファイルのインポート、p. 76

iDRAC ウェブインタフェースを使用したサーバープロファイルのバックアップ

iDRAC ウェブインタフェースを使用してサーバープロファイルをバックアップするには、次の手順を実行します。

1. [概要] > [iDRAC の設定] > [サーバープロファイル] と移動します。
   [サーバープロファイルのバックアップとエクスポート] ページが表示されます。
2. 次のいずれかを選択して、バックアップファイルイメージを保存します。
   - [ネットワーク] を選択して、バックアップファイルイメージを CIFS または NFS 共有に保存。
   - [vFlash] を選択して、バックアップファイルイメージを vFlash カードに保存。
3. バックアップファイル名と暗号化パスフレーズを入力します（オプション）。
4. ファイルの場所として [ネットワーク] を選択した場合は、ネットワーク設定を入力します。

   メモ: ネットワーク共有設定を指定する場合は、ユーザー名とパスワードに特殊記号を使用しないようにするか、特殊文字をパーセントエンコードすることが推奨されます。

   フィールドについては、『iDRAC オンラインヘルプ』を参照してください。
5. [今すぐバックアップ] をクリックします。
   バックアップ操作が開始され、[ジョブキュー] ページでステータスを確認できます。操作が正常に完了すると、指定された場所にバックアップファイルが作成されます。

RACADM を使用したサーバプロファイルのバックアップ

RACADM を使用してサーバプロファイルをバックアップするには、`systemconfig backup` コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

サーバープロファイルの自動バックアップのスケジュール

特定の日、週、または月単位で、ファームウェアとサーバー構成の定期的バックアップを有効にしてスケジュールすることができます。

サーバープロファイルの自動バックアップをスケジュールする前に、次を確認してください。

- Lifecycle Controller および再起動時にシステムインベントリを収集（CSIOR）オプションが有効になっている。
- 次のスケジュール済みジョブが作成されるときに、実際にスケジュールされたジョブを実行する時刻が時間のずれに影響されないよう、ネットワークタイムプロトコル（NTP）が有効になっている。
- vFlash SD カードのバックアップを実行するには、次の手順を行います。
  - Dell がサポートする vFlash SD カードが挿入され、有効で、初期化されている。
  - vFlash SD カードにはバックアップファイルを格納するために十分なスペースがある。

メモ: IPv6 アドレスは、サーバープロファイルの自動バックアップのスケジュール向けにサポートされていません。

ウェブインタフェースを使用したサーバープロファイルの自動バックアップのスケジュール

サーバープロファイルの自動バックアップをスケジュールするには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、[概要] > [iDRAC 設定] > [サーバープロファイル] と移動します。
   [サーバープロファイルのバックアップとエクスポート] ページが表示されます。
2. [自動バックアップ] タブをクリックします。
3. [自動バックアップの有効化] オプションを選択します。
4. 次のいずれかを選択して、バックアップファイルイメージを保存します。
   - [ネットワーク] を選択して、バックアップファイルイメージを CIFS または NFS 共有に保存。
   - [vFlash] を選択して、バックアップファイルイメージを vFlash カードに保存。
5. バックアップファイル名と暗号化パスフレーズを入力します（オプション）。
6. ファイルの場所として **ネットワーク** を選択した場合は、ネットワーク設定を入力します。

   メモ: ネットワーク共有設定を指定する場合は、ユーザー名とパスワードに特殊記号を使用しないようにするか、特殊文字をパーセントエンコードすることが推奨されます。

   フィールドについては、『iDRAC オンラインヘルプ』を参照してください。
7. [バックアップ時間帯スケジュール] セクションで、バックアップ操作の開始時刻と頻度（毎日、毎週、または毎月）を指定します。
   フィールドについては、『iDRAC オンラインヘルプ』を参照してください。
8. [バックアップのスケジュール] をクリックします。
   反復ジョブは、スケジュールされた次回バックアップ操作の開始日時と共にジョブキューに表示されます。反復ジョブの初回インスタンス開始の 5 分後に次の期間のジョブが作成されます。サーバープロファイルのバックアップ操作は、スケジュールされた日付と時刻に実行されます。

RACADM を使用したサーバープロファイルの自動バックアップのスケジュール

自動バックアップを有効化するには、次のコマンドを使用します。

```
racadm set lifecyclecontroller.lcattributes.autobackup Enabled
```

サーバープロファイルのバックアップをスケジュールする：

```
racadm systemconfig backup –f <filename> <target> [-n <passphrase>] -time <hh:mm> -dom
<1-28,L,’*’> -dow<*,Sun-Sat> -wom <1-4, L,’*’> -rp  <1-366>-mb <Max Backups>
```

現在のバックアップのスケジュールを表示する

```
racadm systemconfig getbackupscheduler
```

自動バックアップを無効にするには、次のコマンドを使用します：

```
racadm set LifeCycleController.lcattributes.autobackup Disabled
```

バックアップのスケジュールをクリアするには、次のコマンドを使用します：

```
racadm systemconfig clearbackupscheduler
```

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

サーバプロファイルのインポート

バックアップイメージファイルを使用して、サーバを再起動せずに、同じサーバの設定およびファームウェアをインポートまたは復元できます。

インポート機能はライセンスされていません。

メモ: 復元操作では、システムサービスタグとバックアップファイル内のサービスタグが一致している必要があります。復元操作は、バックアップファイルにキャプチャされたものと同一で、同じ場所またはスロットに存在するすべてのシステムコンポーネントに適用されます。コンポーネントが異なるか、同じ場所にない場合は変更されず、復元の失敗が Lifecycle ログに記録されます。

インポート操作を行う前に、Lifecycle Controller が有効になっていることを確認します。Lifecycle Controller が無効になっているときにインポート操作を開始すると、次のメッセージが表示されます。

```
Lifecycle Controller is not enabled, cannot create Configuration job.
```

インポートがすでに進行中のときにインポート操作を再度開始すると、次のエラーメッセージが表示されます。

```
Restore is already running
```

インポートイベントが Lifecycle ログに記録されます。

簡単な復元

メモ: 簡単な復元は、簡単な復元フラッシュメモリを持つ第 13 世代 PowerEdge サーバでのみ利用可能です。PowerEdge R930 では利用できません。

お使いのサーバのマザーボードを交換した後に、簡単な復元で以下のデータを自動的にリストアできます。

- System Service Tag（システムサービスタグ）
- ライセンスデータ
- UEFI 診断アプリケーション
- システム構成の設定 — BIOS、iDRAC、および NIC

簡単な復元では、簡単な復元フラッシュメモリを使用してデータをバックアップします。 システムのマザーボードと電源を交換すると、BIOS が iDRAC にクエリを行い、バックアップされたデータを復元を促すプロンプトを表示します。最初の BIOS 画面には、サービスタグ、ライセンス、UEFI 診断アプリケーションの復元を促すプロンプトが表示されます。2 番目の BIOS 画面には、システム構成の設定を復元することを促すプロンプトが表示されます。最初の BIOS 画面でデータを復元しないことを選択した場合や、別の方法でサービスタグを設定しない場合は、最初の BIOS 画面がもう一度表示されます。2 番目の BIOS 画面は、一度だけ表示されます。

メモ:

- システム構成の設定は CSIOR が有効になっている場合のみバックアップされます。Lifecycle Controller と CSIOR が有効になっていることを確認します。
- システムの消去では、簡単な復元フラッシュメモリからのデータは消去されません。
- 簡単な復元では、ファームウェアイメージ、vFlash のデータ、またはアドインカードデータなどの他のデータはバックアップされません。

関連タスク

復元操作の順序 、p. 77

iDRAC ウェブインタフェースを使用したサーバープロファイルのインポート

iDRAC ウェブインタフェースを使用してサーバープロファイルをインポートするには、次の手順を実行します。

1. ［概要］ > ［iDRAC 設定］ > ［サーバープロファイル］ > ［インポート］ と移動します。
   ［サーバープロファイルのインポート］ ページが表示されます。
2. 次のいずれかを選択して、バックアップファイルの場所を指定します。
   - ［ネットワーク ］
   - ［vFlash］
3. バックアップファイル名と復号化パスフレーズを入力します（オプション）。
4. ファイルの場所として ［ネットワーク］ を選択した場合は、ネットワーク設定を入力します。

   メモ: ネットワーク共有設定を指定する場合は、ユーザー名とパスワードに特殊記号を使用しないようにするか、特殊文字をパーセントエンコードすることが推奨されます。

   フィールドについては、『iDRAC オンラインヘルプ』を参照してください。
5. ［仮想ディスク設定とハードディスクデータ］ のために次のいずれかを選択します。
   - ［保存］ — システム内の RAID レベル、仮想ディスク、コントローラ属性、およびハードディスクデータを保存し、バックアップイメージファイルを使用して以前の既知の状態にシステムを復元します。
   - ［削除および置換］ — システム内の RAID レベル、仮想ディスク、コントローラ属性、およびハードディスク設定情報を削除し、バックアップイメージファイルのデータと置き換えます。
6. ［インポート］ をクリックします。
   サーバープロファイルのインポート操作が開始されます。

RACADM を使用したサーバプロファイルのインポート

RACADM を使用してサーバプロファイルをインポートするには、 `systemconfig restore` コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

復元操作の順序

復元操作の順序は次のとおりです。

1. ホストシステムがシャットダウンします。
2. Lifecycle Controller の復元にバックアップファイル情報が使用されます。
3. ホストシステムに電源が入ります。
4. デバイスのファームウェアおよび設定の復元プロセスが完了します。
5. ホストシステムがシャットダウンします。
6. iDRAC ファームウェアおよび設定の復元プロセスが完了します。
7. iDRAC が再起動します。
8. 復元されたホストシステムに電源が入り、通常の操作が再開されます。

他のシステム管理ツールを使用した iDRAC の監視

iDRAC は、Dell Management Console または 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、ファームウェアのアップデート、および Active Directory のセットアップ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

iDRAC の設定

iDRAC では、リモート管理タスクを実行するために iDRAC 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。

iDRAC を設定する前に、iDRAC 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、必要なライセンスがアップデートされていることを確認します。iDRAC で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。

次のものを使用して iDRAC を設定できます。

- iDRAC 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）

iDRAC を設定するには、次の手順を実行します。

1. iDRAC 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: iDRAC 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 iDRAC 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. iDRAC 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. 必要に応じてタイムゾーンおよびネットワークタイムプロトコル（NTP）を設定します。
7. iDRAC 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
8. 必要な証明書を取得します。
9. iDRAC ユーザーを追加し、権限を設定します。
10. 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。
11. 必要に応じて電力上限ポリシーを設定します。
12. 前回のクラッシュ画面を有効にします。
13. 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。
14. 必要に応じて vFlash SD カードを設定します。
15. 必要に応じて最初の起動デバイスを設定します。
16. 必要に応じて OS を iDRAC パススルーに設定します。

関連概念

iDRAC へのログイン、p. 30
ネットワーク設定の変更、p. 79
サービスの設定、p. 82
前面パネルディスプレイの設定、p. 86
管理下システムの場所のセットアップ、p. 50
タイムゾーンおよび NTP の設定、p. 87
iDRAC 通信のセットアップ、p. 108
ユーザーアカウントと権限の設定、p. 126
電源の監視と管理、p. 169
前回のクラッシュ画面の有効化、p. 89

[仮想コンソールの設定と使用 、p. 225](#)
[仮想メディアの管理 、p. 234](#)
[vFlash SD カードの管理 、p. 244](#)
[最初の起動デバイスの設定 、p. 88](#)
[OS から iDRAC へのパススルーの有効化または無効化 、p. 89](#)

関連タスク

アラートを送信するための iDRAC の設定 、p. 153

トピック：

- iDRAC 情報の表示
- ネットワーク設定の変更
- FIPS モード
- サービスの設定
- VNC クライアントを使用したリモートサーバーの管理
- 前面パネルディスプレイの設定
- タイムゾーンおよび NTP の設定
- 最初の起動デバイスの設定
- OS から iDRAC へのパススルーの有効化または無効化
- 証明書の取得
- RACADM を使用した複数の iDRAC の設定
- ホストシステムでの iDRAC 設定を変更するためのアクセスの無効化

iDRAC 情報の表示

iDRAC 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 iDRAC 情報の表示

iDRAC 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、iDRAC 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、『iDRAC オンラインヘルプ』を参照してください。

- 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
- 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 iDRAC 情報の表示

RACADM を使用して iDRAC 情報を表示するには、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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 iDRAC ネットワーク設定を設定した後も、iDRAC 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。

iDRAC 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、[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、iDRAC 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

iDRAC 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. iDRAC 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. 要件に従ってネットワーク設定、共通設定、IPv4、IPv6、IPMI、VLAN 設定を指定して、[適用] をクリックします。
   [ネットワーク設定] で [自動専用 NIC] を選択した場合、iDRAC がその NIC 選択を共有 LOM (1、2、3、または 4) としており、iDRAC 専用 NIC でリンクが検出されると、iDRAC は NIC 選択を専用 NIC に変更します。専用 NIC でリンクが検出されない場合、iDRAC は共有 LOM を使用します。共有から専用への切り替えのタイムアウトは 5 秒で、専用から共有への切り替えは 30 秒です。このタイムアウト値は、RACADM または WS-MAN を使用して設定できます。

   各種フィールドについては、『iDRAC 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、コマンドを使用します。

```
racadm get iDRAC.Nic
```

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 DHCPEnable オブジェクトを書き込み、この機能を有効にします。

```
racadm set iDRAC.IPv4.DHCPEnable 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 set iDRAC.Nic.Enable 1
racadm set iDRAC.IPv4.Address 192.168.0.120
racadm set iDRAC.IPv4.Netmask 255.255.255.0
racadm set iDRAC.IPv4.Gateway 192.168.0.120
racadm set iDRAC.IPv4.DHCPEnable 0
racadm set iDRAC.IPv4.DNSFromDHCP 0
racadm set iDRAC.IPv4.DNS1 192.168.0.5
racadm set iDRAC.IPv4.DNS2 192.168.0.6
racadm set iDRAC.Nic.DNSRegister 1
racadm set iDRAC.Nic.DNSRacName RAC-EK00002
racadm set iDRAC.Nic.DNSDomainFromDHCP 0
racadm set iDRAC.Nic.DNSDomainName MYDOMAIN
```

メモ: iDRAC.Nic.Enable を [0] に設定すると、DHCP が有効な場合でも iDRAC LAN は無効になります。

IP フィルタの設定

ユーザー認証に加え、次のオプションを使用して iDRAC 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、iDRAC 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。受信ログインの 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 iDRAC 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。
- 特定の IP アドレスからのログインが繰り返し失敗した場合は、そのアドレスから iDRAC へのログインが、事前に選択された時間ブロックされます。ログインの失敗が 2 回までの場合は、30 秒後に再びログインする必要があります。ログインの失敗が 2 回を超える場合は、60 秒後に再びログインする必要があります。

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 exchange identification: Connection closed by remote host というメッセージが表示される場合があります。

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。

iDRAC ウェブインタフェースを使用した IP フィルタの設定

これらの手順を実行するには、設定権限が必要です。

IP フィルタを設定するには、次の手順を実行します。

1. iDRAC 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 フィルタ設定を指定します。
   オプションの詳細については、『iDRAC オンラインヘルプ』を参照してください。
4. 設定を保存するには、[適用] をクリックします。

RACADM を使用した IP フィルタの設定

これらの手順を実行するには、設定権限が必要です。

IP フィルタを設定するには、`iDRAC.IPBlocking` グループの次の RACADM オブジェクトを使用します。

- RangeEnable
- RangeAddr
- RangeMask

`RangeMask` プロパティは、入力される IP アドレスと `RangeAddr` 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、受信ログイン要求に iDRAC へのアクセスが許可されます。この範囲外の IP アドレスからログインすると、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。

```
RangeMask & (<incoming-IP-address> ^ RangeAddr)
```

&

数量のビット積

^

ビット排他論理和

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 set iDRAC.IPBlocking.RangeEnable 1
racadm set iDRAC.IPBlocking.RangeAddr 192.168.0.57
racadm set iDRAC.IPBlocking.RangeMask 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、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 set iDRAC.IPBlocking.RangeEnable 1
racadm set iDRAC.IPBlocking.RangeAddr 192.168.0.212
racadm set iDRAC.IPBlocking.RangeMask 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。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインリファレンスガイド*』を参照してください。

FIPS モード

FIPS は米国政府機関や請負業者が使用する必要のあるコンピュータセキュリティ基準です。iDRAC はバージョン 2.40.40.40 から FIPS モードを有効にできます。

IDRAC は今後 FIPS モードのサポートを正式に認証します。

FIPS モードのサポートと検証済み FIPS との違い

暗号モジュール検証プログラムを完了して検証されたソフトウェアは、FIPS 検証済みとみなされます。FIPS 検証の完了には時間がかかるため、iDRAC の全バージョンで検証済みであるわけではありません。iDRAC の FIPS 検証の最新状況については、NIST Web サイトの暗号モジュール検証プログラムのページを参照してください。

FIPS モードの有効化

注意: FIPS モードを有効にすると、iDRAC を工場出荷時の設定にリセットします。設定を復元する場合は、FIPS モードを有効にする前にサーバ設定プロファイル（SCP）をバックアップし、iDRAC の再起動後に SCP を復元します。

メモ: iDRAC ファームウェアを再インストール、またはアップグレードすると、FIPS モードが無効になります。

ウェブインタフェースを使用した FIPS モードの有効化

1. iDRAC の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。
2. [オプション] の横の [詳細設定] をクリックします。
3. [FIPS モード] で、[有効] を選択して [適用] をクリックします。
4. 変更の確認を求めるメッセージが表示されます。[OK] をクリックします。
   iDRAC が FIPS モードで再起動します。iDRAC に再接続するまでに少なくとも 60 秒間待機します。
5. iDRAC の信頼できる証明書をインストールします。

   メモ: デフォルトの SSL 証明書は、 FIPS モードで許可されていません。

メモ: IPIM や SNMP の標準準拠の実装のような一部の iDRAC インタフェースは、FIPS コンプライアンスをサポートしていません。

RACADM を使用した FIPS モードの有効化

RACADM CLI を使用して、次のコマンドを実行します。

```
racadm set iDRAC.Security.FIPSMode <Enable>
```

FIPS モードの無効化

FIPS モードを無効にするには、iDRAC を工場出荷時のデフォルト設定にリセットする必要があります。

サービスの設定

iDRAC では、次のサービスを設定し、有効にできます。

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 iDRAC 設定へのアクセス（ホストシステムから）を無効にします。
Web サーバ	IDRAC ウェブインタフェースへのアクセスを有効にします。ウェブインタフェースを無効にすると、リモート RACADM も無効になります。ローカル RACADM を使用して、Web サーバとリモート RACADM を再度有効にします。
SSH	ファームウェア RACADM から iDRAC にアクセスします。
Telnet	ファームウェア RACADM から iDRAC にアクセスします。
リモート RACADM	IDRAC にリモートアクセスします。

Redfish	Redfish RESTful API のサポートを有効にします。
SNMP エージェント	iDRAC で SNMP クエリ（GET、GETNEXT、および GETBULK 操作）のサポートを有効にします。
自動システムリカバリエージェント	前回のシステムクラッシュ画面を有効にします。
VNC サーバ	SSL 暗号化あり、または無しで VNC サーバを有効にします。

ウェブインタフェースを使用したサービスの設定

iDRAC 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. iDRAC 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。
   各種設定については、『iDRAC オンラインヘルプ』を参照してください。

   メモ: ［このページで追加のダイアログを作成しない］ チェックボックスを選択しないでください。このオプションを選択するとサービスの設定ができなくなります。

RACADM を使用したサービスの設定

RACADM を使用してサービスを有効にして設定するには、次のオブジェクトグループのオブジェクトで `set` コマンドを使用します。

- iDRAC.LocalSecurity
- iDRAC.LocalSecurity
- iDRAC.SSH
- iDRAC.Webserver
- iDRAC.Telnet
- iDRAC.Racadm
- iDRAC.SNMP

これらのオブジェクトの詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

HTTPs リダイレクトの有効化または無効化

デフォルトの iDRAC 証明書における証明書警告問題、またはデバッグ目的の一時的な設定を理由に、HTTP から HTTPs への自動リダイレクトを行いたくない場合は、http ポート（デフォルトは 80）から https ポート（デフォルトは 443）へのリダイレクトが無効化されるように iDRAC を設定することができます。このリダイレクトはデフォルトで有効化されています。この設定を有効にするには、iDRAC からログアウトしてログインする必要があります。この機能を無効にすると、警告メッセージが表示されます。

HTTPs リダイレクトを有効化または無効化するには、iDRAC 権限が必要です。

この機能を有効化または無効化すると、Lifecycle Controller ログファイルにイベントが記録されます。

HTTP から HTTPs へのリダイレクトを無効化する場合：

```
racadm set iDRAC.Webserver.HttpsRedirection Disabled
```

HTTP から HTTPs へのリダイレクトを有効化する場合：

```
racadm set iDRAC.Webserver.HttpsRedirection Enabled
```

HTTP から HTTPs へのリダイレクトのステータスを表示する場合：

```
racadm get iDRAC.Webserver.HttpsRedirection
```

TLS の設定

デフォルトでは、iDRAC は TLS 1.1 以降を使用するように設定されます。次のいずれかを使用するように iDRAC を設定できます。

- TLS 1.0 以降
- TLS 1.1 以降
- TLS 1.2 のみ

メモ: セキュアな接続を確保するため、デルは TLS 1.1 以上の使用をお勧めします。

ウェブインタフェースを使用した TLS 設定

1. ［概要］ > ［iDRAC 設定］ > ［ ネットワーク］ と移動します。
2. ［サービス］ タブをクリックし、［Web サーバ］ をクリックします。
3. ［TLS プロトコル］ ドロップダウンで、TLS のバージョンを選択し ［適用］ をクリックします。

RACADM を使用した TLS の設定

設定された TLS のバージョンを確認するには :

```
racadm get idrac.webserver.tlsprotocol
```

TLS のバージョンを設定するには :

```
racadm set idrac.webserver.tlsprotocol <n>
```

<n>=0

TLS 1.0 以降

<n>=1

TLS 1.1 以降

<n>=2

TLS 1.2 のみ

VNC クライアントを使用したリモートサーバーの管理

標準 VNC オープンクライアントを使用し、デスクトップと、Dell Wyse PocketCloud などのモバイルデバイスの両方を使用して、リモートサーバーを管理することができます。データセンター内のサーバーの機能が停止したとき、iDRAC またはオペレーティングシステムは、管理ステーション上のコンソールに警告を送信します。コンソールはモバイルデバイスに必要な情報を電子メールまたは SMS で送信して、管理ステーション上で VNC ビューアアプリケーションを起動します。この VNC ビューアはサーバー上の OS/ ハイパーバイザに接続して、必要な対応策を実行するためにホストサーバーのキーボード、ビデオ、およびマウスへのアクセスを提供します。VNC クライアントを起動する前に、VNC サーバーを有効にして、iDRAC で VNC サーバーのパスワードや VNC ポート番号、SSL 暗号化、タイムアウト値などの設定を行う必要があります。これらの設定は iDRAC ウェブインタフェースまたは RACADM を使用して行うことができます。

メモ: VNC 機能はライセンスされており、iDRAC Enterprise ライセンスで使用できます。

RealVNC や Dell Wyse PocketCloud など、多くの VNC アプリケーションまたはデスクトップクライアントから選択することができます。

一度にアクティブにすることができる VNC セッションは、1 つのみです。

VNC セッションがアクティブである場合、仮想メディアは、仮想コンソールビューアではなく 仮想コンソールの起動 でしか起動できません。

ビデオ暗号化が無効になっている場合、VNC クライアントが直接 RFB ハンドシェイクを起動し、SSL ハンドシェイクは不要です。VNC クライアントのハンドシェイク中 (RFB または SSL)、別の VNC セッションがアクティブまたは、仮想コンソールセッションが開いている場合、新しい VNC クライアントセッションは拒否されます。初回ハンドシェイクが完了すると、VNC サーバーで仮想コンソールが無効にされ、仮想メディアのみが許可されます。VNC セッション終了後、VNC サーバーは仮想コンソールの元の状態 (有効または無効) を復元します。

メモ:

- iDRAC の NIC が共有モードであり、ホストシステムの電源が入れ直された場合、ネットワーク接続は数秒間失われます。この時間の間に、アクティブな VNC クライアントでアクションを実行すると、VNC セッションが閉じられることがあります。タイムアウト（iDRAC ウェブインタフェースの ［サービス］ ページの VNC サーバー設定で指定された値）を待って、VNC 接続を再確立する必要があります。
- VNC クライアントウィンドウが最小化され 60 秒を超えると、クライアントウィンドウは閉じられます。この場合は、VNC セッションを新たに開く必要があります。60 秒以内に VNC クライアントウィンドウを最大化すると、クライアントウィンドウを使用し続けることができます。

iDRAC ウェブインタフェースを使用した VNC サーバーの設定

VNC サーバーの設定を行うには、以下を行います。

1. iDRAC 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. ［VNC サーバー］ セクションで VNC サーバーを有効にし、パスワードとポート番号を指定して、SSL 暗号化を有効または無効にします。

   フィールドについては、『iDRAC 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。
   VNC サーバーが設定されました。

RACADM を使用した VNC サーバーの設定

VNC サーバーを設定するには、`VNCserver` のオブジェクトに `set` コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

SSL 暗号化を伴う VNC ビューアの設定

iDRAC での VNC サーバー設定中に ［SSL 暗号化］ オプションが無効になっている場合、iDRAC VNC サーバーとの SSL 暗号化接続を確立できるよう、VNC ビューアと SSL トンネルアプリケーションを一緒に使用する必要があります。

メモ: ほとんどの VNC クライアントには、SSL 暗号化サポートが内蔵されていません。

SSL トンネルアプリケーションを設定するには、次の手順を実行します。

1. SSL トンネルが、 `<localhost>:<localport number>` での接続を受け入れるように設定します。例えば、127.0.0.1:5930。
2. SSL トンネルが、 `<iDRAC IP address>:<VNC server port Number>` に接続するように設定します。例えば、192.168.0.120:5901。
3. トンネルアプリケーションを起動します。

   SSL 暗号化チャネル上での iDRAC VNC サーバーとの接続を確立するには、VNC ビューアをローカルホスト（リンクローカル IP アドレス）およびローカルポート番号（127.0.0.1:< ローカルポート番号 >）に接続します。

SSL 暗号化なしでの VNC ビューアのセットアップ

一般的に、すべてのリモートフレームバッファ（RFB）準拠の VNC ビューアは、VNC サーバー用に設定された iDRAC の IP アドレスとポート番号を使用して VNC サーバーに接続します。iDRAC での VNC サーバー設定中に SSL 暗号化オプションが無効になっている場合、VNC ビューアに接続するには、以下を実行します。

［VNC ビューア］ ダイアログボックスで、iDRAC の IP アドレスと VNC ポート番号を、［VNC サーバー］ フィールドに入力します。

形式は、 `<iDRAC IP address:VNC port number>`

例えば、iDRAC IP アドレスが 192.168.0.120 で VNC ート番号が 5901 の場合、 `192.168.0.120:5901` と入力します。

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。

関連概念

LCD の設定 、p. 86
システム ID LED の設定 、p. 87

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 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 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)
   - アセットタグ
   - DRAC MAC アドレス
   - DRAC IPv4 アドレス
   - DRAC IPv6 アドレス
   - システム電源
   - 周囲温度
   - 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. 仮想コンソール表示を有効にします (オプション)。有効にすると、アクティブな仮想コンソールセッションがある場合に、サーバーの前面パネルライブフィードセクションと LCD パネルに、`Virtual console session active` メッセージが表示されます。
4. [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

サーバの 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、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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、[前面パネルセキュリティ] に移動します。
   [iDRAC 設定。前面パネルセキュリティ] ページが表示されます。
2. 電源ボタンを有効化または無効化します。
3. 以下を指定します。
   - 前面パネルへのアクセス
   - LCD メッセージ文字列
   - システム電源装置、周囲温度装置、およびエラーディスプレイ
4. 仮想コンソール表示を有効化または無効化します。
   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。
5. [戻る]、[終了] の順にクリックし、[はい] をクリックします。

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. iDRAC 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。
   - 点滅オフ
   - 点滅オン
   - 点滅オン 1 日タイムアウト
   - 点滅オン 1 週間タイムアウト
   - 点滅オン 1 ヶ月タイムアウト
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、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

タイムゾーンおよび NTP の設定

BIOS またはホストシステム時間ではなく、ネットワークタイムプロトコル (NTP) を使用して iDRAC のタイムゾーンを設定し、iDRAC 時間を同期することができます。

タイムゾーンまたは NTP の設定には、設定権限が必要です。

iDRAC ウェブインタフェースを使用したタイムゾーンと NTP の設定

iDRAC ウェブインタフェースを使用してタイムゾーンと NTP を設定するには、次の手順を実行します。

1. [概要] > [iDRAC 設定] > [プロパティ] > [設定] と移動します。
   [タイムゾーンと NTP] ページが表示されます。
2. タイムゾーンを設定するには、[タイムゾーン] ドロップダウンメニューから該当するタイムゾーンを選択し、[適用] をクリックします。
3. NTP を設定するには、NTP を有効にして、NTP サーバーアドレスを入力し、[適用] をクリックします。
   フィールドについては、『iDRAC オンラインヘルプ』を参照してください。

RACADM を使用したタイムゾーンと NTP の設定

タイムゾーンと NTP を設定するには、`iDRAC.Time` と `iDRAC.NTPConfigGroup` グループのオブジェクトで `set` コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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

次回起動時のみ、または後続のすべての再起動時の、最初の起動デバイスを設定できます。後続のすべての起動時に使用するデバイスを設定すると、iDRAC ウェブインタフェースまたは BIOS 起動順序のいずれかから再度変更されるまで、そのデバイスが BIOS 起動順序の最初の起動デバイスのままになります。

最初の起動デバイスは次のいずれかに設定できます。

- 通常起動
- PXE
- BIOS セットアップ
- ローカルフロッピー / プライマリリムーバブルメディア
- ローカル CD/DVD
- ハードドライブ
- 仮想フロッピー
- 仮想 CD/DVD/ISO
- ローカル SD カード
- vFlash
- Lifecycle Controller
- BIOS 起動マネージャ
- UEFI デバイスパス

メモ:

- BIOS セットアップ（F2）、Lifecycle Controller（F10）、BIOS 起動マネージャ（F11）は永続的な起動デバイスとして設定できません。
- iDRAC ウェブインタフェースの最初の起動デバイスの設定は、システム BIOS 起動設定よりも優先されます。
- Redfish インタフェースを使用して UEFI デバイスパスの値を設定します。UEFI デバイスパスへの起動は、デルの第 13 世代以降のサーバでサポートされています。

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

iDRAC 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、『iDRAC 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、`iDRAC.ServerBoot.FirstBootDevice` オブジェクトを使用します。
- デバイスの 1 回限りの起動を有効にするには、`iDRAC.ServerBoot.BootOnce` 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、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

仮想コンソールを使用した最初の起動デバイスの設定

サーバーが起動時のシーケンスを実行する前、サーバーが仮想コンソールビューアで表示されるときに、起動デバイスを選択することができます。「最初の起動デバイスの設定」にリストされている対応デバイスすべてに対して一回限りの起動を実行できます。

仮想コンソール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. 仮想コンソールを起動します。
2. 仮想コンソールビューアの ［次回起動］ メニューから、必要なデバイスを最初の起動デバイスとして設定します。

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、iDRAC 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。

メモ: Server Administrator の詳細については、**dell.com/support/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。iSM の詳細については、iDRAC サービスモジュールの使用 、p. 262 を参照してください。

1. *Dell Systems Management Tools and Documentation* DVD、またはデルサポートウェブサイトから、管理下システムの Server Administrator または iDRAC サービスモジュール（iSM）をインストールします。
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 ［自動リカバリ］ タイマーを有効化し、自動リカバリ処置を ［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）。
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 —『*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 — `racadm config -g cfgRacTuning -o cfgRacTuneAsrEnable 1` コマンドを使用します。
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。

OS から iDRAC へのパススルーの有効化または無効化

ネットワークドーターカード（NDC）または内蔵 LAN On Motherboard（LOM）デバイスがあるサーバでは、OS から iDRAC へのパススルー機能を有効にできます。この機能は、共有 LOM（ラックまたはタワーサーバ）、専用 NIC（ラック、タワー、またはブレードサーバ）、または USB NIC を介して iDRAC とホストオペレーティングシステム間の高速相方向帯域内通信を提供します。この機能は、iDRAC Enterprise ライセンスで使用可能です。

メモ: iDRAC サービスモジュール（iSM）は、オペレーティングシステムから iDRAC を管理するための多くの機能を提供します。詳細については、**dell.com/support/manuals** にある『*iDRAC サービスモジュールインストールガイド*』を参照してください。

専用 NIC 経由で有効にした場合は、ホストオペレーティングシステムでブラウザを起動してから、iDRAC ウェブインタフェースにアクセスできます。ブレードサーバーの専用 NIC は、Chassis Management Controller 経由です。

専用 NIC または共有 LOM の切り替えには、ホストオペレーティングシステムまたは iDRAC の再起動またはリセットは必要ありません。

このチャネルは以下を使用して有効化できます。

- iDRAC ウェブインタフェース
- RACADM または WS-MAN（ポストオペレーティングシステム環境）
- 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）

ネットワーク設定を iDRAC ウェブインタフェースから変更した場合は、OS から iDRAC へのパススルーを有効化する前に、少なくとも 10 秒間待つ必要があります。

RACADM または WS-MAN を介して XML 設定ファイルを使用していて、ネットワーク設定をこのファイル内で変更した場合、OS から iDRAC へのパススルー機能を有効化する、または OS ホスト IP アドレスを設定するためには、15 秒間待つ必要があります。

OS から iDRAC へのパススルーを有効化する前に、以下を確認してください。

- iDRAC は、専用 NIC または共有モードを使用するように設定されている。（NIC の選択が、LOM の 1 つに割り当てられていることを意味する。）
- ホストオペレーティングシステムと iDRAC が同一サブネットおよび同一 VLAN 内にある。
- ホストオペレーティングシステム IP アドレスが設定されている。

- OS から iDRAC へのパススルー機能をサポートするカードが装備されている。
- 設定権限がある。

この機能を有効にする場合は、以下に留意してください。

- 共有モードでは、ホストオペレーティングシステムの IP アドレスが使用されます。
- 専用モードでは、ホストオペレーティングシステムの有効な IP アドレスを指定する必要があります。複数の LOM がアクティブになっている場合は、最初の LOM の IP アドレスを入力します。

OS から iDRAC のパススルー機能が有効化後も機能しない場合は、次の点をチェックするようにしてください。

- iDRAC 専用 NIC ケーブルが正しく接続されている。
- 少なくとも 1 つの LOM がアクティブになっている。

メモ: デフォルト IP アドレスを使用します。USB NIC インタフェースの IP アドレスが iDRAC またはホスト OS IP アドレスと同じネットワークサブネット内にないことを確認してください。この IP アドレスがホストシステムまたはローカルネットワークのその他インタフェースの IP アドレスと競合する場合は、その IP アドレスを変更する必要があります。

メモ: 169.254.0.3 および 169.254.0.4 の IP アドレスは使用しないでください。これらの IP アドレスは、A/A ケーブル使用時の前面パネルの USB NIC ポート用に予約されています。

関連参照文献

OS から iDRAC へのパススルー用の対応カード 、p. 90
USB NIC 対応のオペレーティングシステム 、p. 90
ウェブインタフェースを使用した OS to iDRAC パススルーの有効化または無効化 、p. 92
RACADM を使用した OS から iDRAC へのパススルーの有効化または無効化 、p. 93
iDRAC 設定ユーティリティを使用した OS から iDRAC へのパススルーの有効化または無効化 、p. 93

OS から iDRAC へのパススルー用の対応カード

次の表には、LOM を使用した OS から iDRAC へのパススルー機能をサポートするカードのリストが示されています。

表 11. : LOM を使用した OS から iDRAC へのパススルー — 対応カード

カテゴリ	製造元	タイプ
NDC	Broadcom	• 5720 QP rNDC 1G BASE-T • 57810S DP bNDC KR • 57800S QP rNDC (10G BASE-T + 1G BASE-T) • 57800S QP rNDC (10G SFP + 1G BASE-T) • 57840、10G KR (4 個) • 57840 rNDC
	Intel	• i540 QP rNDC (10G BASE-T + 1G BASE-T) • i350 QP rNDC 1G BASE-T • x520/i350 rNDC 1GB
	QLogic	QMD8262 ブレード NDC

組み込み型 LOM カードも OS から iDRAC へのパススルー機能に対応しています。

次のカードは、OS から iDRAC へのパススルー機能をサポートしません。

- Intel 10 GB NDC
- コントローラ 2 個を装備した Intel rNDC – 10G コントローラはサポートしません。
- Qlogic bNDC
- PCIe、メザニン、およびネットワークインタフェースカード

USB NIC 対応のオペレーティングシステム

USB NIC 対応のオペレーティングシステムは次のとおりです。

- Windows Server 2008 R2 SP1
- Windows Server 2008 SP2 （64 ビット）

- Windows Server 2012
- Windows Server 2012 R2
- SUSE Linux Enterprise Server バージョン 10 SP4（64 ビット）
- SUSE Linux Enterprise Server バージョン 11 SP2（64 ビット）
- SUSE Linux Enterprise Server 11 SP4
- RHEL 5.9（32 ビットおよび 64 ビット）
- RHEL 6.4
- RHEL 6.7
- vSphere v5.0 U2 ESXi
- vSphere v5.1 U3
- vSphere v5.1 U1 ESXi
- vSphere v5.5 ESXi
- vSphere v5.5 U3
- vSphere 6.0
- vSphere 6.0 U1
- CentOS 6.5
- CentOS 7.0
- Ubuntu 14.04.1 LTS
- Ubuntu 12.04.04 LTS
- Debian 7.6（Wheezy）
- Debian 8.0

Windows 2008 SP 2、64 ビットオペレーティングシステムのサーバーでは、iDRAC 仮想 CD USB デバイスは自動的に検出されません（または有効になりません）。これは手動で有効にする必要があります。詳細に関しては、Microsoft が推奨する手順を参照して、このデバイス用のドライバ、Remote Network Driver Interface Specification（RNDIS）を手動で更新してください。

Linux オペレーティングシステムの場合、USB NIC を DHCP としてホストオペレーティングシステムに設定した後で、USB NIC を有効化します。

ホスト上のオペレーティングシステムが、SUSE Linux Enterprise Server 11、CentOS 6.5、CentOS 7.0、Ubuntu 14.04.1 LTS、または Ubuntu 12.04.4 LTS である場合、USB NIC を iDRAC で有効化した後、ホストオペレーティングシステムで DHCP クライアントを手動で有効化する必要があります。DHCP を有効にするための情報は、SUSE Linux Enterprise Server、CentOS、および Ubuntu オペレーティングシステムのマニュアルを参照してください。

vSphere の場合、VIB ファイルをインストールしてから、USB NIC を有効化する必要があります。

次のオペレーティングシステムの場合、Avahi および nss-mdns パッケージをインストールする場合は、**https://idrac.local** 使用して、ホストオペレーティングシステムから iDRAC を起動します。これらのパッケージがインストールされていない場合は、**https://169.254.0.1** を使用して iDRAC を起動します。

オペレーティングシステム	ファイアウォールのステータス	Avahi パッケージ	nss-mdns パッケージ
RHEL 5.9 32 ビット	Disable（無効）	別のパッケージとしてインストール（`avahi-0.6.16-10.el5_6.i386.rpm`）	別のパッケージとしてインストール（`nss-mdns-0.10-4.el5.i386.rpm`）
RHEL 6.4 64 ビット	Disable（無効）	別のパッケージとしてインストール（`avahi-0.6.25-12.el6.x86_64.rpm`）	別のパッケージとしてインストール（`nss-mdns-0.10-8.el6.x86_64.rpm`）
SLES 11 SP 3 64 ビット	Disable（無効）	Avahi パッケージは、オペレーティングシステム DVD に含まれています	nss-mdns は、Avahi のインストール中にインストールされます

ホストシステムでは、RHEL 5.9 オペレーティングシステムのインストール中に、USB NIC パススルーモードが無効状態になっています。インストール完了後にこのモードを有効にすると、USB NIC デバイスに対応するネットワークインタフェースは自動的にアクティブにはなりません。USB NIC デバイスをアクティブにするには、次のいずれかを実行します。

- ネットワークマネージャツールを使用して、USB NIC インタフェースを設定します。[システム] > [管理者] > [ネットワーク] > [デバイス] > [新規] > [イーサネット接続] と移動して、[Dell computer corp.iDRAC 仮想 NIC USB デバイス] を選択します。有効にするアイコンをクリックして、デバイスを有効にします。詳細に関しては、RHEL 5.9 のマニュアルを参照してください。
- 対応するインタフェースの設定ファイルを、`/etc/sysconfig/network-script/` ディレクトリ内に `ifcfg-ethX` として作成します。基本エントリ、DEVICE、BOOTPROTO、HWADDR、ONBOOT を追加します。`ifcfg-ethX` ファイルに TYPE を追加し、`service network restart` コマンドを使用してネットワークサービスを再起動します。
- システムを再起動します。
- システムの電源を切り、システムの電源を入れます。

RHEL 5.9 オペレーティングシステムを搭載しているシステムでは、USB NIC が無効にされた状態でシステムの電源を切るか、この逆の状態で、システムの電源を入れたときに USB NIC が有効になっていると、USB NIC デバイスは自動的にアクティブにはなりません。アクティブにするには、`/etc/sysconfig/network-script` ディレクトリ内で USB NIC インタフェースに `ifcfg-ethX.bak` ファイルを使用可能かを、チェックします。使用可能な場合は、名前 `ifcfg-ethX` に変更してから `ifup ethX` コマンドを使用します。

関連タスク

VIB ファイルのインストール 、p. 92

VIB ファイルのインストール

vSphere のオペレーティングシステムでは、USB の NIC を有効にする前に、VIB ファイルをインストールする必要があります。

VIB ファイルをインストールするには、以下を実行します。

1. Windows-SCP を使用して、VIB ファイルを ESX-i ホストオペレーティングシステムの `/tmp/` フォルダにコピーします。
2. ESXi プロンプトに移動し、次のコマンドを実行します。

```
esxcli software vib install -v /tmp/ iDRAC_USB_NIC-1.0.0-799733X03.vib --no-sig-check
```

出力は次のとおりです。

```
Message: The update completed successfully, but the system needs to be rebooted for the
changes to be effective.
Reboot Required: true
VIBs Installed: Dell_bootbank_iDRAC_USB_NIC_1.0.0-799733X03
VIBs Removed:
VIBs Skipped:
```

3. サーバーを再起動します。
4. ESXi プロンプトで、コマンド、`esxcfg-vmknic -l` を実行します。
出力は usb0 エントリを表示します。

ウェブインタフェースを使用した OS to iDRAC パススルーの有効化または無効化

ウェブインタフェースを使用して OS to iDRAC パススルーを有効にするには、次の手順を実行します。

1. [概要] > [iDRAC 設定] > [ネットワーク] > [OS to iDRAC パススルー] と移動します。
[OS to iDRAC パススルー] ページが表示されます。
2. 次のいずれかのオプションを選択して、OS to iDRAC パススルーを有効化します。
   - [LOM] — iDRAC とホストオペレーティングシステム間の OS から iDRAC へのパススルーリンクが LOM または NDC 経由で確立されます。
   - [USB NIC] — iDRAC とホストオペレーティングシステム間の OS から iDRAC へのパススルーリンクが内蔵 USB バス経由で確立されます。

   この機能を無効にするには、[無効] を選択します。
3. パススルー設定として [LOM] を選択し、専用モードを使ってサーバーが接続されている場合は、オペレーティングシステムの IPv4 アドレスを入力します。

   メモ: サーバーが共有 LOM モードで接続されている場合、[OS IP アドレス] フィールドが無効化されます。
4. [USB NIC] をパススルー設定として選択した場合、USB NIC の IP アドレスを入力します。

   デフォルト値は 169.254.0.1 です。デフォルトの IP アドレスを使用することが推奨されます。ただし、この IP アドレスとホストシステムまたはローカルネットワークの他のインタフェースの IP アドレスの競合が発生した場合は、これを変更する必要があります。

   169.254.0.3 IP および 169.254.0.4 IP は入力しないでください。これらの IP は、A/A ケーブル使用時の、前面パネルの USB NIC ポート用に予約されています。
5. 設定を適用するには、[適用] をクリックします。

6. ［ネットワーク設定のテスト］をクリックして、IP がアクセス可能で、iDRAC とホストオペレーティングシステム間のリンクが確立されているかどうかをチェックします。

RACADM を使用した OS から iDRAC へのパススルーの有効化または無効化

RACADM を使用して OS から iDRAC へのパススルーを有効または無効にするには、`iDRAC.OS-BMC` グループのオブジェクトを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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 OS から iDRAC へのパススルーの有効化または無効化

iDRAC 設定ユーティリティを使用して OS から iDRAC へのパススルー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、［通信権限］に移動します。
   ［iDRAC 設定通信権限］ページが表示されます。
2. 次のいずれかのオプションを選択して、OS から iDRAC へのパススルーを有効化します。
   - ［LOM］— iDRAC とホストオペレーティングシステム間の OS から iDRAC へのパススルーリンクが LOM または NDC 経由で確立されます。
   - ［USB NIC］— iDRAC とホストオペレーティングシステム間の OS から iDRAC へのパススルーリンクが内蔵 USB バス経由で確立されます。

   この機能を無効にするには、［無効］を選択します。

   メモ: LOM オプションは、OS から iDRAC へのパススルー機能をサポートするカードでのみ選択できます。それ以外ではこのオプションはグレー表示となります。

3. パススルー設定として［LOM］を選択し、専用モードを使ってサーバーが接続されている場合は、オペレーティングシステムの IPv4 アドレスを入力します。

   メモ: サーバーが共有 LOM モードで接続されている場合、［OS IP アドレス］フィールドが無効化されます。

4. ［USB NIC］をパススルー設定として選択した場合、USB NIC の IP アドレスを入力します。

   デフォルト値は 169.254.0.1 です。ただし、この IP アドレスがホストシステムまたはローカルネットワークの別のインタフェースの IP アドレスと競合する場合は、値を変更する必要があります。IP アドレス 169.254.0.3 と 169.254.0.4 は入力しないでください。これらの IP は、A/A ケーブルが使用される場合に前面パネルの USB NIC ポート用に予約されています。
5. ［戻る］、［終了］の順にクリックし、［はい］をクリックします。
   詳細が保存されます。

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 12. 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	信頼済み CA 証明書	CSR を生成し、認証局の署名を取得します。 SHA-2 証明書もサポートされています。
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 • 信頼済み 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。

表 12. ログインタイプに基づいた証明書のタイプ （続き）

ログインタイプ	証明書タイプ	取得方法
		● 信頼済み CA 証明書 — この証明書は、CA によって発行されます。 SHA-2 証明書もサポートされています。
Active Directory ユーザーログイン	信頼済み CA 証明書	この証明書は、CA によって発行されます。 SHA-2 証明書もサポートされています。
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: iDRAC 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。iDRAC 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。 SHA-2 証明書もサポートされています。

関連概念

SSL サーバー証明書 、p. 94
新しい証明書署名要求の生成 、p. 95

SSL サーバー証明書

iDRAC 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 Web サーバが含まれています。SSL 暗号化オプションは、脆弱な暗号を無効にするために提供されています。非対称暗号テクノロジを基盤とする SSL は、クライアントとサーバとの間での通信に認証と暗号化を適用し、ネットワーク上での盗聴を防止する、という目的で広く利用されています。

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

メモ: SSL 暗号化を 256 ビット以上に設定する場合は、それに見合うレベルの暗号化を設定した iDRAC プラグイン（vConsole など）の使用が許可されるよう、仮想マシン環境（JVM、IcedTea）の暗号化設定で、Unlimited Strength Java Cryptography Extension ポリシーファイルをインストールすることが必要になる場合があります。ポリシーファイルのインストール方法の詳細については、Java のマニュアルを参照してください。

iDRAC ウェブサーバには、デフォルトで、一意の Dell 自己署名 SSL デジタル証明書があります。デフォルト SSL 証明書は、主要な認証局（CA）によって署名された証明書に置き換えることができます。認証局とは、IT 業界において、信頼のおける審査や識別などの重要なセキュリティ基準を高い水準で満たしていると認められた事業体です。CA には、Thawte や VeriSign などがあります。CA 署名済み証明書を取得するプロセスを開始するには、iDRAC 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、会社の情報で証明書署名要求（CSR）を生成します。次に、生成された CSR を VeriSign や Thawte などの CA に提出します。CA は、ルート CA の場合も中間 CA の場合もあります。CA 署名済み SSL 証明書を受信したら、それを iDRAC にアップロードします。

各 iDRAC が管理ステーションによって信頼されるようにするには、その iDRAC の SSL 証明書を管理ステーションの証明書ストアに配置する必要があります。SSL 証明書が管理ステーションにインストールされると、サポート対象のブラウザからは、証明書警告を受けることなく iDRAC にアクセスできるようになります。

デフォルトの署名証明書に依存することなく、カスタム署名証明書をアップロードして SSL 証明書に署名することも可能です。1 つのカスタム署名証明書をすべての管理ステーションにインポートすることにより、そのカスタム署名証明書を使用するすべての iDRAC が信頼されます。カスタム SSL 証明書が既に使用されているときにカスタム署名証明書がアップロードされると、カスタム SSL 証明書は無効になり、カスタム署名証明書で署名された 1 回限りの自動生成 SSL 証明書が使用されます。カスタム署名証明書はプライベートキーなしでダウンロードできます。既存のカスタム署名証明書を削除することもできます。カスタム署名証明書を削除すると、iDRAC はリセットされ、新しい自己署名 SSL 証明書が自動生成されます。自己署名証明書が再生成されると、iDRAC と管理ステーションとの間での信頼関係を再確立する必要が生じます。自動生成された SSL 証明書は自己署名済みで、有効期限は 7 年と 1 日、開始日は 1 日前となります（管理ステーションと iDRAC とでタイムゾーン設定が異なる場合があるため）。

iDRAC ウェブサーバの SSL 証明書は、証明書署名要求（CSR）の生成時における共通名（CN）の左端部分の一部として、アスタリスク文字（*）をサポートします。例えば、*.qa.com や *.company.qa.com のように表記することができます。これは、ワイルドカード証明書と呼ばれます。ワイルドカード CSR が iDRAC 外で生成された場合でも、1 つの署名済みワイルドカード SSL 証明書を複数の iDRAC にアップロードすることが可能であり、すべての iDRAC はサポート対象ブラウザによって信頼されます。ワイルドカード証明書に対応しているサポート対象ブラウザを使用して iDRAC ウェブインタフェースに接続している間は、iDRAC はブラウザから信頼されます。ビューアの起動中であっても、iDRAC はビューアのクライアントにより信頼されます。

関連概念

新しい証明書署名要求の生成、p. 95
サーバー証明書のアップロード、p. 96
サーバー証明書の表示、p. 96
カスタム署名証明書のアップロード、p. 97
カスタム SSL 証明書署名証明書のダウンロード、p. 97
カスタム SSL 証明書署名証明書の削除、p. 98

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 iDRAC にアップロードできます。iDRAC 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、iDRAC 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。

関連概念

SSL サーバー証明書、p. 94

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、iDRAC は証明書を受け入れません。

1. iDRAC 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、［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、『iDRAC オンラインヘルプ』を参照してください。
3. ［生成］をクリックします。
   新しい CSR が生成されます。これ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

RACADM を使用して CSR を生成するには、`iDRAC.Security` グループのオブジェクトで `set` コマンドを使用して、次に `sslcsrgen` コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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、署名済み SSL サーバー証明書を iDRAC ファームウェアにアップロードできます。証明書を適用するには、iDRAC をリセットする必要があります。iDRAC は、X509 の Base-64 エンコードされたウェブサーバー証明書のみを受け入れます。SHA-2 証明書もサポートされています。

注意: リセット中は、iDRAC が数分間使用できなくなります。

関連概念

SSL サーバー証明書 、p. 94

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. iDRAC 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 iDRAC にアップロードされます。
4. iDRAC をすぐに、または後でリセットするかどうかを尋ねるポップアップメッセージが表示されます。必要に応じて、[iDRAC をリセット] または [iDRAC を後でリセット] をクリックします。
   iDRAC はリセットされ、新しい証明書が適用されます。リセット中は、iDRAC を数分間使用できなくなります。

   メモ: 新しい証明書を適用するには iDRAC をリセットする必要があります。iDRAC がリセットされるまで、既存の証明書がアクティブになります。

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。詳細に関しては、**dell.com/idracmanuals** にある『iDRAC 向け RACADM コマンドラインリファレンスガイド』を参照してください。

iDRAC の外でプライベートキーを使用して CSR が生成された場合に、iDRAC に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. CSR を既知のルート CA に送信します。CA は CSR に署名し、CSR は有効な証明書になります。
2. リモート racadm `sslkeyupload` コマンドを使用して、プライベートキーをアップロードします。
3. リモート racadm `sslcertupload` コマンドを使用して、署名された証明書を iDRAC にアップロードします。
   新しい証明書が iDRAC にアップロードされます。iDRAC をリセットするかどうかを確認するメッセージが表示されます。
4. iDRAC をリセットするには、racadm `racreset` コマンドを実行します。
   iDRAC はリセットされ、新しい証明書が適用されます。リセット中は、iDRAC を数分間使用できなくなります。

   メモ: 新しい証明書を適用するには iDRAC をリセットする必要があります。iDRAC がリセットされるまで、既存の証明書がアクティブになります。

サーバー証明書の表示

現在 iDRAC で使用されている SSL サーバー証明書を表示できます。

関連概念

SSL サーバー証明書 、p. 94

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

iDRAC ウェブインタフェースで、[概要] > [iDRAC 設定] > [ネットワーク] > [SSL] と移動します。[SSL] ページの上部に、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、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

カスタム署名証明書のアップロード

カスタム署名証明書をアップロードして SSL 証明書に署名することができます。SHA-2 証明書もサポートされています。

ウェブインタフェースを使用したカスタム署名証明書のアップロード

iDRAC ウェブインタフェースを使用してカスタム署名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. ［概要］>［iDRAC 設定］>［ネットワーク］>［SSL］と移動します。
   ［SSL］ページが表示されます。
2. ［カスタム SSL 証明書署名証明書］で、［カスタム SSL 証明書署名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。
   ［カスタム SSL 証明書署名証明書のアップロード］ページが表示されます。
3. ［参照］をクリックして、カスタム SSL 証明書署名証明書ファイルを選択します。
   Public-Key Cryptography Standards #12（PKCS #12）準拠の証明書のみがサポートされます。
4. 証明書がパスワードで保護されている場合は、［PKCS#12 パスワード］フィールドにパスワードを入力します。
5. ［適用］をクリックします。
   証明書が iDRAC にアップロードされます。
6. iDRAC をすぐに、または後でリセットするかどうかを尋ねるポップアップメッセージが表示されます。必要に応じて、［iDRAC をリセット］または［iDRAC を後でリセット］をクリックします。
   iDRAC のリセット後に、新しい証明書が適用されます。リセット中は、iDRAC を数分間使用できなくなります。

   メモ: 新しい証明書を適用するには iDRAC をリセットする必要があります。iDRAC がリセットされるまで、既存の証明書がアクティブになります。

RACADM を使用したカスタム SSL 証明書署名証明書のアップロード

RACADM を使用してカスタム SSL 証明書署名証明書をアップロードするには、sslcertupload コマンドを使用し、次に racreset コマンドを使用して iDRAC をリセットします。

詳細について、**www.dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインリファレンスガイド*』を参照してください。

カスタム SSL 証明書署名証明書のダウンロード

iDRAC ウェブインタフェースまたは RACADM を使用して、カスタム署名証明書をダウンロードできます。

カスタム署名証明書のダウンロード

iDRAC ウェブインタフェースを使用してカスタム署名証明書をダウンロードするには、次の手順を実行します。

1. ［概要］>［iDRAC 設定］>［ネットワーク］>［SSL］と移動します。
   ［SSL］ページが表示されます。
2. ［カスタム SSL 証明書署名証明書］で、［カスタム SSL 証明書署名証明書のダウンロード］を選択して［次へ］をクリックします。
   選択した場所にカスタム署名証明書を保存できるポップアップメッセージが表示されます。

RACADM を使用したカスタム SSL 証明書署名証明書のダウンロード

カスタム SSL 証明書署名証明書をダウンロードするには、sslcertdownload サブコマンドを使用します。詳細に関しては、**dell.com/idracmanuals** にある『iDRAC RACADM コマンドラインインタフェースリファレンスガイド』を参照してください。

カスタム SSL 証明書署名証明書の削除

iDRAC ウェブインタフェースまたは RACADM を使用して、既存のカスタム署名証明書を削除することもできます。

iDRAC ウェブインタフェースを使用したカスタム署名証明書の削除

iDRAC ウェブインタフェースを使用してカスタム署名証明書を削除するには、次の手順を実行します。

1. ［概要］ > ［iDRAC 設定］ > ［ ネットワーク］ > ［SSL］ と移動します。
   ［SSL］ ページが表示されます。
2. ［カスタム SSL 証明書署名証明書］ で、［カスタム SSL 証明書署名証明書の削除］ を選択して ［次へ］ をクリックします。
3. iDRAC をすぐに、または後でリセットするかどうかを尋ねるポップアップメッセージが表示されます。必要に応じて、［iDRAC をリセット］ または ［iDRAC を後でリセット］ をクリックします。
   iDRAC のリセット後に、新しい自己署名証明書が生成されます。

RACADM を使用したカスタム SSL 証明書署名証明書の削除

RACADM を使用してカスタム SSL 証明書署名証明書を削除するには、`sslcertdelete` サブコマンドを使用します。次に、`racreset` コマンドを使用して iDRAC をリセットします。

詳細について、**www.dell.com/idracmanuals** にある『*iDRAC RACADM コマンドライン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 iDRAC の設定

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

メモ:

- 設定ファイルには、特定のサーバーに関連する情報が含まれています。この情報は、さまざまなオブジェクトのグループに分類されています。
- いくつかの設定ファイルには固有の iDRAC 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 iDRAC にインポートする前に、あらかじめその情報を変更しておく必要があります。

システム設定プロファイルを使用して、RACADM で複数の iDRAC を設定することもできます。システム設定 XML ファイルにはコンポーネント設定情報が含まれています。このファイルを使用してターゲットシステムにインポートすることで、BIOS、iDRAC、RAID、および NIC の設定を適用できます。詳細については、**dell.com/support/manuals** または Dell Tech Center にある『*XML 設定ワークフロー*』ホワイトペーパーを参照してください。

設定ファイルを使用して複数の iDRAC 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、必要な設定を含むターゲット iDRAC をクエリします。

   ```
   racadm get -f <file_name>.xml -t xml
   ```

   コマンドは iDRAC 設定を要求し、設定ファイルを生成します。

   メモ: `get -f` を使用した iDRAC 設定のファイルへのリダイレクトは、ローカルおよびリモート RACADM インタフェースでのみサポートされています。

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

   `get` 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、ユーザーのすべての設定プロパティを表示します。

2. 必要に応じて、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。

   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. ターゲット iDRAC で、次のコマンドを使用して設定を変更します。

```
racadm set -f <file_name>.xml -t xml
```

これによって、その他の iDRAC に情報がロードされます。`set` コマンドを使用して、ユーザーおよびパスワードデータベースを Server Administrator と同期することができます。
4. `racadm racreset` コマンドを使用して、ターゲットの iDRAC をリセットします。

iDRAC 設定ファイルの作成

設定ファイルは次のとおりです。

- 作成済み。
- `racadm get -f <file_name>.xml -t xml` コマンドを使用して取得済み。
- `racadm get -f <file_name>.xml -t xml` を使用して取得して編集済み。

`get` コマンドの詳細については、**dell.com/idracmanuals** にある*『iDRAC RACADM コマンドラインインタフェースリファレンスガイド』*を参照してください。

設定ファイルはまず、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。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 iDRAC に送信されません。ユーザーは、そのファイルを使用して iDRAC 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。

注意: `racresetcfg` コマンドを使用して、データベースと iDRAC NIC 設定を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。

ホストシステムでの iDRAC 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 iDRAC 設定を変更するためのアクセスを無効にできます。ただし、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. iDRAC 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。
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: アクセスが無効になると、Server Administrator または IPMITool を使用して iDRAC 設定を使用できません。ただし、IPMI オーバー LAN を使用できます。

5

iDRAC と管理下システム情報の表示

iDRAC 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。

関連概念

トピック：

管理下システムの正常性とプロパティの表示

iDRAC 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] で管理下システムの正常性や基本的な iDRAC 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を行ったり、電源オン / オフ、パワーサイクル、ログの表示、ファームウェアのアップデートとロールバック、前面パネル LED のスイッチオン / オフ、および iDRAC のリセットなどのタスクをを迅速に開始することが可能になります。

[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、『iDRAC オンラインヘルプ』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。

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コンポーネントと、インストールされたファームウェアコンポーネントに関する情報を表示することができます。これを行うには、iDRAC 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、『iDRAC オンラインヘルプ』を参照してください。

ハードウェアインベントリ セクションは、管理下システムで利用可能な以下のコンポーネントの情報を表示します。

- iDRAC
- RAID コントローラ
- バッテリ
- CPU
- DIMM
- HDD
- バックプレーン
- ネットワークインタフェースカード（内蔵および組み込み型）
- ビデオカード
- SD カード
- 電源装置ユニット（PSU）
- ファン
- Fibre Channel HBA
- USB
- NVMe PCIe SSD デバイス

ファームウェアインベントリセクションは、次のコンポーネントのファームウェアバージョンを表示します。

- BIOS
- Lifecycle Controller
- iDRAC
- OS ドライバパック
- 32 ビット診断
- システム CPLD
- PERC コントローラ
- バッテリ
- 物理ディスク
- 電源装置
- NIC
- Fibre Channel
- バックプレーン
- エンクロージャ
- PCIe SSD

メモ: ソフトウェアインベントリは、ファームウェアバージョンの最後の 4 バイトしか表示しません。例えば、ファームウェアバージョンが FLVDL06 である場合、ファームウェアインベントリは DL06 を表示します。

メモ: Dell PowerEdge FX2/FX2s サーバーでは iDRAC GUI に表示される CMC バージョンの命名規則が CMC GUI で表示されるバージョンとは異なりますが、バージョンは変わりません。

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ときは、再起動時にシステムインベントリを収集するため、[Collect System Inventory on Reboot]（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、iDRAC 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 分間かかる場合があります。

メモ: CSIOR オプションはデフォルトで有効化されます。

メモ: オペレーティングシステム内で行われた設定変更とファームウェアアップデートは、サーバーを再起動するまでインベントリに適切に反映されないことがあります。

[エクスポート] をクリックして、ハードウェアインベントリを XML 形式でエクスポートして、任意の場所に保存します。

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）上のバッテリーに関する情報を提供します。

  メモ: ストレージ ROMB のバッテリー設定は、システムにバッテリー装備の ROMB がある場合にのみ利用可能です。
- **ファン**（ラックおよびタワーサーバの場合のみ利用可能）— システムファンに関する情報を提供します（ファン冗長性、およびファン速度としきい値を表示するファンのリスト）。

- **CPU** — 管理下システム内の CPU の正常性と状態を示します。プロセッサの自動スロットルと予測障害も報告します。
- **メモリ** — 管理下システムにある Dual In-line Memory Module（DIMM）の正常性と状態を示します。
- **イントルージョン** — シャーシについての情報を提供します。
- **電源装置**（ラックおよびタワーサーバの場合のみ利用可能）— 電源装置と電源装置の冗長性状態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** — 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 の冗長性が有効化されているときは、「IDSDM 冗長性ステータス、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。

    メモ: IDSDM 再構築操作中にホストシステムを再起動すると、iDRAC は IDSDM 情報を表示しません。この問題を解決するには、IDSDM を再び再構築するか、iDRAC をリセットします。

    メモ: デルの第 13 世代 PowerEdge サーバでは、IDSDM 再構築操作はバックグラウンドで実行され、再構築プロセス中にシステムが停止することはありません。再構築操作のステータスを表示するには、Lifecycle Controller のログを確認します。デルの第 12 世代 PowerEdge サーバでは、再構築操作の実行中、システムが停止されます。
  - 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** — システム基板の吸気口温度と排気口温度に関する情報を提供します（ラックサーバにのみ該当）。この温度プローブは、プローブのステータスが事前設定された警告と重要しきい値の範囲内にあるかどうかを示します。
- **電圧** — さまざまなシステムコンポーネントの電圧センサーの状態と読み取り値を示します。

次の表は、iDRAC ウェブインタフェースと RACADM を使用したセンサー情報の表示に関する情報を示しています。ウェブインタフェースに表示されたプロパティの詳細ついては、『*iDRAC オンラインヘルプ*』を参照してください。

メモ: ハードウェアの概要ページには、お使いのシステムにあるセンサーのデータのみ表示されます。

表 13. 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
バッテリー	［概要］ > ［ハードウェア］ > ［バッテリー］	`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、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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］	
CPU	［概要］ > ［ハードウェア］ > ［CPU］	
メモリ	［概要］ > ［ハードウェア］ > ［メモリ］	
イントルージョン	［概要］ > ［サーバ］ > ［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］ > ［電源 / 温度］ > ［温度］	

表 13. 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 （続き）

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
電圧	[概要] > [サーバ] > [電源 / 温度] > [電圧]	

CPU、メモリ、および I/O モジュールのパフォーマンスインデックスの監視

デルの第 13 世代 Dell PowerEdge サーバでは、Intel ME が Compute Usage Per Second (CUPS) 機能をサポートしています。CUPS 機能は、システムに関する CPU、メモリ、および I/O 使用率とシステムレベルの使用率インデックスのリアルタイム監視を行います。Intel ME は帯域外 (OOB) で監視を実行できるため、CPU リソースを消費しません。Intel ME にはシステム CUPS センサーが搭載されており、これは、計算、メモリ、および I/O リソースの使用率値を CUPS インデックスとして示します。iDRAC は、全体的なシステム使用率に対してこの CUPS インデックスを監視し、CPU、メモリ、および I/O 使用率インデックスの瞬間的な値も監視します。

メモ: この機能は、 poweredge R930 サーバではサポートされません。

CPU とチップセットには専用のリソース監視カウンタ (RMC) があります。システムリソースの使用率情報は、これらの RMC からデータを照会することによって取得されます。RMC からのデータは各システムリソースの累積使用率を測定するためにノードマネージャによって集約されます。これらのデータは既存の相互通信メカニズムを使用して iDRAC から読み取られ、帯域外マネジメントインタフェース経由で提供されます。

パフォーマンスパラメータとインデックス値の Intel センサーの表示は物理システム全体に関するものなので、システムが仮想化され、複数の仮想ホストがある場合でも、インタフェース上のパフォーマンスデータの表示は物理システム全体に関するものになります。

パフォーマンスパラメータを表示するには、サポートされているセンサーがサーバーに存在する必要があります。

4 つのシステム使用率のパラメータは次のとおりです。

- **CPU 使用率** - 各 CPU コアの RMC からのデータはシステム内のすべてのコアの累積使用率を提供するために集約されます。この使用率はアクティブ状態で費やされた時間と、非アクティブ状態で費やされた時間に基づくものです。RMC のサンプルは 6 秒ごとに取得されます。
- **メモリ使用率** - RMC は各メモリチャネルまたはメモリコントローラインスタンスで発生するメモリトラフィックを測定します。RMC からのデータは、システム上のすべてのメモリチャネル間の累積メモリトラフィックを測定するために集約されます。これは、メモリ使用量ではなく、メモリ帯域幅消費量の測定になります。iDRAC では、このデータを 1 分間集約するので、Linux の **top** のような他の OS ツールが示すメモリ使用率と一致しない場合があります。iDRAC が表示するメモリ帯域幅の使用率は、メモリを多く消費する作業負荷であるかどうかを示します。
- **I/O 使用率** - ルートポートおよび下位セグメントから発信される、またはそこに到達する PCI Express トラフィックを測定するため、PCI Express Root Complex のルートポートにつき 1 つの RMC があります。これらの RMC からのデータは、パッケージから発信される、すべての PCI Express セグメントに対する PCI Express トラフィックを測定するために集約されます。これは、システムの I/O 帯域幅使用率の測定になります。
- **システムレベルの CUPS インデックス** - CUPS インデックスは、各システムリソースに対して事前に定義された負荷要因を考慮した CPU、メモリ、および I/O インデックスを集約することによって計算されます。負荷要因は、システム上の作業負荷の性質によって異なります。CUPS インデックスは、サーバ上で使用できる計算ヘッドルームの測定を示します。システムの CUPS インデックスが大きい場合、そのシステム上には追加の作業負荷を割り当てるための制限付きヘッドルームが存在します。リソースの消費が減少すると、システムの CUPS インデックスも減少します。CUPS インデックスが低い場合は、大きな計算ヘッドルームが存在すること、サーバが新規の作業負荷を受け入れられること、およびサーバが電力消費を抑えるために低電力状態になっていることを示します。作業負荷の監視をデータセンター全体に適用して、データセンターの作業負荷の高レベルで総合的なビューを提供することができるため、ダイナミックデータセンターソリューションが実現します。

メモ: CPU、メモリ、I/O 使用率のインデックスは、1 分で集約されます。そのため、これらのインデックスに瞬間的な急上昇が存在する場合に抑制することが可能です。これらはリソース使用量ではなく、作業負荷のパターンを示します。

使用率インデックスのしきい値に達した場合に、センサーイベントが有効であると、IPMI、SEL、および SNMP トラップが生成されます。センサーイベントフラグはデフォルトで無効になっています。このフラグは、標準の IPMI インタフェースを使用して有効にすることができます。

必要な権限は次のとおりです。

- パフォーマンスデータを監視するにはログイン権限が必要です。
- 警告しきい値設定とピーク履歴のリセットには、設定権限が必要です。
- 静的データ履歴を読み取るには、ログイン権限と Enterprise ライセンスが必要です。

ウェブインタフェースを使用した CPU、メモリ、および I/O モジュールのパフォーマンスインデックスの監視

CPU、メモリ、および I/O モジュールのパフォーマンスインデックスを監視するには、iDRAC ウェブインタフェースで、[概要] > [ハードウェア] と移動します。**ハードウェア概要** ページには、次の情報が表示されます。

- [ハードウェア] セクション - 必要なリンクをクリックして、コンポーネントの正常性を表示します。
- [システムパフォーマンス] セクション - CPU、メモリ、および I/O 使用インデックスと、システムレベルの CUPS インデックスの現在の読み取りおよび警告をグラフィカルに表示します。
- [システムパフォーマンス履歴データ] セクション：
  - CPU、メモリ、I/O の使用率の統計情報と、システムレベルの CUPS インデックスを示します。ホストシステムの電源がオフになっている場合は、0 パーセントを下回る電源オフラインがグラフに表示されます。
  - 特定のセンサーのピーク時の使用率をリセットすることができます。[ピーク履歴のリセット] をクリックします。ピーク値をリセットするには、設定権限を持っている必要があります。
- [パフォーマンスメトリック] セクション：
  - ステータスおよび現在の読み取り値を表示します。
  - 使用率限度の警告しきい値を表示または指定します。しきい値を設定するには、サーバ設定権限を持っている必要があります。

メモ: このページに表示される情報は、お使いのサーバでサポートされているセンサーによって異なります。すべての Dell PowerEdge 第 12 世代サーバおよび一部の Dell PowerEdge 第 13 世代サーバでは、[システムパフォーマンス] セクション、[システムパフォーマンス履歴データ] セクション、および [パフォーマンスメトリック] セクションは表示されません。

表示されるプロパティについては、『*iDRAC オンラインヘルプ*』を参照してください。

RACADM を使用した CPU、メモリ、および I/O モジュールのパフォーマンスインデックスの監視

SystemPerfStatistics サブコマンドを使用して、CPU、メモリ、および I/O モジュールのパフォーマンスインデックスを監視します。詳細については、**dell.com/esmmanuals** にある『iDRAC RACADM コマンドラインリファレンスガイド』を参照してください。

システムの Fresh Air 対応性のチェック

外気による空冷は、外気を直接データセンターに使用してシステムを冷却しています。Fresh Air 対応のシステムは、通常の環境動作温度範囲を超えて動作します (最大 45 ºC (113 ºF) まで)。

メモ: 一部のサーバーまたは特定のサーバーの設定は、Fresh Air 対応ではない場合があります。Fresh Air 対応性に関する詳細については、特定サーバーのマニュアルを参照してください。または詳細についてデルにお問い合わせください。

システムの Fresh Air 対応性をチェックするには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、[概要] > [サーバー] > [電源 / サーマル] > [温度] の順に移動します。
   [温度] ページが表示されます。
2. サーバーが Fresh Air 対応かどうかについては、[Fresh Air] の項を参照してください。

温度の履歴データの表示

システムが、通常サポートされる環境温度のしきい値を超過した温度で稼動した時間を、パーセンテージで監視することができます。システム基板の温度センサーによるデータは､温度の監視用に一定期間収集されます。データの収集はシステムが工場出荷後初めて 電源を投入された時点で開始します。システムの電源がオンになっている間はデータの収集および表示が行われます。過去 7 年間監視された温度を追跡したり、保存したりすることができます。

メモ: フレッシュエア対応ではないシステムについても、温度履歴を追跡することができます。ただし、生成されたしきい値制限とフレッシュエアに関する警告は、フレッシュエアがサポートする制限に基づきます。警告の制限は 42 ºC、重大の制限は 47 ºC です。 これらの値は、2 ºC のマージン付き精度で 40 ºC と 45 ºC のフレッシュエア制限に対応します。

フレッシュエア制限に関連付られた次の 2 つの固定温度領域が追跡されます。

- 警告領域 - システムが温度センサーの警告しきい値 (42 ºC) を超えて稼動した期間を指します。システムが警告領域で稼動できるのは、12 ヶ月間の時間のうち 10 % です。

- 重大領域 - システムが温度センサーの重要しきい値（47 ºC）を超えて稼動した時間を指します。システムが重要領域で稼動できるのは、12 ヶ月間の時間のうち 1% であり、これは警告領域での稼動時間としても加算されます。

収集されたデータはグラフ形式で表示され 10% と 1% レベルを追跡します。記録された温度データは工場出荷前にのみクリアすることができます。

システムが通常サポートされている温度しきい値を超えた状態で一定時間稼動を続けると、イベントが生成されます。一定の稼働時間の平均温度が、警告レベル以上（8% 以上）または重大レベル以上（0.8% 以上）の場合、Lifecycle ログにイベントが記録され、該当する SNMP トラップが生成されます。イベントには以下があります。

- 警告イベント：温度が過去 12 ヶ月に警告しきい値を超過した状態が全稼動時間のうち 8 % 以上あった場合
- 重要イベント：温度が過去 12 ヶ月に警告しきい値を超過した状態が全稼動時間のうち 10 % 以上あった場合
- 警告イベント：温度が過去 12 ヶ月に重要しきい値を超過した状態が全稼動時間のうち 0.8 % 以上あった場合
- 重要イベント：温度が過去 12 ヶ月に重要しきい値を超過した状態が全稼動時間のうち 1 % 以上あった場合

追加のイベントを生成できるように iDRAC を設定することもできます。詳細については、「アラート反復イベントの設定」の項を参照してください。

iDRAC ウェブインタフェースを使用した温度の履歴データの表示

温度の履歴データを表示するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、［概要］ > ［サーバー］ > ［電源 / サーマル］ > ［温度］ の順に移動します。
   ［温度］ ページが表示されます。
2. 過去 1 日、過去 30 日、過去 1 年の温度の保存データ（平均およびピーク値）のグラフを表示するには、「［システム基板温度の歴史的データ］」の項を参照してください。

   詳細については、『iDRAC オンラインヘルプ』を参照してください。

   メモ: iDRAC ファームウェアのアップデートまたは iDRAC のリセット完了後、一部の温度データがグラフに表示されない場合があります。

RACADM を使用した温度の履歴データの表示

RACADM を使用して履歴データを表示するには、`inlettemphistory` コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインリファレンスガイド*』を参照してください。

吸気口温度の警告しきい値の設定

システム基板の吸気口温度センサーの最小および最大警告しきい値を修正できます。デフォルト処置にリセットすると、温度しきい値はデフォルト値に設定されます。吸気口温度センサーの警告しきい値を設定するには、設定ユーザー権限を持っている必要があります。

ウェブインタフェースを使用した吸気口温度の警告しきい値の設定

吸気口温度の警告しきい値を設定するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、［概要］ > ［ サーバー］ > ［ 電源 / サーマル］ > ［ 温度］の順に移動します。
   ［温度］ ページが表示されます。
2. ［温度プローブ］ セクションで、［システム基板吸気口温度］ に対する ［警告しきい値］ の最小値と最大値を摂氏または華氏単位で入力します。値を摂氏で入力すると、システムは自動的に華氏値に計算され、表示されます。同様に華氏を入力すると、摂氏値が表示されます。
3. ［適用］ をクリックします。

   値が設定されます。

   メモ: チャートの範囲は外気制限値にのみ対応するので、デフォルトしきい値を変更しても履歴データチャートには反映されません。カスタムしきい値の超過に関する警告は、外気しきい値の超過に関連する警告とは異なります。

ホスト OS で使用可能なネットワークインタフェースの表示

サーバーに割り当てられている IP アドレスなど、ホストオペレーティングシステム上で使用できるすべてのネットワークインタフェースについての情報を表示することができます。iDRAC サービスモジュールは、この情報を iDRAC に提供します。OS の IP アドレス情報には、IPv4 および IPv6 アドレス、MAC アドレス、サブネットマスクまたはプレフィックス長、ネットワークデバイスの FQDD、ネットワークインタフェース名、ネットワークインタフェースの説明、ネットワークインタフェースステータス、ネットワークインタフェースの種類（イーサネット、トンネル、ループバックなど）、ゲートウェイアドレス、DNS サーバーアドレス、および DHCP サーバーのアドレスが含まれます。

メモ: この機能は、iDRAC Express および iDRAC Enterprise ライセンスでご利用いただけます。

OS の情報を表示するには、次を確認してください。

- ログイン権限がある。
- iDRAC サービスモジュールがホストオペレーティングシステムにインストールされ、実行中である。
- ［概要］ > ［サーバー］ > ［サービスモジュール］ページで、OS 情報 オプションが有効になっている。

iDRAC は、ホスト OS に設定されているすべてのインタフェースの IPv4 アドレスと IPv6 アドレスを表示できます。

ホスト OS が DHCP サーバーを検出する方法によっては、対応する IPv4 または IPv6 DHCP サーバーのアドレスが表示されない場合があります。

ウェブインタフェースを使用したホスト OS で使用可能なネットワークインタフェースの表示

ウェブインタフェースを使用して、ホスト OS で使用可能なネットワークインタフェースを表示するには、次の手順を実行します。

1. ［概要］ > ［ホスト OS］ > ［ネットワークインタフェース］に移動します。
   ［ネットワークインタフェース］ページに、ホストのオペレーティングシステムで使用可能なすべてのネットワークインタフェースが表示されます。
2. ネットワークデバイスに関連付けられているネットワークインタフェースの一覧を表示するには、［ネットワークデバイス FQDD］ドロップダウンメニューからネットワークデバイスを選択し、［適用］をクリックします。
   ［ホスト OS ネットワークインタフェース］セクションに、OS IP の詳細が表示されます。
3. ［デバイス FQDD］列から、ネットワークデバイスリンクをクリックします。
   ［ハードウェア］ > ［ネットワークデバイス］セクションから対応するデバイスのページが表示されます。このページでは、デバイス詳細の表示が可能です。プロパティについての情報は、『*iDRAC オンラインヘルプ*』を参照してください。
4. 詳細を表示するには、 ＋ アイコンをクリックします。
   同様に、[［ハードウェア］] > [［ネットワークデバイス］] ページから、ネットワークデバイスに関連付けられたホスト OS ネットワークインタフェース情報を表示できます。［ホスト OS ネットワークインタフェースの表示］をクリックしてください。

   メモ: v2.3.0 以降の iDRAC サービスモジュール内の ESXi ホスト OS については、**追加詳細** リストの **説明** 列が次のフォーマットで表示されます。

   ```
   <List-of-Uplinks-Configured-on-the-vSwitch>/<Port-Group>/<Interface-name>
   ```

RACADM を使用したホスト OS で使用可能なネットワークインタフェースの表示

RACADM を使用してホストオペレーティングシステムで使用可能なネットワークインタフェースを表示するには、`gethostnetworkinterfaces` コマンドを使用します。詳細については、**dell.com/esmmanuals** にある『*iDRAC RACADM コマンドラインリファレンスガイド*』を参照してください。

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。

iDRAC 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、**dell.com/support/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 設定を有効化または無効化すると、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 iDRAC に実装されます。iDRAC の FlexAddress 機能では、シャーシ内の iDRAC 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、iDRAC の起動時、あるいは CMC の FlexAddress が有効化されたときに、iDRAC 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、iDRAC 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）、iDRAC IP アドレスも変更されます。

iDRAC セッションの表示または終了

現在 iDRAC 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 iDRAC セッションの終了

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

iDRAC 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. iDRAC 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、『iDRAC 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 iDRAC セッションの終了

RACADM を使用して iDRAC 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。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

6

iDRAC 通信のセットアップ

次のいずれかのモードを使用して iDRAC と通信できます。

- iDRAC 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）- ラックサーバまたはタワーサーバの場合のみ
- IPMI シリアルオーバー LAN
- IPMI Over LAN
- リモート RACADM
- ローカル RACADM
- リモートサービス

メモ: ローカル RACADM のインポートまたはエクスポートコマンドが正しく動作していることを確認するには、USB 大容量ストレージホストがオペレーティングシステムで有効になっていることを確認します。USB ストレージホストの有効化についての情報は、お使いのオペレーティングシステムのマニュアルを参照してください。

次の表は、対応プロトコル、対応コマンド、および前提条件の概要を記載しています。

表 14. 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
iDRAC ウェブインタフェース	インターネットプロトコル（https）	該当なし	Web サーバ
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	iDRAC 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
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
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
SMCLP	SSH Telnet	SMCLP	iDRAC 上で SSH または Telnet が有効
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
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
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
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
	Redfish	各種ブラウザのプラグイン、CURL（Windows と Linux）、Python リクエスト、JSON モジュール	プラグイン、CURL、Python モジュールがインストール済み

表 14. 通信モード — サマリ （続き）

通信のモード	対応プロトコル	対応コマンド	前提条件
[1] 詳細に関しては、**dell.com/idracmanuals** にある『*Lifecycle Controller Remote Services ユーザーズガイド*』を参照してください。			

関連概念

DB9 ケーブルを使用したシリアル接続による iDRAC との通信 、p. 109
DB9 ケーブル使用中の RAC シリアルとシリアルコンソール間の切り替え 、p. 112
IPMI SOL を使用した iDRAC との通信 、p. 112
IPMI over LAN を使用した iDRAC との通信 、p. 118
リモート RACADM の有効化または無効化 、p. 119
ローカル RACADM の無効化 、p. 120
管理下システムでの IPMI の有効化 、p. 120
起動中の Linux のシリアルコンソールの設定 、p. 120
サポート対象の SSH 暗号スキーム 、p. 122

トピック：

- DB9 ケーブルを使用したシリアル接続による iDRAC との通信
- DB9 ケーブル使用中の RAC シリアルとシリアルコンソール間の切り替え
- IPMI SOL を使用した iDRAC との通信
- IPMI over LAN を使用した iDRAC 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
- サポート対象の SSH 暗号スキーム

DB9 ケーブルを使用したシリアル接続による iDRAC 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またはタワーサーバ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、**dell.com/support/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. 管理ステーションのシリアルポートから管理下システムの外部シリアルコネクタにヌルモデム DB9 ケーブルを接続します。
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）

   管理下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. iDRAC 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。

関連概念

BIOS のシリアル接続用設定 、p. 110
RAC シリアル接続の有効化 、p. 110
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 、p. 110

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 iDRAC 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［セットアップユーティリティ］を終了します。

RAC シリアル接続の有効化

BIOS でシリアル接続を設定した後、iDRAC 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 iDRAC 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、次のコマンドを実行します。

1. iDRAC 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。
   RAC 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

RACADM を使用して RAC シリアル接続を有効にするには、`iDRAC.Serial` グループのオブジェクトで `set` コマンドを使用します。

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

iDRAC への BIOS の IPMI シリアルルーティングを有効にするには、iDRAC 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 iDRAC 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 iDRAC 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。

関連概念

BIOS のシリアル接続用設定、p. 110
IPMI シリアルターミナルモード用の追加設定、p. 111

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 シリアルを設定するには、次の手順を実行します。

1. iDRAC 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、『iDRAC 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、RAC シリアルインタフェースを無効にしてから、IPMI モードを有効にします。

```
racadm set iDRAC.Serial.Enable 0
racadm set iDRAC.IPMISerial.ConnectionMode <n>
```

n=0 — ターミナルモード

n=1 — 基本モード

RACADM を使用したシリアル接続 IPMI のシリアル設定の有効化

1. 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 set iDRAC.Serial.Enable 0
```

2. コマンドを使用して、IPMI シリアルボーレートを設定します。

```
racadm set iDRAC.IPMISerial.BaudRate <baud_rate>
```

パラメータ	指定可能な値 (bps)
<baud_rate>	9600、19200、57600、115200

3. コマンドを使用して、 IPMI シリアルハードウェアフロー制御を有効にします。

```
racadm set iDRAC.IPMISerial.FlowContro 1
```

4. コマンドを使用して、 IPMI シリアルチャネルの最小権限レベルを設定します。

```
racadm set iDRAC.IPMISerial.ChanPrivLimit <level>
```

パラメータ	権限レベル
<level> = 2	ユーザー
<level> = 3	オペレータ
<level> = 4	システム管理者

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. iDRAC 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、『iDRAC 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、`idrac.ipmiserial` グループのオブジェクトで `set` コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

DB9 ケーブル使用中の RAC シリアルとシリアルコンソール間の切り替え

iDRAC 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時に、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、Esc+Shift、9 を押します。

このキーシーケンスを使用すると、「`iDRAC Login`」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) に移行します。

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場合にシリアルコンソールモードに切り替えるには、Esc+Shift、Q キーを押します。

ターミナルモードのときに接続をシリアルコンソールモードに切り替えるには、Esc+Shift、Q キーを押します。

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、Esc+Shift、9 キーを押します。

IPMI SOL を使用した iDRAC 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 iDRAC 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 iDRAC 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。

関連概念

BIOS のシリアル接続用設定 、p. 113
SOL を使用するための iDRAC の設定 、p. 113
対応プロトコルの有効化 、p. 114

BIOS のシリアル接続用設定

メモ: これは、ラックおよびタワーサーバー上の iDRAC 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 に設定されている場合は、［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。

   メモ: BIOS は、画面シリアルデータを 25 x 80 の形式で送信します。`console com2` コマンドを呼び出すために使用される SSH ウィンドウは 25 x 80 に設定する必要があります。設定後に、リダイレクトされた画面は正常に表示されます。

   メモ: ブートローダまたはオペレーティングシステムが GRUB または Linux などのシリアルリダイレクトを提供する場合、BIOS の ［起動後にリダイレクト］ 設定を無効にする必要があります。これは、シリアルポートにアクセスする複数のコンポーネントの潜在的な競合状態を回避するためです。

SOL を使用するための iDRAC 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、iDRAC の SOL 設定を指定できます。

iDRAC ウェブインタフェースを使用した SOL を使用するための iDRAC 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. iDRAC 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、『iDRAC オンラインヘルプ』を参照してください。

RACADM を使用した SOL を使用するための iDRAC 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. コマンドを使用して IPMI シリアルオーバー LAN を有効にします。

```
racadm set iDRAC.IPMISol.Enable 1
```

2. コマンドを使用して IPMI SOL の最小権限レベルをアップデートします。

```
racadm set iDRAC.IPMISol.MinPrivilege <level>
```

パラメータ	権限レベル
<level> = 2	ユーザー
<level> = 3	オペレータ
<level> = 4	システム管理者

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. コマンドを使用して IPMI SOL のボーレートをアップデートします。

```
racadm set iDRAC.IPMISol.BaudRate <baud_rate>
```

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。

パラメータ	指定可能な値（bps）
<baud_rate>	9600、19200、57600、115200

4. コマンドを使用して SOL を有効にします。

```
racadm set iDRAC.Users.<id>.SolEnable 2
```

パラメータ	説明
<id>	ユーザー固有の ID

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ます。

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 を使用した対応プロトコルの有効化

SSH または Telnet を有効にするには、次のコマンドを使用します。

- Telnet

```
racadm set iDRAC.Telnet.Enable 1
```

- SSH

```
racadm set iDRAC.SSH.Enable 1
```

SSH ポートを変更するには

```
racadm set iDRAC.SSH.Port <port number>
```

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

関連タスク

IPMI プロトコルを使用した SOL 、p. 115
SSH または Telnet プロトコルを使用した SOL 、p. 115

IPMI プロトコルを使用した SOL

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。

iDRAC 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、iDRAC 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、次のコマンドを実行し、iDRAC から SOL を開始します。

   ```
   ipmitool -H <iDRAC-ip-address> -I lanplus -U <login name> -P <login password> sol activate
   ```

   このコマンドで、管理ステーションが管理下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、~ を押して . (ピリオド) を押します。

   メモ: SOL セッションが終了しない場合は、iDRAC 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、iDRAC 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。iDRAC 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。iDRAC 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 または 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、iDRAC 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 iDRAC 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. iDRAC に SOL を設定。
3. iDRAC 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 <--> iDRAC

   シリアルからネットワークへの変換が iDRAC 内で行われるため、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が必要ありません。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。

関連タスク

Windows での PuTTY からの SOL の使用 、p. 116
Linux での OpenSSH または Telnet からの SOL の使用 、p. 116

Windows での PuTTY からの SOL の使用

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。

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。

1. iDRAC に接続するには、次のコマンドを実行します。

```
putty.exe [-ssh | -telnet] <login name>@<iDRAC-ip-address> <port number>
```

   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 プロトコルを使用した管理下システムへの SOL セッションが開始されます。iDRAC 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のオプション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。

関連概念

iDRAC コマンドラインコンソールでの SOL セッションの切断 、p. 118

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 iDRAC に接続します。
   - SSH の場合：ssh *<iDRAC-ip-address>* -l *<login name>*
   - Telnet の場合：telnet *<iDRAC-ip-address>*

   ⓘ **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、iDRAC 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、iDRAC 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、iDRAC 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。

   ⓘ **メモ:** コンソール com1 またはコンソール com2 を使用して SOL を開始できます。サーバーを再起動して接続を確立します。

   `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 set iDRAC.Serial.HistorySize <number>
   ```

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。

関連タスク

Telnet 仮想コンソールの使用 、p. 117
Telnet セッション用の Backspace キーの設定 、p. 118
iDRAC コマンドラインコンソールでの SOL セッションの切断 、p. 118

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. コマンドを使用して iDRAC に接続します

   ```
   telnet <IP address>:<port number>
   ```

パラメータ	説明
<IP address>	iDRAC の IP アドレスです
<port number>	Telnet のポート番号です（新しいポートを使用している場合）

Telnet セッション用の 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 will be sent as delete` というメッセージが表示されます。

iDRAC 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、iDRAC 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>、<T> キーを押します。
  SOL セッションが閉じます。
- Linux で Telnet からの SOL セッションを終了するには、<Ctrl> +<]> を長押しします。
  Telnet のプロンプトが表示されます。`quit` と入力して、Telnet を終了します。

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 iDRAC との通信

iDRAC 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。IPMI over LAN 設定を行わない場合、外部システムは IPMI コマンドを介して iDRAC サーバーと通信することができません。

メモ: iDRAC v2.30.30.30 以降から、IPMI は Linux ベースのオペレーティングシステムに対して IPv6 アドレスプロトコルもサポートします。

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. iDRAC 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、『iDRAC 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。

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。
IPMI Over LAN が設定されます。

RACADM を使用した IPMI over LAN の設定

1. IPMI over LAN を有効にします。

```
racadm set iDRAC.IPMILan.Enable 1
```

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. IPMI チャネル権限をアップデートします。

```
racadm set iDRAC.IPMILan.PrivLimit <level>
```

パラメータ	権限レベル
<level> = 2	ユーザー
<level> = 3	オペレータ
<level> = 4	システム管理者

3. 必要に応じて、IPMI LAN チャネルの暗号化キーを設定します。

```
racadm set iDRAC.IPMILan.EncryptionKey <key>
```

パラメータ	説明
<key>	有効な 16 進形式の 20 文字の暗号化キー

メモ: iDRAC 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

iDRAC 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。

メモ: リモート RACADM はデフォルトで有効に設定されています。

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

1. iDRAC 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。
2. [リモート RACADM] で希望のオプションを選択し、[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

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。

- リモート RACADM を無効にする場合：

```
racadm set iDRAC.Racadm.Enable 0
```

- リモート RACADM を有効にする場合：

```
racadm set iDRAC.Racadm.Enable 1
```

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、「ホストシステムでの iDRAC 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、[dell.com/support/manuals] で『Dell Open Manage Server Administrator ユーザーズガイド』を参照してください。

メモ: iDRAC v2.30.30.30 以降から、IPMI は Linux ベースのオペレーティングシステムに対して IPv6 アドレスプロトコルをサポートします。

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/sdal
# initrd /boot/initrd-version.img
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

serial --unit=1 --speed=57600
terminal --timeout=10 serial
```

```
title Red Hat Linux Advanced Server (2.4.9-e.3smp) root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0
console=ttyS1,115200n8r
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。

メモ: ブートローダまたはオペレーティングシステムが GRUB または Linux などのシリアルリダイレクトを提供する場合、BIOS の［起動後にリダイレクト］設定を無効にする必要があります。これは、シリアルポートにアクセスする複数のコンポーネントの潜在的な競合状態を回避するためです。

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
```

サポート対象の SSH 暗号スキーム

SSH プロトコルを使用して iDRAC 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 15. SSH 暗号化スキーム

スキームの種類	アルゴリズム
非対称暗号化	
公開キー	ssh-rsa ecdsa-sha2-nistp256
対称暗号	
キー交換	curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha1

表 15. SSH 暗号化スキーム （続き）

スキームの種類	アルゴリズム
暗号化	chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com
MAC	hmac-sha1 hmac-ripemd160 umac-64@openssh.com
Compression（圧縮）	なし

メモ: OpenSSH 7.0 以降を有効にすると、DSA 公開キーのサポートが無効になります。iDRAC のセキュリティ強化のため、デルは DSA 公開キーのサポートを有効にしないことをお勧めします。

SSH の公開キー認証の使用

iDRAC 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、iDRAC へのログインにユーザー名を入力する必要があります。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。

メモ: OpenSSH 7.0 以降を有効にすると、DSA 公開キーのサポートが無効になります。iDRAC のセキュリティ強化のため、デルは DSA 公開キーのサポートを有効にしないことをお勧めします。

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 iDRAC 間での信頼関係を確立するため、公開キーは iDRAC 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 iDRAC 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選択し、キーの種類に対する RSA を選択します。
2. キーのビット数を入力します。ビット数は 2048 ~ 4096 ビットにする必要があります。
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 2048 -C testing` と入力します。

ここで、

- `-t` は *rsa* です。
- `-b` は 2048 ~ 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: iDRAC 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。iDRAC 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. iDRAC 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、『iDRAC 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 to 16> -k <1 to 4> -f <filename>`
- Telnet または SSH を使用するリモート RACADM の場合：`racadm sshpkauth -i <2 to 16> -k <1 to 4> -t <key-text>`

たとえば、ファイルを使用して最初のキースペースの iDRAC 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

iDRAC 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 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（*役割ベースの権限*）を持つユーザーアカウントをセットアップし、iDRAC 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、iDRAC 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 iDRAC 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。

iDRAC は、関連付けられた一連の権限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。

関連概念

ローカルユーザーの設定 、p. 127
Active Directory ユーザーの設定 、p. 128
汎用 LDAP ユーザーの設定 、p. 145

トピック：

ユーザー名およびパスワードで推奨される文字

このセクションでは、ユーザー名およびパスワードの作成および使用時に推奨される文字についての詳細を提供します。

次の文字はユーザー名およびパスワードの作成時に使用します：

表 16. ユーザー名に推奨される文字

文字	長さ
0 ~ 9 A ~ Z a ~ z - ! # $ % & ( ) * / ; ? @ [\ ] ^ _ ` { | } ~ + < = >	1 ~ 16

表 17. パスワードに推奨される文字

文字	長さ
0 ~ 9 A ~ Z a ~ z ' - ! " # $ % & ( ) * , ./ : ; ? @ [\ ] ^ _ ` { | } ~ + < = >	1 ~ 20

メモ: これら以外の文字を含むユーザー名およびパスワードを作成することができる場合があります。ただし、すべてのインターフェイスとの互換性を確保するため、デルでは、ここにリストされている文字のみを使用することを推奨しています。

メモ: ネットワーク共有のユーザー名とパスワードで使用できる文字は、ネットワーク共有のタイプによって異なります。iDRAC では、ネットワーク共有の資格情報については、各共有タイプで有効と定義される文字をサポートしていますが、<、>、および , (カンマ) は除きます。

メモ: セキュリティを向上させるため、小文字のアルファベット、大文字のアルファベット、数字、および特殊文字が含まれる 8 文字以上の複雑なパスワードを使用することが推奨されます。また、可能な限り、パスワードを定期的に変更することも推奨されます。

ローカルユーザーの設定

iDRAC では、特定のアクセス許可を持つローカルユーザーを最大 16 人設定できます。iDRAC 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、iDRAC 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。ユーザーごとに SNMPv3 認証を有効または無効にすることもできます。

iDRAC 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 iDRAC 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: iDRAC 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. iDRAC 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 番号をクリックします。

   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 を有効化して、ユーザーのユーザー名、パスワード、アクセス権限を指定します。ユーザーについて、SNMPv3 認証を有効にすることもできます。オプションの詳細については、『iDRAC 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 iDRAC ユーザーを設定できます。

同じ設定で複数の iDRAC ユーザーを設定するには、次の手順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バッチファイルを実行します。
- iDRAC 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 set` コマンドを実行します。

新規の iDRAC 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。`racadm racresetcfg` コマンドは iDRAC をデフォルト値にリセットします。

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 iDRAC 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。

ユーザーが存在するかどうかを確認するには、各インデックス (1～16) に対して次のコマンドを 1 回入力します。

```
racadm get iDRAC.Users.<index>.UserName
```

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。キーフィールドは、`iDRAC.Users.UserName=` です。ユーザー名が = の後に表示されている場合、そのインデックス番号は取得されています。

メモ: `racadm get -f` *<myfile.cfg>* を使用して、iDRAC 設定パラメータのすべてが含まれる **myfile.cfg** ファイルを表示、または編集することもできます。

ユーザーに対して SNMP v3 認証を有効にするには、[SNMPv3AuthenticationType]、[SNMPv3Enable]、[SNMPv3PrivacyType] オブジェクトを使用します。詳細に関しては、**dell.com/idracmanuals** にある『RACADM コマンドラインインタフェースガイド』を参照してください。

設定 XML ファイルを使用している場合は、[AuthenticationProtocol]、[ProtocolEnable]、 および [PrivacyProtocol] 属性を使用して SNMPv3 認証を有効にします。

RACADM を使用した iDRAC ユーザーの追加

1. インデックスおよびユーザー名を設定します。

```
racadm set idrac.users.<index>.username <user_name>
```

パラメータ	説明
<index>	ユーザー固有のインデックス
<user_name>	ユーザー名

2. パスワードを設定します。

```
racadm set idrac.users.<index>.password <password>
```

3. ユーザー権限を設定します。

   詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

4. ユーザーを有効にします。

```
racadm set.idrac.users.<index>.enable 1
```

確認するには、次のコマンドを使用します。

```
racadm get idrac.users.<index>
```

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

許可を持つ iDRAC 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. 使用可能なユーザーインデックスを探します。

```
racadm get iDRAC.Users <index>
```

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 set iDRAC.Users.<index>.Privilege <user privilege bit mask value>
```

メモ: デフォルトの権限値は 0 です。これはユーザーに有効な権限がないことを示します。特定のユーザー権限に対する有効なビットマスク値のリストについては、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

Active Directory ユーザーの設定

会社で Microsoft Active Directory ソフトウェアを使用している場合、iDRAC 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 iDRAC 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 iDRAC 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。

iDRAC 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。

iDRAC の役割および権限の名前は、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 18. iDRAC の役割

現在の世代	以前の世代	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
オペレータ	パワーユーザー	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
読み取り専用	ゲストユーザー	ログイン
なし	なし	なし

表 19. iDRAC ユーザー権限

現在の世代	以前の世代	説明
ログイン	iDRAC へのログイン	ユーザーによる iDRAC へのログインを可能にします。
設定	iDRAC の設定	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	ログのクリア	ユーザーによるシステムイベントログ（SEL）のクリアを可能にします。
システム制御	サーバー制御コマンドの実行	ホストシステムのパワーサイクルを許可します。
仮想コンソールへのアクセス	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）	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。
システム操作	アラートのテスト	ユーザー開始およびユーザー生成のイベントを許可します。情報は非同期通知として送信され、ログされます。
デバッグ	診断コマンドの実行	ユーザーによる診断コマンドの実行を可能にします。

関連概念

iDRAC の Active Directory 認証を使用するための前提条件 、p. 129
サポートされている Active Directory 認証メカニズム 、p. 131

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

iDRAC 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。iDRAC 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、iDRAC 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。

関連タスク

ドメインコントローラでの SSL の有効化 、p. 130

ドメインコントローラでの SSL の有効化

iDRAC 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 iDRAC へのアップロードも行われます。iDRAC 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 iDRAC にエクスポートします。
3. iDRAC ファームウェア SSL 証明書をインポートします。

関連タスク

各ドメインコントローラの SSL 証明書のインストール 、p. 130
ドメインコントローラのルート CA 証明書の iDRAC へのエクスポート 、p. 130
iDRAC ファームウェアの SSL 証明書のインポート 、p. 131

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 iDRAC 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 iDRAC 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. ［スタート ］>［ ファイル名を指定して実行 ］ をクリックします。
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 iDRAC にアップロードします。

iDRAC ファームウェアの SSL 証明書のインポート

iDRAC SSL 証明書は、iDRAC 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 iDRAC 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、iDRAC 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: iDRAC 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済み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済み証明書のリストに iDRAC ファームウェア SSL 証明書をインポートするには、次の手順を実行します。

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

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

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] > [信頼済みルート認証局] 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 [信頼済みルート認証局] に iDRAC 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 [信頼済みルート認証局] 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。iDRAC 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済み証明書リストにインポートされます。

サポートされている Active Directory 認証メカニズム

Active Directory を使用して、次の 2 つの方法を使用する iDRAC 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 iDRAC 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。

関連概念

標準スキーマ Active Directory の概要 、p. 131
拡張スキーマ Active Directory の概要 、p. 134

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 iDRAC の両方での設定が必要となります。

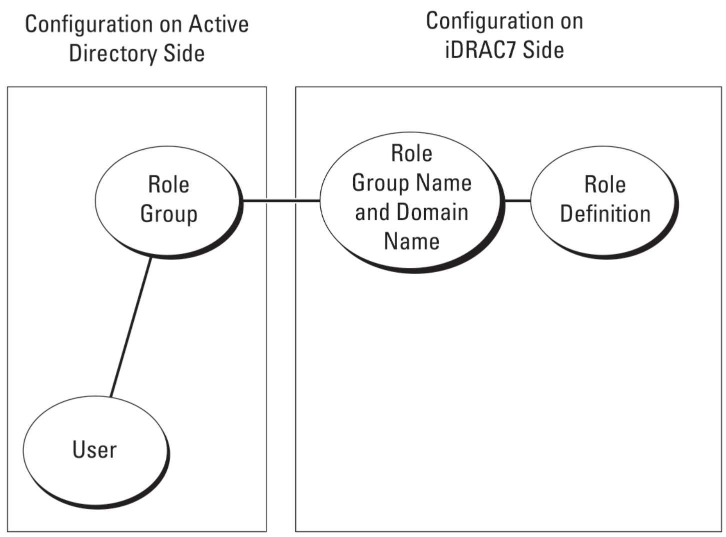


図 1. Active Directory 標準スキーマでの iDRAC の設定

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。iDRAC 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 iDRAC へのアクセスを与えるには、その特定の iDRAC 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 iDRAC で定義されます。各 iDRAC 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 20. デフォルトの役割グループ権限

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 iDRAC 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 iDRAC 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 ログインアクセスのために iDRAC 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。iDRAC にアクセスするために､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. iDRAC ウェブインタフェースまたは RACADM を使用して、iDRAC 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。

関連タスク

iDRAC 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 、p. 133
RACADM を使用した標準スキーマでの Active Directory の設定 、p. 133

iDRAC 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: 各種フィールドについては､『iDRAC オンラインヘルプ』を参照してください。

1. iDRAC ウェブインタフェースで､[概要] > [iDRAC 設定] > [ユーザー認証] > [ローカルサービス] と移動します。
   [ディレクトリサービス] ページが表示されます。
2. [Microsoft Active Directory] オプションを選択し､[適用] をクリックします。
   [Active Directory の設定と管理] ページが表示されます。
3. [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。
4. 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。
5. [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。

6. 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、iDRAC ログイン時に iDRAC 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。

7. [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。
8. [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。
9. 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。
10. [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。
11. 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。

12. [終了] をクリックします。標準スキーマ用の Active Directory 設定が行われます。

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

1. 次のコマンドを使用します。

```
racadm set iDRAC.ActiveDirectory.Enable 1
racadm set iDRAC.ActiveDirectory.Schema 2
racadm set iDRAC.ADGroup.Name <common name of the role group>
racadm set iDRAC.ADGroup.Domain <fully qualified domain name>
racadm set iDRAC.ADGroup.Privilege <Bit-mask value for specific RoleGroup permissions>
racadm set iDRAC.ActiveDirectory.DomainController1 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController2 <fully qualified domain name or IP
```

```
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController3 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog1 <fully qualified domain name or IP address
of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog2 <fully qualified domain name or IP address
of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog3 <fully qualified domain name or IP address
of the domain controller>
```

- ドメインの完全修飾ドメイン名（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。
- 特定の役割グループ許可用のビットマスク値については、「デフォルトの役割グループ権限」を参照してください。
- 3 つのドメインコントローラアドレスのうち少なくとも 1 つを入力する必要があります。iDRAC 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。
- 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。
- 証明書の検証が有効な場合、このフィールドで指定する FQDN または IP アドレスが、ドメインコントローラの証明書のサブジェクトまたはサブジェクト代替名フィールドに一致する必要があります。
- SSL ハンドシェイク中に証明書の検証を無効にするには、次のコマンドを使用します。

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 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（オプション）中に証明書の検証を実施するには、次のコマンドを使用します。

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 1
  ```

  この場合、次の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 root CA certificate>
  ```

  メモ: 証明書の検証が有効な場合は、ドメインコントローラサーバ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。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 certificate>
  ```

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

   ```
   racadm set iDRAC.IPv4.DNSFromDHCP 1
   ```

3. iDRAC 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 set iDRAC.IPv4.DNSFromDHCP 0
   racadm set iDRAC.IPv4.DNSFromDHCP.DNS1 <primary DNS IP address>
   racadm set iDRAC.IPv4.DNSFromDHCP.DNS2 <secondary DNS IP address>
   ```

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、次のコマンドを使用します。

   ```
   racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address of the
   domain controller>
   ```

   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。

拡張スキーマのためのベストプラクティス

拡張スキーマはデル関連オブジェクトを使用して iDRAC と許可を結びつけます。これにより、与えられたすべての許可に基づいて iDRAC を使用できます。デル関連オブジェクトのデフォルトのアクセスコントロールリスト（ACL）で自己管理者およびドメイン管理者は iDRAC オブジェクトの許可と範囲を管理できます。

デフォルトでは、デル関連オブジェクトは親の Active Directory オブジェクトからすべての許可を継承するわけではありません。デル関連オブジェクトの継承を有効にしている場合は、その関連オブジェクトの継承された許可が選択されたユーザーおよびグループに付与されます。これは意図しない権限が iDRAC に与えられる原因となる場合があります。

拡張スキーマを安全に使用するために、デルは、拡張スキーマの実装においてデル関連オブジェクトの継承を有効にしないことをお勧めします。

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 は、Active Directory を使用したリモート管理認証および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`

iDRAC 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 iDRAC 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、iDRAC 権限、および iDRAC 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 iDRAC 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 iDRAC 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 iDRAC 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 iDRAC 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 iDRAC 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 iDRAC 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。

iDRAC 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 iDRAC ファームウェアへのリンクです。iDRAC 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 iDRAC 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 iDRAC 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。

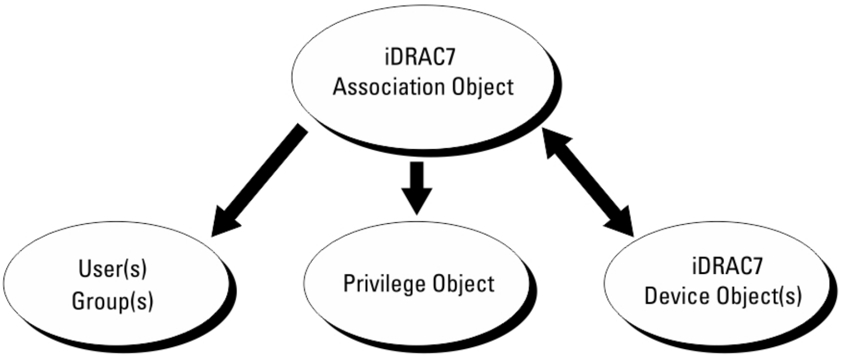


図 2. Active Directory オブジェクトの標準的なセットアップ

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、iDRAC 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 iDRAC ごとに、1 つの iDRAC 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、iDRAC 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、iDRAC 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 iDRAC 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 iDRAC 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。

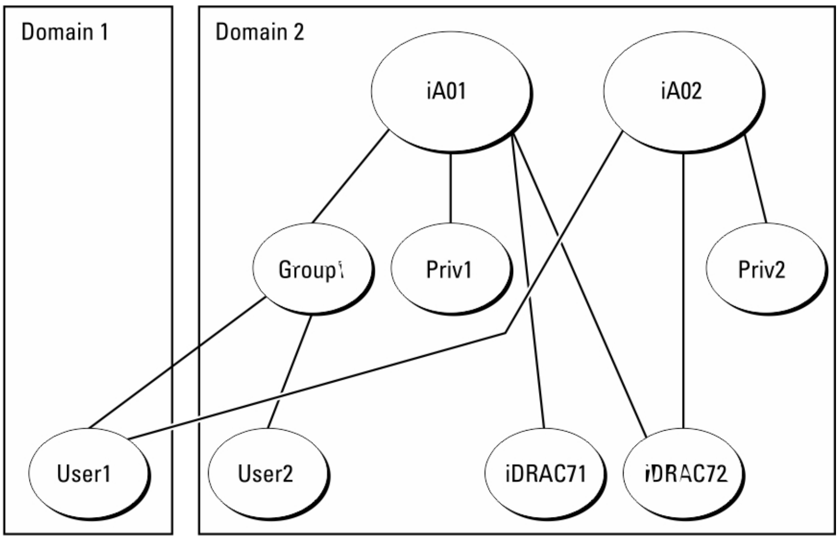


図 3. ユーザーのための権限の蓄積

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 iDRAC2 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 iDRAC2 に対する Priv1 権限と Priv2 権限の両方を所有しており、iDRAC1 に対しては Priv1 権限のみを所有しています。ユーザー 2 は iDRAC1 と iDRAC2 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し、グループのメンバーになることができ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 iDRAC 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 iDRAC ユーザーと権限を追加します。
4. iDRAC ウェブインタフェースまたは RACADM を使用して、iDRAC Active Directory のプロパティを設定します。

関連概念

拡張スキーマ Active Directory の概要 、p. 134
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 、p. 141
Active Directory への iDRAC ユーザーと権限の追加 、p. 141

関連タスク

iDRAC ウェブインタフェースを使用した拡張スキーマでの Active Directory の設定 、p. 143
RACADM を使用した拡張スキーマでの Active Directory の設定 、p. 143

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 およびマニュアル* DVD』の次のディレクトリに入っています。

- DVDdrive :`\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files`
- <DVDdrive>: `\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. ［次へ］をクリックして、Dell Schema Extender を実行します。
5. ［終了］をクリックします。

   スキーマが拡張されました。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 21. 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 22. DelliDRACdevice クラス

OID	1.2.840.113556.1.8000.1280.1.7.1.1
説明	Dell iDRAC デバイスを表します。Active Directory では、iDRAC は delliDRACDevice として設定する必要があります。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	構造型クラス
SuperClasses	dellProduct
属性	dellSchemaVersion dellRacType

表 23. 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	構造型クラス
SuperClasses	グループ
属性	dellProductMembers dellPrivilegeMember

表 24. dellRAC4Privileges クラス

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

表 25. dellPrivileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.4
説明	デルの権限（認証権）のコンテナクラスとして使用されます。
クラスタイプ	構造型クラス
SuperClasses	ユーザー
属性	dellRAC4Privileges

表 26. 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	構造型クラス
SuperClasses	コンピュータ
属性	dellAssociationMembers

表 27. 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、	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

表 27. Active Directory スキーマに追加された属性のリスト （続き）

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
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		
[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
[dellsLogClearAdmin] 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
[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

表 27. Active Directory スキーマに追加された属性のリスト （続き）

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
[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、iDRAC デバイス、ユーザーとユーザーグループ、iDRAC 関連付け、iDRAC 権限などを管理できるように、Active Directory ユーザーとコンピュータスナップインも拡張する必要があります。

『*Dell Systems Management 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、Microsoft のマニュアルを参照してください。

Active Directory への iDRAC 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、iDRAC 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

関連概念

関連オブジェクトへのオブジェクトの追加 、p. 142

関連タスク

iDRAC デバイスオブジェクトの作成 、p. 141
権限オブジェクトの作成 、p. 142
関連オブジェクトの作成 、p. 142

iDRAC デバイスオブジェクトの作成

iDRAC 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、iDRAC 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 iDRAC 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. ［コンソールのルート］（MMC）ウィンドウでコンテナを右クリックします。
2. ［新規］>［Dell 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: iDRAC 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. ［コンソールのルート］（MMC）ウィンドウでコンテナを右クリックします。
2. ［新規］>［Dell リモート管理オブジェクトの詳細設定］を選択します。
   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。

関連タスク

関連オブジェクトのユーザーアクセス権限の付与、p. 142

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、iDRAC デバイスまたは iDRAC 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 iDRAC デバイスのグループを追加できます。

関連タスク

ユーザーまたはユーザーグループの追加、p. 142
権限の追加、p. 143
iDRAC デバイスまたは iDRAC デバイスグループの追加、p. 143

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、iDRAC 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、iDRAC 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。

iDRAC デバイスまたは iDRAC デバイスグループの追加

iDRAC デバイスまたは iDRAC 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. iDRAC デバイスまたは iDRAC 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. [製品] 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使用可能なネットワークに接続している iDRAC 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。

iDRAC ウェブインタフェースを使用した拡張スキーマでの 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、『iDRAC オンラインヘルプ』を参照してください。

1. iDRAC 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、ログイン処理中に AD からの応答を iDRAC 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。
   - ユーザーと iDRAC オブジェクトが異なるドメイン内に存在する場合は、[ログインからのユーザードメイン] オプションを選択しないでください。代わりに、[ドメインの指定] オプションを選択し、iDRAC オブジェクトが利用可能なドメイン名を入力します。

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. [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 iDRAC 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での Active Directory の設定

RACADM 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。

1. 次のコマンドを使用します。

```
racadm set iDRAC.ActiveDirectory.Enable 1
racadm set iDRAC.ActiveDirectory.Schema 2
racadm set iDRAC.ActiveDirectory.RacName <RAC common name>
racadm set iDRAC.ActiveDirectory.RacDomain <fully qualified rac domain name>
racadm set iDRAC.ActiveDirectory.DomainController1 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController2 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController3 <fully qualified domain name or IP
address of the domain controller>
```

   - ドメインの完全修飾ドメイン名（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。
   - 3 つのアドレスのうち少なくとも 1 つを入力する必要があります。iDRAC 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 iDRAC 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 ハンドシェイク中に証明書の検証を無効にするには、次のコマンドを使用します。

     ```
     racadm set iDRAC.ActiveDirectory.CertValidationEnable 0
     ```

     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 set iDRAC.ActiveDirectory.CertValidationEnable 1
     ```

     この場合、次の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 root CA certificate>
     ```

     メモ: 証明書の検証が有効な場合は、ドメインコントローラサーバのアドレスおよび 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 certificate>
     ```

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

```
racadm set iDRAC.IPv4.DNSFromDHCP 1
```

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

```
racadm set iDRAC.IPv4.DNSFromDHCP 0
racadm set iDRAC.IPv4.DNSFromDHCP.DNS1 <primary DNS IP address>
racadm set iDRAC.IPv4.DNSFromDHCP.DNS2 <secondary DNS IP address>
```

4. iDRAC 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、次のコマンドを使用します。

```
racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address of the
domain controller>
```

   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。

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。

iDRAC 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. iDRAC 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. [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]) を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、iDRAC 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、iDRAC 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、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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

iDRAC 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。

iDRAC LDAP の実装を汎用にするために、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、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、iDRAC で設定できます。

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。

関連タスク

iDRAC 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 、p. 145
RACADM を使用した汎用 LDAP ディレクトリサービスの設定 、p. 146

iDRAC 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、『iDRAC オンラインヘルプ』を参照してください。

1. iDRAC 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、`iDRAC.LDAP` および `iDRAC.LDAPRole` グループのオブジェクトを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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。

iDRAC ウェブインタ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. iDRAC 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. [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、iDRAC 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、iDRAC 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、iDRAC 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、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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 iDRAC 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 iDRAC 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。

iDRAC 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。

関連タスク

Active Directory ユーザーのための iDRAC SSO ログインの設定 、p. 149
ローカルユーザーのための iDRAC スマートカードログインの設定 、p. 149
Active Directory ユーザーのための iDRAC スマートカードログインの設定 、p. 151

トピック：

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

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。

- iDRAC の時刻を Active Directory ドメインコントローラの時刻と同期させます。これを行わないと、iDRAC での Kerberos 認証に失敗します。タイムゾーンおよび NTP 機能を使用して時刻を同期できます。これを行うには、「タイムゾーンと NTP の設定」を参照してください。
- iDRAC 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（Kerberos 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、iDRAC 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。
- ブラウザを SSO ログインをサポートするように設定します。詳細については、対応ウェブブラウザの設定 、p. 57 を参照してください。

  メモ: Google Chrome と Safari は SSO ログインのための Active Directory をサポートしません。

関連タスク

Active Directory ルートドメイン内のコンピュータとしての iDRAC の登録 、p. 148
Kerberos Keytab ファイルの生成 、p. 148
Active Directory オブジェクトの作成と権限の付与 、p. 148

Active Directory ルートドメイン内のコンピュータとしての iDRAC の登録

Active Directory ルートドメインに iDRAC 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、『iDRAC 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、iDRAC 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。iDRAC 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 iDRAC 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 iDRAC 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 AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass
   [password] -out c:\krbkeytab
   ```

   暗号化タイプは、AES256-SHA1 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、［このアカウントに AES 暗号化タイプを使用する］プロパティが有効になっている必要があります。

   メモ: iDRACname 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/iDRACname.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 iDRAC 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。

関連概念

Active Directory への iDRAC ユーザーと権限の追加 、p. 141

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

iDRAC 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 iDRAC を設定できます。

関連概念

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 、p. 147

関連タスク

iDRAC 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 、p. 133
RACADM を使用した標準スキーマでの Active Directory の設定 、p. 133
iDRAC ウェブインタフェースを使用した拡張スキーマでの Active Directory の設定 、p. 143
RACADM を使用した拡張スキーマでの Active Directory の設定 、p. 143

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 iDRAC SSO ログインの設定

Active Directory SSO ログイン用に iDRAC 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、『iDRAC オンラインヘルプ』を参照してください。

1. iDRAC DNS 名が iDRAC 完全修飾ドメイン名に一致するかどうかを確認します。確認するには、iDRAC 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 ユーザーのための iDRAC SSO ログインの設定

SSO を有効にするには、Active Directory の設定手順を完了し、次のコマンドを実行します。

```
racadm set iDRAC.ActiveDirectory.SSOEnable 1
```

ローカルユーザーのための iDRAC 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 iDRAC 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済み CA 証明書を iDRAC 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。

関連概念

証明書の取得 、p. 93
スマートカードユーザー証明書のアップロード 、p. 150
スマートカードログインの有効化または無効化 、p. 151

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。SHA-2 証明書もサポートされています。

関連概念

証明書の取得 、p. 93

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. iDRAC 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

スマートカードの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、**dell.com/idracmanuals** にある『*iDRACRACADM コマンドラインインタフェース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済み 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。

関連概念

証明書の取得 、p. 93

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済み 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済み 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. iDRAC 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、[信頼済み 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。
   [信頼済み CA 証明書のアップロード] ページが表示されます。
4. 信頼済み 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済み CA 証明書のアップロード

スマートカードログインのために信頼済み 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、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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 iDRAC スマートカードログインの設定

Active Directory ユーザー用の iDRAC 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 iDRAC に設定するには、次の手順を実行します。

1. iDRAC 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。
   - 信頼済み 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、『iDRAC オンラインヘルプ』を参照してください。

関連概念

スマートカードログインの有効化または無効化 、p. 151
証明書の取得 、p. 93
Kerberos Keytab ファイルの生成 、p. 148
iDRAC 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 、p. 133
RACADM を使用した標準スキーマでの Active Directory の設定 、p. 133
iDRAC ウェブインタフェースを使用した拡張スキーマでの Active Directory の設定 、p. 143
RACADM を使用した拡張スキーマでの Active Directory の設定 、p. 143

スマートカードログインの有効化または無効化

iDRAC 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。

- iDRAC 許可を設定していること。
- 適切な証明書での iDRAC 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。

関連概念

証明書の取得 、p. 93
Active Directory ユーザーのための iDRAC スマートカードログインの設定 、p. 151
ローカルユーザーのための iDRAC スマートカードログインの設定 、p. 149

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. iDRAC 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、『iDRAC オンラインヘルプ』を参照してください。

3. 設定を適用するには、[適用] をクリックします。
   今後の iDRAC 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、`iDRAC.SmartCard` グループのオブジェクトで `set` コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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 iDRAC 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。イベントは、システムコンポーネントのステータスが事前定義された条件を上回るときに発生します。イベントがイベントフィルタに一致し、このフィルタがアラート（電子メール、SNMP トラップ、IPMI アラート、リモートシステムログ、Redfish イベントまたは WS イベント）を生成するように設定されている場合、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、パワーサイクル、電源オフなど）を実行するようにも設定されている場合は、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 iDRAC 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、SNMP トラップ、リモートシステムログ、オペレーティングシステムログ、Redfish イベント、および / または WS イベントを設定します。
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。
   - 電子メールアラート、IPMI アラート、SNMP トラップ、リモートシステムログ、Refish イベント、オペレーティングシステムログ、または WS イベントを設定済みの宛先に送信する。
   - 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。

関連概念

アラートの有効化または無効化 、p. 153
アラートのフィルタ 、p. 154
イベントアラートの設定 、p. 155
アラート反復イベントの設定 、p. 156
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 、p. 157
リモートシステムロギングの設定 、p. 168
WS Eventing の設定 、p. 160
Redfish Eventing の設定 、p. 160
アラートメッセージ ID 、p. 161

トピック：

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。

関連概念

アラートのフィルタ 、p. 154

[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 、p. 157]

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. iDRAC 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

次のコマンドを使用します。

```
racadm set iDRAC.IPMILan.AlertEnable <n>
```

n=0 — 無効

n=1 — 有効

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。

関連概念

[アラートの有効化または無効化 、p. 153]
[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 、p. 157]

iDRAC 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. iDRAC 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。
   - システム正常性
   - 保管時
   - 設定
   - 監査
   - アップデート
   - 作業メモ

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。詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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

E- メールアラート、IPMI アラート、SNMP トラップ、リモートシステムログ、オペレーティングシステムログ、および WS イベントなどのイベントアラートを、設定された宛先に送信されるように設定できます。

関連概念

アラートの有効化または無効化 、p. 153
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 、p. 157
アラートのフィルタ 、p. 154
リモートシステムロギングの設定 、p. 168
WS Eventing の設定 、p. 160
Redfish Eventing の設定 、p. 160

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、SNMP トラップ設定、および / またはリモートシステムログが設定されていることを確認します。
2. [概要] > [サーバー] > [アラート] と移動します。
   [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
   - リモートシステムログ
   - OS ログ
   - WS イベンティング
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。
6. オプションで、テストイベントを送信できます。[イベントをテストするためのメッセージ ID] フィールドで、アラートが生成されるかどうかをテストするためのメッセージ ID を入力して、[テスト] をクリックします。メッセージ ID のリストについては、**dell.com/support/manuals** にある『イベントメッセージガイド』を参照してください。

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、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

アラート反復イベントの設定

システムが吸気口温度のしきい値制限を超過して稼動し続けた場合に、iDRAC が追加のイベントを特定の間隔で生成するよう設定することができます。デフォルトでの間隔は 30 日です。有効な値は、0 ~ 365 日です。値が 0 になっているときは、イベントの反復が無効であることを意味します。

メモ: アラート反復の値を設定する前に iDRAC 特権を設定する必要があります。

iDRAC ウェブインタフェースを使用したアラート反復イベントの設定

アラート反復の値を設定するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、[概要] > [サーバー] > [アラート] > [アラート反復] の順に移動します。
   [アラート反復ページ] が表示されます。
2. [反復] 列で、必要なカテゴリ、アラート、重大性に関するアラート頻度の値を入力します。
   詳細については、『iDRAC 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。
   アラート反復の設定が保存されます。

RACADM を使用したアラート反復イベントの設定

RACADM を使用してアラート反復イベントを設定するには、**eventfilters** コマンドを使用します。詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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。

関連概念

アラートのフィルタ 、p. 154
アラートの有効化または無効化 、p. 153

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. iDRAC 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
   - 処置の必要なし
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、`eventfilters` コマンドを使用します。詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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、iDRAC 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管理ステーションにとって、発生し得るすべての状態について各 iDRAC 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できます。また、SNMP トラップの送信先となる SNMP v3 ユーザーを指定できます。

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。

関連概念

IP アラート送信先の設定、p. 157
電子メールアラートの設定、p. 159

IP アラート送信先の設定

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。

SNMP を使用してサーバを監視するために必要な iDRAC MIB に関する詳細については、**dell.com/support/manuals** にある『*SNMP リファレンスガイド*』を参照してください。

ウェブインタフェースを使用した 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アラート送信先設定を行うには、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、トラップを受け取るために、アラート宛先（IPv4 アドレス、IPv6 アドレス、または完全修飾ドメイン名（FQDN））を有効化します。

   最大 8 つの宛先アドレスを指定できます。オプションの詳細については、『iDRAC オンラインヘルプ』を参照してください。
3. SNMP トラップの送信先となる SNMP v3 ユーザーを選択します。
4. iDRAC SNMP コミュニティ文字列（SNMPv1 と v2 にのみ適用可能）と SNMP アラートポート番号を入力します。

   オプションの詳細については、『iDRAC 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、iDRAC 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 iDRAC 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。
5. 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。
6. ［適用］をクリックします。

   アラート送信先が設定されます。
7. ［SNMP トラップフォーマット］セクションで、トラップ宛先でトラップの送信に使用されるプロトコルバージョンである［SNMP v1］、［SNMP v2］、または［SNMP v3］を選択して、［適用］をクリックします。

   メモ:［SNMP トラップフォーマット］オプションは、SNMP トラップにのみ適用され、IPMI トラップには適用されません。IPMI トラップは常に SNMP v1 フォーマットで送信され、設定された［SNMP トラップフォーマット］オプションに基づくものではありません。

   SNMP トラップフォーマットが設定されます。

RACADM を使用した IP アラート送信先の設定

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。

```
racadm set idrac.SNMP.Alert.<index>.Enable <n>
```

パラメータ	説明
<index>	送信先のインデックスです。 指定できる値は 1～8 です。
<n>=0 **<n>**=1	トラップの無効化 トラップの有効化

2. トラップの送信先アドレスを設定するには、次の手順を実行します。

```
racadm set idrac.SNMP.Alert.<index>.DestAddr <Address>
```

パラメータ	説明
<index>	送信先のインデックスです。 指定できる値は 1～8 です。
<Address>	有効な IPv4、IPv6、または FQDN 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 set idrac.ipmilan.communityname <community_name>
```

パラメータ	説明
<community_name>	SNMP コミュニティ名です。

4. SNMP の送信先を設定するには、次の手順を実行します。
   - SNMPv3 の SNMP トラップの送信先を設定します。

     ```
     racadm set idrac.SNMP.Alert.<index>.DestAddr <IP address>
     ```
   - トラップの送信先の SNMPv3 ユーザーを設定します。

     ```
     racadm set idrac.SNMP.Alert.<index>.SNMPv3Username <user_name>
     ```
   - ユーザーの SNMPv3 を有効にします。

     ```
     racadm set idrac.users.<index>.SNMPv3Enable Enabled
     ```
5. 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 <index>
```

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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してアラート送信先（IPv4、IPv6、または FQDN）を設定できます。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 ［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、IPv6、または FQDN 宛先アドレスを入力します。最大 8 個の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］ の順にクリックし、［はい］ をクリックします。

アラート送信先が設定されます。

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、iDRAC 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 iDRAC 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。

関連概念

SMTP 電子メールサーバーアドレス設定、p. 160

ウェブインタフェースを使用した電子メールアラートの設定

ウェブインタフェースを使用して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. [概要] > [サーバー] > [アラート] > [SNMP と電子メール設定] 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、『iDRAC 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、設定された電子メールアラート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の設定

1. 電子メールアラートを有効にする：

```
racadm set iDRAC.EmailAlert.Enable.[index] [n]
```

パラメータ	説明
index	電子メールの送信先のインデックスです。 指定できる値は 1～4 です。
n=0 **n**=1	電子メールアラートを無効にします。 電子メールアラートを有効にします。

2. 電子メール設定を行う：

```
racadm set iDRAC.EmailAlert.Address.[index] [email-address]
```

パラメータ	説明
index	電子メールの送信先のインデックスです。 指定できる値は 1～4 です。
email-address	プラットフォームイベントアラートを受信す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 set iDRAC.EmailAlert.CustomMsg.[index] [custom-message]
```

パラメータ	説明
index	電子メールの送信先のインデックスです。 指定できる値は 1～4 です。
custom-message	カスタムメッセージ

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 [index]
```

パラメータ	説明
`index`	テストする電子メールの送信先のインデックスです。 指定できる値は 1～4 です。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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

電子メールアラートを指定の送信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。

iDRAC 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. iDRAC 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. 設定で使用する SMTP サーバーの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。
3. [認証の有効化] オプションを選択し、（SMTP サーバーにアクセスできるユーザーの）ユーザー名とパスワードを入力します。
4. SMTP ポート番号 を入力します。

   上記のフィールドの詳細については、『iDRAC 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。

   SMTP が設定されます。

RACADM を使用した SMTP 電子メールサーバアドレスの設定

SMTP 電子メールサーバを設定するには、次の手順を実行します。

```
racadm set iDRAC.RemoteHosts.SMTPServerIPAddress <SMTP E-mail Server IP Address>
```

WS Eventing の設定

WS Eventing プロトコルは、クライアントサービス（サブスクライバ）が、サーバーイベント（通知またはイベントメッセージ）を含むメッセージの受信用にサーバー（イベントソース）にインタレスト（サブスクリプション）を登録するために使用されます。WS Eventing メッセージの受信に関心を持つクライアントは、iDRAC にサブスクライブして Lifecycle Controller ジョブ関連のイベントを受信することができます。

Lifecycle Controller ジョブに関連する変更についての WS Eventing メッセージを受信するための WS Eventing 機能の設定に必要な手順は、iDRAC 1.30.30 向け Web Service Eventing サポートの仕様書に記載されています。この仕様書の他にも、DSP0226（DMTF WS 管理仕様）の第 10 項「通知」（Eventing）文書で、WS Eventing プロトコルについての完全な情報を参照してください。Lifecycle Controller 関連のジョブは、DCIM ジョブ制御プロファイルマニュアルに記載されています。

Redfish Eventing の設定

Redfish Eventing プロトコルは、クライアントサービス（サブスクライバ）が、Redfish イベント（通知またはイベントメッセージ）を含むメッセージの受信用にサーバー（イベントソース）にインタレスト（サブスクリプション）を登録するために使用されます。Redfish Eventing メッセージの受信に関心を持つクライアントは、iDRAC にサブスクライブして Lifecycle Controller ジョブ関連のイベントを受信することができます。

シャーシイベントの監視

PowerEdge FX2/FX2s シャーシでは、iDRAC で［シャーシの管理と監視］を有効にして、シャーシコンポーネントの監視、アラートの設定、iDRAC RACADM を使用した CMC RACADM コマンドの実行、およびシャーシ管理ファームウェアのアップデートなどのシャーシの管理と監視タスクを実行することができます。この設定では、CMC がネットワーク上にない場合でも、シャーシ内のサーバーを管理できます。シャーシイベントを転送するには、値を［無効］に設定します。デフォルトでは、この設定は［有効］に設定されます。

メモ: この設定を有効にするには、CMC で［サーバーでのシャーシ管理］設定が［監視］または［管理と監視］になっていることを確認する必要があります。

［シャーシの管理と監視］オプションが［有効］に設定されている場合、iDRAC はシャーシイベントを生成し、ログに記録します。生成されたイベントは、iDRAC イベントサブシステムに統合され、その他のイベントと同様にアラートが生成されます。

また、CMC は、生成されたイベントを iDRAC に転送します。サーバー上の iDRAC が機能していない場合、CMC は最初の 16 個のイベントをキューに入れ、残りを CMC ログに記録します。これらの 16 個のイベントは、［シャーシの監視］が有効に設定された時点で iDRAC に送信されます。

iDRAC が必要な CMC 機能がないことを検知した場合、CMC のファームウェアアップグレードなしでは使用できない機能があることを知らせる警告メッセージが表示されます。

iDRAC ウェブインタフェースを使用したシャーシイベントの監視

iDRAC ウェブインタフェースを使用してシャーシイベントを監視するには、次の手順を実行します。

メモ: このセクションは、［サーバーモードでのシャーシ管理］が CMC で［監視］または［管理と監視］に設定されている場合に PowerEdge FX2/FX2s シャーシに対してのみ表示されます。

1. CMC インタフェースで、［シャーシ概要］>［セットアップ］>［一般］をクリックします。
2. ［サーバーモードでのシャーシ管理］ドロップダウンメニューで［管理と監視］を選択して、［適用］をクリックします。
3. iDRAC ウェブインタフェースを起動し、［概要］>［iDRAC 設定］>［CMC］をクリックします。
4. ［サーバーでのシャーシ管理］セクションで、［iDRAC からの機能］ドロップダウンボックスが［有効］に設定されていることを確認します。

RACADM を使用したシャーシイベントの監視

この設定は、［サーバーモードでのシャーシ管理］が CMC で［監視］または［管理と監視］に設定されている場合に PowerEdge FX2/FX2s サーバーのみに適用されます。

iDRAC RACADM を使用してシャーシイベントを監視するには：

```
racadm get system.chassiscontrol.chassismanagementmonitoring
```

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

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 28. 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

表 28. アラートメッセージ ID （続き）

メッセージ ID	説明
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
IPA	DRAC IP 変更
ITR	イントルージョン
JCP	ジョブ制御
LC	Lifecycle Controller
LIC	ライセンス付与
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展開
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

表 28. アラートメッセージ ID （続き）

メッセージ ID	説明
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	保管時
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
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

表 28. アラートメッセージ ID（続き）

メッセージ ID	説明
VRM	仮想コンソール
WRK	作業メモ

10

ログの管理

iDRAC 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 Lifecycle 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。Lifecycle ログは、iDRAC 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。

Lifecycle 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、コメントを追加することができます。アーカイブされたログを表示するには、Lifecycle 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。

関連概念

システムイベントログの表示 、p. 165
Lifecycle ログの表示 、p. 166
Lifecycle Controller ログのエクスポート 、p. 167
作業メモの追加 、p. 168
リモートシステムロギングの設定 、p. 168

トピック：

- システムイベントログの表示
- Lifecycle ログの表示
- Lifecycle Controller ログのエクスポート
- 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、iDRAC ウェブインタフェースで、［概要］ > ［サーバー］ > ［ログ］ 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。詳細については、『iDRAC 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］ を希望の場所に保存します。

メモ: Internet Explorer を使用し、保存時に問題が発生した場合は、Internet Explorer の Cumulative Security Update をダウンロードしてください。このセキュリティアップデートは、Microsoft のサポートサイト ［support.microsoft.com ］からダウンロードできます。

ログをクリアするには、［ログのクリア］ をクリックします。

メモ: ［ログのクリア］ は、ログのクリア権限がある場合のみ表示されます。

SEL がクリアされた後、Lifecycle Controller ログにエントリが記録されます。このログエントリには、ユーザー名および SEL をクリアした IP アドレスが含まれます。

RACADM を使用したシステムイベントログの表示

SEL を表示する場合

`racadm getsel <options>`

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場合：`racadm getsel -i`

SEL のエントリをクリアする場合：`racadm clrsel`

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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システムイベントログの表示

iDRAC 設定ユーティリティを使用してシステムイベントログ（SEL）のレコードの総数を確認し、ログをクリアすることができます。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、［システムイベントログ］に移動します。
   ［iDRAC 設定システムイベントログ］に、［レコードの総数］が表示されます。
2. レコードをクリアするには、［はい］を選択します。それ以外の場合は、［いいえ］を選択します。
3. システムイベントを表示するには、［システムイベントログの表示］をクリックします。
4. ［戻る］、［終了］の順にクリックし、［はい］をクリックします。

Lifecycle ログの表示

Lifecycle Controller ログは、管理下システムにインストールされたコンポーネントに関連する変更履歴を提供します。作業メモを各ログエントリに追加することもできます。

次のイベントとアクティビティが記録されます。

- システムイベント
- ストレージデバイス
- ネットワークデバイス
- 設定
- 監査
- アップデート

次のいずれかのインタフェースを使用して iDRAC へのログインまたはログアウトを行うと、ログイン、ログアウト、またはログインのエラーイベントが Lifecycle ログに記録されます。

- Telnet
- SSH
- ウェブインタフェース
- RACADM
- SM-CLP
- IPMI over LAN
- シリアル
- 仮想コンソール
- 仮想メディア

カテゴリおよび重要度に基づいてログを表示し、フィルタリングできます。また作業メモをログイベントにエクスポートして追加することもできます。

メモ: パーソナリティモード変更に対する Lifecycle ログは、ホストのウォームブート中にしか生成されません。

RACADM CLI または iDRAC ウェブインタフェースを使用して設定ジョブを開始する場合、Lifecycle ログには、ユーザー、使用されているインタフェース、およびジョブを開始するシステムの IP アドレスに関する情報が含まれています。

関連タスク

Lifecycle ログのフィルタ 、p. 167
ウェブインタフェースを使用した Lifecycle Controller ログのエクスポート 、p. 167
Lifecycle ログへのコメントの追加 、p. 167

ウェブインタフェースを使用した Lifecycle ログの表示

Lifecycle ログを表示するには、[概要] > [サーバー] > [ログ] > [Lifecycle ログ] とクリックします。[Lifecycle ログ] ページが表示されます。オプションの詳細については、『iDRAC オンラインヘルプ』を参照してください。

Lifecycle ログのフィルタ

ログは、カテゴリ、重大度、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。

Lifecycle ログをフィルタするには、次の手順を実行します。

1. [Lifecycle 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。
    - [重大度] ドロップダウンリストから重大度を選択します。
    - 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。

Lifecycle ログへのコメントの追加

Lifecycle 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. [Lifecycle 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 Lifecycle ログの表示

Lifecycle 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、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

Lifecycle Controller ログのエクスポート

Lifecycle Controller ログ全体 (アクティブとアーカイブされた項目) を 1 つの圧縮 XML ファイル形式をネットワーク共有、またはローカルシステムにエクスポートすることができます。圧縮 XML ファイルの拡張子は `.xml.gz` です。このファイルのエントリは、それらの番号順に、小さい数から大きい数の順になります。

ウェブインタフェースを使用した Lifecycle Controller ログのエクスポート

ウェブインタフェースを使用して Lifecycle Controller ログをエクスポートするには、次の手順を使用します。

1. [Lifecycle ログ] ページで、[エクスポート] をクリックします。
2. 次のオプションを任意に選択します。
    - [ネットワーク] — Lifecycle Controller のログをネットワーク上の共有の場所にエクスポートします。
    - [ローカル] — Lifecycle Controller のログをローカルシステム上の場所にエクスポートします。

   メモ: ネットワーク共有設定を指定する場合は、ユーザー名とパスワードに特殊記号を使用しないようにするか、特殊文字をパーセントエンコードすることが推奨されます。

   フィールドについては、『iDRAC オンラインヘルプ』を参照してください。
3. [エクスポート] をクリックしてログを指定した場所にエクスポートします。

RACADM を使用した Lifecycle Controller ログのエクスポート

Lifecycle Controller ログをエクスポートするには、`lclog export` コマンドを使用します。

詳細については、**dell.com/support/manuals** にある『*iDRAC RACADM コマンドラインインタフェース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

iDRAC 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 Lifecycle ログに保存されます。作業メモを追加するには iDRAC 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. iDRAC 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。詳細については、『iDRAC 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

Lifecycle 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。

- iDRAC 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 iDRAC 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. iDRAC 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ついては、『iDRAC 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。Lifecycle 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

リモートシステムロギングを設定するには、`iDRAC.SysLog` グループのオブジェクトで `set` コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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

iDRAC 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。
- [電源上限] — 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源上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。
- [電源装置オプション] - 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。

関連概念

電力の監視 、p. 169
電源制御操作の実行 、p. 170
電源上限 、p. 171
電源装置オプションの設定 、p. 172
電源ボタンの有効化または無効化 、p. 173
電力消費量の警告しきい値の設定 、p. 170

トピック :

電力の監視

iDRAC 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)

メモ: システムの電力消費傾向 (時間単位、日単位、週単位) のヒストグラムが維持されるのは iDRAC の実行中のみです。iDRAC が再起動されると、既存の電力消費データが失われ、ヒストグラムも再び開始されます。

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、iDRAC 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。詳細については、『iDRAC 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

電源の監視情報を表示するには、System.Power グループのオブジェクトで get コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

電力消費量の警告しきい値の設定

ラックおよびタワーシステム内の電力消費センサーに対する警告しきい値を設定することができます。ラックおよびタワーシステムに対する警告 / 重要電力しきい値により、PSU の容量と冗長ポリシーに基づいて、システムの電源サイクルが変更される場合があります。ただし、冗長ポリシーの電源装置容量が変更される場合でも、警告しきい値が重要しきい値を超えることはできません。

ブレードシステムの警告電力しきい値は、CMC 電力割り当てに設定されます。

デフォルト処置にリセットすると、電源しきい値はデフォルトに設定されます。

電力消費センサーに対する警告しきい値を設定するには、設定ユーザー権限を持っている必要があります。

メモ: 警告のしきい値は、racreset または iDRAC アップデートを実行した後にデフォルト値にリセットされます。

ウェブインタフェースを使用した電力消費量の警告しきい値の設定

1. iDRAC ウェブインタフェースで、[概要] > [サーバー] > [電源 / サーマル] > [電源監視] の順に移動します。
   電源監視 ページが表示されます。
2. [現在の電源読み取り値およびしきい値] セクションの [警告しきい値] 列で、[ワット] または [BTU/ 時] 単位で値を入力します。

   この値は、[障害しきい値] の値より低くする必要があります。値は、14 で割り切れる最も近い値に丸められます。[ワット] を入力すると、自動的に [BTU/ 時] の値が計算されて表示されます。同様に、BTU/ 時を入力すると、[ワット] の値が表示されます。
3. [適用] をクリックします。値が設定されます。

電源制御操作の実行

iDRAC 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、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。詳細に関しては、**dell.com/idracmanuals** にある『*Lifecycle Controller Remote Services クイックスタートガイド*』、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。

iDRAC から開始されるサーバの電源制御操作は BIOS で設定される電源ボタンの動作には関係ありません。物理的な電源ボタンを押しても何もしないように BIOS で設定されていても、PushPowerButton 機能を使用して、システムをグレースフルシャットダウンしたり、電源をオンにしたりできます。

ウェブインタフェースを使用した電源制御操作の実行

電源制御操作を実行するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、[概要] > [サーバー] > [電源 / 熱] > [電源設定] > [電源制御] と移動します。[電源制御] ページが表示されます。
2. 必要な電源制御操作を選択します。
   - システムの電源を入れる
   - システムの電源を切る
   - NMI (マスクなし割り込み)
   - 正常なシャットダウン
   - システムをリセットする (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。詳細については、『iDRAC オンラインヘルプ』を参照してください。

RACADM を使用した電源制御操作の実行

電源操作を実行するには、[serveraction] コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

電源上限

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源上限

PowerEdge M1000e または PowerEdge VRTX シャーシのブレードサーバーに電源が投入される前に、iDRAC は CMC に電源要件を提示します。これはブレードが消費できる実際の電力よりも高く、限られたハードウェアインベントリ情報に基づいて計算されています。サーバーの起動後、iDRAC はサーバーによって実際に消費される電力に基づいて要件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、サーバーが最大割り当て量に近い電力を消費している場合、iDRAC は潜在的最大消費電力の増加を要求する場合があり、これによってパワーエンベロープが増加することになります。iDRAC は、CMC に対する潜在的最大消費電力の要求のみを増加させます。消費が減少しても、iDRAC は潜在的最小電力を減少させる要求は行いません。iDRAC 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、iDRAC 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回収し、回収された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または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、iDRAC はシステムに電源を投入します。

電力上限ポリシーの表示と設定

電力上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源上限が施行されます。電力上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。

電力上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、iDRAC は要求された電力上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/ 時間で電力上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上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源上限ポリシーの設定

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 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源上限ポリシー] セクションに表示されます。
2. [iDRAC 電源上限ポリシー] 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して設定するには、`set` コマンドと一緒に次のオブジェクトを使用します。

- System.Power.Cap.Enable
- System.Power.Cap.Watts
- System.Power.Cap.Btuhr
- System.Power.Cap.Percent

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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上限ポリシーの設定

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 ］ に進みます。

   メモ: ［ 電源設定 ］ リンクは、サーバーの電源装置が電源監視をサポートする場合にのみ使用可能です。

   ［ iDRAC 設定の電源設定 ］ ページが表示されます。
2. ［ 電力上限ポリシー ］ 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. 推奨設定を使用するか、［ ユーザー定義の電源上限ポリシー ］ 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。
   電力上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 PSU システムでは、PSU1 または PSU2 をプライマリ PSU として設定できます。4 台 PSU システムでは、PSU のペア（ 1+1 または 2+2 ）をプライマリ PSU として設定する必要があります。

ホットスペアが有効になっていると、PSU がアクティブになり負荷に基づいてスリープ状態に移行できます。ホットスペアが有効になっている場合、2 台の PSU 間の電流の非均等な配分が有効になります。1 台の PSU が *アウェイク*状態で、大部分の電流を提供します。もう 1 台の PSU はスリープモードになり、小量の電流を提供します。これは 2 台の PSU による 1+0 と呼ばれることが多く、ホットスペアは有効になっています。すべての PSU-1 が回路 -A にあり、すべての PSU-2 が回路 -B 上にある場合、ホットスペアを有効にする（ 工場出荷時のデフォルト設定 ）と、回路 -B への負荷は大幅に低くなり、警告がトリガされます。ホットスペアを無効にしている場合、電源の共有は、2 台の PSU 間で五分五分となり、回路 -A と回路 -B は通常、同一の負荷を分担します。

パワーファクタは、皮相電力に対する実際に消費された電力の割合です。パワーファクタ補正が有効になっている場合、サーバーは、ホストがオフのときに少量の電力しか消費しません。デフォルトでは、サーバーの工場出荷時にパワーファクタ補正が有効化されています。

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. iDRAC 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、『iDRAC 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、`set` コマンドと一緒に次のオブジェクトを使用します。

- System.Power.RedundancyPolicy
- System.Power.Hotspare.Enable
- System.Power.Hotspare.PrimaryPSU
- System.Power.PFC.Enable

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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。

   メモ: [電源設定] リンクは、サーバーの電源装置が電源監視をサポートする場合にのみ使用可能です。

   [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、[前面パネルセキュリティ] に移動します。
   [iDRAC 設定前面パネルセキュリティ] ページが表示されます。
2. [有効] を選択して電源ボタンを有効にする、または [無効] を選択して無効にします。
3. [戻る]、[終了] の順にクリックし、[はい] をクリックします。
   設定が保存されます。

12

ネットワークデバイスのインベントリ、監視、および設定

次のネットワークデバイスをインベントリ、監視、および設定できます。

- 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）

CNA デバイスで NPAR または個々のパーティションを無効にする前に、必ずすべての I/O アイデンティティ属性（例 : IP アドレス、仮想アドレス、イニシエータ、およびストレージターゲット）とパーティションレベルの属性（例：帯域幅の割り当て）をクリアしてください。VirtualizationMode 属性の設定を NPAR に変更するか、またはパーティションのすべてのパーソナリティを無効にすることでパーティションを無効にできます。

インストールされている CNA デバイスのタイプによって、パーティション属性の設定が、パーティションがアクティブだった最後の時点から保持されないことがあります。パーティションを有効にする場合は、すべての I/O アイデンティティ属性とパーティション関連の属性を設定します。VirtualizationMode 属性の設定を NPAR に変更するか、またはパーティションでパーソナリティ（例 : NicMode）を有効にすることでパーティションを有効にできます。

関連概念

FC HBA デバイスのインベントリと監視、p. 175
仮想アドレス、イニシエータ、およびストレージターゲットのダイナミック設定、p. 175

トピック：

ネットワークデバイスのインベントリと監視

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。

デバイスごとに、ポートおよび有効化されたパーティションの次の情報を表示することができます。

- リンクステータス
- プロパティ
- 設定と機能
- 受信および送信統計情報
- iSCSI、FCoE イニシエータ、およびターゲットの情報

関連概念

ネットワークデバイスのインベントリ、監視、および設定、p. 174
仮想アドレス、イニシエータ、およびストレージターゲットのダイナミック設定、p. 175

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、『iDRAC 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に関する情報を表示するには、`hwinventory` コマンドと `nicstatistics` コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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、iDRAC 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。

FC HBA デバイスのインベントリと監視

管理下システム内の Fibre Channel Host Bus Adapters （FC HBA）デバイスの正常性の監視とインベントリの表示をリモートで行うことができます。Emulex および QLogic FC HBA がサポートされています。各 FC HBA デバイスのポートについての以下の情報を表示できます。

- リンク状態および情報
- ポートのプロパティ
- 受信および送信統計情報

関連概念

ネットワークデバイスのインベントリ、監視、および設定 、p. 174

ウェブインタフェースを使用した FC HBA デバイスの監視

ウェブインタフェースを使用して FC HBA デバイス情報を表示するには、[概要] > [ハードウェア] > [Fibre Channel] と移動します。表示されるプロパティの詳細については、『iDRAC オンラインヘルプ』を参照してください。

ページ名は、FC HBA デバイスが使用可能なスロット番号と FC HBA デバイスのタイプも示します。

RACADM を使用した FC HBA デバイスの監視

RACADM を使用して FC HBA デバイス情報を表示するには、`hwinventory` コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

仮想アドレス、イニシエータ、およびストレージターゲットのダイナミック設定

仮想アドレス、イニシエータ、およびストレージターゲットの設定は動的に表示および設定し、永続性ポリシーを適用することができます。これにより、アプリケーションは電源状態の変化（つまり、オペレーティングシステムの再起動、ウォームリセット、コールドリセット、または AC サイクル）に基づいて、また、その電源状態に対する永続性ポリシーに基づいて設定を適用できます。このことから、システム作業負荷を別のシステムに迅速に再設定する必要がある導入環境に高い柔軟性をもたらします。

仮想アドレスは次のとおりです。

- 仮想 MAC アドレス
- 仮想 iSCSI MAC アドレス
- 仮想 FIP MAC アドレス
- 仮想 WWN
- 仮想 WWPN

メモ: 永続性ポリシーをクリアすると、すべての仮想アドレスが工場で設定されたデフォルトの永続アドレスにリセットされます。

メモ: 仮想 FIP、仮想 WWN、および仮想 WWPN MAC 属性を持つ一部のカードでは、仮想 FIP を設定するときに仮想 WWN および仮想 WWPN MAC 属性が自動的に設定されます。

IO アイデンティティ機能を使用すると、次の操作を行うことが出来ます。

- ネットワークおよび Fibre Channel デバイスに対する仮想アドレスの表示と設定（たとえば、NIC、CNA、FC HBA）。
- イニシエータ（iSCSI および FCoE 用）およびストレージターゲット設定（iSCSI、FCoE、および FC 用）の設定。
- システム AC 電源の喪失、システムのコールドリセットとウォームリセットに対する設定値の永続性またはクリアランスの指定。

仮想アドレス、イニシエータ、およびストレージターゲットに設定された値は、システムリセット時の主電源の処理方法や、NIC、CNA、または FC HBA デバイスに補助電源があるかどうかに基づいて変更される場合があります。IO アイデンティティ設定の永続性は、iDRAC を使用したポリシー設定に基づいて実現することができます。

I/O アイデンティティ機能が有効になっている場合にのみ、永続性ポリシーが有効になります。システムのリセットまたは電源投入のたびに、値はポリシー設定に基づいて保持されるか、またはクリアされます。

メモ: 値がクリアされた後は、設定ジョブを実行するまで値を再適用することはできません。

関連概念

ネットワークデバイスのインベントリ、監視、および設定 、p. 174
I/O アイデンティティ最適化対応のカード 、p. 176
I/O アイデンティティ最適化の対応 NIC ファームウェアバージョン 、p. 177
I/O アイデンティティ最適化の有効化または無効化 、p. 179
永続性ポリシーの設定 、p. 180

I/O アイデンティティ最適化対応のカード

次の表に、I/O のアイデンティティ最適化機能に対応しているカードを示します。

表 29. I/O アイデンティティ最適化対応のカード

製造元	タイプ
Broadcom	• 5720 PCIe 1 GB • 5719 PCIe 1 GB • 57810 PCIe 10 GB • 57810 bNDC 10 GB • 57800 rNDC 10 GB + 1 GB • 57840 rNDC 10 GB • 57840 bNDC 10 GB • 5720 rNDC 1 GB • 5719 Mezz 1 GB • 57810 Mezz 10 GB • 5720 bNDC 1 GB
Intel	• i350 Mezz 1 Gb • x520+i350 rNDC 10 Gb+1 Gb • I350 bNDC 1 Gb • x540 PCIe 10 Gb • x520 PCIe 10 Gb • i350 PCIe 1 Gb • x540+i350 rNDC 10 Gb+1 Gb • i350 rNDC 1 Gb • x520 bNDC 10 Gb • 40G 2P XL710 QSFP+ rNDC
Mellanox	• ConnectX-3 10G • ConnectX-3 40G • ConnectX-3 10G • ConnectX-3 Pro 10G

表 29. I/O アイデンティティ最適化対応のカード （続き）

製造元	タイプ
	• ConnectX-3 Pro 40G • ConnectX-3 Pro 10G
QLogic	• QME2662 Mezz FC16 • QLE2660 PCIe FC16 • QLE2662 PCIe FC16
Emulex	• LPM16002 Mezz FC16 • LPe16000 PCIe FC16 • LPe16002 PCIe FC16 • LPM16002 Mezz FC16 • LPM15002 • LPe15000 • LPe15002 • OCm14104B-UX-D • OCm14102B-U4-D • OCm14102B-U5-D • OCe14102B-UX-D • OCm14104B-UX-D • OCm14102B-U4-D • OCm14102B-U5-D • OCe14102B-UX-D • OCm14104-UX-D rNDC 10 Gb • OCm14102-U2-D bNDC 10 Gb • OCm14102-U3-D Mezz 10 Gb • OCe14102-UX-D PCIe 10 Gb

I/O アイデンティティ最適化の対応 NIC ファームウェアバージョン

第 13 世代 Dell PowerEdge サーバーでは、必要な NIC ファームウェアがデフォルトで表示されます。

次の表では、I/O アイデンティティ最適化機能向けの NIC ファームウェアバージョンを示しています。

iDRAC が FlexAddress モードまたはコンソールモードに設定されている場合の仮想 /FlexAddress と永続性ポリシーの動作

次の表では、CMC における FlexAddress 機能状況、iDRAC で設定されているモード、iDRAC における I/O アイデンティティ機能状況、および XML 設定に応じた仮想アドレス管理（VAM）設定と永続性ポリシーの動作が説明されています。

表 30. 仮想 /FlexAddress と永続性ポリシーの動作

CMC における FlexAddress 機能状況	iDRAC で設定されているモード	iDRAC における IO アイデンティティ機能状況	XML 設定	永続性ポリシー	永続性ポリシーのクリア - 仮想アドレス
FlexAddress 有効	FlexAddress モード	有効	仮想アドレス管理（VAM）設定済み	設定された VAM が持続	Flex Address に設定
FlexAddress 有効	FlexAddress モード	有効	VAM 未設定	Flex Address に設定	永続性なし - FlexAddress に設定
FlexAddress 有効	FlexAddress モード	無効	Lifecycle Controller で指定したパスを使って設定済み	当該のサイクルに対して FlexAddress に設定	永続性なし - FlexAddress に設定
FlexAddress 有効	FlexAddress モード	無効	VAM 未設定	Flex Address に設定	Flex Address に設定

表 30. 仮想 /FlexAddress と永続性ポリシーの動作 （続き）

CMC における FlexAddress 機能状況	iDRAC で設定されているモード	iDRAC における IO アイデンティティ機能状況	XML 設定	永続性ポリシー	永続性ポリシーのクリア - 仮想アドレス
FlexAddress 無効	FlexAddress モード	有効	VAM 設定済み	設定された VAM が持続	永続性のみ - クリアは使用できません。
FlexAddress 無効	FlexAddress モード	有効	VAM 未設定	ハードウェア MAC アドレスに設定	永続性のサポートなし。カードの動作に依存
FlexAddress 無効	FlexAddress モード	無効	Lifecycle Controller で指定したパスを使って設定済み	当該のサイクルに対して Lifecycle Controller 設定が持続	永続性のサポートなし。カードの動作に依存
FlexAddress 無効	FlexAddress モード	無効	VAM 未設定	ハードウェア MAC アドレスに設定	ハードウェア MAC アドレスに設定
FlexAddress 有効	コンソールモード	有効	VAM 設定済み	設定された VAM が持続	永続性とクリアの両方が機能することが必要
FlexAddress 有効	コンソールモード	有効	VAM 未設定	ハードウェア MAC アドレスに設定	ハードウェア MAC アドレスに設定
FlexAddress 有効	コンソールモード	無効	Lifecycle Controller で指定したパスを使って設定済み	当該のサイクルに対して Lifecycle Controller 設定が持続	永続性のサポートなし。カードの動作に依存
FlexAddress 無効	コンソールモード	有効	VAM 設定済み	設定された VAM が持続	永続性とクリアの両方が機能することが必要
FlexAddress 無効	コンソールモード	有効	VAM 未設定	ハードウェア MAC アドレスに設定	ハードウェア MAC アドレスに設定
FlexAddress 無効	コンソールモード	無効	Lifecycle Controller で指定したパスを使って設定済み	当該のサイクルに対して Lifecycle Controller 設定が持続	永続性のサポートなし。カードの動作に依存
FlexAddress 有効	コンソールモード	無効	VAM 未設定	ハードウェア MAC アドレスに設定	ハードウェア MAC アドレスに設定

FlexAddress および I/O アイデンティティに対するシステム動作

	CMC における FlexAddress 機能状況	iDRAC における IO アイデンティティ機能状況	再起動サイクルに対するリモートエージェント VA の可用性	VA プログラミングソース	再起動サイクル VA 持続動作
FA と同等の永続性を持つサーバー	有効	無効		CMC からの FlexAddress	FlexAddress 仕様による
	N/A、有効、または無効	有効	はい - 新規または永続的	リモートエージェント仮想アドレス	FlexAddress 仕様による
			いいえ	仮想アドレスがクリア済み	
	無効	無効			

	CMC における FlexAddress 機能状況	iDRAC における IO アイデンティティ機能状況	再起動サイクルに対するリモートエージェント VA の可用性	VA プログラミングソース	再起動サイクル VA 持続動作
VAM 永続性ポリシー機能を備えたサーバー	有効	無効		CMC からの FlexAddress	FlexAddress 仕様による
	有効	有効	はい - 新規または永続的	リモートエージェント仮想アドレス	リモートエージェントポリシー設定による
			いいえ	CMC からの FlexAddress	FlexAddress 仕様による
	無効	有効	はい - 新規または永続的	リモートエージェント仮想アドレス	リモートエージェントポリシー設定による
			いいえ	仮想アドレスがクリア済み	
	無効	無効			

I/O アイデンティティ最適化の有効化または無効化

通常、システム起動後にデバイスが設定され、再起動後にデバイスが初期化されますが、I/O アイデンティティー最適化機能を有効にすると、起動最適化を行うことができます。この機能を有効にすると、デバイスがリセットされてから初期化されるまでの間に仮想アドレス、イニシエータ、およびストレージターゲットの属性が設定されるため、2 回目の BIOS 再起動が必要なくなります。デバイス設定と起動操作は、一回のシステム起動で実行され、起動時間が最適化されます。

I/O アイデンティティ最適化を有効にする前に、次を確認してください。

- ログイン、設定、およびシステム管理の権限がある。
- BIOS、iDRAC、およびネットワークカードが最新のファームウェアにアップデートされている。サポートされるバージョンについての情報は、「I/O アイデンティティ最適化対応のカード 、p. 176」および「I/O アイデンティティ最適化対応の NIC ファームウェアバージョン」を参照してください。

I/O アイデンティティ最適化機能を有効にした後、iDRAC から XML 設定ファイルをエクスポートし、XML 設定ファイル内の必要な I/O アイデンティティ属性を変更して、ファイルを元の iDRAC にインポートして戻します。

XML 設定ファイルで変更可能な I/O アイデンティティ最適化の属性のリストについては、**delltechcenter.com/idrac** で *NIC プロファイル*のマニュアルを参照してください。

メモ: I/O アイデンティティ最適化に関係のない属性は変更しないでください。

ウェブインタフェースを使用した I/O アイデンティティ最適化の有効化または無効化

I/O アイデンティティ最適化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 ウェブインタフェースで、[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。
2. [I/O アイデンティティ最適化] タブをクリックし、[I/O アイデンティティ最適化] オプションを選択して、この機能を有効にします。無効にするには、このオプションをクリアします。
3. 設定を適用するには、[適用] をクリックします。

RADCAM を使用した I/O アイデンティティ最適化の有効化または無効化

I/O アイデンティティ最適化を有効化するには、次のコマンドを使用します。

```
racadm set idrac.ioidopt.IOIDOptEnable Enabled
```

この機能を有効にした後、設定を有効にするには、システムを再起動してください。

I/O アイデンティティ最適化を無効化するには、次のコマンドを使用します。

```
racadm set idrac.ioidopt.IOIDOptEnable Disabled
```

I/O アイデンティティ最適化設定を表示するには、次のコマンドを使用します。

```
racadm get iDRAC.IOIDOpt
```

永続性ポリシーの設定

I/O アイデンティティを使用して、仮想アドレス、イニシエータ、およびストレージターゲット設定の永続性またはクリアランスを決定するシステムリセットおよびパワーサイクルの動作を指定するポリシーを設定できます。個々の永続性ポリシー属性は、それぞれシステム内の適用可能なすべてのデバイスのすべてのポートとパーティションに適用されます。デバイスの動作は、補助電源駆動デバイスと非補助電源駆動デバイスで異なります。

メモ: iDRAC で **VirtualAddressManagement** 属性が FlexAddress モードに設定されている場合、および **FlexAddress** 機能が CMC で無効になっている場合、[永続性ポリシー] 機能は動作しません。iDRAC で [VirtualAddressManagement] 属性を **コンソール** モードに設定されているか、CMC で FlexAddress 機能が有効になっていることを確認します。

次の永続性ポリシーを設定することができます。

- 仮想アドレス : 補助電源駆動デバイス
- 仮想アドレス : 非補助電源駆動デバイス
- イニシエータ
- ストレージターゲット

永続性ポリシーを適用する前に、次の操作を行ってください。

- ネットワークハードウェアのインベントリを少なくとも 1 回実行します。つまり、Collect System Inventory On Restart を有効にします。
- I/O アイデンティティ最適化を有効にします。

次の場合に、イベントは Lifecycle Controller ログに記録されます。

- I/O アイデンティティ最適化が有効または無効になっている。
- 持続性ポリシーが変更された。
- 仮想アドレス、イニシエータ、およびターゲットの値が、ポリシーに基づいて設定された。ポリシーが適用される場合に、設定済みのデバイスとそれらのデバイスに設定された値について、単一のログエントリが記録されます。

イベントアクションは SNMP、電子メール、または WS-eventing 通知用に有効化されています。リモート syslog にはログも含まれています。

永続性ポリシーのデフォルト値

永続性ポリシー	AC 電源喪失	コールドブート	ウォームブート
仮想アドレス : 補助電源駆動デバイス	選択されていません	選択済み	選択済み
仮想アドレス : 非補助電源駆動デバイス	選択されていません	選択されていません	選択済み
イニシエータ	選択済み	選択済み	選択済み
ストレージターゲット	選択済み	選択済み	選択済み

メモ: 永続的ポリシーが無効になっているとき、および仮想アドレスを削除するための操作を実行するときは、永続的ポリシーを再度有効にしても仮想アドレスは取得されません。永続的ポリシーを有効にした後で再度仮想アドレスを設定する必要があります。

メモ: 永続性ポリシーが有効で、CNA デバイスのパーティションで仮想アドレス、イニシエータ、またはストレージターゲットが設定されている場合は、VirtualizationMode またはパーティションのパーソナリティを変更する前に、仮想アドレス、イニシエータ、およびストレージターゲットに設定された値をリセットまたはクリアしないでください。永続性ポリシーを無効にすると、アクションは自動的に実行されます。設定ジョブを使用して、仮想アドレスの属性を 0 に、イニシエータとストレージタ

ーゲットの値を iSCSI イニシエータとストレージターゲットのデフォルト値 、p. 181 に定義された通りに明示的に設定することもできます。

関連概念

I/O アイデンティティ最適化の有効化または無効化 、p. 179

iDRAC ウェブインタフェースを使用した永続性ポリシーの設定

永続性ポリシーを設定するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、[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。
2. [I/O アイデンティティ最適化] タブをクリックします。
3. [永続性ポリシー] セクションで、それぞれの永続性ポリシーに対して次の 1 つまたは複数選択します。
   - [A/C 電源喪失] - AC 電源喪失状況が発生した場合に持続される仮想アドレスまたはターゲット設定。
   - [コールドブート] - コールドリセット状況が発生した場合に持続される仮想アドレスまたはターゲット設定。
   - [ウォームブート] - ウォームリセット状況が発生した場合に持続される仮想アドレスまたはターゲット設定。
4. [適用] をクリックします。
   永続性ポリシーが設定されます。

RACADM を使用した永続性ポリシーの設定

永続性ポリシーを設定するには、次の racadm オブジェクトと **set** サブコマンドを使用します。

- 仮想アドレスには、**iDRAC.IOIDOpt.VirtualAddressPersistencePolicyAuxPwrd** および **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyNonAuxPwrd** オブジェクトを使用
- イニシエータには、**iDRAC.IOIDOPT.InitiatorPersistencePolicy** オブジェクトを使用
- ストレージターゲットには、**iDRAC.IOIDOpt.StorageTargetPersistencePolicy** オブジェクトを使用

詳細については、**dell.com/esmmanuals** にある『iDRAC RACADM コマンドラインインタフェースリファレンスガイド』を参照してください。

iSCSI イニシエータとストレージターゲットのデフォルト値

次の表は、永続性ポリシーがクリアされたときの iSCSI イニシエータおよびストレージターゲットのデフォルト値の一覧です。

表 31. iSCSI イニシエータ - デフォルト値

iSCSI イニシエータ	IPv4 モードでのデフォルト値	IPv6 モードでのデ
IscsiInitiatorIpAddr	0.0.0.0	::
IscsiInitiatorIpv4Addr	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Addr	::	::
IscsiInitiatorSubnet	0.0.0.0	0.0.0.0
IscsiInitiatorSubnetPrefix	0	0
IscsiInitiatorGateway	0.0.0.0	::
IscsiInitiatorIpv4Gateway	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Gateway	::	::
IscsiInitiatorPrimDns	0.0.0.0	::
IscsiInitiatorIpv4PrimDns	0.0.0.0	0.0.0.0

表 31. iSCSI イニシエータ - デフォルト値 （続き）

iSCSI イニシエータ	IPv4 モードでのデフォルト値	IPv6 モードでのデ
IscsiInitiatorIpv6PrimDns	::	::
IscsiInitiatorSecDns	0.0.0.0	::
IscsiInitiatorIpv4SecDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6SecDns	::	::
IscsiInitiatorName	値がクリア	値がクリア
IscsiInitiatorChapId	値がクリア	値がクリア
IscsiInitiatorChapPwd	値がクリア	値がクリア
IPVer	Ipv4	

表 32. iSCSI ストレージターゲットの属性 - デフォルト値

iSCSI ストレージターゲットの属性	IPv4 モードでのデフォルト値	IPv6 モードでのデ
ConnectFirstTgt	無効	無効
FirstTgtIpAddress	0.0.0.0	::
FirstTgtTcpPort	3260	3260
FirstTgtBootLun	0	0
FirstTgtIscsiName	値がクリア	値がクリア
FirstTgtChapId	値がクリア	値がクリア
FirstTgtChapPwd	値がクリア	値がクリア
FirstTgtIpVer	Ipv4	
ConnectSecondTgt	無効	無効
SecondTgtIpAddress	0.0.0.0	::
SecondTgtTcpPort	3260	3260
SecondTgtBootLun	0	0
SecondTgtIscsiName	値がクリア	値がクリア
SecondTgtChapId	値がクリア	値がクリア
SecondTgtChapPwd	値がクリア	値がクリア
SecondTgtIpVer	Ipv4	

13

ストレージデバイスの管理

iDRAC 2.00.00.00 リリースからは、iDRAC が新しい PERC9 コントローラの直接設定が含まれるように、エージェントフリーの管理を拡張します。それによって、システムに接続されたストレージコンポーネントをランタイムにリモートで設定できます。これらのコンポーネントには、RAID および非 RAID コントローラと、チャネル、ポート、エンクロージャ、およびそれらに接続されたディスクが含まれます。

Comprehensive Embedded Management（CEM）フレームワークでのストレージサブシステムの完全な検出、トポロジー、正常性の監視と設定は、I2C インタフェース経由の MCTP プロトコルを使用した内部および外部 PERC コントローラとのインタフェースによって実現します。リアルタイム設定の場合、CEM は PERC9 コントローラをサポートします。PERC9 コントローラのファームウェアバージョンは、9.1 またはそれ以降である必要があります。

iDRAC を使用して、OpenManage Storage Management で使用可能な、リアルタイム（再起動以外）設定コマンドなどのほとんどの機能を実行できます。オペレーティングシステムをインストールする前に、RAID を完全に設定できます。

BIOS にアクセスせずにコントローラ機能を設定し、管理することができます。これらの機能には、仮想ディスクの設定と、RAID レベルおよびデータ保護用のホットスペアの適用が含まれます。再構築とトラブルシューティングなど、その他多くのコントローラ機能を開始できます。データ冗長性の設定またはホットスペアの割り当てによって、データを保護できます。

ストレージデバイスには、次のものがあります。

- コントローラ - ほとんどのオペレーティングシステムでは、ディスクから直接データの読み取りと書き込みを行わず、読み取りと書き込みの指示をコントローラに送信します。コントローラは、システム内のハードウェアで、データの書き込みと取り出しを行うためにディスクと直接やり取りします。コントローラには、1 つまたは複数の物理ディスクに接続されたコネクタ（チャネルまたはポート）、または物理ディスクを収容するエンクロージャが搭載されています。RAID コントローラは、ディスクの境界をまたがり、複数のディスクの容量を使用して拡張されたストレージ空間、すなわち仮想ディスクを作成できます。また、コントローラは、再構築の開始やディスクの初期化など、その他のタスクも実行します。これらのタスクを完了するため、コントローラはファームウェアおよびドライバと呼ばれる特別なソフトウェアを必要とします。コントローラが正常に機能するには、必要最低限のバージョンのファームウェアとドライバがインストールされていることが必要です。コントローラによって、データの読み取りおよび書き込み方法や、タスクの実行方法の特徴が異なります。これらの機能を理解しておくと、ストレージを最も効率的に管理するのに役立ちます。
- 物理ディスクまたは物理デバイス - エンクロージャ内にあるか、コントローラに接続されています。RAID コントローラでは、物理ディスクまたはデバイスを使って仮想ディスクを作成します。
- 仮想ディスク - RAID コントローラによって 1 つまたは複数の物理ディスクから作成されたストレージです。仮想ディスクは複数の物理ディスクから作成されますが、オペレーティングシステムはこれを 1 つのディスクとして認識します。使用する RAID レベルによって、仮想ディスクはディスク障害発生時に冗長データを保持する場合や、特定の性能属性を備える場合があります。仮想ディスクは、RAID コントローラ上でのみ作成できます。
- エンクロージャ - これはシステムに外部接続されますが、バックプレーンとその物理ディスクはシステム内蔵です。
- バックプレーン - エンクロージャに似ています。バックプレーンで、コントローラのコネクタと物理ディスクがエンクロージャに接続されますが、外付けのエンクロージャに関する管理機能（温度プローブ、アラームなど）は搭載されません。物理ディスクは、エンクロージャに収容するか、またはシステムのバックプレーンに接続することができます。

エンクロージャに収容された物理ディスクの管理に加え、エンクロージャ内のファン、電源装置、および温度プローブのステータスを監視することができます。エンクロージャはホットプラグ可能です。ホットプラグとは、オペレーティングシステムの実行中にシステムにコンポーネントを追加することを意味しています。

コントローラに接続された物理デバイスには、最新のファームウェアが必要です。最新の対応ファームウェアについては、サービスプロバイダにお問い合わせください。

PERC からのストレージイベントは、適用可能として SNMP トラップおよび WSMAN イベントにマップされます。ストレージ構成に対する変更はすべて、Lifecycle ログに記録されます。

PERC 機能	**CEM 設定応コントローラ（PERC 9.1 以降）**	**CEM 設定非対応のコントローラ（PERC 9.0 およびそれ以前）**
リアルタイム	コントローラに対して保留中の既存のジョブもスケジュールされたジョブも存在しない場合、設定が適用されます。 そのコントローラに対して保留中またはスケジュール済のジョブがある場合は、ジョブをクリアするか、ジョブが完了するま	設定が適用されます。エラーメッセージが表示されます。ジョブの作成が正常に完了せず、ウェブインタフェースを使用してリアルタイムジョブを作成できません。

PERC 機能	CEM 設定応コントローラ（PERC 9.1 以降）	CEM 設定非対応のコントローラ（PERC 9.0 およびそれ以前）
	で待ってからランタイムに設定を適用する必要があります。ランタイムまたはリアルタイムは、再起動を必要としないことを意味します。	
ステージング	設定オペレーションがすべてステージングされている場合、設定は再起動後にステージングされ、適用されるか、リアルタイムで適用されます。	設定は再起動後に適用されます。

関連概念

RAID の概念について 、p. 184
ストレージデバイスのインベントリと監視 、p. 196
ストレージデバイスのトポロジの表示 、p. 197
コントローラの管理 、p. 205
物理ディスクの管理 、p. 197
エンクロージャまたはバックプレーンの管理 、p. 216
PCIe SSD の管理 、p. 213
仮想ディスクの管理 、p. 199
コンポーネント LED の点滅または点滅解除 、p. 223

関連参照文献

対応コントローラ 、p. 193
対応エンクロージャ 、p. 194
ストレージデバイスの対応機能のサマリ 、p. 194

トピック：

RAID の概念について

Storage Management は、ストレージ管理機能を提供するために Redundant Array of Independent Disks（RAID）技術を使用します。Storage Management について理解するには、RAID についての概念の他、システムにおいて RAID コントローラとオペレーティングシステムがディスク容量をどのように認識するかについてもある程度把握しておく必要があります。

RAID とは?

RAID は、システム内に搭載または接続された物理ディスク上にあるデータの保存を管理するためのテクノロジです。RAID の重要な要素は、複数の物理ディスクの容量を組み合わせを単一の拡張ディスク容量として扱うことができるように、物理ディスクをスパンする機能です。RAID のその他の重要な要素には、ディスク障害が発生した場合にデータを復元するために使用できる冗長データを維持する機能があります。RAID では、ストライピング、ミラーリング、パリティなどの異なる方法を使用してデータの保存と再構築を行います。RAID レベルには、データの保存と再構築のために異なる方法を使う異なるレベルがあります。RAID レベルには、読み書きパフォーマンス、データ保護、ストレージ容量という観点では異なる特徴があります。冗長データはすべての RAID レベルで維持されるものではなく、一部の RAID レベルでは失われたデータを復元できません。選択する RAID レベルは、優先事項がパフォーマンスか、保護か、ストレージ容量かによって変わります。

メモ: RAB (RAID Advisory Board) は、RAID の実装に使用される仕様を定義しています。RAB は RAID レベルを定義しますが、異なるベンダーによる RAID レベルの商用実装は、実際の RAID 仕様が異なる場合があります。特定のベンダーの実装は、読み取りおよび書き込みパフォーマンスとデータの冗長性の度合いに影響することがあります。

ハードウェアとソフトウェア RAID

RAID は、ハードウェアとソフトウェアのどちらを使っても実装することができます。ハードウェア RAID を使用するシステムには、RAID レベルを実装し、物理ディスクに対するデータの読み書きを処理する RAID コントローラがあります。オペレーティングシステム提供のソフトウェア RAID を使用するときは、オペレーティングシステムが RAID レベルを実装します。このため、ソフトウェア RAID のみの使用はシステムパフォーマンスを低下させることがあります。ただし、ハードウェア RAID ボリュームとソフトウェア RAID を合わせて使用することによって、パフォーマンスと RAID ボリュームの設定の多様性を向上させることができます。たとえば、2 つの RAID コントローラ間でハードウェア RAID 5 ボリュームのペアをミラーリングすることによって RAID コントローラの冗長性を提供することができます。

RAID の概念

RAID では特定の方法を使用してデータをディスクに書き込みます。これらの方法を使うと、RAID でデータの冗長性またはパフォーマンスの向上を実現できます。次の方法があります。

- ミラーリング — 1 つの物理ディスクから別の物理ディスクにデータを複製します。ミラーリングを行うと、同じデータの 2 つのコピーを異なる物理ディスクに保管することでデータの冗長性が得られます。ミラーのディスクのうち 1 つが失敗すると、システムは影響を受けていないディスクを使用して動作を続行できます。ミラーリングしたディスクの両方に常に同じデータが入っています。ミラーのいずれも動作側として機能します。ミラーリングされた RAID ディスクグループは、読み取り操作で RAID 5 ディスクグループのパフォーマンスと同等ですが、書き込み速度はより高速です。
- ストライピング — 仮想ディスク内のすべての物理ディスク全体にわたって、データを書き込みます。各ストライプは、仮想ディスク内の各物理ディスクにシーケンシャルパターンを使用して固定サイズの単位でマップされた連続する仮想ディスクデータアドレスで構成されます。たとえば、仮想ディスクに 5 つの物理ディスクがある場合、ストライプは繰り返しなしで物理ディスクの 1 から 5 にデータを書き込みます。ストライプで使用される容量は各物理ディスクで同じです。物理ディスク上に存在するストライプ部分はストリライプエレメントです。ストライピング自体にはデータの冗長性はありません。ストライピングをパリティと組み合わせることでデータの冗長性を提供します。
- ストライプサイズ — パリティディスクを含まない、ストライプによって消費される総ディスク容量。たとえば、ストライプは 64KB のディスク容量で、ストライプの各ディスクには 16KB のデータがあるとします。この場合、ストライプサイズは 64KB でストライプエレメントサイズは 16KB です。
- ストライプエレメント — 単一の物理ディスク上にあるストライプの一部分です。
- ストライプエレメントサイズ — ストライプエレメントによって消費されるディスク容量。たとえば、ストライプは 64KB のディスク容量で、ストライプの各ディスクには 16KB のデータが存在するとします。この場合、ストライプサイズは 16KB でストライプエレメントサイズは 64KB です。
- パリティ — ストライピングとアルゴリズムを組み合わせて使用することによって維持される冗長データ。ストライピングを行っているディスクの 1 つが失敗すると、アルゴリズムを使用してパリティ情報からデータを再構築することができます。
- スパン — 物理ディスクグループのストレージ容量を RAID 10、50 または 60 の仮想ディスクとして組み合わせるために使用する RAID 技術。

RAID レベル

各 RAID レベルではミラーリング、ストライピング、パリティを併用することでデータ冗長性や読み書きパフォーマンスの向上を実現します。各 RAID レベルの詳細については、「RAID レベルの選択」を参照してください。

可用性とパフォーマンスを高めるためのデータストレージの編成

RAID は、ディスクストレージをまとめるための異なる方法または RAID レベルを提供します。一部の RAID レベルでは、ディスクの障害発生後にデータを復元できるように冗長データが維持されます。RAID レベルが異なると、システムの I/O（読み書き）パフォーマンスが影響を受けることがあります。

冗長データを維持するには、追加の物理ディスクを使用する必要があります。ディスク数が増えると、ディスク障害の可能性も増加します。I/O パフォーマンスと冗長性に違いがあるため、オペレーティング環境のアプリケーションと保存するデータの性質によってはある RAID レベルが他の RAID レベルより適している場合があります。

RAID レベルを選択する場合は、パフォーマンスとコストに関する次の注意事項が適用されます。

- 可用性または耐障害性 — 可用性または耐障害性とは、システムのコンポーネントの 1 つに障害が発生しても動作を継続し、データへのアクセスを提供することができる、システムの能力を指します。RAID ボリュームでは、可用性またはフォールトトレランスは冗長データを維持することによって達成できます。冗長データにはミラー（複製データ）とパリティ情報（アルゴリズムを使用したデータの再構成）が含まれています。
- パフォーマンス — 選択する RAID レベルによって、読み取りおよび書き込みパフォーマンスが向上したり低下したりします。アプリケーションによって、より適している RAID レベルがあります。
- コスト効率 — RAID ボリュームに関連付けられている冗長データまたはパリティ情報を維持するには、追加のディスク容量が必要です。データが一時的なものである、簡単に複製できる、不可欠ではない、といった場合は、データ冗長性のためのコスト増は妥当とは言えません。
- 平均故障間隔（MTBF）— データ冗長性を維持するために追加ディスクを使用することは、常にディスク障害の可能性を増加させます。冗長データが必要な状況ではこのオプションは避けられませんが、社内のシステムサポートスタッフの仕事量は増加すると考えられます。
- ボリューム — ボリュームは、単一ディスクによる非 RAID 仮想ディスクを指します。O-ROM<Ctrl> <r> などの外部ユーティリティを使ってボリュームを作成できます。Storage Management はボリュームの作成をサポートしません。ただし、十分な空き容量がある場合は、ボリュームを表示し、これらのボリュームからドライブを使って新しいボリュームディスクや既存の仮想ディスクの Online Capacity Expansion（OCE）を作成できます。

RAID レベルの選択

RAID を使用して、複数のディスクのデータストレージをコントロールすることができます。それぞれの RAID レベルまたは連結には異なるパフォーマンスとデータ保護機能があります。

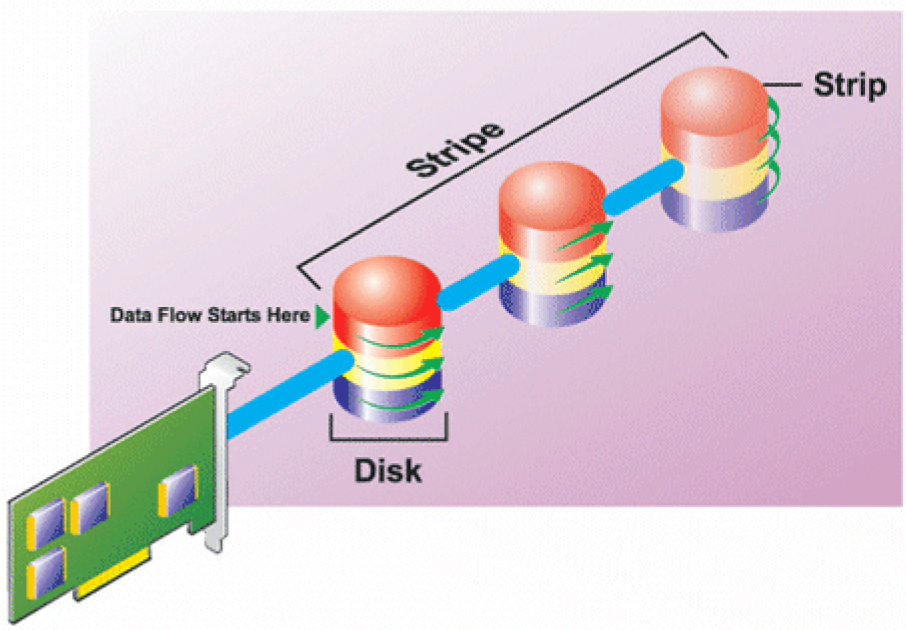
メモ: H3xx PERC コントローラは RAID レベル 6 および 60 をサポートしません。

各 RAID レベルでデータを保存する方法と、それぞれのパフォーマンスおよび保護機能について次のトピックで説明します。

- RAID レベル 0（ストライピング）
- RAID レベル 1（ミラーリング）
- RAID レベル 5（分散パリティを用いたストライピング）
- RAID レベル 6（追加された分散パリティを用いたストライピング）
- RAID レベル 50（RAID 5 セット全体へのストライピング）
- RAID レベル 60（RAID 6 セット全体へのストライピング）
- RAID レベル 10（ミラーセット全体へのストライピング）

RAID レベル 0（ストライピング）

RAID 0 はデータのストライピングを使用します。つまり複数の物理ディスクにわたり同じサイズのセグメントにデータを書き込みます。RAID 0 はデータの冗長性を提供しません。

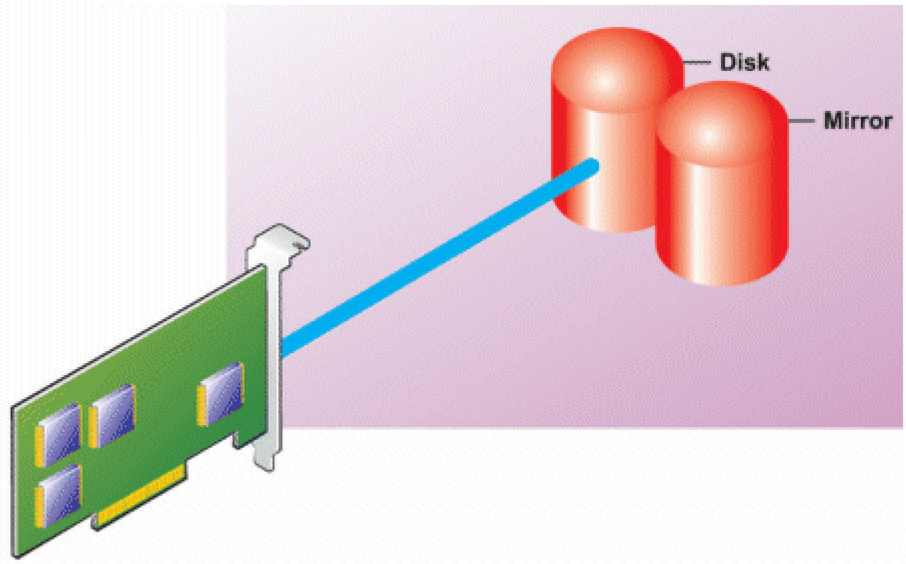


RAID 0 の特徴

- *n* 個のディスクを、(最小ディスクサイズ) * *n* 個分のディスク容量を備えた 1 つの大容量仮想ディスクとしてまとめます。
- データは各ディスクに交互に保存されます。
- 冗長データは保存されません。1 つのディスクに障害が発生すると大容量仮想ディスクにもエラーが発生し、データを再構築する方法はありません。
- 読み書きのパフォーマンスが向上します。

RAID レベル 1 (ミラーリング)

RAID 1 は冗長データを維持する最もシンプルな方式です。RAID 1 では、データは 1 台または複数台の物理ディスクにミラー化 (複製) されます。物理ディスクに障害が発生した場合、ミラーの反対側からのデータを使用してデータを再構築することができます。



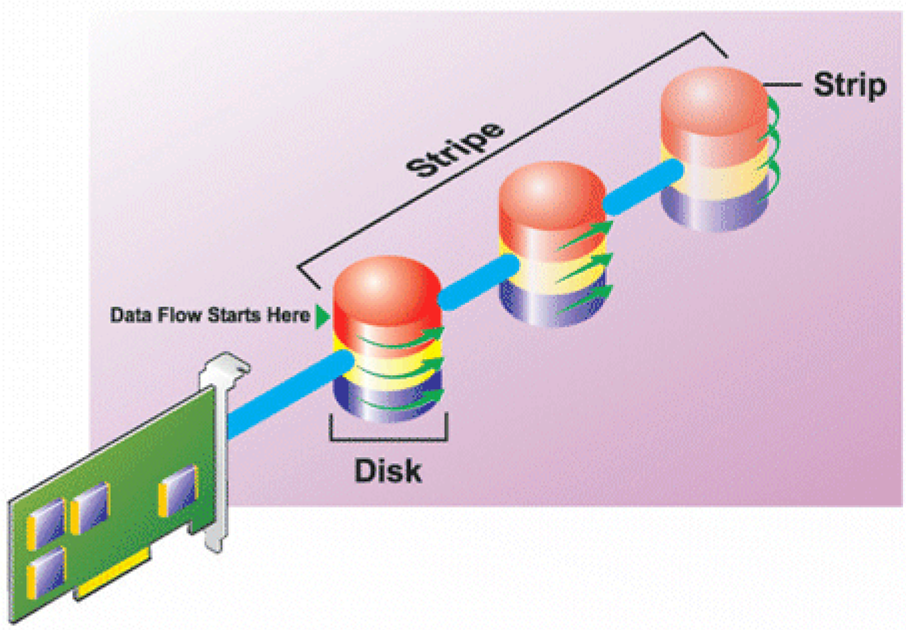
RAID 1 の特徴

- *n* + *n* ディスクを *n* ディスクの容量を持つ 1 つの仮想ディスクとしてグループ化します。Storage Management で現在サポートされているコントローラでは、RAID 1 の作成時に 2 つのディスクを選択できます。これらのディスクはミラー化されるため、ストレージの総容量はディスク 1 つ分に等しくなります。
- データは両方のディスクに複製されます。
- いずれかのディスクで障害が発生しても、仮想ディスクは継続して機能します。データは障害のあったディスクのミラーから読み取られます。

- 読み取りパフォーマンスが向上しますが、書き込みパフォーマンスは若干低下します。
- 冗長性でデータを保護します。
- RAID 1 では冗長性なしでデータを保存するのに必要なディスク数の 2 倍のディスクを使用するため、ディスク容量の点ではより高価です。

RAID レベル 5（分散パリティを用いたストライピング）

RAID 5 は、データのストライピングをパリティ情報と組み合わせることでデータの冗長性を提供します。物理ディスクをパリティ専用に割り当てるのではなく、パリティ情報は物理グループ内のすべての物理ディスクにストライピングされます。

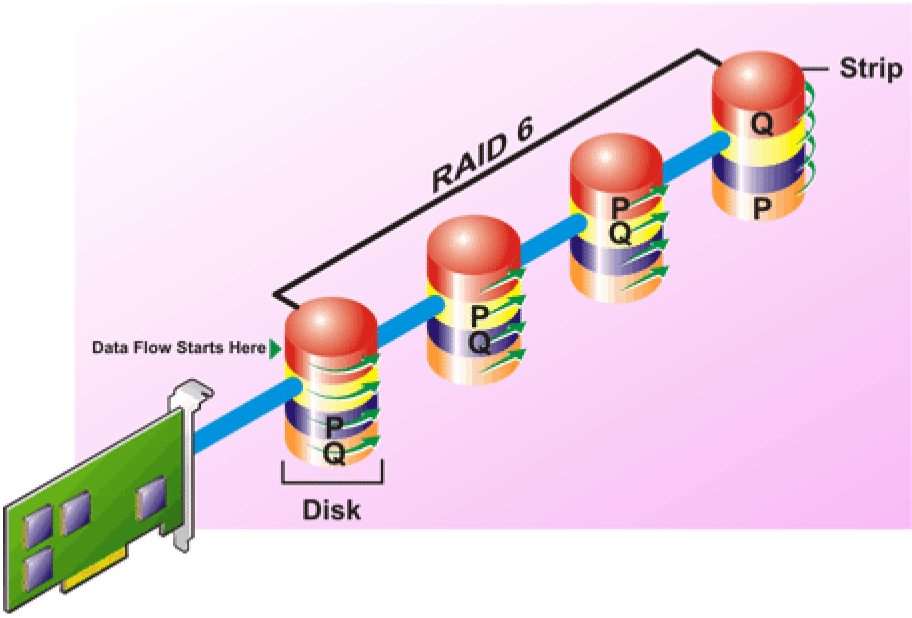


RAID 5 の特徴

- *n* 個のディスクを（*n*-1）のディスクの容量を持つ 1 つの大容量仮想ディスクとしてグループ化します。
- 冗長情報（パリティ）はすべてのディスクに交互に保存されます。
- ディスクに障害が発生すると、仮想ディスクはまだ機能しますが、劣化状態で動作します。データは障害の発生していないディスクから再構築されます。
- 読み込みパフォーマンスが向上しますが、書き込みパフォーマンスは低下します。
- 冗長性でデータを保護します。

RAID レベル 6（追加の分散パリティを用いたストライピング）

RAID 6 は、データのストライピングをパリティ情報と組み合わせることでデータの冗長性を提供します。RAID 5 と同様、パリティは各ストライプに分散されます。ただし RAID 6 では追加の物理ディスクを使用して、ディスクグループ内の各ストライプがパリティ情報を持つ 2 つのディスクブロックを維持するという方法でパリティを維持します。追加パリティは、2 つのディスクに障害が発生した場合にデータを保護します。次の図には、2 セットのパリティ情報が **P** および **Q** として示されています。



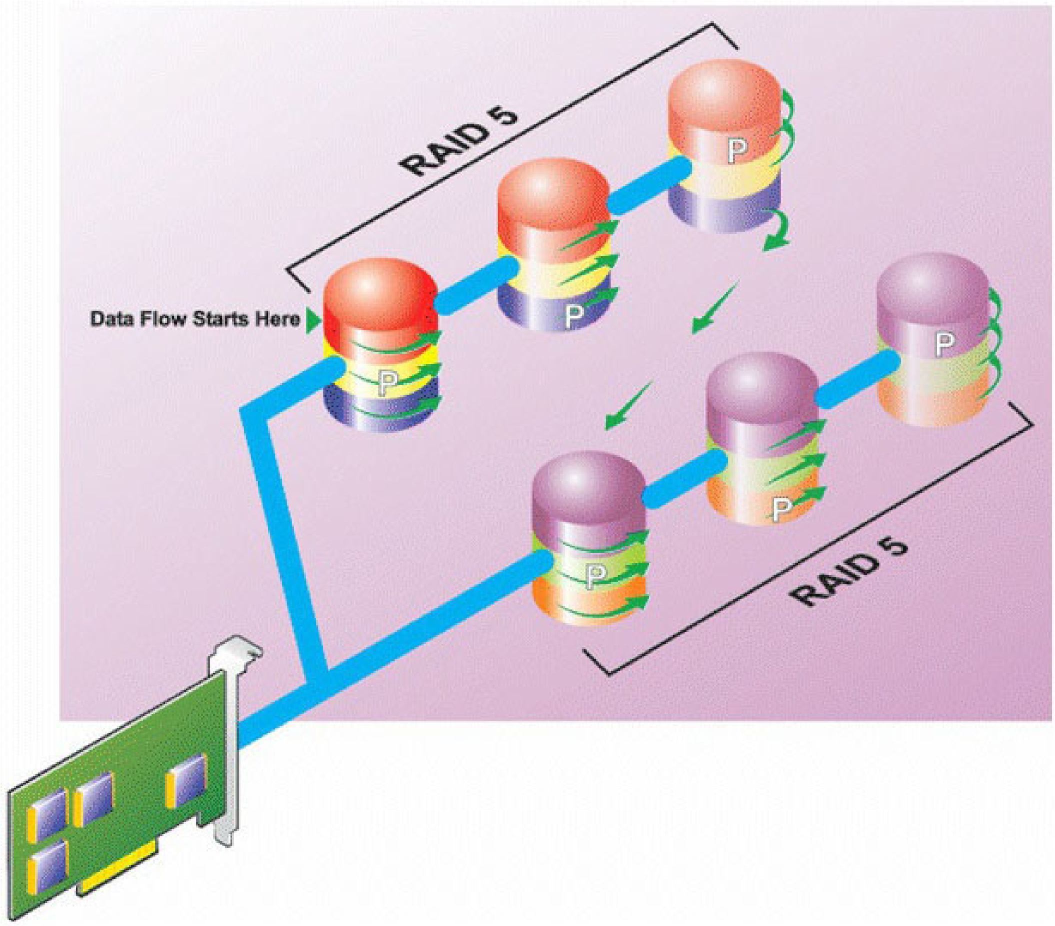
RAID 6 の特徴

- *n* 個のディスクを（*n*-2）のディスクの容量を持つ 1 つの大容量仮想ディスクとしてグループ化します。
- 冗長情報（パリティ）はすべてのディスクに交互に保存されます。
- 仮想ディスクは､最大 2 つのディスク障害が発生するまで機能します。データは障害の発生していないディスクから再構築されます。
- 読み込みパフォーマンスが向上しますが、書き込みパフォーマンスは低下します。
- データ保護の冗長性は強化されます。
- パリティには、1 スパンあたり 2 つのディスクが必要です。RAID 6 はディスク容量の点でより高価です。

RAID レベル 50（RAID 5 セット全体へのストライピング）

RAID 50 は複数の物理ディスクに分けてストライピングを行います。たとえば、3 つの物理ディスクで実装された RAID 5 ディスクグループがさらに 3 つの物理ディスク実装されたディスクグループへと継続されると RAID 50 になります。

ハードウェアで直接サポートされていなくても RAID 50 を実装することは可能です。このような場合、複数の RAID 5 仮想ディスクを実装してから RAID 5 ディスクをダイナミックディスクに変換します。続いて、すべての RAID 5 仮想ディスクに分散するダイナミックボリュームを作成します。

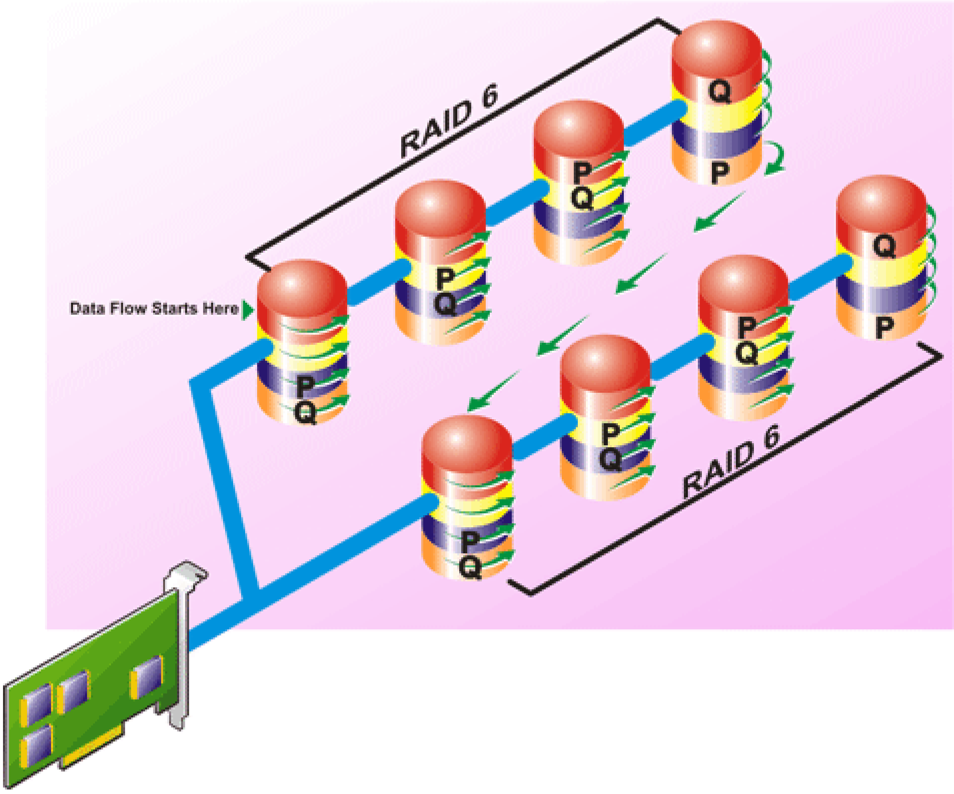


RAID 50 の特徴

- *n***s* のディスクを *s**（*n*-1）ディスクの容量を持つ 1 つの大容量仮想ディスクとしてグループ化します。ここで *s* はスパンの数を、*n* は各スパンの中のディスク数を表します。
- 冗長情報（パリティ）は、各 RAID 5 スパンの各ディスクに交互に保存されます。
- 読み込みパフォーマンスが向上しますが、書き込みパフォーマンスは低下します。
- 標準 RAID 5 と同量のパリティ情報が必要です。
- データはすべてのスパンにストライプされます。RAID 50 はディスク容量の点でより高価です。

RAID レベル 60（RAID 6 セット全体へのストライピング）

RAID 60 は、RAID 6 として構成された複数の物理ディスクに分けてストライピングします。たとえば、4 つの物理ディスクを使用して実装しさらに 4 つの物理ディスクを持つディスクグループを使用して続行する RAID 6 ディスクグループは、RAID 60 になります。

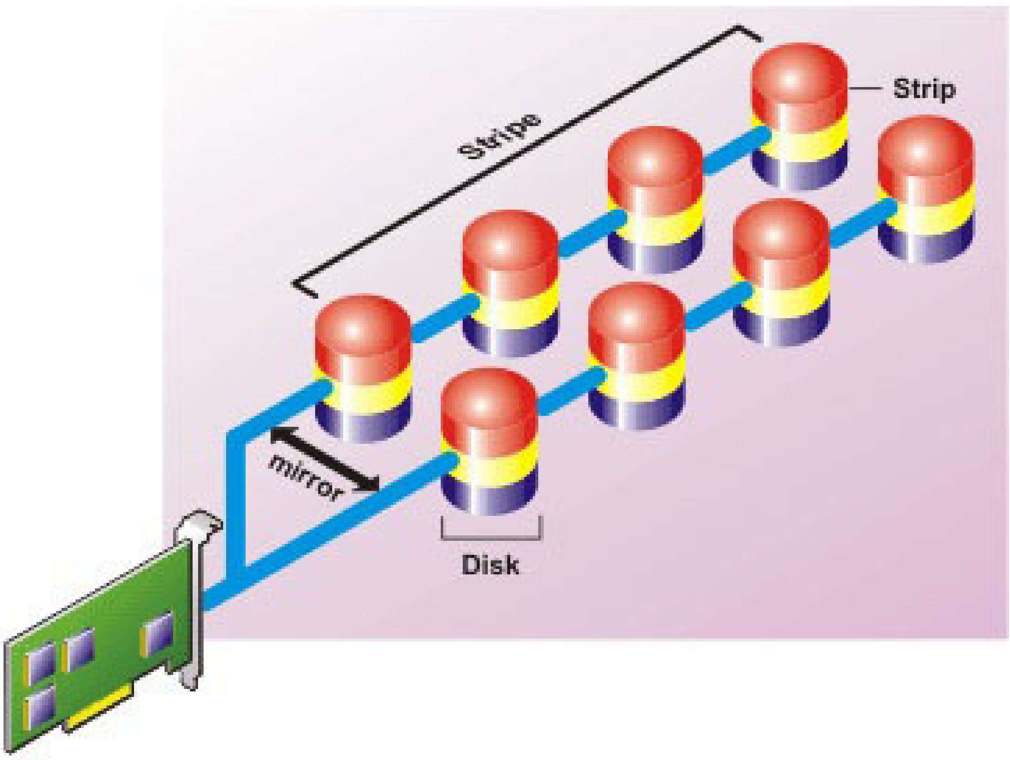


RAID 60 の特徴

- *n*s* のディスクを *s**(*n*-2)ディスクの容量を持つ 1 つの仮想ディスクとしてグループ化します。ここで *s* はスパンの数を、*n* は各スパンの中のディスク数を表します。
- 冗長情報(パリティ)は、各 RAID 6 スパンのすべてのディスクに交互に保管されます。
- 読み込みパフォーマンスが向上しますが、書き込みパフォーマンスは低下します。
- 冗長性の向上によって、RAID 50 よりも優れたデータ保護を提供します。
- RAID 6 と同量に比例するパリティ情報が必要です。
- パリティには、1 スパンあたり 2 つのディスクが必要です。RAID 60 はディスク容量の点でより高価です。

RAID レベル 10(ストライプ化ミラー)

RAB は RAID レベル 10 を RAID レベル 1 の実装とみなします。RAID 10 は物理ディスクのミラーリング(RAID 1)とデータストライピング(RAID 0)の組み合わせです。RAID 10 では、データは複数の物理ディスクに分かれてストライプされます。ストライプされたディスクグループは別の物理ディスクセットにミラーされます。RAID 10 は*ストライプのミラー*と考えることができます。



RAID 10 の特徴

- *n* 個のディスクを (*n*/2) ディスクの容量を持つ 1 つの大容量仮想ディスクとしてグループ化します。ここで *n* は偶数を表します。
- データのミラーイメージは物理ディスクのセット全体にストライピングされます。このレベルでは、ミラーリングを通じて冗長性が提供されます。
- いずれかのディスクで障害が起きても、仮想ディスクの動作は中断されません。データはミラーリングされた障害の発生していないディスクのペアから読み取られます。
- 読み取りおよび書き込みパフォーマンスが向上します。
- 冗長性でデータを保護します。

RAID レベルパフォーマンスの比較

次の表は、最も一般的な RAID レベルに関するパフォーマンスの特徴を比較したものです。この表は、RAID レベルを選択する際の一般的な指針です。使用する環境条件を評価した後で RAID レベルを選択してください。

表 33. RAID レベルパフォーマンスの比較

RAID レベル	データの可用性	読み取りパフォーマンス	書き込みパフォーマンス	再構築パフォーマンス	必要な最小ディスク数	使用例
RAID 0	なし	大変良好	大変良好	該当なし	N	非重要データ。
RAID 1	優秀	大変良好	良	良	2N (N = 1)	小規模のデータベース、データベースログ、および重要情報。
RAID 5	良	連続読み取り：良。トランザクション読み取り：大変良好	ライトバックキャッシュを使用しない限り普通	普通	N + 1(N = ディスクが最低限 2 台)	データベース、および読み取り量の多いトランザクションに使用。

表 33. RAID レベルパフォーマンスの比較 （続き）

RAID レベル	データの可用性	読み取りパフォーマンス	書き込みパフォーマンス	再構築パフォーマンス	必要な最小ディスク数	使用例
RAID 10	優秀	大変良好	普通	良	2N x X	データの多い環境（大きいレコードなど）。
RAID 50	良	大変良好	普通	普通	N + 2(N = 最低限 4 台）	中規模のトランザクションまたはデータ量が多い場合に使用。
RAID 6	優秀	連続読み取り：良。トランザクション読み取り：大変良好	ライトバックキャッシュを使用しない限り普通	不良	N + 2(N = ディスクが最低限 2 台）	重要情報。データベース、および読み取り量の多いトランザクションに使。用
RAID 60	優秀	大変良好	普通	不良	X x (N + 2)（N = 最低限 2 台）	重要情報。中規模のトランザクションまたはデータ量が多い場合に使用。
N = 物理ディスク数 X = RAID セットの数						

対応コントローラ

対応 RAID コントローラ

iDRAC インタフェースは次の PERC 9 コントローラをサポートしています。

- PERC H830
- PERC H730P
- PERC H730
- PERC H330

iDRAC インタフェースは次の PERC8 コントローラをサポートしています。

- PERC H810
- PERC H710P
- PERC H710
- PERC H310

iDRAC インタフェースは次のモジュラー PERC コントローラをサポートしています。

- PERC FD33xS
- PERC FD33xD

メモ: PERC FD33xS および PERC FD33xD コントローラでのコントローラモードの設定および変更の詳細については、**dell.com/support/manuals** で入手できる『Dell Chassis Management Controller（CMC）for Dell PowerEdge FX2/FX2s バージョン 1.2 リリースノート』を参照してください。

サポートされる非 RAID コントローラ

iDRAC インタフェースは、12 Gbps SAS HBA 外付けコントローラ、および HBA330 内蔵コントローラをサポートし、HBA330 内蔵コントローラに対してのみ SATA ドライブをサポートします。

対応エンクロージャ

iDRAC は MD1200、MD1220、MD1400、および MD1420 のエンクロージャをサポートします。

メモ: HBA コントローラに接続されている Redundant Array of Inexpensive Disks（RBODS）はサポートされません。

ストレージデバイスの対応機能のサマリ

次の表に、iDRAC 経由でストレージデバイスによってサポートされる機能を示します。

メモ: 取り外し準備やコンポーネントの点滅または点滅解除は、HHHL PCIe SSD カードでは使用できません。

機能名	PERC 9 コントローラ						PERC 8 コントローラ				PCIe SSD
	H830	H 730P	H730	H330	FD33xS	FD33xD	H810	H710P	H710	H310	
グローバルホットスペアとしての物理ディスクの割り当てまたは割り当て解除	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
仮想ディスクの作成	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
仮想ディスクキャッシュポリシーの編集	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
仮想ディスク整合性チェック	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
整合性チェックのキャンセル	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	適用なし	適用なし	適用なし	適用なし	適用なし
仮想ディスクの初期化	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
初期化のキャンセル	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	適用なし	適用なし	適用なし	適用なし	適用なし
仮想ディスクの暗号化	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
専用ホットスペアの割り当てと割り当て解除	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
仮想ディスクの削除	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
巡回読み取りモードの設定	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
未設定領域の巡回読み取り	リアルタイム（ウェブイ	リアルタイム（ウェブイ	リアルタイム（ウェブインタフェ	リアルタイム（ウェブインタフェ	リアルタイム（ウェブインタフェ	リアルタイム（ウェブインタフェ	ステージング（ウェブインタ	ステージング（ウェブインタフェースのみ）	ステージング（ウェブインタ	ステージング（ウェブインタ	適用なし

機能名	PERC 9 コントローラ						PERC 8 コントローラ				PCIe SSD
	H830	H 730P	H730	H330	FD33xS	FD33xD	H810	H710P	H710	H310	
	ンタフェースのみ）	ンタフェースのみ）	ースのみ）	ースのみ）	ースのみ）	ースのみ）	フェースのみ）		フェースのみ）	フェースのみ）	
整合性チェックモード	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
コピーバックモード	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
ロードバランスモード	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
整合性チェック率	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
再構築率	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
BGI 率	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
再構成率	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
外部設定のインポート	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
外部設定の自動インポート	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
外部設定のクリア	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
コントローラ設定のリセット	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
セキュリティキーの作成または変更	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	ステージング	ステージング	ステージング	ステージング	適用なし
PCIe SSD デバイスのインベントリとリモートでの正常性の監視	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	リアルタイム
PCIe SSD を取り外す準備。	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	リアルタイム
データを安全に消去	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	ステージング

機能名	PERC 9 コントローラ						PERC 8 コントローラ				PCIe SSD
	H830	H 730P	H730	H330	FD33x S	FD33x D	H810	H710P	H710	H310	
バックプレーンモードの設定	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	適用なし	適用なし	適用なし	適用なし	適用なし
コンポーネント LED の点滅または点滅解除	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
コントローラモードの切り替え	ステージング	ステージング	ステージング	ステージング	ステージング	ステージング	適用なし	適用なし	適用なし	適用なし	適用なし

ストレージデバイスのインベントリと監視

iDRAC ウェブインタフェースを使用して、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。

- RAID コントローラ、非 RAID コントローラ、および PCIe エクステンダ
- 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
- バッテリー

ただし、RACADM および 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。

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 Lifecycle ログに記録されます。

メモ: PSU ケーブルを取り外す間にシステムにエンクロージャビューの WSMAN コマンドを列挙する場合、エンクロージャビューのプライマリステータスは、**警告** ではなく **正常** として報告されます。

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ログ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、主要なストレージコンポーネントの階層的な物理コンテインメントを表示します。
- ［概要］>［ストレージ］>［物理ディスク］>［プロパティ］と移動して、物理ディスク情報を表示します。［物理ディスクプロパティ］ページが表示されます。
- ［概要］>［ストレージ］>［仮想ディスク］>［プロパティ］と移動して、仮想ディスク情報を表示します。［仮想ディスクプロパティ］ページが表示されます。
- ［概要］>［ストレージ］>［コントローラ］>［プロパティ］と移動して、RAID コントローラ情報を表示します。［コントローラプロパティ］ページが表示されます。
- ［概要］>［ストレージ］>［エンクロージャ］>［プロパティ］と移動して、エンクロージャ情報を表示します。［エンクロージャプロパティ］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、『iDRAC 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表示するには、`storage` コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドライン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バックプレーンの監視

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 Settings.System の概要] ページが表示されます。[バックプレーンインベントリ] セクションにバックプレーン情報が表示されます。フィールドの詳細については、『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。

ストレージデバイスのトポロジの表示

主要ストレージコンポーネントの階層型物理コンテインメントビューを表示できます。つまり、コントローラ、コントローラに接続されているエンクロージャ、および各エンクロージャに収容されている物理ディスクへのリンクが一覧表示されます。コントローラに直接接続されている物理ディスクも表示されます。

ストレージデバイスのトポロジを表示するには、[概要] > [ストレージ] > [トポロジ] をクリックします。**トポロジ** ページは、システム内のストレージコンポーネントを階層的に表したものです。

各コンポーネントの詳細を表示するには、対応するリンクをクリックします。

物理ディスクの管理

物理ディスクについて、次のことを実行できます。

- 物理ディスクプロパティの表示
- グローバルホットスペアとしての物理ディスクの割り当てまたは割り当て解除
- RAID 対応ディスクへの変換
- 非 RAID ディスクへの変換
- LED の点滅または点滅解除

関連概念

ストレージデバイスのインベントリと監視 、p. 196
グローバルホットスペアとしての物理ディスクの割り当てまたは割り当て解除 、p. 197

グローバルホットスペアとしての物理ディスクの割り当てまたは割り当て解除

グローバルホットスペアは、ディスクグループの一部になっている未使用のバックアップディスクです。ホットスペアはスタンバイモードになります。仮想ディスクで使用されている物理ディスクに障害が発生すると、割り当てられたホットスペアが有効になり、システムに割り込みされたり介入要求されることなく、故障した物理ディスクと置換されます。ホットスペアが有効になると、故障した物理ディスクを使用していたすべての冗長仮想ディスクのデータが再構築されます。

メモ: iDRAC v2.30.30.30 以降からは、仮想ディスクが作成されていないときにグローバルホットスペアを追加することができます。

ホットスペアの割り当ては、ディスクの割り当てを解除し、必要に応じて別のディスクを割り当てることで変更できます。複数の物理ディスクをグローバルホットスペアとして割り当てることができます。

グローバルホットスペアの割り当てと割り当て解除は手動で行う必要があります。グローバルホットスペアは特定の仮想ディスクには割り当てられません。仮想ディスクにホットスペアを割り当てる (仮想ディスク内でエラーが発生する物理ディスクの代替となります) 場合は、「専用ホットスペアの割り当てまたは割り当て解除」を参照してください。

仮想ディスクを削除する場合、コントローラに関連する最後の仮想ディスクが削除されると、割り当てられたグローバルホットスペアがすべて自動的に割り当て解除される可能性があります。

設定をリセットすると、仮想ディスクが削除され、すべてのホットスペアの割り当てが解除されます。

ホットスペアに関連したサイズ要件とその他の考慮事項を把握しておいてください。

物理ディスクをグローバルホットスペアとして割り当てる前に、次のことを行います。

- Lifecycle Controller が有効になっていることを確認します。
- 準備完了状態のディスクドライブがない場合は、追加ディスクドライブを挿入し、そのドライブが準備完了状態であることを確認してください。

- 仮想ディスクが存在しない場合は、少なくとも 1 つの仮想ディスクを作成します。
- 物理ディスクが非 RAID モードである場合は、iDRAC ウェブインタフェース、RACADM、WS-MAN などの iDRAC インタフェースを使用する、または <Ctrl+R> を使用して RAID モードに変換します。

保留中の操作に追加 モードで物理ディスクをグローバルホットスペアとして割り当てると、保留中の操作が作成されますが、ジョブは作成されません。その後、同じディスクをグローバルホットスペアとして割り当てようとすると、保留中のグローバルホットスペアの割り当て操作がクリアされます。

保留中の操作に追加 モードで物理ディスクのグローバルホットスペアとしての割り当てを解除すると、保留中の操作が作成されますが、ジョブは作成されません。その後、同じディスクをグローバルホットスペアとして割り当てようとすると、保留中のグローバルホットスペアの割り当て解除操作がクリアされます。

ウェブインタフェースを使用したグローバルホットスペアの割り当てまたは割り当て解除

物理ディスクドライブのためのグローバルホットスペアを割り当てる、または割り当て解除するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、[概要] > [ストレージ] > [物理ディスク] > [セットアップ] と移動します。
   [物理ディスクのセットアップ] ページが表示されます。
2. [コントローラ] ドロップダウンメニューから、コントローラを選択して関連する物理ディスクを表示します。
3. グローバルホットスペアとして割り当てるには、[アクション - すべてに割り当て] 列のドロップダウンメニューから、1 つまたは複数の物理ディスクに対して [グローバルホットスペア] を選択します。
4. ホットスペアの割り当てを解除するには、[アクション - すべてに割り当て] 列のドロップダウンメニューから、1 つまたは複数の物理ディスクに対して [ホットスペアの割り当て解除] を選択します。
5. **操作モードの適用** ドロップダウンメニューから、設定を適用するタイミングを選択します。
6. **適用** をクリックします。
   選択した操作モードに基づいて、設定が適用されます。

関連タスク

ウェブインタフェースを使用した操作モードの選択、p. 220

RACADM を使用したグローバルホットスペアの割り当てまたは割り当て解除

`storage` コマンドを使用して、タイプをグローバルホットスペアとして指定します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンド ライン リファレンス ガイド*』を参照してください。

関連タスク

RACADM を使用した操作モードの選択、p. 221

物理ディスクの RAID または非 RAID モードへの変換

物理ディスクを RAID モードに変換することにより、ディスクですべての RAID 操作が可能になります。ディスクが非 RAID モードである場合、そのディスクは未設定の良好なディスクとは異なりオペレーティングシステムに公開され、ダイレクトパススルーモードで使用されます。

物理ディスクドライブは、次の手順を実行することによって RAID または非 RAID モードに変換することができます。

- iDRAC ウェブインタフェース、RACADM、または WS-MAN などの iDRAC インタフェースを使用する。
- サーバーの再起動中に Ctrl+R キーを押し、必要なコントローラを選択する。

メモ: モードの変換は、HBA モードで実行されている PERC ハードウェアコントローラではサポートされません。

メモ: PERC 8 コントローラに対する非 RAID モードへの変換は、PERC H310 および H330 コントローラに対してのみサポートされます。

メモ: PERC コントローラに接続されている物理ドライブが非 RAID モードである場合、iDRAC GUI、RACADM、および WS-MAN などの iDRAC インタフェースに表示されるディスクのサイズは、ディスクの実際のサイズよりわずかに小さくなることがあります。ただし、ディスクの全容量を使用してオペレーティングシステムを導入することができます。

iDRAC ウェブインタフェースを使用した物理ディスクの RAID 対応または非 RAID モードへの変換

物理ディスクを RAID モードまたは非 RAID モードに変換するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、[概要] > [ストレージ] > [物理ディスク] > [セットアップ] とクリックします。
   [プロパティ] ページが表示されます。
2. [コントローラ] ドロップダウンメニューから、コントローラを選択します。
   選択したコントローラに関連付けられている物理ディスクが表示されます。
3. [アクション - すべてに割り当て] ドロップダウンメニューから、すべてのディスクに対して必要なオプション ([RAID に変換] または [非 RAID に変換]) を選択するか、[アクション] ドロップダウンメニューから特定のディスクに対するオプションを選択します。
4. [操作モードの適用] ドロップダウンメニューから、設定を適用するタイミングを選択します。
5. [適用] をクリックします。
   これらの設定は、操作モードで選択したオプションに基づいて適用されます。

RACADM を使用した物理ディスクの RAID 対応または非 RAID モードへの変換

RAID モードに変換するか、または非 RAID モードに変更するかに応じて、次の RACADM コマンドを使用します。

- RAID モードに変換するには、`racadm storage converttoraid` コマンドを使用します。
- 非 RAID モードに変換するには、`racadm storage converttononraid` コマンドを使用します。

詳細については、**dell.com/esmmanuals** にある『iDRAC RACADM コマンドラインリファレンスガイド』を参照してください。

仮想ディスクの管理

仮想ディスクに対して次の操作を実行できます。

- 作成
- 削除
- ポリシーの編集
- 初期化
- 整合性チェック
- 整合性チェックのキャンセル
- 仮想ディスクの暗号化
- 専用ホットスペアの割り当てまたは割り当て解除
- 仮想ディスクの点滅および点滅解除

メモ: PERC コントローラ BIOS、Human Interface Infrastructure (HII)、および Dell OpenManage Server Administrator (OMSA) を介して自動設定が有効になっている場合は、192 台の仮想ディスクを管理および監視できます。

関連概念

仮想ディスクの作成 、p. 200
仮想ディスクキャッシュポリシーの編集 、p. 201
仮想ディスクの削除 、p. 202
仮想ディスク整合性のチェック 、p. 202
仮想ディスクの初期化 、p. 202
仮想ディスクの暗号化 、p. 203
専用ホットスペアの割り当てまたは割り当て解除 、p. 203
ウェブインタフェースを使用した仮想ディスクの管理 、p. 203
RACADM を使用した仮想ディスクの管理 、p. 204

仮想ディスクの作成

RAID 機能を実装するには、仮想ディスクを作成する必要があります。仮想ディスクとは、RAID コントローラによって 1 つまたは複数の物理ディスクから作成されたストレージを指します。仮想ディスクは複数の物理ディスクから作成されますが、オペレーティングシステムはこれを単一のディスクとして認識します。

仮想ディスクを作成する前に、「仮想ディスクを作成する前の考慮事項」を理解しておく必要があります。

RERC コントローラに接続された物理ディスクを使用して、仮想ディスクを作成することができます。仮想ディスクを作成するには、サーバー制御ユーザーの権限を持っている必要があります。最大 64 の仮想ドライブと、同じドライブ グループで最大 16 の仮想ドライブのグループを作成できます。

次の場合は、仮想ディスクを作成できません。

- 仮想ディスクを作成するために物理ディスクドライブを利用できない。追加の物理ディスクドライブを取り付けてください。
- コントローラ上に作成できる仮想ディスクの最大数に達している。少なくとも 1 つの仮想ディスクを削除してから、新しい仮想ディスクを作成する必要があります。
- ドライブグループがサポートする仮想ディスクの最大数に達している。選択したグループから仮想ディスクを 1 つ削除した後で、新しい仮想ディスクを作成する必要があります。
- 選択したコントローラ上でジョブが現在実行中、またはスケジュールされている。このジョブが完了するまで待つ必要があります。または、このジョブを削除してから新しい操作を試行することができます。スケジュールされたジョブのステータスは、ジョブキュー ページで表示および管理することができます。
- 物理ディスクが非 RAID モードである。iDRAC ウェブインタフェース、RACADM、WS-MAN などの iDRAC インタフェースを使用する、または <Ctrl+R> を使用して RAID モードに変換する必要があります。

メモ: 保留中の操作に追加 モードで仮想ディスクを作成し、ジョブが作成されない場合、またその後に仮想ディスクを削除した場合は、仮想ディスクに対する保留中の作成操作がクリアされます。

仮想ディスクを作成する前の考慮事項

仮想ディスクを作成する前に、次を考慮します。

- コントローラ上に保存されない仮想ディスク名 - 作成する仮想ディスクの名前は、コントローラ上に保存されません。異なるオペレーティングシステムを使って再起動した場合、新しいオペレーティングシステムが独自の命名規則を使って仮想ディスク名を変更することがあります。
- ディスクグループとは、1 つ、または複数の仮想ディスクが作成される RAID コントローラに接続されたディスクを論理的にグループ化したものです。その際、ディスクグループのすべての仮想ディスクはディスクグループのすべての物理ディスクを使用します。現在の実装では、論理デバイス作成の際に、混在したディスクグループのブロックがサポートされています。
- 物理ディスクはディスクグループにまとめられるので、1 つのディスクグループで RAID レベルが混在することはありません。
- 仮想ディスクに含める物理ディスク数には制限があります。これらの制限はコントローラによって異なります。仮想ディスクの作成で、コントローラは一定数のストライプとスパン（物理ディスクのストレージを組み合わせる方法）をサポートします。ストライプとスパンの合計数が制限されているため、使用できる物理ディスク数も限られます。ストライプとスパンの制限によって、RAID レベルは次のような影響を受けます。
  - 最大スパン数は、RAID 10 、RAID 50、および RAID 60 に影響します。
  - 最大ストライプ数は、RAID 0、RAID 5、RAID 50、RAID 6 および RAID 60 に影響します。
  - 1 つのミラー内の物理ディスク数は常に 2 です。これは RAID 1 および RAID 10 に影響します。
- PCIe SSD 上で仮想ディスクを作成できません。

ウェブインタフェースを使用した仮想ディスクの作成

仮想ディスクを作成するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、[概要] > [ストレージ] > [仮想ディスク] > [作成] を選択します。
   [仮想ディスクの作成] ページが表示されます。
2. [設定] セクションで、次の手順を実行します。
   a. 仮想ディスクの名前を入力します。
   b. [コントローラ] ドロップダウンメニューから、仮想ディスクを作成するコントローラを選択します。
   c. [レイアウト] ドロップダウンメニューから、仮想ディスクの RAID レベルを選択します。
      コントローラでサポートされている RAID レベルのみがドロップダウンメニューに表示されます。また、RAID レベルは、使用可能な物理ディスクの合計台数に基づいて使用できます。
   d. [メディアタイプ]、[ストライプサイズ]、[読み取りポリシー]、[書き込みポリシー]、[ディスクキャッシュポリシー]、[T10 PI 機能] を選択します。

コントローラでサポートされている値のみが、これらのプロパティのドロップダウンメニューに表示されます。

e. ［容量］フィールドに、仮想ディスクのサイズを入力します。

ディスクを選択すると、最大サイズが表示され、更新されます。

f. ［スパン数］フィールドは、選択した物理ディスク（手順 3）に基づいて表示されます。この値を設定することはできません。これは、複数の RAID レベルを選択した後で自動的に計算されます。RAID 10 を選択した場合、およびコントローラが不均等 RAID 10 をサポートしている場合、スパン数の値は表示されません。コントローラは、適切な値を自動的に設定します。

3. **物理ディスクの選択** セクションでは、物理ディスクの数を選択します。

   フィールドの詳細については、『iDRAC オンラインヘルプ』を参照してください。

4. **操作モードの適用** ドロップダウンメニューから、設定を適用するタイミングを選択します。
5. ［仮想ディスクの作成］をクリックします。

   選択した［操作モードの適用］に基づいて、設定が適用されます。

RACADM を使用した仮想ディスクの作成

`racadm storage createvd` コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインリファレンスガイド*』を参照してください。

仮想ディスクキャッシュポリシーの編集

仮想ディスクの読み取り、書き込み、またはディスクキャッシュポリシーを変更することができます。

メモ: コントローラによって、サポートされない読み取りまたは書き込みポリシーがあります。そのため、ポリシーを適用すると、エラーメッセージが表示されます。

読み取りポリシーは、コントローラがデータを探すときに、仮想ディスクの連続セクタを読み取るかどうかを指定します。

- **適応先読み** — 2 件の最新読み取り要求がディスクの連続セクタにアクセスした場合にのみ、コントローラは先読みを開始します。後続の読み取り要求がディスクのランダムセクタにアクセスする場合、コントローラは先読みなしのポリシーに戻ります。コントローラは読み取り要求がディスクの連続セクタにアクセスしているかを引き続き評価し、必要に応じて先読みを開始します。

  メモ: 従来世代の PERC コントローラは、［先読みなし］、［先読み］、および［適応先読み］の読み取りポリシー設定をサポートします。PERC 8 および PERC 9 では、［先読み］および［適応型先読み］設定の機能が、コントローラレベルで同等となります。 下位互換性を保つ目的で、一部の システム管理インタフェースおよび PERC 8 と 9 のコントローラで、読み取りポリシーの設定に［適応先読み］が許可されています。PERC 8 または PERC 9 で［先読み］または［適応型先読み］の設定が可能であっても、機能の違いはありません。

- **先読み** — コントローラはデータシーク時に仮想ディスクの連続セクタを読み取ります。データが仮想ディスクの連続セクタに書かれている場合、先読みポリシーによってシステムパフォーマンスが向上します。
- **先読みなし** — 先読みなしポリシーを選択すると、コントローラは先読みポリシーを使用しません。

書き込みポリシーは、コントローラが書き込み要求完了信号を、データがキャッシュに保存された後、またはディスクに書き込まれた後のどちらの時点で送信するかを指定します。

- **ライトスルー** — コントローラは、データがディスクドライブに書き込まれた後でのみ書き込み要求完了信号を送信します。ライトスルーキャッシュは、ディスクドライブにデータが無事に書き込まれた後にのみデータが利用可能になるとシステムが判断することから、ライトバックキャッシュよりも優れたデータセキュリティを提供します。
- **ライトバック** — コントローラは、データがコントローラのキャッシュに保存されたがディスクには書き込まれていない時点で、書き込み要求完了信号を送信します。ライトバックキャッシュは、後続の読み取り要求が、ディスクと比べてキャッシュからより素早くデータを取得できるため、パフォーマンスが向上します。ただし、ディスクへのデータ書き込みを阻むシステム障害の発生時に、データ損失が生じる可能性があります。他のアプリケーションでも、処置がデータがディスクにあると想定したときに、問題が発生する可能性があります。
- **ライトバック強制** — コントローラにバッテリが搭載されているかどうかに関係なく、書き込みキャッシュが有効になります。コントローラにバッテリが搭載されていない場合、強制ライトバックキャッシングが使用されると、電源障害時にデータの損失が発生する可能性があります。

ディスクキャッシュポリシーは、特定の仮想ディスクでの読み取りに適用されます。この設定は先読みポリシーには影響しません。

メモ:

- コントローラキャッシュのコントローラ不揮発性キャッシュおよびバッテリバックアップは、コントローラがサポートできる読み取りポリシーまたは書き込みポリシーに影響します。すべての PERC にバッテリとキャッシュが搭載されているとは限りません。

- 先読みおよびライトバックにはキャッシュが必要になります。つまり、コントローラにキャッシュがない場合は、ポリシーの値を設定することはできません。

  同様に、PERC にキャッシュがあってもバッテリがなく、ポリシーがキャッシュへのアクセスを必要とする設定になっている場合、ベースの電源がオフになるとデータロスが生じる恐れがあります。そのため、一部の PERC ではこのポリシーは許可されません。

  したがって、PERC に応じてポリシーの値が設定されます。

仮想ディスクの削除

仮想ディスクを削除すると、仮想ディスクに常駐するファイルシステムおよびボリュームなどの情報がすべて破壊され、コントローラの設定からその仮想ディスクが削除されます。仮想ディスクを削除する場合、コントローラに関連する最後の仮想ディスクが削除されと、割り当てられたグローバルホットスペアがすべて自動的に割り当て解除される可能性があります。ディスクグループの最後の仮想ディスクを削除すると、割り当てられている専用ホットスペアすべてが自動的にグローバルホットスペアになります。

仮想ディスクを削除するには、ログインおよびサーバー制御の権限を持っている必要があります。

この操作が許可されている場合、起動仮想ドライブを削除することができます。この操作はサイドバンドから実行されるもので、オペレーティングシステムには依存しません。そのため、仮想ドライブを削除する前に警告メッセージが表示されます。

仮想ディスクを削除した直後に、削除したディスクと特性がすべて同じ新規仮想ディスクを作成した場合、コントローラは最初の仮想ディスクが全く削除されなかったかのようにデータを認識します。このような状況では、新規仮想ディスクの作成後に古いデータが必要なければ、仮想ディスクを再初期化します。

仮想ディスク整合性のチェック

この操作は、冗長（パリティ）情報の正確さを検証します。このタスクは冗長仮想ディスクにのみ適用されます。必要に応じて、整合性チェックタスクで冗長データが再構築されます。仮想ドライブが低下状態の場合、整合性チェックを実行することで仮想ドライブを準備完了状態に戻すことができる場合があります。ウェブインタフェースまたは RACADM を使用して整合性チェックを実行できます。

整合性チェック操作をキャンセルすることもできます。整合性チェックのキャンセルは、リアルタイム操作です。

仮想ディスクの整合性をチェックするには、ログインおよびサーバー制御の権限を持っている必要があります。

メモ: 整合性チェックは、RAID0 モードでドライバをセットアップしている場合はサポートされません。

仮想ディスクの初期化

仮想ディスクの初期化では、ディスク上のすべてのデータが消去されますが、仮想ディスクの設定が変更されることはありません。仮想ディスクを使用するには、設定されている仮想ディスクを初期化する必要があります。

メモ: 既存の構成を再作成している時に仮想ディスクの初期化を行わないでください。

高速初期化または完全初期化を実行することも、初期化操作をキャンセルすることもできます。

メモ: 初期化のキャンセルはリアルタイム操作です。初期化のキャンセルには、RACADM ではなく iDRAC ウェブインタフェースのみを使用できます。

高速初期化

高速初期化操作は、仮想ディスクにあるすべての物理ディスクを初期化します。この操作によって、物理ディスクのメタデータがアップデートされ、すべてのディスク容量が今後の書き込み操作に使用できるようになります。この初期化タスクは、物理ディスク上の情報が消去されてないので迅速に終了しますが、物理ディスク上の情報は今後の書き込み操作で上書きされます。

高速初期化では、起動セクターとストライプ情報のみが削除されます。高速初期化は、時間の制約がある場合か、ハードドライブが新規または未使用である場合にのみ実行してください。高速初期化は完了までにあまり時間がかかりません（通常は 30～60 秒）。

注意: 高速初期化の実行中は既存のデータにアクセスできなくなります。

高速初期化タスクは物理ディスク上のディスクブロックにゼロを書き込みません。これは、高速初期化タスクが書き込み操作を実行しないためであり、それによってディスクの劣化が少なくなります。

仮想ディスクの高速初期化では、仮想ディスクの最初と最後の 8 MB が上書きされ、ブートレコードすべてまたはパーティション情報がクリアされます。操作完了にかかるのは 2～3 秒で、仮想ディスク再作成時に推奨されます。

バックグラウンド初期化は高速初期化の完了 5 分後に開始されます。

完全または低速初期化

完全初期化（低速初期化とも呼ばれます）操作は、仮想ディスクにあるすべての物理ディスクを初期化します。これにより、物理ディスクのメタデータがアップデートされ、すべての既存のデータとファイルシステムが消去されます。完全初期化は仮想ディスクの作成後に実行することができます。高速初期化操作と比較して、物理ディスクに問題がある場合、または不良ディスクブロックがあると思われる場合は完全初期化の使用が必要になることがあります。完全初期化操作は、不良ブロックを再マップし、すべてのディスクブロックにゼロを書き込みます。

仮想ディスクの完全初期化を実行した場合、バックグランド初期化は必要ありません。完全初期化の間、ホストは仮想ディスクにアクセスできません。完全初期化中にシステムを再起動すると、操作は中止され、バックグラウンド初期化プロセスが仮想ディスク上で開始されます。

前にデータが保存されていたドライブには、完全初期化を実行することが常に推奨されます。完全初期化は、1 GB あたり 1～2 分かかる場合があります。初期化の速度は、コントローラのモデル、ハードドライブの速度、およびファームウェアのバージョンによって異なります。

完全初期化タスクは 1 度に 1 台ずつ物理ディスクを初期化します。

メモ: 完全初期化は、リアルタイムでのみサポートされます。完全初期化をサポートするコントローラはほんの一部です。

仮想ディスクの暗号化

コントローラで暗号化が無効になっている場合（つまり、セキュリティキーが削除されている場合）、SED ドライブを使って作成された仮想ディスクの暗号化を手動で有効にします。コントローラで暗号化を有効にした後、仮想ディスクを作成すると、仮想ディスクは自動的に暗号化されます。仮想ディスクの作成時に有効な暗号化オプションを無効にした場合を除き、暗号化仮想ディスクとして自動的に設定されます。

暗号化キーを管理するには、ログインおよびサーバー制御の権限を持っている必要があります。

専用ホットスペアの割り当てまたは割り当て解除

専用ホットスペアは、仮想ディスクに割り当てられた未使用のバックアップディスクです。仮想ディスク内の物理ディスクが故障すると、ホットスペアがアクティブ化されて故障した物理ディスクと交換されるため、システムが中断したり、ユーザー介入が必要になったりすることはありません。

この操作を実行するには、ログインおよびサーバー制御の権限を持っている必要があります。

T10 PI（DIF）対応物理ディスクのみをホットスペアとして T10 PI（DIF）有効仮想ディスクに割り当てることができます。専用ホットスペアとして割り当てられている T10 PI（DIF）以外のドライブは、T10 PI（DIF）が後で仮想ディスク上で有効になった場合にホットスペアとはなりません。

4K ドライブのみを 4K 仮想ディスクにホットスペアとして割り当てることができます。

保留中の操作への追加 モードで物理ディスクを専用ホットスペアとして割り当てた場合、保留中操作が作成されますが、ジョブは作成されません。その後で専用ホットスペアの割り当てを解除しようとすると、専用ホットスペアを割り当てる保留中操作がクリアされます。

保留中の操作への追加 モードで物理ディスクを専用ホットスペアとしての割り当てから解除した場合、保留中操作が作成されますが、ジョブは作成されません。その後で専用ホットスペアの割り当てを行おうとすると、専用ホットスペアの割り当てを解除する保留中操作がクリアされます。

メモ: ログエクスポート操作進行中は、［仮想ディスクの管理］ ページで専用ホットスペアに関する情報を表示することができません。ログエクスポート操作の完了後、［仮想ディスクの管理］ ページを再ロードまたは更新して情報を表示します。

ウェブインタフェースを使用した仮想ディスクの管理

1. iDRAC ウェブインタフェースで、［概要］ > ［ ストレージ ］ > ［ 仮想ディスク ］ > ［ 管理 ］ に移動します。

[仮想ディスクの管理] ページが表示されます。

2. [コントローラ] ドロップダウンメニューから、仮想ディスクを管理するコントローラを選択します。
3. 1 つまたは複数の仮想ディスクの場合、各 [処置] ドロップダウンメニューから処置を選択します。

   仮想ドライブに複数の処置を指定できます。処置を選択すると、追加の [処置] ドロップダウンメニューが表示されます。別の処置をこのドロップダウンメニューから選択します。選択された処置は追加の [処置] ドロップダウンメニューには表示されません。また、[削除] リンクが選択された処置の隣に表示されます。 このリンクをクリックして、選択した処置を削除します。

   - [削除]
   - [編集ポリシー : 読み取りキャッシュ] - 読み取りキャッシュポリシーを、次のいずれかのオプションに変更します。
     - [先読みなし]
     - [先読み]
     - [適応先読み]

       メモ: 従来世代の PERC コントローラは、[先読みなし]、[先読み]、および [適応先読み] の読み取りポリシー設定をサポートします。PERC 8 および PERC 9 では、[先読み] および [適応型先読み] 設定の機能が、コントローラレベルで同等となります。 下位互換性を保つ目的で、一部の システム管理インタフェースおよび PERC 8 と 9 のコントローラで、読み取りポリシーの設定に [適応先読み] が許可されています。PERC 8 または PERC 9 で [先読み] または [適応型先読み] の設定が可能であっても、機能の違いはありません。
   - [編集ポリシー : 書き込みキャッシュ] - 書き込みキャッシュポリシーを、次のいずれかのオプションに変更します。
     - [ライトスルー]
     - [ライトバック]
     - [ライトバックの強制]
   - [編集ポリシー : ディスクキャッシュ] - ディスクキャッシュポリシーを、次のいずれかのオプションに変更します。
     - [デフォルト]
     - [有効]
     - [無効]
   - [初期化 : 高速] - 物理ディスク上のメタデータが更新され、それにより、すべてのディスク容量が今後の書き込み操作に使用できるようになります。初期化オプションは、物理ディスク上の既存の情報が消去されないのですぐに完了できますが、今後の書き込み操作により、物理ディスクに残された情報が上書きされます。
   - [初期化 : 完全] — 既存のデータとファイルシステムがすべて消去されます。

     メモ: [初期化 : 完全] オプションは PERC H330 コントローラには適用できません。
   - [整合性チェック] — 仮想ディスクの整合性をチェックするには、対応するドロップダウンメニューから [整合性チェック] 選択します。

     メモ: 整合性チェックは、RAID0 モードでセットアップしたドライブではサポートされません。
   - [仮想ディスクの暗号化] - 仮想ディスクドライブを暗号化します。コントローラが暗号化対応である場合、セキュリティキーの作成、変更、または削除が可能です。

     メモ: [仮想ディスクの暗号化] オプションは、仮想ディスクが自己暗号化ドライブ (SED) を使用して作成された場合にのみ、使用できます。
   - [専用ホットスペアの管理] - 物理ディスクを専用ホットスペアとして割り当て、または割り当て解除します。有効な専用ホットスペアのみが表示されます。有効なホットスペアが存在しない場合、このセクションは、ドロップダウンメニューに表示されません。

   これらのオプションの詳細については、『*iDRAC オンラインヘルプ*』を参照してください。
4. [操作モードの適用] ドロップダウンメニューから、設定を適用するタイミングを選択します。
5. [Apply (適用)] をクリックします。

   選択した操作モードに基づいて、設定が適用されます。

RACADM を使用した仮想ディスクの管理

仮想ディスクの管理には、次のコマンドを使用します。

- 仮想ディスクを削除するには :

```
racadm storage deletevd:<VD FQDD>
```

- 仮想ディスクを初期化するには :

```
racadm storage init:<VD FQDD> -speed {fast|full}
```

- 仮想ディスクの整合性をチェックするには（RAID0 ではサポートされません）：

```
racadm storage ccheck:<vdisk fqdd>
```

整合性チェックをキャンセルするには：

```
racadm storage cancelcheck: <vdisks fqdd>
```

- 仮想ディスクを暗号化するには：

```
racadm storage encryptvd:<VD FQDD>
```

- 専用ホットスペアを割り当て、または割り当て解除するには：

```
racadm storage hotspare:<Physical Disk FQDD> -assign <option> -type dhs -vdkey: <FQDD of
VD>
```

<option>=yes
ホットスペアの割り当て

<Option>=no
ホットスペアの割り当て解除

コントローラの管理

コントローラに対して次の操作を実行することができます。

- コントローラプロパティの設定
- 外部設定のインポートまたは自動インポート
- 外部設定のクリア
- コントローラ設定のリセット
- セキュリティキーの作成、変更、または削除

関連概念

コントローラのプロパティの設定 、p. 205
外部設定のインポートまたは自動インポート 、p. 208
外部設定のクリア 、p. 209
コントローラ設定のリセット 、p. 210
対応コントローラ 、p. 193
ストレージデバイスの対応機能のサマリ 、p. 194
物理ディスクの RAID または非 RAID モードへの変換 、p. 198

コントローラのプロパティの設定

コントローラについて次のプロパティを設定することができます。

- 巡回読み取りモード（自動または手動）
- 巡回読み取りモードが手動に設定されている場合の巡回読み取りの開始または停止
- 未設定領域の巡回読み取り
- 整合性チェックモード
- コピーバックモード
- ロードバランスモード
- 整合性チェック率
- 再構築率
- BGI 率

- 再構成率
- 拡張自動インポート外部設定
- セキュリティキーの作成または変更

コントローラのプロパティを設定するには、ログインおよびサーバー制御の権限を持っている必要があります。

巡回読み取りモードに関する考慮事項

巡回読み取りは、ディスクの故障とデータの損失または破壊を防止するために、ディスクエラーを検出します。

次の状況では、巡回読み取りが物理ディスク上で実行されません。

- 物理ディスクが仮想ディスクに含まれていない、またはホットスペアとして割り当てられていない。
- 物理ディスクは、次のタスクのうち 1 つを実行している仮想ディスクに含まれます。
  - 再構築
  - 再構成または再構築
  - バックグラウンド初期化
  - 整合性チェック

さらに、巡回読み取り操作は高負荷の I/O 動作中は一時停止され、その I/O が終了すると再開されます。

メモ: 自動モードにおいて巡回読み取りタスクが実行される頻度に関する詳細については、お使いのコントローラのマニュアルを参照してください。

メモ: コントローラ内に仮想ディスクがない場合、[開始] や [停止] などの巡回読み取りモード動作はサポートされません。iDRAC インタフェースを使用して動作を正常に呼び出すことはできますが、関連付けられているジョブが開始すると操作は失敗します。

負荷バランス

負荷バランス プロパティを使用すると、同一エンクロージャに接続されたコントローラポートまたはコネクタを両方自動的に使用して、I/O 要求をルートできます。このプロパティは、SAS コントローラでのみ使用可能です。

BGI 率

PERC コントローラでは、冗長仮想ディスクのバックグラウンド初期化が仮想ディスクの作成 0 ~ 5 分後に自動的に開始されます。冗長仮想ディスクのバックグラウンド初期化によって、仮想ディスクは冗長データの維持と書き込みパフォーマンスの向上に備えます。たとえば、RAID 5 仮想ディスクのバックグラウンド初期化完了後、パリティ情報が初期化されます。RAID 1 仮想ディスクのバックグラウンド初期化完了後は、物理ディスクがミラーリングされます。

バックグラウンド初期化プロセスは、コントローラが、後に冗長データに発生するおそれのある問題を識別し、修正するのに役立ちます。この点では、バックグラウンド初期化プロセスは整合性チェックに似ています。バックグラウンド初期化は、完了するまで実行する必要があります。キャンセルすると、0 ~ 5 分以内に自動的に再開されます。バックグラウンド初期化の実行中は、読み取りや書き込みなどの一部のプロセスは操作可能です。仮想ディスクの作成のような他の処理はバックグラウンド初期化と同時に実行することはできません。これらのプロセスによって、バックグラウンド初期化はキャンセルされます。

0 ~ 100 % の範囲で設定可能なバックグラウンド初期化率は、バックグラウンド初期化タスクの実行専用のシステムリソースの割合を表します。0 % では、コントローラに対するバックグラウンド初期化の優先順位が最も低く、完了までに最も時間がかかり、システムパフォーマンスへの影響が最も少ない設定となります。バックグラウンド初期化率 0 % は、バックグラウンド初期化の停止や一時停止を意味するものではありません。100 % では、バックグラウンド初期化はコントローラに対して最優先になります。バックグラウンド初期化の時間が最短になりますが、システムパフォーマンスへの影響が最も高く設定されます。

整合性チェック

整合性チェック タスクは、冗長 (パリティ) 情報の正確さを検証します。このタスクは冗長仮想ディスクにのみ適用されます。必要なときは、整合性チェック タスクが冗長データを再構築します。仮想ディスクが失敗した冗長性状態にある場合、整合性チェックを実行することによって、仮想ディスクを準備完了状態に戻すことができる可能性があります。

0 ~ 100 % の範囲で設定可能な整合性チェック率は、整合性チェック タスクの実行専用のシステムリソースの割合を表します。0 % では、コントローラに対する整合性チェックの優先順位が最も低く、完了までに最も時間がかかり、システムパフォーマンスへの影響が最も少ない設定となります。整合性チェック率 0 % は、整合性チェックの停止や一時停止を意味するものではありません。

100 % では、整合性チェックはコントローラに対して最優先になります。整合性チェックの時間が最短になりますが、システムパフォーマンスへの影響が最も高く設定されます。

セキュリティキーの作成または変更

コントローラのプロパティを設定するときは、セキュリティキーを作成したり、変更したりすることができます。コントローラの暗号化キーを使用して SED へのアクセスをロックまたはロック解除します。暗号化キーは、暗号化対応コントローラ 1 台につき 1 つのみ作成できます。セキュリティキーはローカルキー管理（LKM）機能を使用して管理されます。LKM を使用して、キー ID と、仮想ディスクの保護に必要なパスワードまたはキーを生成します。LKM を使用している場合、セキュリティキー識別子とパスフレーズを指定して暗号化キーを作成する必要があります。

このタスクは、HBA モードで実行されている PERC ハードウェアコントローラではサポートされません。

「保留中の操作に追加」モードにおいてセキュリティキーを作成し、ジョブが作成されていない状態においてセキュリティキーを削除すると、「セキュリティキーの作成」の保留中の操作がクリアされます。

ウェブインタフェースを使用したコントローラプロパティの設定

1. iDRAC ウェブインタフェースで、［概要］ > ［ストレージ］ > ［コントローラ］ > ［セットアップ］と移動します。
   ［コントローラのセットアップ］ページが表示されます。
2. ［コントローラプロパティの設定］セクションの［コントローラ］ドロップダウンメニューから、設定するコントローラを選択します。
3. 各種プロパティで必要な情報を指定します。

   ［現在の値］列に、各プロパティの既存の値が表示されます。この値を変更するには、プロパティごとに［処置］ドロップダウンメニューのオプションを選択します。

   フィールドについては、『iDRAC オンラインヘルプ』を参照してください。
4. ［操作モードの適用］ドロップダウンメニューから、設定を適用するタイミングを選択します。
5. ［適用］をクリックします。
   選択した操作モードに基づいて、設定が適用されます。

RACADM を使用したコントローラプロパティの設定

- 巡回読み取りモードを設定するには、次のコマンドを使用します。

  ```
  racadm set storage.controller.<index>.PatrolReadMode  {Automatic | Manual | Disabled}
  ```

- 巡回読み取りモードが手動に設定されている場合、次のコマンドを使用して巡回読み取りモードを開始および停止します。

  ```
  racadm storage patrolread:<Controller FQDD> -state {start|stop}
  ```

  メモ: コントローラ内に仮想ディスクがない場合、開始や停止などの巡回読み取りモードの動作はサポートされません。iDRAC インタフェースを使用して動作を正常に呼び出すことはできますが、関連付けられているジョブが開始すると操作は失敗します。

- 整合性チェックモードを指定するには、**Storage.Controller.CheckConsistencyMode** オブジェクトを使用します。
- コピーバックモードを有効または無効にするには、**Storage.Controller.CopybackMode** オブジェクトを使用します。
- 負荷バランスモードを有効または無効にするには、**Storage.Controller.PossibleloadBalancedMode** オブジェクトを使用します。
- 冗長仮想ディスクで整合性チェックを実行する専用のシステムリソースの割合を指定するには、**Storage.Controller.CheckConsistencyRate** オブジェクトを使用します。
- 障害の発生したディスクを再構築する専用のコントローラのリソースの割合を指定するには、**Storage.Controller.RebuildRate** オブジェクトを使用します。
- 作成した後に仮想ディスクのバックグラウンド初期化（BGI）を実行する専用のコントローラのリソースの割合を指定するには、**Storage.Controller.BackgroundInitializationRate** オブジェクトを使用します。

- 物理ディスクの追加またはディスクグループ上の仮想ディスクの RAID レベルの変更後にディスクグループを再構成する専用のコントローラのリソースの割合を指定するには、**Storage.Controller.ReconstructRate** オブジェクトを使用します。
- コントローラに対する外部設定の拡張自動インポートを有効または無効にするには、**Storage.Controller.EnhancedAutoImportForeignConfig** オブジェクトを使用します。
- 仮想ドライブを暗号化するためのセキュリティキーを作成、変更、または削除するには、次のコマンドを使用します。

```
racadm storage createsecuritykey:<Controller FQDD> -key <Key id> -passwd <passphrase>
racadm storage modifysecuritykey:<Controller FQDD> -key <key id> -oldpasswd <old
passphrase> -newpasswd <new passphrase>
racadm storage deletesecuritykey:<Controller FQDD>
```

外部設定のインポートまたは自動インポート

外部設定は、1 つのコントローラから別のコントローラへ移動された物理ディスク上のデータです。移動された物理ディスクにある仮想ディスクは、外部設定と見なされます。

外部設定をインポートして、物理ディスクの移動後に仮想ドライブが失われないようにすることができます。外部設定は、準備完了状態または劣化状態の仮想ディスク、あるいはインポート可能かすでに存在している仮想ディスク専用のホットスペアが含まれている場合にのみインポートできます。

すべての仮想ディスクデータが存在する必要がありますが、仮想ディスクが冗長 RAID レベルを使用している場合、追加の冗長データは不要です。

たとえば、外部設定に RAID 1 仮想ディスクのミラーリングの片方のみが含まれる場合、仮想ディスクは劣化状態なのでインポートできます。一方、元は 3 台の物理ディスクを使用する RAID 5 として設定された物理ディスク 1 台のみが外部設定に含まれる場合、RAID 5 仮想ディスクが失敗状態にあり、インポートできません。

仮想ディスクの他に、コントローラには、1 台のコントローラでホットスペアとして割り当てられた後、別のコントローラに移動された物理ディスクが含まれる場合があります。外部設定のインポート タスクは新しい物理ディスクをホットスペアとしてインポートします。物理ディスクが以前のコントローラで専用ホットスペアとして設定されたがホットスペアが割り当てられた仮想ディスクが外部設定に存在しないという場合、物理ディスクはグローバルホットスペアとしてインポートされます。

ローカルキーマネージャ (LKM) を使用してロックされた外部設定が検出された場合、このリリースでは iDRAC で外部設定のインポート操作を行うことはできません。CTRL-R を使用してドライブをロック解除して、iDRAC から外部設定のインポートを続ける必要があります。

コントローラが外部設定を検出した場合にのみ 外部設定のインポート タスクが表示されます。物理ディスクの状況をチェックして、物理ディスクに外部設定 (仮想ディスクまたはホットスペア) が含まれるかを識別することもできます。物理ディスク状況が外部 の場合、物理ディスクに仮想ディスクのすべてまたは一部が含まれるか、ホットスペア割り当てがあります。

メモ: 外部設定のインポートタスクは、コントローラに追加された物理ディスクにあるすべての仮想ディスクをインポートします。複数の外部仮想ディスクが存在する場合は、全設定がインポートされます。

PERC9 コントローラでは、ユーザーの介入を必要としない外部設定の自動インポートをサポートします。自動インポートは有効または無効にできます。有効にすると、PERC コントローラでは、手動による介入なしに、検出された外部設定を自動インポートできます。無効にすると、PERC は外部設定を自動インポートしません。

外部設定をインポートするには、ログインおよびサーバー制御の権限を持っている必要があります。

このタスクは、HBA モードで実行されている PERC ハードウェアコントローラではサポートされません。

メモ: システムでオペレーティングシステムを実行している最中に外部エンクロージャのケーブルを抜くことは推奨されません。ケーブルを抜くと、接続の再確立時に外部設定が生じる原因となる可能性があります。

次の場合に外部構成を管理できます。

- 構成内のすべての物理ディスクが取り外され、再度挿入されている。
- 構成内の一部の物理ディスクが取り外され、再度挿入されている。
- 仮想ディスク内のすべての物理ディスクが取り外され (ただし、取り外しは同時には行われなかった)、再度挿入されている。
- 非冗長仮想ディスク内の物理ディスクが取り外されている。

インポートを検討している物理ディスクには以下の制約が適用されます。

- 物理ディスクの状態は、実際にインポートされる際に、外部構成がスキャンされたときから変わっている場合があります。外部インポートでは、未構成良好状態のディスクのみがインポートされます。
- 故障状態またはオフライン状態のドライブはインポートできません。

- ファームウェアの制約により、8 つを超える外部構成をインポートすることはできません。

ウェブインタフェースを使用した外部設定のインポート

外部設定をインポートするには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、[概要] > [ストレージ] > [コントローラ] > [セットアップ] と移動します。
   [コントローラのセットアップ] ページが表示されます。
2. [外部設定] セクションの [コントローラ] ドロップダウンメニューから、設定するコントローラを選択します。
3. [操作モードの適用] ドロップダウンメニューからインポートするタイミングを選択します。
4. [外部設定のインポート] をクリックします。

   選択した操作モードに基づいて、設定がインポートされます。

   外部構成を自動的にインポートするには、[コントローラプロパティの設定] セクションで、[外部設定の拡張自動インポート] オプションを有効にして、[操作モードの適用] を選択し、[適用] をクリックします。

   メモ: インポートする外部設定に対して [外部設定の拡張自動インポート] オプションを有効にした後で、システムを再起動する必要があります。

RACADM を使用した外部設定のインポート

外部設定をインポートするには、次の手順を実行します。

```
racadm storage importconfig:<Controller FQDD>
```

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンド ライン リファレンス ガイド*』を参照してください。

外部設定のクリア

物理ディスクを 1 つのコントローラから別のコントローラに移動した後で、物理ディスクに仮想ディスクのすべてまたは一部 (外部設定) が含まれることが判明する場合があります。以前使用した物理ディスクに外部設定 (仮想ディスク) が含まれるかを識別するには、物理ディスクの状態をチェックします。物理ディスクの状態が外部の場合は、物理ディスクに仮想ディスクのすべてまたは一部が含まれます。新しく接続した物理ディスクから仮想ディスク情報をクリアまたは消去できます。

外部設定のクリア 操作を実行すると、コントローラに接続される物理ディスク上のすべてのデータが永続的に削除されます。複数の外部仮想ディスクが存在する場合、すべての設定が消去されます。データを破壊するよりも仮想ディスクのインポートが望ましい場合もあります。外部データを削除するには、初期化を実行する必要があります。インポートできない不完全な外部設定がある場合は、外部設定のクリア オプションを使用して物理ディスク上の外部データを消去できます。

ウェブインタフェースを使用した外部設定のクリア

外部設定をクリアするには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、[概要] > [ストレージ] > [コントローラ] > [セットアップ] と移動します。
   [コントローラのセットアップ] ページが表示されます。
2. [外部設定] セクションの [コントローラ] ドロップダウンメニューから、外部設定をクリアするコントローラを選択します。
3. [操作モードの適用] ドロップダウンメニューから、データをクリアするタイミングを選択します。
4. [クリア] をクリックします。
   選択した操作モードに基づいて、物理ディスクに存在する仮想ディスクが消去されます。

RACADM を使用した外部設定のクリア

外部設定をクリアするには、次の手順を実行します。

```
racadm storage clearconfig:<Controller FQDD>
```

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインリファレンスガイド*』を参照してください。

コントローラ設定のリセット

コントローラの設定をリセットすることができます。この操作を実行すると、仮想ディスクドライブが削除され、コントローラ上のホットスペアがすべて割り当て解除されます。設定からディスクが削除される以外に、データは消去されません。また、設定をリセットしても、外部設定は削除されません。この機能のリアルタイムサポートは PERC 9.1 ファームウェアでのみ使用できます。設定をリセットしても、データは消去されません。初期化せずにまったく同じ設定を再作成できるので、データが修復される可能性があります。サーバー制御の権限を持っている必要があります。

メモ: コントローラ設定をリセットしても、外部設定は削除されません。外部設定を削除するには、設定のクリア操作を実行します。

ウェブインタフェースを使用したコントローラの設定のリセット

コントローラの設定をリセットするには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、[概要] > [ストレージ] > [コントローラ] > [トラブルシューティング] と移動します。
   [コントローラのトラブルシューティング] ページが表示されます。
2. [処置] ドロップダウンメニューから、1 つまたは複数のコントローラの [設定のリセット] を選択します。
3. コントローラごとに [操作モードの適用] ドロップダウンメニューから、設定を適用するタイミングを選択します。
4. [適用] をクリックします。
   選択した操作モードに基づいて、設定が適用されます。

RACADM を使用したコントローラの設定のリセット

コントローラの設定をリセットするには、次の手順を実行します。

```
racadm storage resetconfig:<Controller FQDD>
```

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインリファレンスガイド*』を参照してください。

コントローラモードの切り替え

PERC 9.1 以降のコントローラでは、モードを RAID から HBA に切り替えることでコントローラのパーソナリティを変更できます。コントローラは、ドライバがオペレーティングシステムを経由する際の HBA コントローラと同様に動作します。コントローラモードの変更はステージングされた操作であり、リアルタイムでは行われません。コントローラモードを RAID から HBA に変更する前に、次を確認してください。

- RAID コントローラがコントローラモードの変更をサポートしている。コントローラモードを変更するオプションは、RAID パーソナリティがライセンスを必要とするコントローラでは使用できません。
- すべての仮想ディスクが削除されている。
- ホットスペアが削除されている。
- 外部設定がクリアまたは削除されている。
- 障害の発生した状態のすべての物理ディスクが削除されている。
- SED に関連付けられているローカルセキュリティキーを削除する必要があります。
- コントローラに保存キャッシュが存在していない (必須)。
- コントローラモードを切り替えるためのサーバー制御権限がある。

メモ: モードを切り替えるとデータが削除されるため、外部設定、セキュリティキー、仮想ディスク、およびホットスペアをバックアップしてからモードを切り替えるようにしてください。

メモ: コントローラモードを変更する前に、PERC FD33xS および FD33xD ストレージスレッドに対して CMC ライセンスが使用可能であることを確認してください。ストレージスレッドに対する CMC ライセンスの詳細については、**dell.com/support/manuals** にある『PowerEdge FX2/FX2s 対応 Dell Chassis Management Controller バージョン 1.2 ユーザーズガイド』を参照してください。

コントローラモードの切り替え時の例外

次のリストに、ウェブインタフェース、RACADM、および WS-MAN などの iDRAC インタフェースを使用してコントローラモードを設定する際の例外を示します。

● PERC コントローラが RAID モードに設定されている場合は、HBA モードに変更する前に、仮想ディスク、ホットスペア、外部設定、コントローラキー、または保存キャッシュをクリアする必要があります。
● コントローラモードの設定中にその他の RAID 操作を設定することはできません。たとえば、PERC が RAID モードであるときに PERC の保留中の値を HBA モードに設定して、BGI 属性を設定しようとすると、保留中の値が開始されません。
● PERC コントローラを HBA から RAID モードに切り替えると、ドライブは 非 RAID 状態のままとなり、準備完了 状態に自動的に設定されません。また、**RAIDEnhancedAutoImportForeignConfig** 属性は自動的に ［ 有効 ］ に設定されます。

次のリストに、WS-MAN または RACADM インタフェースでサーバー設定プロファイル機能を使用してコントローラモードを設定するときの例外を示します。

● サーバー設定プロファイル機能を使用すると、コントローラモードの設定と共に複数の RAID 操作を設定できます。たとえば、PERC コントローラが HBA モードである場合、コントローラモードを RAID に変更し、ドライブを準備完了に変換して仮想ディスクを作成するようにエクスポート xml を編集できます。
● RAID から HBA にモードを変更するときに、**RAIDaction pseudo** 属性がアップデート (デフォルトの動作) に設定されます。属性が実行され、仮想ディスクが作成されますが、これは失敗します。コントローラモードは変更されますが、ジョブはエラーで終了します。この問題を回避するには、XML ファイルで RAIDaction 属性をコメントアウトする必要があります。
● PERC コントローラが HBA モードであるときに、コントローラモードを RAID に変更するように編集したエクスポート xml でインポートプレビューを実行し、VD を作成しようとすると、仮想ディスクの作成に失敗します。インポートプレビューでは、コントローラモードの変更を伴う RAID スタック操作の検証をサポートしていません。

iDRAC ウェブインタフェースを使用したコントローラモードの切り替え

コントローラモードを切り替えるには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、［ 概要 ］ > ［ ストレージ ］ > ［ コントローラ ］ をクリックします。
2. ［ コントローラ ］ ページで、［ セットアップ ］ > ［ コントローラ ］ をクリックします。
   ［ 現在の値 ］ 列にコントローラの現在の設定が表示されます。
3. ドロップダウンメニューから目的のコントローラモードを選択し、［ 適用 ］ をクリックします。
   変更を有効にするためにシステムを再起動します。

RACADM を使用したコントローラモードの切り替え

RACADM を使用してコントローラモードを切り替えるには、以下のコマンドを実行します。

● コントローラの現在のモードを表示するには：

```
$ racadm get Storage.Controller.1.RequestedControllerMode[key=<Controller_FQDD>]
```

  次の出力が表示されます。

```
RequestedControllerMode = NONE
```

● HBA としてコントローラモードを設定するには：

```
$ racadm set Storage.Controller.1.RequestedControllerMode  HBA [Key=<Controller_FQDD>]
```

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

12 Gbps SAS HBA アダプタの操作

非 RAID コントローラは、RAID 機能が導入されていない HBA です。これらのコントローラは仮想ディスクをサポートしません。

このリリースでは、iDRAC インタフェースは 12 Gbps SAS HBA コントローラおよび HBA330 内蔵コントローラのみをサポートしています。

非 RAID コントローラについて、次のことを実行できます。

● 非 RAID コントローラに適用可能なコントローラ、物理ディスク、およびエンクロージャのプロパティの表示。また、エンクロージャに関連付けられた EMM、ファン、電源装置、および温度プローブのプロパティを表示します。これらのプロパティは、コントローラの種類に基づいて表示されます。
● ソフトウェアとハードウェアのインベントリ情報の表示。
● 12 Gbps SAS HBA コントローラの裏側にあるエンクロージャのファームウェアのアップデート (ステージング)。
● 変更が検出された場合の物理ディスクの SMART トリップステータスに対するポーリングまたはポーリング頻度の監視。

- 物理ディスクのホットプラグまたはホット取り外しステータスの監視。
- LED の点滅または点滅解除。

メモ:

- 非 RAID コントローラをインベントリまたは監視する前に、再起動時のシステムインベントリの収集（CSIOR）操作を実行する必要があります。
- ファームウェアアップデートを実行した後にシステムを再起動します。
- SMART 対応ドライブおよび SES エンクロージャセンサーに対するリアルタイム監視は、12 Gbps SAS HBA コントローラおよび HBA330 内蔵コントローラに対してのみ実行されます。

関連概念

ストレージデバイスのインベントリと監視、p. 196
システムインベントリの表示、p. 100
デバイスファームウェアのアップデート、p. 62
ドライブに対する予測障害分析の監視、p. 212
コンポーネント LED の点滅または点滅解除、p. 223

ドライブに対する予測障害分析の監視

ストレージ管理は、SMART 対応の物理ディスクに対する SMART（Self Monitoring Analysis and Reporting Technology）をサポートします。

SMART は各ディスクに対して予測障害分析を行い、ディスク障害が予測された場合はアラートを送信します。コントローラは物理ディスクで障害予測の有無をチェックし、存在する場合は、この情報を iDRAC に渡します。iDRAC はすぐにアラートを記録します。

非 RAID（HBA）モードでのコントローラの操作

コントローラが非 RAID モード（HBA モード）の場合、次のようになります。

- 仮想ディスクまたはホットスペアを使用できません。
- コントローラのセキュリティ状態が無効になります。
- すべての物理ディスクが非 RAID モードになります。

コントローラが非 RAID モードである場合は、次のことを実行できます。

- 物理ディスクの点滅 / 点滅解除。
- 以下を含むすべてのプロパティを設定します。
  - 負荷バランスモード
  - 整合性チェックモード
  - 巡回読み取りモード
  - コピーバックモード
  - コントローラ起動モード
  - 拡張自動インポート外部設定
  - 再構築率
  - 整合性チェック率
  - 再構成率
  - BGI 率
  - エンクロージャまたはバックプレーンのモード
  - 未設定領域の巡回読み取り
- 仮想ディスクに対して予期される RAID コントローラに適用可能な全プロパティの表示。
- 外部設定のクリア

メモ: 操作が非 RAID モードでサポートされていない場合は、エラーメッセージが表示されます。

コントローラが 非 RAID モードである場合、エンクロージャ温度プローブ、ファン、および電源装置を監視することはできません。

複数のストレージコントローラでの RAID 設定ジョブの実行

サポートされている iDRAC インタフェースから、複数のストレージコントローラに対して操作を実行する際は、次のことを確認してください。

- 各コントローラ上で個別にジョブを実行する。各ジョブが完了するのを待ってから、次のコントローラに対する設定とジョブの作成を開始します。
- スケジュール設定オプションを使用して、複数のジョブを後で実行するようにスケジュールする。

PCIe SSD の管理

Peripheral Component Interconnect Express（PCIe）Solid State Device（SSD）は、低レイテンシ、高 IOPS（1 秒あたり入出力回数）、さらにストレージにエンタープライズクラスの信頼性とサービス性が求められるソリューション向けにデザインされた、高パフォーマンスなストレージデバイスです。PCIe SSD は、Single Level Cell（SLC）およびマルチレベルセル（MLC）NAND フラッシュテクノロジに基づいて設計され、高速 PCIe 2.0 または PCIe 3.0 に準拠したインタフェースを装備しています。iDRAC 2.20.20.20 以降のバージョンは、デルの第 13 世代 PowerEdge ラック＆タワー型サーバーおよび Dell PowerEdge R920 サーバーで Half-Height Half-Length（HHHL）PCIe SSD カードをサポートしています。HHHL SSD カードは、PCIe SSD がサポートされているバックプレーンを搭載していないサーバーの PCI スロットに、直接挿入することができます。これらのカードは、サポートされているバックプレーンを備えたサーバー上でも使用できます。

iDRAC インタフェースを使用して、NVMe PCIe SSD の表示および設定が行えます。

PCIe SSD には、次の主な機能があります。

- ホットプラグ対応
- 高性能デバイス

PCIe SSD サブシステムは、バックプレーン、システムのバックプレーンに接続され、シャーシ前面の最大 4 または 8 個の PCIe SSD に対応する PCIe 接続性を提供する PCIe エクステンダカード、および PCIe SSD で構成されます。

PCIe SSD に対して次の操作を実行できます。

- サーバー内の PCIe SSD のインベントリと正常性のリモート監視
- PCIe SSD の取り外し準備
- データを安全に消去
- デバイスの LED の点滅または点滅解除

HHHL SSD に対しては次の操作を実行できます。

- サーバー内の HHHL SSD インベントリおよびリアルタイム監視
- ドライブのオンライン、障害発生、オフラインなどのステータスレポート
- iDRAC および OMSS での障害の発生したカードの報告およびログの記録
- 安全なデータ消去およびカードの取り外し
- TTY ログレポート

メモ: ホットプラグ機能、取り外し準備、およびデバイスの点滅または点滅解除は、HHHL PCIe SSD デバイスには適用されません。

関連概念

PCIe SSD のインベントリと監視、p. 213
PCIe SSD の取り外しの準備、p. 214
PCIe SSD デバイスデータの消去、p. 215

PCIe SSD のインベントリと監視

次のインベントリと監視情報は PCIe SSD で利用可能です。

- ハードウェア情報：
  - PCIe SSD エクステンダカード
  - PCIe SSD バックプレーン

    システムに専用の PCIe バックプレーンがある場合、2 つの FQDD が表示されます。1 つは標準ドライブ用で、もう 1 つは SSD 用です。バックプレーンが共有されている（ユニバーサル）場合、FQDD は 1 つしか表示されません。
- ソフトウェアインベントリには、PCIe SSD のファームウェアのバージョンだけが含まれます。

ウェブインタフェースを使用した PCIe SSD のインベントリと監視

PCIe SSD デバイスをインベントリおよび監視するには、iDRAC ウェブインタフェースで、[概要] > [ストレージ] > [物理ディスク] に移動します。[プロパティ] ページが表示されます。PCIe SSD の場合、[名前] 列に [PCIe SSD] と表示されます。展開してプロパティを表示します。

RACADM を使用した PCIe SSD のインベントリおよび監視

`racadm storage get controllers:<PcieSSD controller FQDD>` コマンドを使用して、PCIe SSD のインベントリおよび監視を行います。

PCIe SSD ドライブのすべてを表示するには、次のコマンドを使用します。

```
racadm storage get pdisks
```

PCIe エクステンダカードを表示するには、次のコマンドを使用します。

```
racadm storage get controllers
```

PCIe SSD バックプレーン情報を表示するには、次のコマンドを使用します。

```
racadm storage get enclosures
```

メモ: 記載されているすべてのコマンドについては、PERC デバイスも表示されます。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインリファレンスガイド*』を参照してください。

PCIe SSD の取り外しの準備

PCIe SSD は、デバイスが取り付けられているシステムを停止したり、再起動したりすることなくデバイスの追加や削除を行える、秩序だったホットスワップをサポートします。データロスを防止するには、デバイスを物理的に取り外す前に、取り外しの準備 操作を使用する必要があります。

秩序だったホットスワップは、対応オペレーティングシステムを実行している対応システムに PCIe SSD が取り付けられている場合にのみサポートされます。お使いの PCIe SSD の設定が正しいことを確認するには、システム専用のオーナーズマニュアルを参照してください。

取り外しの準備 操作は、VMware vSphere (ESXi) システム と HHHL PCIe SSD デバイス上の PCIe SSD ではサポートされていません。

メモ: 取り外しの準備 操作は、IDRAC サービスモジュール バージョン 2.1 以降を使用する ESXi 6.0 搭載システムでサポートされています。

取り外しの準備 操作は iDRAC サービスモジュールを使用してリアルタイムで実行できます。

取り外しの準備 操作は、バックグラウンドでのアクティビティと続行中の I/O アクティビティを停止するので、デバイスを安全に取り外すことができます。これにより、デバイスのステータス LED が点滅します。取り外しの準備 操作を開始した後、次の状況下でシステムからデバイスを安全に取り外すことができます。

- PCIe SSD が安全な取り外し LED パターンで点滅している。
- PCIe SSD にシステムからアクセスできない。

PCIe SSD の取り外しを準備する前に、以下を確認してください。

- iDRAC サービスモジュールが取り付けられている。
- Lifecycle Controller が有効化されている。
- サーバ制御およびログインの権限がある。

ウェブインタフェースを使用した PCIe SSD の取り外しの準備

PCIe SSD の取り外しを準備するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、[概要] > [ストレージ] > [物理ディスク] > [セットアップ] と移動します。
   [物理ディスクのセットアップ] ページが表示されます。
2. [コントローラ] ドロップダウンメニューから、エクステンダを選択して関連する PCIe SSD を表示します。

3. ドロップダウンメニューから、1 つまたは複数の PCIe SSD に対する［取り外しの準備］を選択します。
   ［取り外しの準備］を選択した場合に、ドロップダウンメニューのその他のオプションを表示するには、［処置］を選択し、ドロップダウンメニューをクリックしてその他のオプションを表示します。

   メモ: `preparetoremove` 操作を実行するには、iSM がインストールおよび実行されていることを確認します。

4. ［操作モードの適用］ドロップダウンメニューから、［今すぐ適用］を選択してただちに処置を適用します。
   完了予定のジョブがある場合、このオプションはグレー表示になります。

   メモ: PCIe SSD デバイスの場合は、［今すぐ適用］オプションのみが利用可能です。この操作は、ステージングされたモードではサポートされません。

5. ［適用］をクリックします。
   ジョブが作成されていない場合は、ジョブの作成に成功しなかったことを示すメッセージが表示されます。また、メッセージ ID および推奨される対応処置が表示されます。

   ジョブが正常に作成されると、選択されたコントローラにジョブ ID が作成されたことを示すメッセージが表示されます。［ジョブキュー］をクリックして［ジョブのキュー］ページのジョブの進行状況を表示します。

   保留中の操作が作成されていない場合は、エラーメッセージが表示されます。保留中の操作が成功し、ジョブの作成が正常終了しなかった場合は、エラーメッセージが表示されます。

RACADM を使用した PCIe SSD の取り外しの準備

PCIeSSD ドライブの取り外しを準備するには、次の手順を実行します。

```
racadm storage preparetoremove:<PCIeSSD FQDD>
```

`preparetoremove` コマンドを実行した後にターゲットジョブを作成するには、次の手順を実行します。

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW --realtime
```

返されたジョブ ID を問い合わせるには、次の手順を実行します。

```
racadm jobqueue view -i <job ID>
```

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインリファレンスガイド*』を参照してください。

PCIe SSD デバイスデータの消去

安全消去機能は、ディスク上のすべてのデータを完全に消去します。PCIe SSD に対して暗号消去を実行すると、すべてのブロックが上書きされて PCIe SSD 上のすべてのデータが永久に失われる結果となります。暗号消去の間、ホストは PCIe SSD にアクセスできなくなります。変更はシステムの再起動後に適用されます。

暗号消去中にシステムが再起動したり電源が失われたりすると、操作はキャンセルされます。システムを再起動して処理を再開する必要があります。

PCIe SSD デバイスのデータを消去する前に、次を確認してください。
- Lifecycle Controller が有効化されている。
- サーバ制御およびログインの権限がある。

メモ:
- PCIe SSD の消去は、ステージング操作としてのみ実行できます。
- ドライブは消去された後、オンラインとしてオペレーティングシステムに表示されますが初期化されていません。ドライブを再度使用する前に、初期化とフォーマットを行う必要があります。
- PCIe SSD のホットプラグを実行した後、ウェブインタフェースで表示されるまでに数秒かかる場合があります。
- セキュア消去機能は、ホットプラグ対応 PCIe SSD ではサポートされません。

ウェブインタフェースを使用した PCIe SSD デバイスデータの消去

PCIe SSD デバイス上のデータを消去するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、[概要] > [ストレージ] > [物理ディスク] > [セットアップ] と移動します。
   [物理ディスクのセットアップ] ページが表示されます。
2. [コントローラ] ドロップダウンメニューから、コントローラを選択して関連付けられている PCIe SSD を表示します。
3. ドロップダウンメニューから、1 つまたは複数の PCIe SSD に対する [セキュア消去] を選択します。

   [セキュア消去] を選択した場合、その他のオプションをドロップダウンメニューに表示するには、[処置] を選択して、ドロップダウンメニューをクリックしてその他のオプションを表示します。
4. [操作モードの適用] ドロップダウンメニューから、次のいずれかのオプションを選択します。
   - **次の再起動時** - このオプションを選択して、処置を次回のシステム再起動時に適用します。これは PERC 8 コントローラのデフォルトオプションです。
   - **スケジュールされた時刻** - このオプションを選択して、スケジュールされた日付と時刻に処置を適用します。
     - **開始時刻** と **終了時刻** - カレンダーのアイコンをクリックして日付を選択します。ドロップダウンメニューから、時刻を選択します。開始時刻と終了時刻の間に処置が適用されます。
     - ドロップダウンメニューから、再起動のタイプを選択します。
       - 再起動なし (システムを手動で再起動)
       - 正常なシャットダウン
       - 強制シャットダウン
       - システムのパワーサイクル (コールドブート)

       メモ: PERC 8 以前のコントローラでは、[正常なシャットダウン] がデフォルトオプションになっています。PERC 9 コントローラでは、[再起動なし (システムを手動で再起動)] がデフォルトのオプションです。
5. [適用] をクリックします。

   ジョブが作成されていない場合は、ジョブの作成に成功しなかったことを示すメッセージが表示されます。また、メッセージ ID および推奨される対応処置が表示されます。

   ジョブが正常に作成されると、選択されたコントローラにジョブ ID が作成されたことを示すメッセージが表示されます。[ジョブキュー] をクリックして ジョブのキュー ページのジョブの進行状況を表示します。

   保留中の操作が作成されていない場合は、エラーメッセージが表示されます。保留中の操作が成功し、ジョブの作成が正常終了しなかった場合は、エラーメッセージが表示されます。

RACADM を使用した PCIe SSD デバイスデータの消去

PCIe SSD デバイスを安全に消去するには、次の手順を実行します。

```
racadm storage secureerase:<PCIeSSD FQDD>
```

secureerase コマンドを実行した後にターゲットジョブを作成するには、次の手順を実行します。

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW -e <start_time>
```

返されたジョブ ID を問い合わせるには、次の手順を実行します。

```
racadm jobqueue view -i <job ID>
```

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインリファレンスガイド*』を参照してください。

エンクロージャまたはバックプレーンの管理

エンクロージャまたはバックプレーンについて、次のことを実行できます。
- プロパティの表示
- ユニバーサルモードまたはスプリットモードの設定
- スロット情報の表示 (ユニバーサルまたは共有)
- SGPIO モードの設定

関連概念

ストレージデバイスの対応機能のサマリ 、p. 194

対応エンクロージャ 、p. 194
バックプレーンモードの設定 、p. 217
ユニバーサルスロットの表示 、p. 219
SGPIO モードの設定 、p. 220

バックプレーンモードの設定

デルの第 13 世代 PowerEdge サーバは、新しい内蔵ストレージトポロジをサポートします。このトポロジでは、1 つのエキスパンダを通して 2 台のストレージコントローラ (PERC) を 1 組みの内蔵ドライブに接続することができます。この構成ではフェールオーバーや高可用性 (HA) 機能のない高パフォーマンスモードに使用されます。エキスパンダは、2 台のストレージコントローラ間で内蔵ドライブアレイを分割します。このモードでは、仮想ディスクの作成で特定のコントローラに接続されたドライブのみが表示されます。この機能のライセンス要件はありません。この機能は、一部のシステムでのみサポートされています。

バックプレーンは次のモードをサポートします。

- 統合モード - これがデフォルトモードです。2 台目の PERC コントローラが取り付けられている場合でも、バックプレーンに接続されたすべてのドライブへのアクセス権はプライマリ PERC コントローラにあります。
- 分割モード - 1 台のコントローラは最初の 12 ドライブにアクセスでき、2 台目のコントローラは残りの 12 ドライブにアクセスできます。1 台目のコントローラに接続されているドライブには 0 ~ 11 の番号が付けられ、2 台目のコントローラに接続されているドライブには 12 ~ 23 の番号が付けられます。
- 分割モード 4:20 - 1 台のコントローラは最初の 4 ドライブにアクセスでき、2 台目のコントローラは残りの 20 ドライブにアクセスできます。1 台目のコントローラに接続されているドライブには 0 ~ 3 の番号が付けられ、2 台目のコントローラに接続されているドライブには 4 ~ 23 の番号が付けられます。
- 分割モード 8:16 - 1 台のコントローラは最初の 8 ドライブにアクセスでき、2 台目のコントローラは残りの 16 ドライブにアクセスできます。1 台目のコントローラに接続されているドライブには 0 ~ 7 の番号が付けられ、2 台目のコントローラに接続されているドライブには 8 ~ 23 の番号が付けられます。
- 分割モード 16:8 - 1 台のコントローラは最初の 16 ドライブにアクセスでき、2 台目のコントローラは残りの 8 ドライブにアクセスできます。1 台目のコントローラに接続されているドライブには 0 ~ 15 の番号が付けられ、2 台目のコントローラに接続されているドライブには 16 ~ 23 の番号が付けられます。
- 分割モード 20:4 - 1 台のコントローラは最初の 20 ドライブにアクセスでき、2 台目のコントローラは残りの 4 ドライブにアクセスできます。1 台目のコントローラに接続されているドライブには 0 ~ 19 の番号が付けられ、2 台目のコントローラに接続されているドライブには 20 ~ 23 の番号が付けられます。
- 情報が利用不可 — コントローラ情報は利用できません。

エキスパンダにこの設定をサポートする機能がある場合、iDRAC で分割モード設定が許可されます。2 台目のコントローラを取り付ける前に、このモードを有効にするようにしてください。iDRAC は、このモードの設定を許可する前にエキスパンダの機能をチェックしますが、2 台目の PERC コントローラが存在するかどうかはチェックしません。

設定を変更するには、サーバー制御権限を持っている必要があります。

他の RAID 操作が保留中の状態であるか、または RAID ジョブがスケジュールされている場合、バックプレーンモードを変更できません。同様に、この設定が保留されている場合、他の RAID ジョブをスケジュールできません。

メモ:

- 設定が変更されるときは、データロスのおそれがあることを示す警告メッセージが表示されます。
- LC ワイプまたは iDRAC のリセット操作では、このモードに対するエキスパンダ設定は変更されません。
- この操作は、リアルタイムでのみサポートされており、ステージされません。
- バックプレーン設定は複数回変更することができます。
- バックプレーンの分割処理は、ドライブの関連付けが一つのコントローラから別のコントローラに変更された場合、データ損失または外部設定を引き起こす可能性があります。
- バックプレーンの分割処理中は、ドライブの関連付けに応じて RAID 設定が影響を受ける場合があります。

この設定の変更は、システムの電源リセット後にのみ有効になります。分割モードから統合モードに変更すると、次回起動時に 2 台目のコントローラがドライブを認識しないことを示すエラーメッセージが表示されます。また、1 台目のコントローラは外部設定を認識します。エラーを無視すると、既存の仮想ディスクが失われます。

ウェブインタフェースを使用したバックプレーンモードの設定

iDRAC ウェブインタフェースを使用してバックプレーンモードを設定するには、次の手順を実行します。

1. iDRAC のウェブインタフェースで、[概要] > [ストレージ] > [エンクロージャ] > [セットアップ] と移動します。
   [エンクロージャのセットアップ] ページが表示されます。

2. [コントローラ] ドロップダウンメニューで設定するコントローラを選択して、関連するエンクロージャを設定します。
3. [値] 列で、必要なバックプレーンまたはエンクロージャに対して必要なモードを選択します。
   - 統合モード
   - 分割モード
   - 分割モード 4:20
   - 分割 8:16
   - 分割モード 16:8
   - 分割モード 20:4
   - 情報が利用不可
4. [操作モードの適用] ドロップダウンメニューから [今すぐ適用] を選択してただちに処置を適用し、次に [適用] をクリックします。
   ジョブ ID が作成されます。
5. [ジョブキュー] ページに移動して、ジョブのステータスが完了になっていることを確認します。
6. システムのパワーサイクルを実行して設定を有効にします。

RACADM を使用したエンクロージャの設定

エンクロージャまたはバックプレーンを設定するには、**BackplaneMode** のオブジェクトで `set` コマンドを使用します。

たとえば、スプリットモードに BackplaneMode 属性を設定するには、次の手順を実行します。

1. 現在のバックプレーンモードを表示するには、次のコマンドを実行します。

   ```
   racadm get storage.enclosure.1.backplanecurrentmode
   ```

   出力は次のとおりです。

   ```
   BackplaneCurrentMode=UnifiedMode
   ```
2. 要求されたモードを表示するには、次のコマンドを実行します。

   ```
   racadm get storage.enclosure.1.backplanerequestedmode
   ```

   出力は次のとおりです。

   ```
   BackplaneRequestedMode=None
   ```
3. 要求されたバックプレーンモードをスプリットモードに設定するには、次のコマンドを実行します。

   ```
   racadm set storage.enclosure.1.backplanerequestedmode "splitmode"
   ```

   コマンドが成功したことを示すメッセージが表示されます。
4. 次のコマンドを実行して、**backplanerequestedmode** 属性がスプリットモードに設定されていることを確認します。

   ```
   racadm get storage.enclosure.1.backplanerequestedmode
   ```

   出力は次のとおりです。

   ```
   BackplaneRequestedMode=None (Pending=SplitMode)
   ```
5. `storage get controllers` コマンドを実行して、コントローラのインスタンス ID を書き留めます。
6. ジョブを作成するには、次のコマンドを実行します。

   ```
   racadm jobqueue create <controller instance ID> -s TIME_NOW --realtime
   ```

   ジョブ ID が返されます。
7. ジョブステータスのクエリを実行するには、次のコマンドを実行します。

   ```
   racadm jobqueue view -i JID_xxxxxxxx
   ```

ここで、`JID_xxxxxxxx` は手順 6 のジョブ ID です。

ステータスが保留中として表示されます。

完了ステータスが表示されるまで、ジョブ ID のクエリを続行します（このプロセスには最大で 3 分かかります）。

8. `backplanerequestedmode` 属性値を表示するには、次のコマンドを実行します。

```
racadm get storage.enclosure.1.backplanerequestedmode
```

出力は次のとおりです。

```
BackplaneRequestedMode=SplitMode
```

9. サーバをコールドリブートするには、次のコマンドを実行します。

```
racadm serveraction powercycle
```

10. システムは POST と CSIOR を完了した後、次のコマンドを入力して `backplanerequestedmode` を確認します。

```
racadm get storage.enclosure.1.backplanerequestedmode
```

出力は次のとおりです。

```
BackplaneRequestedMode=None
```

11. バックプレーンモードがスプリットモードに設定されていることを確認するには、次のコマンドを実行します。

```
racadm get storage.enclosure.1.backplanecurrentmode
```

出力は次のとおりです。

```
BackplaneCurrentMode=SplitMode
```

12. 次のコマンドを実行して、ドライブ 0~11 のみが表示されていることを確認します。

```
racadm storage get pdisks
```

RACADM コマンドの詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

ユニバーサルスロットの表示

一部の第 13 世代 PowerEdge サーババックプレーンは同じスロットで SAS/SATA と PCIe SSD ドライブの両方をサポートします。これらのスロットはユニバーサルスロットと呼ばれ、プライマリストレージコントローラ（PERC）と PCIe エクステンダカードに配線されています。バックプレーンファームウェアは、この機能をサポートするスロットの情報を提供します。バックプレーンは、SAS/SATA ディスクまたは PCIe SSD をサポートします。 通常、上から 4 つの番号のスロットがユニバーサルです。たとえば、24 のスロットをサポートしているユニバーサルバックプレーンでは、0 ～ 19 のスロットが SAS/SATA ディスクのみサポートし、20 ～ 23 のスロットは SAS/SATA または PCIe SSD のどちらかをサポートします。

エンクロージャのロールアップ正常性ステータスは、エンクロージャ内のすべてのドライブについて結合された正常性ステータスを示します。［トポロジ］ページ上のエンクロージャリンクには、どちらのコントローラが関連付けられているかに関係なく、エンクロージャ情報全体が表示されます。2 台のストレージコントローラ（PERC および PCIe エクステンダ）が同じバックプレーンに接続される可能性があるため、PERC コントローラに関連付られたバックプレーンのみが ［システムインベントリ］ ページに表示されます。

［ストレージ］ > ［エンクロージャ］ > ［プロパティ］ ページの ［物理ディスクの概要］ セクションに、次の情報が表示されます。

- ［空きスロット］ — スロットが空の場合に表示されます。
- ［PCIe 対応］ — PCIe 対応スロットがない場合、この列は表示されません。
- ［バスプロトコル］ — ユニバーサルバックプレーンのスロットの 1 つに PCIe SSD が取り付けられている場合、この列に ［PCIe］が表示されます。
- ［ホットスペア］ — この列は PCIe SSD には適用されません。

メモ: ホットスワップはユニバーサルスロットに対してサポートされています。PCIe SSD ドライブを取り外し、SAS/SATA ドライブと交換する場合は、必ず最初に PCIe SSD ドライブに対する PrepareToRemove タスクを完了させてください。このタスクを実行しないと、ホストオペレーティングシステムでブルースクリーンやカーネルパニックなどの問題が発生する場合があります。

SGPIO モードの設定

ストレージコントローラは、I2C モード（Dell バックプレーンのデフォルト設定）または Serial General Purpose Input/Output（SGPIO）モードのバックプレーンに接続できます。この接続は、ドライブ上の LED を点滅させるために必要です。Dell PERC コントローラとバックプレーンは、この両方のモードをサポートします。特定のチャネルアダプタをサポートするには、バックプレーンモードを SGPIO モードに変更する必要があります。

SGPIO モードは、パッシブバックプレーンのみでサポートされます。このモードは、ダウンストリームモードのエキスパンダベースバックプレーンまたはパッシブバックプレーンではサポートされません。バックプレーンのファームウェアは、機能、現在の状態、および要求された状態に関する情報を示します。

LC ワイプ操作の後、または iDRAC をデフォルトにリセットした後は、SGPIO モードが無効な状態にリセットされます。これによって、iDRAC 設定とバックプレーン設定が比較されます。バックプレーンが SGPIO モードに設定されている場合、iDRAC の設定はバックプレーン設定と一致するように変更されます。

設定の変更を有効にするには、サーバーの電源を入れ直す必要があります。

この設定を変更するには、サーバー制御の特権権限を持っている必要があります。

メモ: iDRAC ウェブインタフェースを使用して、SGPIO モードを設定することはできません。

RACADM を使用した SGPIO モードの設定

SGPIO モードを設定するには、`SGPIOMode` グループのオブジェクトで `set` コマンドを使用します。

無効にすると、I2C モードになります。有効にすると、SGPIO モードになります。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

設定を適用する操作モードの選択

仮想ディスクの作成および管理、物理ディスク、コントローラ、およびエンクロージャの設定、またはコントローラのリセットを行う際は、さまざまな設定を適用する前に、操作モードを選択する必要があります。つまり、次の中から設定を適用するタイミングを指定します。

- 今すぐ
- 次回のシステム再起動時
- スケジュールされた時刻
- 保留中の操作が単一ジョブに含まれるバッチとして適用されるとき

ウェブインタフェースを使用した操作モードの選択

操作モードを選択して設定を適用するには、次の手順を実行します。

1. 次のページのいずれかを表示している場合は、操作モードを選択できます。
   - [概要] [ストレージ] [物理ディスク] [設定]
   - [概要] > [ストレージ] > [仮想ディスク] > [作成]
   - [概要] > [ストレージ] > [仮想ディスク] > [管理]
   - [概要] > [ストレージ] > [コントローラ] > [セットアップ]
   - [概要] > [ストレージ] > [コントローラ] > [トラブルシューティング]
   - [概要] > [ストレージ] > [エンクロージャ] > [セットアップ]
   - [概要] > [ストレージ] > [保留中の操作]
2. **操作モードの適用** ドロップダウンメニューから次のいずれかを選択します。

- ［今すぐ適用］- ただちに設定を適用するには、このオプションを選択します。このオプションは、PERC 9 コントローラのみで使用できます。完了予定のジョブがあると、このオプションはグレー表示になります。このジョブの完了には、2 分以上かかります。
- ［次の再起動時］- 次回のシステム再起動時に設定を適用するには、このオプションを選択します。これは PERC 8 コントローラのデフォルトオプションです。
- ［スケジュールされた時刻］- このオプションを選択して、スケジュールされた日付と時刻に設定を適用します。
  - ［開始時刻］と［終了時刻］- カレンダーのアイコンをクリックして日付を選択します。ドロップダウンメニューから、時刻を選択します。開始時刻と終了時刻の間に設定が適用されます。
  - ドロップダウンメニューから、再起動のタイプを選択します。
    - 再起動なし（システムを手動で再起動）
    - 正常なシャットダウン
    - 強制シャットダウン
    - システムのパワーサイクル（コールドブート）

    メモ: PERC 8 以前のコントローラでは、［正常なシャットダウン］がデフォルトオプションになっています。PERC 9 コントローラでは、［再起動なし（システムを手動で再起動）］がデフォルトのオプションです。
- ［保留中の操作に追加］- このオプションを選択して、設定を適用するための保留中の操作を作成します。コントローラのすべての保留中の操作は、［概要］>［ストレージ］>［保留中の操作］ページで表示することができます。

メモ:

- ［保留中の操作に追加］オプションは［保留中の操作］ページ、および［物理ディスク］>［セットアップ］ページの PCIe SSD には適用されません。
- ［今すぐ適用］オプションは、［エンクロージャのセットアップ］ページのみで使用できます。

3. ［適用］をクリックします。
選択したオペレーションモードに基づいて、設定が適用されます。

RACADM を使用した操作モードの選択

操作モードを選択するには、`jobqueue` コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンド ライン リファレンス ガイド*』を参照してください。

保留中の操作の表示と適用

ストレージコントローラに対する保留中の操作すべてを表示および確定できます。すべての設定は、選択したオプションに基づいて、直ちに、次回の再起動中に、またはスケジュールされた時刻に適用されます。コントローラのすべての保留中の操作を削除することができますが、個々の保留中の操作を削除することはできません。

保留中の操作は、選択したコンポーネント（コントローラ、エンクロージャ、物理ディスク、および仮想ディスク）に対して作成されます。

設定ジョブはコントローラに対してのみ作成されます。PCIe SSD の場合、ジョブは PCIe エクステンダではなく PCIe SSD ディスクに対して作成されます。

ウェブインタフェースを使用した保留中の操作の表示、適用、または削除

1. iDRAC ウェブインタフェースで、［概要］>［ストレージ］>［保留中の操作］に移動します。
［保留中の操作］ページが表示されます。
2. ［コンポーネント］ドロップダウンメニューから、保留中の操作を表示、確定、または削除するコントローラを選択します。
選択したコントローラに対する保留中の操作のリストが表示されます。

   メモ:

   - 保留中の操作は、外部設定のインポート、外部設定のクリア、セキュリティキー操作、および暗号化仮想ディスク用に作成されます。ただし、これらは［保留中の操作］ページおよび 保留中の操作 ポップアップメッセージには表示されません。
   - PCIe SSD のジョブは、［保留中の操作］ページからは作成できません。
3. 選択したコントローラに対する保留中の操作を削除するには、［保留中の操作をすべて削除］をクリックします。
4. ドロップダウンメニューから、次のいずれかを選択して［適用］をクリックし、保留中の操作を確定します。

- ［今すぐ適用］- このオプションを選択して、すべての操作を直ちに確定します。このオプションは、最新のファームウェアバージョンを搭載した PERC 9 コントローラで使用できます。
- ［次の再起動時］- このオプションを選択して、すべての操作を次回のシステム再起動時に確定します。これは PERC 8 コントローラのデフォルトオプションです。このオプションは、PERC 8 以降のバージョンに適用されます。
- ［スケジュールされた時刻］- このオプションを選択して、スケジュールされた日付と時刻に操作を確定します。このオプションは、PERC 8 以降のバージョンに適用されます。
  - ［開始時刻］と［終了時刻］- カレンダーのアイコンをクリックして日付を選択します。ドロップダウンメニューから、時刻を選択します。開始時刻と終了時刻の間に処置が適用されます。
  - ドロップダウンメニューから、再起動のタイプを選択します。
    - 再起動なし（システムを手動で再起動）
    - 正常なシャットダウン
    - 強制シャットダウン
    - システムのパワーサイクル（コールドブート）

    メモ: PERC 8 以前のコントローラでは、［正常なシャットダウン］がデフォルトオプションになっています。PERC 9 コントローラでは、［再起動なし（システムを手動で再起動）］がデフォルトのオプションです。

5. 確定ジョブが作成されていない場合は、ジョブの作成に正常に行われなかったことを示すメッセージが表示されます。また、メッセージ ID および推奨される対応処置も表示されます。
6. 確定ジョブが正常に作成されると、選択されたコントローラにジョブ ID が作成されたことを示すメッセージが表示されます。［ジョブキュー］をクリックして［ジョブのキュー］ページのジョブの進行状況を表示します。

   外部設定のクリア、外部設定のインポート、セキュリティキー操作、または仮想ディスクの暗号化操作が保留中の状態である場合、また、保留中の操作が他に存在しない場合、［保留中の操作］ページからジョブを作成できません。その他のストレージ設定操作を実行するか、RACADM または WSMAN を使用して必要なコントローラに必要な設定ジョブを作成します。

   ［保留中の操作］ページでは、PCIe SSD に対する保留中の操作を表示したりクリアしたりすることはできません。PCIe SSD に対する保留中の操作をクリアするには、racadm コマンドを使用します。

RACADM を使用した保留中の操作の表示と適用

保留中の操作を適用するには、**jobqueue** コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインリファレンスガイド*』を参照してください。

ストレージデバイス — 操作適用のシナリオ

［ケース 1：動作モードの適用（今すぐ適用、次の再起動時、または スケジュールされた時刻）を選択し、既存の保留中の操作がない場合］

［今すぐ適用］、［次の再起動時］、または［スケジュールされた時刻］を選択して［適用］をクリックした場合、まず選択したストレージ設定操作のための保留中の操作が作成されます。

- 保留中の操作が正常に完了し、それ以前に他に既存の保留中の操作がなければ、ジョブが作成されます。ジョブが正常に作成された場合、選択したデバイスにそのジョブ ID が作成されたことを示すメッセージが表示されます。［ジョブキュー］をクリックすると、［ジョブキュー］ページでジョブの進行状況が表示されます。ジョブが作成されなかった場合、ジョブの作成が正常に終了しなかったことを示すメッセージが表示されます。また、メッセージ ID、および推奨される対応処置が表示されます。
- 保留中の操作の作成が正常に行われず、それ以前に既存の保留中の操作がない場合、ID およびエラーメッセージと、推奨される対応処置が表示されます。

［ケース 2：動作モードの適用（今すぐ適用、次の再起動時、または スケジュールされた時刻）を選択し、既存の保留中の操作がある場合］

［今すぐ適用］、［次の再起動時］、または［スケジュールされた時刻］を選択して［適用］をクリックした場合、まず選択したストレージ設定操作のための保留中の操作が作成されます。

- 保留中の操作が正常に作成され、既存の保留中の操作がある場合、メッセージが表示されます。
  - そのデバイスの保留中の操作を表示するには、［保留中の操作の表示］リンクをクリックします。
  - 選択したデバイスにジョブを作成するには、［ジョブの作成］をクリックします。ジョブが正常に作成された場合、選択したデバイスにそのジョブ ID が作成されたことを示すメッセージが表示されます。［ジョブキュー］をクリックすると、［ジョ

ブキュー] ページでジョブの進行状況が表示されます。ジョブが作成されなかった場合、ジョブの作成が正常に終了しなかったことを示すメッセージが表示されます。また、メッセージ ID、および推奨される対応処置が表示されます。
  - ジョブを作成しない場合は、[キャンセル] をクリックします。その場合、続いてストレージ設定操作を行うため、そのページに止まります。
- 保留中の操作が正常に作成されず、既存の保留中の操作がある場合、エラーメッセージが表示されます。
  - そのデバイスの保留中の操作を表示するには、**保留中の操作** をクリックします。
  - 既存の保留中の操作にジョブを作成するには、**正常な操作のためのジョブの作成** をクリックします。ジョブが正常に作成された場合、選択したデバイスにそのジョブ ID が作成されたことを示すメッセージが表示されます。**ジョブキュー** をクリックすると、**ジョブキュー** ページでジョブの進行状況が表示されます。ジョブが作成されなかった場合、ジョブの作成が正常に終了しなかったことを示すメッセージが表示されます。また、メッセージ ID、および推奨される対応処置が表示されます。
  - ジョブを作成しない場合は、**キャンセル** をクリックします。その場合、続いてストレージ設定操作を行うため、そのページに止まります。

[ケース 3 : 保留中の操作に追加 を選択し、既存の保留中の操作がない場合]

保留中の操作に追加 を選択し [適用] をクリックした場合、まず選択されたストレージ設定操作の保留中の操作が作成されます。
- 保留中の操作が正常に作成され、既存の保留中の操作がない場合、次の参考メッセージが表示されます。
  - [OK] をクリックすると、続けてストレージ設定操作を行うため、このページに止まります。
  - [保留中の操作] をクリックすると、デバイスの保留中の操作を表示します。選択したコントローラー上でジョブが作成されるまでは、これらの保留中の操作は適用されません。
- 保留中の操作が正常に作成されず、既存の保留中の操作がない場合、エラーメッセージが表示されます。

[ケース 4 : 保留中の操作に追加 を選択し、それ以前に既存の保留中の操作がある場合]

[保留中の操作に追加] を選択し [適用] をクリックした場合、まず選択されたストレージ設定操作の保留中の操作が作成されます。
- 保留中の操作が正常に作成され、既存の保留中の操作がある場合、次の参考メッセージが表示されます。
  - [OK] をクリックすると、続けてストレージ設定操作を行うため、このページに止まります。
  - そのデバイスの保留中の操作を表示するには、[保留中の操作] をクリックします。
- 保留中の操作が正常に作成されず、既存の保留中の操作がある場合、エラーメッセージが表示されます。
  - [OK] をクリックすると、続けてストレージ設定操作を行うため、このページに止まります。
  - そのデバイスの保留中の操作を表示するには、[保留中の操作] をクリックします。

メモ:
- いかなる時にも、ストレージ設定ページにジョブを作成するオプションがない場合は、既存の保留中の操作を表示し、必要なコントローラでジョブを作成するには、[ストレージの概要] > [保留中の操作] ページにアクセスします。
- PCIe SSD には、ケース 1 および 2 のみが適用されます。PCIe SSD に対して保留中の操作を表示することはできないため、[保留中の操作に追加] オプションは使用できません。racadm コマンドを使用して、PCIe SSD に対する保留中の操作をクリアします。

コンポーネント LED の点滅または点滅解除

ディスク上の発光ダイオード (LED) のいずれかを点滅させることによって、エンクロージャ内の物理ディスク、仮想ディスクドライブ、および PCIe SSD を見つけることができます。

LED を点滅または点滅解除するには、ログイン権限を持っている必要があります。

コントローラは、リアルタイム設定対応であることが必要です。この機能のリアルタイムサポートは、PERC 9.1 以降のファームウェアでのみ使用できます。

メモ: バックプレーンを装備していないサーバーの点滅または点滅解除はサポートされません。

ウェブインタフェースを使用したコンポーネントの LED の点滅または点滅解除

コンポーネント LED を点滅または点滅解除するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、必要に応じて次のいずれかのページに移動します。
   - [概要] > [ストレージ] > [識別] - [コンポーネント LED の識別] ページが表示されるので、そこで物理ディスク、仮想ディスク、および PCIe SSD の点滅または点滅解除を行うことができます。

- ［概要］>［ストレージ］>［物理ディスク］>［識別］-［物理ディスクページの識別］ページが表示されるので、そこで物理ディスクと PCIe SSD の点滅または点滅解除を行うことができます。
- ［概要］>［ストレージ］>［仮想ディスク］>［識別］-［仮想ディスクの識別］ページが表示されるので、そこで仮想ディスクの点滅または点滅解除を行うことができます。

2. ［コンポーネント LED の識別］ページが表示されている場合は、次の手順を実行します。
   - すべてのコンポーネント LED を選択または選択解除 -［すべて選択 / 選択解除］オプションを選択して［点滅］をクリックし、コンポーネントの LED の点滅を開始します。同様に、［点滅解除］をクリックしてコンポーネントの LED の点滅を停止します。
   - 個々のコンポーネント LED を選択または選択解除 - 1 つ、または複数のコンポーネントを選択して［点滅］をクリックし、選択したコンポーネント LED の点滅を開始します。同様に、［点滅解除］をクリックしてコンポーネントの LED の点滅を停止します。
3. ［物理ディスクの識別］ページが表示されている場合は、次の手順を実行します。
   - すべての物理ディスクドライブまたは PCIe SSD を選択または選択解除 -［すべて選択 / 選択解除］オプションを選択して［点滅］をクリックし、すべての物理ディスクドライブと PCIe SSD の LED の点滅を開始します。同様に、［点滅解除］をクリックして LED の点滅を停止します。
   - 個々の物理ディスクドライブまたは PCIe SSD を選択または選択解除 - 1 つまたは複数の物理ディスクを選択し、［点滅］をクリックして物理ディスクドライブまたは PCIe SSD の LED の点滅を開始します。同様に、［点滅解除］をクリックして LED の点滅を停止します。
4. ［仮想ディスクの識別］ページが表示されている場合は、次の手順を実行します。
   - すべての仮想ディスクをを選択または選択解除 -［すべて選択 / 選択解除］オプションを選択し、［点滅］をクリックしてすべての仮想ディスクの LED の点滅を開始します。同様に、［点滅解除］をクリックして LED の点滅を停止します。
   - 個々の仮想ディスクを選択または選択解除 - 1 つまたは複数の仮想ディスクを選択し、［点滅］をクリックして仮想ディスクの LED の点滅を開始します。同様に、［点滅解除］をクリックして LED の点滅を停止します。

   点滅または点滅解除操作に失敗した場合は、エラーメッセージが表示されます。

RACADM を使用したコンポーネント LED の点滅または点滅解除

コンポーネント LED を点滅または点滅解除するには、次のコマンドを使用します。

```
racadm storage blink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

```
racadm storage unblink:<PD FQDD, VD FQDD, or PCIe SSD FQDD>
```

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインリファレンスガイド*』を参照してください。

14

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 6 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。
- Java、ActiveX または HTML5 プラグインを使って、対応ウェブブラウザで仮想コンソールを起動することができます。
- 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。

  メモ: お使いのブラウザを仮想コンソールにアクセスするように設定する場合は、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 、p. 58 を参照してください。

関連概念

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 、p. 58
仮想コンソールの設定 、p. 226
仮想コンソールの起動 、p. 226

トピック :

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 34. 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

表 34. 対応画面解像度とリフレッシュレート （続き）

画面解像度	リフレッシュレート（Hz）
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、ローカルモニタで X11 コンソールを表示できないことがあります。iDRAC 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、iDRAC 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。

関連概念

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 、p. 58
仮想コンソールの起動 、p. 226

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

iDRAC 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 ］ > ［ 仮想コンソール ］ 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、『iDRAC オンラインヘルプ』を参照してください。

   メモ: Nano オペレーティングシステムを使用している場合は、［ 仮想コンソール ］ ページで ［ 自動システムロック ］ 機能を無効にします。

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、**iDRAC.VirtualConsole** グループのオブジェクトで `set` コマンドを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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、iDRAC 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。
- ウェブブラウザは、HTML5、Java、または ActiveX プラグインを使用するように設定されています。
- 最低限のネットワーク帯域幅（1 MB/ 秒）が利用可能。

メモ: 内蔵ビデオコントローラが BIOS で無効化されているときに仮想コンソールを起動した場合、仮想コンソールビューアには何も表示されません。

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、HTML5 を使用、または該当するブラウザで利用可能で必須プラグイン（Java または ActiveX）を使用します。インターネットオプションの設定はすべてのブラウザで共通しています。

Java プラグインを使用して仮想コンソールを起動する間、時折 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。

HTML5 プラグインを使用して仮想コンソールを起動するには、ポップアップブロッカーを無効にする必要があります。

関連概念

URL を使用した仮想コンソールの起動、p. 227
HTML5 ベースのプラグインを使用するための Internet Explorer の設定、p. 59
Java プラグインを使用するためのウェブブラウザの設定、p. 59
ActiveX プラグインを使用するための IE の設定、p. 60
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、p. 227
Java または ActiveX プラグインを使用した仮想コンソールまたは仮想メディアの起動中における警告メッセージの無効化、p. 228
マウスポインタの同期、p. 230

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] > [仮想コンソール] 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。

アプリケーションを起動すると、複数のメッセージボックスが表示されることがあります。アプリケーションへの不許可のアクセスを防ぐため、3 分以内にこれらのメッセージボックスで適切な操作を行ってください。3 分過ぎると、アプリケーションの再起動を求められます。

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。

2 つのマウスポインタがビューアウィンドウに表示されることがあります。1 つは管理下サーバー用で、もう 1 つは管理ステーション用です。カーソルを同期するには、「マウスポインタの同期」を参照してください。

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://iDRAC_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。

Java または ActiveX プラグインを使用した仮想コンソールまたは仮想メディアの起動中における警告メッセージの無効化

Java プラグインを使用して、仮想コンソールまたは仮想メディアの起動中における警告メッセージを無効化することができます。

1. Java プラグインを使用して仮想コンソールまたは仮想メディアを起動した当初、発行元を確認するプロンプトが表示されます。［はい］をクリックします。

   信頼済み証明書が見つからなかったことを示す証明書警告メッセージが表示されます。

   メモ: OS の証明書ストア、または以前に指定されたユーザーの場所で証明書が見つかった場合、この警告メッセージは表示されません。

2. ［続行］をクリックします。

   仮想コンソールビューア、または仮想メディアビューアが起動されます。

   メモ: 仮想コンソールが無効化されている場合は、仮想メディアビューアが起動されます。

3. ［ツール］メニューから［セッションオプション］をクリックし、［証明書］タブをクリックします。
4. ［パスの参照］をクリックしてユーザーの証明書を保存する場所を指定してから、［適用］をクリック、および［OK］をクリックして、ビューアを終了します。
5. 仮想コンソールを再度起動します。
6. 証明書警告メッセージで、［この証明書を常に信頼］オプションを選択して［続行 ］をクリックします。
7. ビューアを終了します。
8. 仮想コンソールを再起動すると、警告メッセージは表示されません。

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、仮想コンソールスケーリング、チャットオプション、キーボードマクロ、電源操作、次の起動デバイス、および仮想メディアへのアクセスなどのさまざまな制御を実行できます。これらの機能の使用方法については、『iDRAC 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 iDRAC の DNS 名または IP アドレスが表示されます。iDRAC 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 name / IPv6 address / IPv4 address>, <Model>, User: <username>, <fps>
  ```

- ブレードサーバーの場合：

  ```
  <DNS name / IPv6 address / IPv4 address>, <Model>, <Slot number>, User: <username>, <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。

HTML5 ベースの仮想コンソール

メモ: HTML ベースの仮想コンソールは、Windows 10 でのみサポートされます。この機能にアクセスするには、Internet Explorer 11 または Google Chrome を使用する必要があります。

メモ: HTML5 を使用して仮想コンソールにアクセスする場合は、クライアントとターゲットとの間で、キーボードレイアウト、OS、およびブラウザの言語を統一しておく必要があります。例えば、すべての設定は英語 (米国) などの対応言語に統一する必要があります。

HTML5 仮想コンソールを起動するには、iDRAC 仮想コンソール ページから仮想コンソール機能を有効にし、[仮想コンソールタイプ] オプションを HTML5 に設定する必要があります。

仮想コンソールは、次のいずれかの方法を使用することによって、ポップアップウィンドウとして起動することができます。

- iDRAC ホームページから、コンソールプレビュー セッションで使用できる [起動] リンクをクリックします
- iDRAC 仮想コンソール ページで、[仮想コンソールの起動] をクリックします。
- iDRAC のログインページで、[https//<iDRAC IP>/console] と入力します。この方法は直接起動と呼ばれます。

HTML5 の仮想コンソールでは、次のメニューオプションを使用できます。

- チャット
- キーボード
- 画面キャプチャ
- 更新
- 全画面
- ビューアを切断
- コンソール制御
- 仮想メディア

[Pass all keystrokes to server (すべてのキーストロークをサーバに渡す)] オプションは、HTML5 仮想コンソールではサポートされません。ファンクションキーはすべて、キーボードおよびキーボードマクロを使用します。

- コンソール制御 - これには次の設定オプションがあります。
  - キーボード
  - キーボードマクロ
  - アスペクト比
  - タッチモード
  - マウスアクセラレーション
- キーボード - このキーボードはオープンソースコードを使用します。物理キーボードとの違いは、[Caps Lock] キーが有効になると、数値キーが特殊文字に切り替わる点です。[Caps Lock] キーが有効になっている時に特殊文字を押しても、機能性は変わらず、数字が入力されます。
- キーボードマクロ - これは HTML5 仮想コンソールでサポートされており、次のドロップダウンオプションとして一覧表示されます。[Apply (適用)] をクリックして、選択されたキーの組み合わせをサーバに適用します。
  - Ctrl+Alt+Del
  - Alt+Tab
  - Alt+ESC
  - Ctrl+ESC
  - Alt+Space
  - Alt+Enter
  - Alt+Hyphen
  - Alt+F4
  - PrntScrn
  - Alt+PrntScrn
  - F1
  - Pause
  - Tab
  - Ctrl+Enter
  - SysRq
  - Alt+SysRq
- アスペクト比 - HTML5 仮想コンソールのビデオイメージは、画像を可視化するためにサイズが自動的に調整されます。次の設定オプションがドロップダウンリストに表示されます。
  - 保守
  - 維持しない

［適用］をクリックしてサーバーに選択された設定を適用します。

- タッチモード - HTML5 仮想コンソールはタッチモード機能をサポートします。次の設定オプションがドロップダウンリストに表示されます。
    - ダイレクト
    - 相対座標

  ［適用］をクリックしてサーバーに選択された設定を適用します。
- マウスアクセラレーション - マウスアクセラレーションは、オペレーティングシステムに基づいて選択します。次の設定オプションがドロップダウンリストに表示されます。
    - 絶対座標（Windows、Linux の最新バージョン、Mac OS-X）
    - 相対座標、アクセラレーションなし
    - 相対座標（RHEL、または Linux の旧バージョン）
    - Linux RHEL 6.x および SUSE Linux Enterprise Server 11 以降

  ［適用］をクリックしてサーバーに選択された設定を適用します。
- 仮想メディア - ［Connect Virtual Media（仮想メディアに接続する）］オプションをクリックして仮想メディアセッションを開始します。仮想メディアメニューには、ISO ファイルや IMG ファイルを参照してマップするための［Browse（参照）］オプションが表示されます。

  メモ: HTML5 ベースの仮想コンソールを使用して USB ベースのドライブ、CD または DVD などの物理メディアをマップすることはできません。

対応ブラウザ

HTML5 仮想コンソールは次のブラウザでサポートされています。

- Internet Explorer 11
- Chrome 36
- Firefox 30
- Safari 7.0

サポートされるブラウザおよびバージョンの詳細については、**dell.com/idracmanuals** にある『*iDRAC リリースノート*』を参照してください。

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。

クライアント仮想コンソールビューアに 2 つのマウスカーソルが表示される場合、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 では一般的で、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での加速設定と異なる場合に発生します。これを解決するには、シングルカーソルに切り替えるか、管理下システムと管理ステーションのマウス加速を一致させます。

- シングルカーソルに切り替えるには、［ツール］メニューから［シングルカーソル］を選択します。
- マウス加速を設定するには、［ツール］>［セッションオプション］>［マウス］と移動します。［マウス加速］タブで、オペレーティングシステムに応じて［Windows］または［Linux］を選択します。

シングルカーソルモードを終了するには、<F9>、または設定した終了キーを押します。

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がインストールされ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。iDRAC 仮想コンソールでマウスを正しく同期化するには、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以下を追加します。

```
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化し、[仮想コンソール] ページで [最大セッション数] を `1` に設定し直す必要があります。

すべてのキーストロークを Java または ActiveX のプラグイン用の仮想コンソール経由で渡す

[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て、すべてのキーストロークとキーの組み合わせを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送信することができます。これが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渡されます。すべてのキーストロークをサーバーに渡すには、仮想コンソールビューアで [ツール] > [セッションオプション] > [一般] タブに移動し、[すべてのキーストロークをサーバーに渡す] オプションを選択して管理ステーションのキーストロークを管理下システムに渡します。

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)。

  Java クライアントの場合、すべてのキーストロークをサーバーに渡す機能とシングルカーソルモードを動作させるには、ネイティブライブラリをロードする必要があります。ネイティブライブラリがない場合は、[すべてのキーストロークをサーバーに渡す] と [シングルカーソル] オプションは選択解除されています。いずれかのオプションを選択しようとすると、選択したオプションはサポートされていないことを示すエラーメッセージが表示されます。

  ActiveX クライアントの場合、すべてのキーストロークをサーバーに渡す機能を動作させるためにはネイティブライブラリをロードする必要があります。ネイティブライブラリがない場合、[すべてのキーストロークをサーバーに渡す] オプションは選択解除されています。このオプションを選択しようとすると、この機能がサポートされていないことを示すエラーメッセージが表示されます。

  MAC オペレーティングシステムの場合、すべてのキーストロークをサーバーに渡す機能を動作させるためには、[ユニバーサルアクセス] 内の [補助装置にアクセスできるようにする] オプションを有効にします。

- 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] 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。

関連概念

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 、p. 231
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 、p. 232
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 、p. 233

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下システムで 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] メニューは管理下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。

リモートコンソール経由での SysRq マジックキーの使用

SysRq マジックキー は、次のいずれかを使用してリモートコンソール経由で有効化することができます。

- Opensource IPMI ツール
- SSH/Telnet または外部シリアルコネクタ

オープンソース IPMI ツールの使用

BIOS/iDRAC 設定が SOL を使用したコンソールリダイレクトをサポートしていることを確認します。

1. コマンドプロンプトで、SOL をアクティブ化するコマンドを入力します。

```
Ipmitool -I lanplus -H <ipaddr> -U <username> -P <passwd> sol activate
```

   SOL セッションがアクティブ化されます。

2. サーバーがオペレーティングシステムから起動したら、`localhost.localdomain` ログインプロンプトが表示されます。オペレーティングシステムのユーザー名とパスワードを使用してログインします。
3. SysRq が有効になっていない場合は、`echo 1 >/proc/sys/kernel/sysrq` を使用して有効にします。
4. ブレークシーケンス、`~B` を実行します。
5. SysRq マジックキーを使用して SysRq 機能を有効にします。たとえば、次のコマンドはコンソールにメモリ情報を表示します。

```
echo m > /proc/sysrq-trigger displays
```

SSH/Telnet または外付けシリアルコネクタの使用（シリアルケーブル経由で直接接続）

1. telnet/SSH セッションでは、iDRAC のユーザー名とパスワードでログインした後、`/admin>` プロンプトで `console com 2` コマンドを実行します。`localhost.localdomain` プロンプトが表示されます。
2. シリアルケーブル経由でシステムに直接接続された外付けシリアルコネクタを使用するコンソールのリダイレクトでは、サーバーがオペレーティングシステムから起動した後、`localhost.localdomain` ログインプロンプトが表示されます。
3. オペレーティングシステムのユーザー名とパスワードを使用してログインします。
4. SysRq が有効になっていない場合は、`echo 1 >/proc/sys/kernel/sysrq` を使用して有効にします。
5. マジックキーを使用して SysRq 機能を有効にします。たとえば、次のコマンドはサーバーを再起動します。

```
echo b > /proc/sysrq-trigger
```

メモ: マジック SysRq キーを使用する前に、ブレークシーケンスを実行する必要はありません。

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。

  `Click Help on the Virtual Console page to view the online Help`

- 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。

15

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 iDRAC 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。

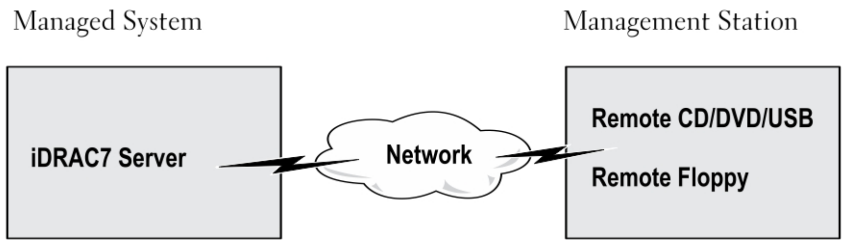


図 4. 仮想メディアセットアップ

トピック：

対応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 35. 対応ドライブとデバイス

ドライブ	対応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。

関連概念

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 、p. 58

iDRAC 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、iDRAC をリセットしないでください。リセットした場合、データロスなど望ましくない結果が生じることがあります。**

1. iDRAC 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、『iDRAC 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、**iDRAC.VirtualMedia** グループのオブジェクトで set コマンドを使用します。

詳細に関しては、**dell.com/idracmanuals** にある『*iDRAC 向け RACADM コマンドライン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できます。この手順は次のとおりです。

1. iDRAC 設定ユーティリティで、［メディアおよび USB ポートの設定］ に移動します。
   ［iDRAC 設定：メディアおよび USB ポートの設定］ ページが表示されます。
2. ［仮想メディア］ セクションで、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。
   仮想メディア設定が設定されます。

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 36. 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。

仮想メディアで仮想デバイスを表示するためのサーバー設定

空のドライブを認識できるようにするには、管理ステーションで次の設定項目を設定する必要があります。これを行うには、Windows エクスプローラで、[整理] メニューから [フォルダと検索のオプション] をクリックします。[表示] タブで、[空のドライブはコンピュータフォルダに表示しない] オプションの選択を解除し、[OK] をクリックします。

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する、しないに関わりなくアクセスすることができます。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。

仮想メディアと RFS は相互排他的です。RFS 接続がアクティブであるときに仮想メディアのクライアントの起動を試みると、*仮想メディアは現在使用できません。仮想メディアまたはリモートファイル共有セッションが使用中です* というエラーメッセージが表示されます。

RFS 接続がアクティブではないときに仮想メディアクライアントの起動を試行すると、クライアントは正常に起動します。その後、仮想メディアクライアントを使って、デバイスとファイルを仮想メディア仮想ドライブにマップすることができます。

関連概念

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 、p. 58
仮想メディアの設定 、p. 235

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 - 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ーフォルダに表示しない] オプションをクリアして、[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. iDRAC ウェブインタフェースで、[概要] > [サーバー] > [仮想コンソール] 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][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 では、Java が仮想コンソールへのアクセスのためのデフォルトのプラグインタイプです。Windows では、`.jnlp` ファイルを開いて Java を使用して、仮想コンソールを起動します。
3. [仮想メディア] > [仮想メディアの接続] の順にクリックします。
   仮想メディアセッションが確立され、[仮想メディア] メニューにマッピングに利用可能なデバイスのリストが表示されます。

   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。

関連概念

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 、p. 58
仮想メディアの設定 、p. 235
Java または ActiveX プラグインを使用した仮想コンソールまたは仮想メディアの起動中における警告メッセージの無効化 、p. 228

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. iDRAC ウェブインタフェースで、[概要] > [サーバー] > [仮想コンソール] 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][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。

   ```
   Virtual Console has been disabled. Do you want to continue using Virtual Media redirection?
   ```

3. [OK] をクリックします。
   [仮想メディア] ウィンドウが表示されます。
4. [仮想メディア] メニューから [CD/DVD のマップ] または、[リムーバブルディスクのマップ] をクリックします。
   詳細については、「仮想ドライブのマッピング」を参照してください。

   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。

   メモ: HTML5 プラグインは、スタンダロン仮想メディアではサポートされません。

関連概念

仮想メディアの設定 、p. 235
Java または ActiveX プラグインを使用した仮想コンソールまたは仮想メディアの起動中における警告メッセージの無効化 、p. 228

仮想メディアイメージの追加

リモートフォルダのメディアイメージを作成し、USB 接続し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することができます。仮想メディアのイメージを追加するには、次の手順を実行します。

1. [仮想メディア] > [イメージの作成...] をクリックします。
2. [ソースフォルダ] フィールドに移動し、[参照] をクリックし、イメージファイルのソースとして使用するフォルダまたはディレクトリに移動します。イメージファイルは管理ステーションまたは管理システムの C: ドライブにあります。
3. [イメージファイル名] フィールドに、作成されたイメージファイルを保管先となるデフォルトパス (通常はデスクトップディレクトリ) が表示されます。この場所を変更するには、[参照] をクリックして場所に移動します。
4. [イメージの作成] をクリックします。
   イメージ作成処理が開始されます。イメージファイルの場所がソースフォルダ内の場合、ソースフォルダ内のイメージファイルの場所が無限ループを生じるため、イメージ作成を続行できませんというメッセージが表示されます。イメージファイルの場所がソースフォルダ内ではない場合は、イメージ作成が続行されます。

   イメージの作成後、成功メッセージが表示されます。
5. [終了] をクリックします。

   イメージが作成されます。

フォルダがイメージとして追加されると、**.img** 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 **.img** ファイルが移動または削除されると、仮想メディアの ［メニュー］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、イメージの使用中に ［.img］ 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、［.img］ 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。

仮想デバイスの詳細情報の表示

仮想デバイスの詳細を表示するには、仮想コンソールビューアで ［ツール］ > ［ 統計］ とクリックします。［ 統計］ ウィンドウの ［仮想メディア］ セクションに、マップされた仮想デバイスと、各デバイスの読み取り / 書き込みアクティビティが表示されます。仮想メディアが接続されていると、この情報が表示されます。仮想メディアが接続されていない場合は、「仮想メディアが接続されていません」というメッセージが表示されます。

仮想コンソールを使用せずに仮想メディアが起動された場合は、［ 仮想メディア ］ セクションがダイアログボックスとして表示されます。このボックスには、マップされたデバイスに関する情報が提供されます。

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. 仮想コンソールビューアで、［ ツール ］ > ［ 統計］ をクリックします。
   ［ 統計］ ウィンドウが表示されます。
2. ［ 仮想メディア ］下で、［ 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。
3. ［ はい ］ をクリックします。

   USB がリセットされます。

   メモ: iDRAC 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、iDRAC 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、iDRAC 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. 仮想メディアセッションを確立するには、［ 仮想メディア ］ メニューで ［ 仮想メディアの接続 ］ をクリックします。

   ホストサーバーからのマップに使用できる各デバイスのために、［ 仮想メディア ］ メニュー下にメニューアイテムが表示されます。メニューアイテムは、次にあるようにデバイスタイプに従って命名されています。

   - CD/DVD をマップ
   - リムーバブルディスクのマップ
   - フロッピーディスクをマップ

   メモ: ［ 連結されたメディア ］ ページで ［ フロッピーのエミュレーション ］ オプションが有効になっていると、リストに ［ フロッピーディスクをマップ ］ メニュー項目が表示されます。［ フロッピーのエミュレーション ］ が有効になっていると、［ リムーバブルフロッピーディスクのマップ ］ が ［ フロッピーディスクをマップ ］ と置き換えられます。

   ［ CD/DVD のマップ ］ オプションは ISO ファイル用に使用することができ、［ リムーバブルディスクのマップ ］ オプションをイメージに使用することができます。

   メモ: HTML5 ベースの仮想コンソールを使用して USB ベースのドライブ、CD または DVD などの物理メディアをマップすることはできません。

2. マップするデバイスのタイプをクリックします。

   メモ: アクティブセッションは、仮想メディアセッションが、現在のウェブインタフェースセッション、別のウェブインタフェースセッション、または VMCLI からアクティブであるかどうかを表示します。

3. ［ ドライブ / イメージファイル ］ フィールドで、ドロップダウンリストからデバイスを選択します。

リストには、マッピングが可能な（マップされていない）デバイス（CD/DVD、リムーバブルディスク、フロッピーディスク）、およびマップできるイメージファイルタイプ（ISO または IMG）が表示されます。イメージファイルはデフォルトのイメージファイルディレクトリ（通常はユーザーのデスクトップ）にあります。ドロップダウンリストにデバイスがない場合は、[参照] をクリックしてデバイスを指定してください。

CD/DVD の正しいファイルの種類は ISO で、リムーバブルディスクとフロッピーディスクでは IMG です。

イメージをデフォルトのパス（デスクトップ）に作成した場合、[リムーバブルディスクをマップ] を選択すると、作成したイメージをドロップダウンメニューから選択できるようになります。

別の場所にイメージを作成した場合、[リムーバブルディスクをマップ] を選択すると、作成したイメージはロップダウンメニューから選択できません。[参照] をクリックして、イメージを指定してください。

4. [読み取り専用] を選択すると、書き込み可能なデバイスが読み取り専用としてマップされます。

   CD/DVD デバイスの場合は、このオプションはデフォルトで有効で、無効にすることはできません。

   メモ: HTML5 仮想コンソールを使用して ISO および IMG ファイルをマップすると、これらは読み取り専用ファイルとしてマップされます。

5. [デバイスのマップ] をクリックして、デバイスをホストサーバーにマップします。

   デバイス / ファイルのマップ後、デバイス名を示すためにその [仮想メディア] メニューアイテムの名前が変わります。たとえば、CD/DVD デバイスが `foo.iso` という名前のイメージファイルにマップされた場合、仮想メディアメニューの CD/DVD メニューアイテムは [CD/DVD にマップされた foo.iso] と命名されます。そのメニューアイテムのチェックマークは、それがマップされていることを示します。

関連概念

マッピング用の正しい仮想ドライブの表示 、p. 239
仮想メディアイメージの追加 、p. 237

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。

関連概念

仮想ドライブのマッピング 、p. 238

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] メニューから、次のいずれかの操作を行います。
   - マッピングを解除するデバイスをクリックします。
   - [仮想メディアの切断] をクリックします。

   確認を求めるメッセージが表示されます。
2. [はい] をクリックします。
   そのメニュー項目のチェックマークは表示されず、ホストサーバーにマップされていないことが示されます。

   メモ: Macintosh オペレーティングシステムを実行しているクライアントシステムから、vKVM に連結されているる USB デバイスをマップ解除した後は、その USM デバイスをクライアント上で使用できなくなる場合があります。システムを再起動するか、クライアントシステムにデバイスを手動でマウントして、デバイスを表示します。

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. iDRAC 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て、起動中に [<F2>] を押します。
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。

関連概念

仮想ドライブのマッピング 、p. 238
仮想メディアの設定 、p. 235

16

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 iDRAC 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導入するために、イメージファイルや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 は TLS 1.0 セキュリティプロトコルのみをサポートします。

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
- iDRAC ファームウェアの ［1 回限りの起動］ オプションが有効な場合のセッションの自動終了
- Secure Socket Layer（SSL）を使用した iDRAC 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。

トピック：

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、iDRAC 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に、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 [parameter] [operating_system_shell_options]`

例：`vmcli -r iDRAC-IP-address:iDRAC-SSL-port`

このパラメータは、VMCLI による指定したサーバーへの接続、iDRAC 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 <iDRAC-IP-address[:iDRAC-SSL-port]> -S -u <iDRAC-user-name> -p <iDRAC-user-password> -c {<device-name> | <image-file>}` — iDRAC 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 Man* ページを参照してください。

関連概念

仮想メディアにアクセスするための VMCLI コマンド 、p. 242
VMCLI オペレーティングシステムのシェルオプション 、p. 242

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 37. 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 or hostname] -u [iDRAC user name] -p [iDRAC user password] -f [device name]`
起動可能なフロッピーまたは USB キーイメージ	`vmcli -r [iDRAC IP address] [iDRAC user name] -p [iDRAC password] -f [floppy.img]`
-f オプションを使用した CD ドライブ	`vmcli -r [iDRAC IP address] -u [iDRAC user name] -p [iDRAC password] -f [device name]|[image file]-f [cdrom - dev ]`
起動可能な CD/DVD イメージ	`vmcli -r [iDRAC IP address] -u [iDRAC user name] -p [iDRAC password] -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。

17

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 iDRAC 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 card not detected. Please insert an SD card of size 256MB or greater.
```

メモ: iDRAC 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。

メモ: FIPS モードが有効の場合は、vFlash 操作を実行できません。

トピック：

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、**dell.com/support/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 機能を有効または無効にしたり、カードを初期化したりするには、仮想メディアへのアクセス権限を持っている必要があります。

関連概念

vFlash SD カードプロパティの表示、p. 244
vFlash 機能の有効化または無効化、p. 245
vFlash SD カードの初期化、p. 246

vFlash SD カードプロパティの表示

vFlash 機能が有効になると、iDRAC 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、iDRAC 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ついては、『iDRAC 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 カードプロパティを表示するには、次のオブジェクトで `get` コマンドを使用します。

- iDRAC.vflashsd.AvailableSize
- iDRAC.vflashsd.Health
- iDRAC.vflashsd.Licensed
- iDRAC.vflashsd.Size
- iDRAC.vflashsd.WriteProtect

これらのオブジェクトの詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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 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［メディアおよび USB ポートの設定］に移動します。［メディアおよび USB ポートの設定］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。

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 機能を有効または無効にするには、次の手順を実行します。

1. iDRAC 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。

```
racadm set iDRAC.vflashsd.Enable [n]
```

n=0
: 無効

n=1
: 有効

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、*ERROR: SD Card not present*（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、[メディアおよび USB ポートの設定] に移動します。
   [iDRAC 設定 : メディアおよび USB ポートの設定] ページが表示されます。
2. [vFlash メディア] セクションで、[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 機能を無効にすることができます。
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。

メモ: SD カードが書込み禁止の場合は、初期化オプションが無効になります。

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. iDRAC 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、初期化操作は失敗し、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。

```
racadm set iDRAC.vflashsd.Initialized 1
```

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。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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 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、[メディアおよび USB ポートの設定] に移動します。
   [iDRAC 設定 : メディアおよび USB ポートの設定] 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 : メディアおよび USB ポートの設定] 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: iDRAC 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

iDRAC 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用し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、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、iDRAC は次のメッセージを表示することがあります。`vFlash is currently in use by another process. Try again after some time.`

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

システムに接続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中ではない。

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. iDRAC 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ついては、『iDRAC 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

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. telnet、SSH、またはシリアルコンソールを使用してシステムにログインします。
2. 次のコマンドを入力します。

   ```
   racadm vflashpartition create -i 1 -o drive1 -t empty -e HDD -f fat16 -s [n]
   ```

   `[n]` はパーティションのサイズです。

   デフォルトでは、空のパーティションが読み取り / 書き込み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 CD（**.iso**）の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中ではない。
- 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。iDRAC 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発生します。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。

メモ: vFlash パーティションは FAT 32 ファイルシステム上のイメージファイルです。したがって、イメージファイルには 4 GB の上限があります。

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. iDRAC 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ついては、『iDRAC 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 4 GB 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、拡張子が .img または .iso ではない。
   - 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. telnet、SSH、またはシリアルコンソールを使用してシステムにログインします。

2. コマンドを入力します。

```
racadm vflashpartition create -i 1 -o drive1 -e HDD -t image -l //myserver/sharedfolder/
foo.iso -u root -p mypassword
```

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. iDRAC 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、『iDRAC 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

使用可能な vFlash パーティションを表示するには、iDRAC 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、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ついては、『iDRAC 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 上での動作ステータスを取得する場合

```
racadm vflashpartition status -i 1
```

- すべての既存パーティションのステータスを取得する場合

```
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 機能が有効になっている。
- [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. DRAC 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. telnet、SSH、またはシリアルコンソールを使用してシステムにログインします。
2. 次の方法のいずれかを使用します。
   - set コマンドを使って、パーティションの読み取り / 書き込み状態を変更します。
     - 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 set iDRAC.vflashpartition.<index>.AccessType 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 set iDRAC.vflashpartition.<index>.AccessType 0
       ```

   - set コマンドを使用して、エミュレーションタイプを指定します。

     ```
     racadm set iDRAC.vflashpartition.<index>.EmulationType <HDD, Floppy, or CD-DVD>
     ```

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、iDRAC 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. DRAC 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. telnet、SSH、またはシリアルコンソールを使用してシステムにログインします。
2. 次のコマンドを使用します。
   - パーティションを連結：

     ```
     racadm set iDRAC.vflashpartition.<index>.AttachState 1
     ```
   - パーティションを分離：

     ```
     racadm set iDRAC.vflashpartition.<index>.AttachState 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、iDRAC 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. DRAC 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（iDRAC 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 権限を持っている。
- vFlash 機能が有効になっている。
- カード上で初期化が実行中ではない。
- 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. iDRAC 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 機能が有効になっている。
- 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

最初の起動デバイスとして vFlash パーティションを設定するには、`iDRAC.ServerBoot` オブジェクトを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェース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（`iDRAC.ServerBoot.BootOnce` 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。

18

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 Server Management Working Group（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、iDRAC 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。iDRAC 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。

トピック：

SMCLP を使用したシステム管理機能

iDRAC 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
- iDRAC 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 iDRAC 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。

iDRAC SMCLP 構文

iDRAC SMCLP は、動詞とターゲットの概念を使用して、CLI 経由でシステム管理機能を提供します。動詞は、実行する操作を示し、ターゲットは、その操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：

```
<verb> [<options>] [<target>] [<properties>]
```

次の表は、動詞とその定義が示されています。

表 38. 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
ヘルプ	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
バージョン	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 39. SMCLP ターゲット

ターゲット	定義
`admin1`	管理ドメイン
`admin1/profiles1`	iDRAC 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

表 39. SMCLP ターゲット （続き）

ターゲット	定義
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
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

表 39. SMCLP ターゲット （続き）

ターゲット	定義
`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
`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

表 39. SMCLP ターゲット （続き）

ターゲット	定義
`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

関連概念

SMCLP コマンドの実行 、p. 254
使用例 、p. 259

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、iDRAC にログインするときのデフォルトの開始ポイントです。`cd` 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 の場合と同様であり、`..` 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=(userid,name) /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適した、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 行につき 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 ウェブサイト (**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。

- サーバー電源管理
- SEL 管理
- MAP ターゲットナビゲーション

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。

  ```
  system1 has been stopped successfully
  ```

- 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。

  ```
  system1 has been started successfully
  ```

- 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。

  ```
  system1 has been reset successfully
  ```

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。

  ```
  /system1/logs1/log1

  Targets:

  Record1

  Record2

  Record3
  ```

```
Record4
Record5
Properties:
InstanceID = IPMI:BMC1 SEL Log
MaxNumberOfRecords = 512
CurrentNumberOfRecords = 5
Name = IPMI SEL
EnabledState = 2
OperationalState = 2
HealthState = 2
Caption = IPMI SEL
Description = IPMI SEL
ElementName = IPMI SEL
コマンド：
cd
show
ヘルプ
exit
version
```

- 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。

  ```
  /system1/logs1/log1/record4

  Properties:
  LogCreationClassName= CIM_RecordLog
  CreationClassName= CIM_LogRecord
  LogName= IPMI SEL
  RecordID= 1
  MessageTimeStamp= 20050620100512.000000-000
  Description= FAN 7 RPM: fan sensor, detected a failure
  ElementName= IPMI SEL Record

  コマンド：
  cd
  show
  ヘルプ
  exit
  version
  ```

- 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。

  `All records deleted successfully`

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`

19

iDRAC サービスモジュールの使用

iDRAC サービスモジュールは、サーバーにインストールすることが推奨されているソフトウェアアプリケーションです（デフォルトではインストールされていません）。このモジュールは、オペレーティングシステムから得られる監視情報によって iDRAC を補完し、ウェブインタフェース、RACADM、または WSMAN などの iDRAC インタフェースで使用できる追加データを提供することによって iDRAC を補完します。iDRAC サービスモジュールによって監視される機能を設定して、サーバーのオペレーティングシステムで消費される CPU とメモリを制御できます。

メモ: iDRAC サービスモジュールは、iDRAC Express または iDRAC Enterprise ライセンスがインストールされている場合にのみ、有効にすることができます。

iDRAC サービスモジュールを使用する前に、以下を確認します。

- iDRAC サービスモジュールの各機能を有効または無効にするための、iDRAC におけるログイン、設定、およびサーバー制御権限を持っている。
- ［ローカル RACADM を使った iDRAC 設定］オプションは無効にしないでください。
- OS から iDRAC へのパススルーチャネルが iDRAC 内の内部 USB バスによって有効化されている。

  メモ:

  - iDRAC サービスモジュールの初回実行時、デフォルトでは、モジュールは iDRAC で OS から iDRAC へのパススルーチャネルを有効にします。iDRAC サービスモジュールをインストールした後に、この機能を無効にする場合は、後で iDRAC で手動で有効にする必要があります。
  - OS から iDRAC へのパススルーチャネルが iDRAC の LOM から有効にされている場合は、iDRAC サービスモジュールを使用できません。

トピック：

iDRAC サービスモジュールのインストール

iDRAC サービスモジュールは **dell.com/support** からダウンロードしてインストールすることができます。iDRAC サービスモジュールをインストールするには、サーバーのオペレーティングシステムのシステム管理者権限を持っている必要があります。インストールの詳細については、**dell.com/support/manuals** にある『iDRAC サービスモジュールインストールガイド』を参照してください。

メモ: この機能は Dell Precision PR7910 システムには適用されません。

iDRAC サービスモジュールでサポートされるオペレーティングシステム

DRAC サービスモジュールでサポートされているオペレーティングシステムのリストについては、**dell.com/openmanagemanuals** にある『iDRAC サービスモジュールインストールガイド』を参照してください。

iDRAC サービスモジュール監視機能

iDRAC サービスモジュール（iSM）は、次の監視機能を備えています。

- ネットワーク属性に対する Redfish プロファイルのサポート

- iDRAC ハードリセット
- ホスト OS（実験的機能）経由の iDRAC アクセス
- 帯域内 iDRAC SNMP アラート
- オペレーティングシステム（OS）情報の表示
- Lifecycle Controller ログのオペレーティングシステムログへの複製
- システムの自動リカバリオプションの実行
- Windows Management Instrumentation（WMI）管理プロバイダの設定
- SupportAssist コレクションとの統合。これは、iDRAC サービスモジュールバージョン 2.0 以降がインストールされている場合にのみ該当します。詳細については、「SupportAssist コレクションの生成」を参照してください。
- NVMe PCIe SSD の取り外し準備。詳細については、「NVMe PCIe SSD の取り外し準備」を参照してください。

メモ: Windows Management Instrumentation プロバイダ、iDRAC 経由での NVMe PCIe SDD の取り外し準備、および SupportAssist コレクションの OS 収集の自動化などの機能がサポートされるのは、最小ファームウェアバージョン 2.00.00.00 以降が搭載されている Dell PowerEdge サーバーのみです。

ネットワーク属性に対する Redfish プロファイルのサポート

iDRAC サービスモジュールバージョン 2.3 以降では、iDRAC に対する追加のネットワーク属性が提供されます。これは、iDRAC から REST クライアントを通じて取得することができます。詳細については、iDRAC Redfish プロファイルサポートを参照してください。

オペレーティングシステム情報

OpenManage Server Administrator は現在、オペレーティングシステムの情報とホスト名を iDRAC と共有しています。iDRAC サービスモジュールは、OS 名、OS バージョン、完全修飾ドメイン名（FQDN）といった同様の情報を iDRAC で提供します。デフォルトでは、この監視機能は有効になっています。OpenManage Server Administrator がホスト OS にインストールされている場合、この機能は無効になっていません。

iDRAC サービスモジュールのバージョン 2.0 以降では、OS ネットワークインタフェース監視によってオペレーティングシステム情報機能が強化されています。iDRAC 2.00.00.00 で iDRAC サービスモジュールのバージョン 2.0 以降を使用すると、オペレーティングシステムのネットワークインタフェースの監視が開始されます。この情報は、iDRAC ウェブインタフェース、RACADM、または WSMAN を使用して表示することができます。詳細については、「ホスト OS で使用可能なネットワークインタフェースの表示」を参照してください。

2.00.00.00 よりも前の iDRAC バージョンで iDRAC サービスモジュールのバージョン 2.0 以降を使用する場合、OS 情報機能による OS ネットワークインタフェース監視は行われません。

OS ログへの Lifecycle ログの複製

iDRAC でこの機能を有効にすると、それ以降、Lifecycle Controller ログを OS ログに複製することができます。これは、OpenManage Server Administrator で実行されるシステムイベントログ（SEL）の複製と同様の機能です。**OS ログ** オプションがターゲットとして選択されているすべてのイベント（**警告** ページ内、または同様の RACADM または WSMAN インタフェース内）は、iDRAC サービスモジュールを使用して OS ログに複製されます。OS ログに含まれるデフォルトのログのセットは、SNMP の警告またはトラップに設定されたものと同じです。

iDRAC サービスモジュールは、オペレーティングシステムが動作していない時に発生したイベントもログします。この iDRAC サービスモジュールが実行する OS のログの記録は、Linux ベースのオペレーティングシステム向けの IETF シスログ規格に基づいています。

メモ: iDRAC サービスモジュールバージョン 2.1 以降では、iDRAC サービスモジュールインストーラを使用して Windows OS ログ内での Lifecycle Controller ログのレプリケーション場所を設定できます。場所の設定は、iDRAC サービスモジュールのインストール時、または iDRAC サービスモジュールインストーラの変更時に行うことができます。

OpenManage Server Administrator がインストールされている場合は、この監視機能は、OS のログ内の SEL エントリの重複を避けるために無効に設定されます。

メモ: Microsoft Windows では、アプリケーションログではなくシステムログに iSM イベントが記録される場合、Windows イベントログサービスを再起動するか、またはホスト OS を再起動します。

システムの自動リカバリオプション

自動システムリカバリ（ASR）機能は、ハードウェアベースのタイマーです。ハードウェアに障害が発生した場合、正常性監視が呼び出されないことがありますが、電源スイッチがアクティブ化された場合と同様にサーバーがリセットされます。ASR は、継続的にカウントダウンする「ハートビート」タイマーを使用して実装されています。正常性監視は、カウンタがゼロにならないようカウンタを頻繁にリロードします。ASR がゼロまでカウントダウンすると、オペレーティングシステムがハングアップしたとみなされ、システムは自動的に再起動を試行します。

サーバーの再起動、電源の入れ直し、指定時間経過後の電源オフといった、システムの自動リカバリ動作を実行することができます。この機能を有効にできるのは、オペレーティングシステムのウォッチドッグタイマーが無効になっている場合のみです。OpenManage Server Administrator がインストールされている場合は、この監視機能は、ウォッチドッグタイマーの重複を避けるために無効になります。

Windows Management Instrumentation プロバイダ

WMI は、オペレーティングシステムインタフェースを提供する Windows ドライバモデルに対する拡張の一式で、これを介して計装コンポーネントが情報と通知を提供します。WMI は、サーバーハードウェア、オペレーティングシステム、およびアプリケーションを管理するための Distributed Management Task Force（DMTF）からの Web-Based Enterprise Management（WBEM）および Common Information Model（CIM）規格の Microsoft の実装です。WMI プロバイダは、Microsoft System Center などのシステム管理コンソールとの統合に役立ち、Microsoft Windows サーバーを管理するためのスクリプト記述を可能にします。

iDRAC で WMI オプションを有効または無効にすることができます。iDRAC は、iDRAC サービスモジュールを使用して WMI クラスを表示し、サーバーの正常性情報を提供します。デフォルトでは、WMI 機能は有効になっています。iDRAC サービスモジュールは、WMI 経由で iDRAC の WSMAN 監視クラスを表示します。クラスは `root/cimv2/dcim` 名前空間に表示されます。

これらのクラスには、標準の WMI クライアントインタフェースを使用してアクセスできます。詳細については、プロファイルマニュアルを参照してください。

次の例では DCIM_account クラスを使用して、iDRAC サービスモジュールで提供される WMI 情報機能を説明します。サポートされるクラスとプロファイルの詳細については、Dell TechCenter にある WSMAN プロファイルマニュアルを参照してください。

CIM インタフェース	WinRM	WMIC	PowerShell
クラスのインスタンスを列挙します。	`winrm e wmi/root/cimv2/dcim/dcim_account`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account`	`Get-WmiObject dcim_account -namespace root/cimv2/dcim`
特定のクラスのインスタンスを取得します。	`winrm g wmi/root/cimv2/dcim/DCIM_Account?CreationClassName=DCIM_Account+Name=iDRAC.Embedded.1#Users.2+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account where Name="iDRAC.Embedded.1#Users.16"`	`Get-WmiObject -Namespace root\cimv2\dcim -Class dcim_account -filter "Name='iDRAC.Embedded.1#Users.16'"`
インスタンスの関連付けされたインスタンスを取得します。	`winrm e wmi/root/cimv2/dcim/* -dialect:association -filter:{object=DCIM_Account?CreationClassName=DCIM_Account+Name=iDRAC.Embedded.1#Users.1+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc}`	`wmic /namespace:\\root\cimv2\dcim PATH dcim_account where Name='iDRAC.Embedded.1#Users.2' ASSOC`	`Get-Wmiobject -Query "ASSOCIATORS OF {DCIM_Account.CreationClassName='DCIM_Account',Name='iDRAC.Embedded.1#Users.2',SystemCreationClassName='DCIM_SPComputerSystem',SystemName='systemmc'}" -namespace root/cimv2/dcim`

CIM インタフェース	WinRM	WMIC	PowerShell
インスタンスの参照を取得します。	`winrm e wmi/root/cimv2/dcim/* -dialect:association -associations -filter:{object=DCIM_Account?CreationClassName=DCIM_Account+Name=iDRAC.Embedded.1#Users.1+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc}`	適用なし	`Get-Wmiobject -Query "REFERENCES OF {DCIM_Account.CreationClassName='DCIM_Account',Name='iDRAC.Embedded.1#Users.2',SystemCreationClassName='DCIM_SPComputerSystem',SystemName='systemmc'}" -namespace root/cimv2/dcim`

iDRAC のリモートハードリセット

iDRAC を使用することにより、重要なシステムハードウェア、ファームウェア、またはソフトウェアの問題についてサポートされているサーバーを監視することができます。時折、iDRAC はさまざまな理由のために応答しなくなる場合がありますが、そのような場合には、サーバーの電源を切って iDRAC をリセットする必要があります。iDRAC CPU をリセットするには、サーバーの電源を切ってから再投入する、または AC パワーサイクルを実行する必要があります。

iDRAC のリモートハードリセット機能を使用することにより、iDRAC が応答不能になったときにはいつでも、AC パワーサイクルを行わずに iDRAC のリモートリセット操作を行うことができます。iDRAC をリモートでリセットするには、ホスト OS の管理者権限があることを確認してください。iDRAC のリモートハードリセット機能はデフォルトで有効になっています。iDRAC のリモートハードリセットは、iDRAC ウェブインタフェース、RACADM、または WS-MAN を使って実行することができます。

メモ: この機能は Dell PowerEdge R930 サーバーではサポートされておらず、デルの第 13 世代以降の PowerEdge サーバーのみでサポートされています。

コマンドの使用方法

本項では、iDRAC のハードリセットを実行するための Windows、Linux、および ESXi のオペレーティングシステムに対するコマンドの使用方法を説明します。

- **Windows**
  - ローカル Windows Management Instrumentation（WMI）を使用する：

    ```
    winrm  i  iDRACHardReset wmi/root/cimv2/dcim/DCIM_iSMService?InstanceID=”
    iSMExportedFunctions”
    ```
  - リモート WMI インタフェースを使用する：

    ```
    winrm i iDRACHardReset wmi/root/cimv2/dcim/dcim_ismservice -u:<admin-username> -p:<admin-
    passwd> -r: http://<remote-hostname OR IP>/wsman -a:Basic -encoding:utf-8 -skipCACheck –
    skipCNCheck
    ```
  - 強制的および非強制的に Windows PowerShell スクリプトを使用する：

    ```
    Invoke-iDRACHardReset –force
    ```

    ```
    Invoke-iDRACHardReset
    ```
  - **プログラムメニュー** のショートカットを使用する：

    簡素化するため、iSM は Windows のオペレーティングシステムの **プログラムメニュー** にショートカットを作成します。[iDRAC のリモートハードリセット] オプションを選択すると、iDRAC のリセットを確認するためのプロンプトが表示されます。確認後、iDRAC がリセットされて、操作の結果が表示されます。

メモ: 次の警告メッセージが **アプリケーションログ** カテゴリ下の **イベントビューア** に表示されます。この警告に対する操作は必要はありません。

```
A provider, ismserviceprovider, has been registered in the Windows Management
Instrumentation namespace Root\CIMV2\DCIM to use the LocalSystem account. This
account is privileged and the provider may cause a security violation if it does not
correctly impersonate user requests.
```

- **Linux**

  iSM は すべての iSM 対応 Linux オペレーティングシステムで実行可能なコマンドを提供します。このコマンドは、SSH、またはそれと同等のプロトコルを使用してオペレーティングシステムにログインすることによって実行できます。

  ```
  Invoke-iDRACHardReset
  ```

  ```
  Invoke-iDRACHardReset –f
  ```

- **ESXi**

  すべての iSM 対応 ESXi オペレーティングシステムにおいて、iSM v2.3 は、WinRM リモートコマンドを使用した iDRAC のリモートリセットを実行するための Common Management Programming Interface（CMPI）メソッドプロバイダをサポートします。

  ```
  winrm i iDRACHardReset http://schemas.dell.com/wbem/wscim/1/cim-schema/2/root/cimv2/dcim/
  DCIM_iSMService?__cimnamespace=root/cimv2/dcim+InstanceID=
  iSMExportedFunctions -u:<root-username> -p:<passwd> -r:https://<Host-IP>:443/wsman -
  a:basic -encoding:utf-8 -skipCNCheck -skipCAcheck -skipRevocationcheck
  ```

  メモ: VMware ESXi オペレーティングシステムは、iDRAC をリセットする前に確認のプロンプトを表示しません。

  メモ: VMware ESXi のオペレーティングシステム上の制限により、リセット後 iDRAC の接続性が完全に回復されません。iDRAC は手動でリセットするようにしてください。詳細については、本書の「iDRAC のリモートハードリセット」を参照してください。

エラー処理

表 40. エラー処理

結果	説明
0	成功
1	iDRAC リセット対応ではない BIOS バージョン
2	非対応プラットフォーム
3	アクセス拒否
4	iDRAC リセット失敗

iDRAC SNMP アラートの帯域内サポート

iDRAC サービスモジュール v2.3 を使用することにより、iDRAC によって生成されるアラートに類似する SNMP アラートをホストオペレーティングシステムから受信することができます。

また、ホスト OS 上で SNMP トラップと宛先を設定することによって、iDRAC を設定せずに iDRAC SNMP アラートを監視し、サーバーをリモートで管理することもできます。iDRAC サービスモジュール v2.3 以降では、この機能が OS ログに複製されたすべての Lifecycle ログを SNMP トラップに変換します。

メモ: この機能は、Lifecycle ログのレプリケーション機能が有効になっている場合にのみアクティブになります。

メモ: Linux オペレーティングシステムでは、この機能は、マスターまたは OS SNMP が SNMP 多重化（SMUX）プロトコルで有効化されていることを必要とします。

この機能はデフォルトで無効になっています。帯域内 SNMP アラートメカニズムは iDRAC SNMP アラートメカニズムと共存可能ではありますが、記録されたログには両方のソースからの重複した SNMP アラートが含まれる場合があります。両方を使用するのではなく、帯域内または帯域外のオプションのいずれかを使用することが推奨されます。

コマンドの使用方法

本項では、Windows、Linux、および ESXi のオペレーティングシステムに対するコマンドの使用方法を説明します。

- **Windows オペレーティングシステム**
  - ローカル Windows Management Instrumentation（WMI）を使用する：

    ```
    winrm i EnableInBandSNMPTraps
    wmi/root/cimv2/dcim/DCIM_iSMService?InstanceID="iSMExportedFunctions" @{state="[0/1]"}
    ```
  - リモート WMI インタフェースを使用する：

    ```
    winrm i EnableInBandSNMPTraps wmi/root/cimv2/dcim/DCIM_iSMService?
    InstanceID="iSMExportedFunctions" @{state="[0/1]"}
    -u:<admin-username> -p:<admin-passwd> -r:http://<remote-hostname OR IP>/wsman  -a:Basic -
    encoding:utf-8 -skipCACheck -skipCNCheck
    ```

- **LINUX オペレーティングシステム**

  iSM は、すべての iSM 対応 Linux オペレーティングシステムで実行可能なコマンドを提供します。このコマンドは、SSH、またはそれと同等のプロトコルを使用してオペレーティングシステムにログインすることによって実行できます。

  iSM 2.4.0 からは、次のコマンドを使用して Agent-x を帯域内 iDRAC SNMP アラートのデフォルトプロトコルとして設定できます。

  ```
  ./Enable-iDRACSNMPTrap.sh 1/agentx -force
  ```

  `-force` が指定されていない場合は、net-SNMP が設定され、snmpd サービスを再起動していることを確認します。

  - この機能を有効にするには、次の手順を実行します。

    ```
    Enable-iDRACSNMPTrap.sh 1
    ```

    ```
    Enable-iDRACSNMPTrap.sh enable
    ```
  - この機能を無効にするには、次の手順を実行します。

    ```
    Enable-iDRACSNMPTrap.sh 0
    ```

    ```
    Enable-iDRACSNMPTrap.sh disable
    ```

  メモ: --force オプションは、トラップを転送するように Net-SNMP を設定します。ただし、トラップ宛先を設定する必要があります。

- **VMware ESXi オペレーティングシステム**

  すべての iSM 対応 ESXi オペレーティングシステムにおいて、iSM v2.3 は、WinRM リモートコマンドを使用することによってこの機能をリモートで有効化するための Common Management Programming Interface（CMPI）メソッドプロバイダをサポートします。

  ```
  winrm i EnableInBandSNMPTraps http://schemas.dell.com/wbem/wscim/1/cim-schema/2/root/cimv2/
  dcim/DCIM_iSMService?
  __cimnamespace=root/cimv2/dcim+InstanceID=iSMExportedFunctions -u:<user-name> -p:<passwd> -
  r:https://<remote-host-name
  ```

  ```
  ip-address>:443/wsman -a:basic -encoding:utf-8 -skipCNCheck -skipCACheck -
  skipRevocationcheck @{state="[0/1]"}
  ```

  メモ: トラップに対する VMware ESXi システム全体の SNMP 設定を見直し、設定する必要があります。

メモ: 詳細については、**http://en.community.dell.com/techcenter/extras/m/white_papers** で利用できる『**In-Band SNMP Alerts**』（帯域内 SNMP アラート）のテクニカルホワイトペーパーを参照してください。

ホスト OS（実験的機能）経由の iDRAC アクセス

この機能を使用することにより、iDRAC IP アドレスを設定することなく、ホスト IP アドレスを使用して、iDRAC ウェブインタフェース、WS-MAN、および RedFish インタフェース経由でハードウェアパラメータを設定および監視することができます。iDRAC サーバーが設定されていない場合はデフォルトの iDRAC 資格情報を使用、または iDRAC サーバーが以前に設定済みである場合は同じ iDRAC 資格情報を使用し続けることができます。

Windows オペレーティングシステム経由の iDRAC アクセス

このタスクは次の方法を使用して実行することができます。

- ウェブパックを使用して iDRAC アクセス機能をインストールする。
- iSM PowerShell スクリプトを使用して設定する。

MSI を使ったインストール

Web パックを使用してこの機能をインストールできます。この機能は、標準 iSM インストールで無効に設定されています。有効の場合、デフォルトのリスニングポート番号は 1266 です。このポート番号は 1024 ~ 65535 の範囲内で変更できます。iSM は iDRAC への接続をリダイレクトします。その後 iSM はインバウンドファイアウォールルールの OS2iDRAC を作成します。リスニングポート番号が、ホストオペレーティングシステムの OS2iDRAC ファイアウォールルールに追加され、受信接続を可能にします。ファイアウォールルールは、この機能が有効の場合、自動的に有効になります。

iSM 2.4.0 からは、次の Powershell コマンドレットを使用して現在のステータスとリスポート設定を回復できます。

```
Enable-iDRACAccessHostRoute –status get
```

このコマンドの出力は、この機能が有効か無効かを示します。機能が有効の場合は、リスニングポート番号を表示します。

メモ: この機能を機能させるには、お使いのシステムで Microsoft IP ヘルパーサービスが実行されてることを確認してください。

iDRAC ウェブインタフェースにアクセスするには、ブラウザで `https://<host-name>` または `OS-IP>:443/login.html` フォーマットを使います。内訳は次のとおりです。

- `<host-name>` — iSM がインストールされ、OS 機能を介した iDRAC アクセスのために設定されたサーバーの完全なホスト名です。ホスト名が存在しない場合は OS IP アドレスを使用できます。
- `443` - デフォルトの iDRAC ポート番号です。これは接続ポート番号と呼ばれ、リッスンポート番号へのすべての受信接続がここにリダイレクトされます。ポート番号は、iDRAC ウェブインタフェース、WS-MAN、および RACADM インタフェース を使って変更することができます。

iSM PowerShell コマンドレットを使用した設定

iSM のインストール中にこの機能が無効になった場合、iSM によって提供される次の Windows PowerShell コマンドを使用してこの機能を再度有効にできます。

```
Enable-iDRACAccessHostRoute
```

この機能がすでに設定されている場合は、PowerShell コマンドと対応するオプションを使用してこれを無効化または変更することができます。利用できるオプションは次の通りです。

- **ステータス** - このパラメータは必須です。値の大文字と小文字は区別されず、値は **true**、 **false**、または **get** です。
- **ポート** - これはリスニングポート番号です。ポート番号を入力しない場合は、デフォルトのポート番号（1266）が使用されます。**ステータス** パラメータの値が FALSE の場合、パラメータの残りの部分は無視できます。この機能に対してまだ設定されていない新しいポート番号を入力する必要があります。新しいポート番号の設定は、既存の OS2iDRAC インバウンドファイアウォールルールを上書きし、新しいポート番号を使用して iDRAC に接続できます。値の範囲は 1024 ~ 65535 です。
- **IPRange** - このパラメータはオプションで、ホストオペレーティングシステム経由で iDRAC に接続することが許可される IP アドレスの範囲を提供します。IP アドレス範囲の形式は、IP アドレスとサブネットのマスクの組み合わせである Classless Inter-Domain Routing（CIDR）フォーマット（例：10.94.111.21/24）です。この範囲外の IP アドレスには iDRAC アクセスが制限されます。

  メモ: この機能は IPv4 アドレスのみをサポートします。

Linux オペレーティングシステム経由の iDRAC アクセス

この機能は、Web パックで利用可能な `setup.sh` ファイルを使ってインストールすることができます。この機能は、デフォルトまたは通常の iSM インストールでは無効になっています。この機能のステータスを得るには、次のコマンドを使用します。

```
Enable-iDRACAccessHostRoute get-status
```

この機能をインストール、有効化、設定するには、次のコマンドを使用します。

```
./Enable-iDRACAccessHostRoute <Enable-Flag> [ <source-port> <source-IP-range/source-ip-range-mask>]
```

<Enable-Flag>=0

Disable（無効）

`<source-port>` と `<source-IP-range/source-ip-range-mask>` は必須ではありません。

<Enable-Flag>=1

Enable（有効）

`<source-port>` は必須ですが、`<source-ip-range-mask>` はオプションです。

<source-IP-range>

IP 範囲は *<IP-Address/subnet-mask>* 形式です。例：10.95.146.98/24

OpenManage Server Administrator と iDRAC サービスモジュールの共存

システムで、OpenManage Server Administrator と iDRAC サービスモジュールの両方を共存させて、正常かつ個別に機能させることができます。

iDRAC サービスモジュールのインストール中に監視機能を有効にしている場合、インストールが完了した後に iDRAC サービスモジュールが OpenManage Server Administrator の存在を検知すると、iDRAC サービスモジュールは重複している監視機能一式を無効にします。OpenManage Server Administrator が実行されている場合は、iDRAC サービスモジュール は OS および iDRAC にログインした後で重複した監視機能を無効にします。

これらの監視機能を iDRAC インタフェースを介して後で再度有効にすると、同じチェックが実行され、OpenManage Server Administrator が実行されているかどうかに応じて、各機能が有効になります。

iDRAC ウェブインタフェースからの iDRAC サービスモジュールの使用

iDRAC ウェブインタフェースから iDRAC サービスモジュールを使用するには、次の手順を実行します。

1. ［概要］>［サーバー］>［サービスモジュール］と移動します。
   ［iDRAC サービスモジュールのセットアップ］ページが表示されます。
2. 次を表示することができます。
   - ホストオペレーティングシステムにインストールされている iDRAC サービスモジュールのバージョン
   - iDRAC サービスモジュールと iDRAC との接続状態
3. 帯域外監視機能を実行するには、次から 1 つまたは複数のオプションを選択します。
   - ［OS 情報］- オペレーティングシステムの情報を表示します。
   - ［Lifacycle ログを OS ログ内に複製］- Lifecycle Controller ログを OS ログに含めます。OpenManage Server Administrator がシステムにインストールされている場合、このオプションは無効になっています。
   - ［WMI 情報］— WMI 情報が表示されます。
   - ［自動システム回復処置］- 指定時間（秒）の経過後、システムで自動リカバリ動作を実行します。
     - ［再起動］
     - ［システムの電源を切る］
     - ［システムの電源を入れ直す］

     このオプションは、システムに OpenManage Server Administrator がインストールされている場合は無効になっています。

RACADM からの iDRAC サービスモジュールの使用

RACADM からの iDRAC サービスモジュールを使用するには、`ServiceModule` グループのオブジェクトを使用します。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

Windows Nano OS での iDRAC サービスモジュールの使用

インストール手順については、『*iDRAC サービスモジュールインストールガイド*』を参照してください。

iSM サービスが実行されているかどうかを確認するには、次のコマンドレットを使用します。

```
Get-Service "iDRAC Service Module"
```

WMI または Windows Powershell クエリを使用して複製された Lifecycle ログを表示できます。

```
GetCimInstance -Namespace root/cimv2 - className win32_NTLogEvent
```

デフォルトでは、ログは［イベントビューア］>［アプリケーションとサービスログ］>［システム］で入手できます。

20

サーバー管理用 USB ポートの使用

Dell PowerEdge 第 12 世代のサーバーでは、すべての USB ポートがサーバー専用です。第 13 世代のサーバーでは、前面パネルの USB ポートのいずれか 1 つが事前プロビジョニングおよびトラブルシューティングなどの管理目的のために iDRAC によって使用されます。このポートには、それが管理用ポートであることを示すアイコンが付いています。LCD パネル装備の全第 13 世代サーバーが、この機能をサポートします。LCD パネル非装備の 200～500 モデルの一部では、このポートは使用できません。そのような場合、これらのポートはサーバーオペレーティングシステム用に使用することができます。

メモ: この機能は、 poweredge R930 サーバではサポートされません。

USB ポートが iDRAC によって使用されている場合は、以下の状態になります。

- iDRAC に接続された USB タイプ A/A ケーブルを使用すると、USB ネットワークインタフェースにより、ノートブックなどのポータブルデバイスから既存の帯域外リモート管理ツールを使用できるようになります。iDRAC には 169.254.0.3、管理デバイスには 169.254.0.4 の IP アドレスが割り当てられます。
- サーバー設定プロファイルを USB デバイスに保存し、USB デバイスからサーバーの設定をアップデートすることができます。

メモ: この機能は以下でサポートされています。

- FAT ファイルシステムと 1 つのパーティションを備えた USB デバイス
- XPS 10 や Venue Pro 8 を含むすべての Dell Windows 8 および Windows RT タブレット。XPS 10 や Venue Pro 8 などの USB ミニポートを備えたデバイスの場合は、On-The-Go（OTG）ドングルとタイプ A/A ケーブルを使用します。

関連概念

USB デバイスのサーバー設定プロファイルを使用した iDRAC の設定 、p. 272

関連タスク

直接 USB 接続を介した iDRAC インタフェースへのアクセス 、p. 271

トピック：

直接 USB 接続を介した iDRAC インタフェースへのアクセス

第 13 世代のサーバーでは、新しい iDRAC ダイレクト機能を使用して、ノートブックや PC の USB ポートを iDRAC ポートに直接接続できます。これにより、iDRAC インタフェース（ウェブインタフェース、RACADM、WSMAN など）と直接やり取りして、高度なサーバー管理やサービスを実現できます。

ノートブック（USB ホストコントローラ）をサーバーの iDRAC（USB デバイス）に接続するには、タイプ A/A ケーブルを使用する必要があります

iDRAC が USB デバイスとして動作し、管理ポートが自動モードに設定されている場合、USB ポートは常に iDRAC によって使用されます。このポートが自動的に OS に切り替わることはありません。

USB ポートを介して iDRAC インタフェースにアクセスするには、次の手順を実行します。

1. ワイヤレスネットワークをすべてオフにし、その他すべての有線ネットワークとの接続を切断します。
2. USB ポートが有効になっていることを確認します。詳細については、「USB 管理ポートの設定」を参照してください。
3. ノートブックと iDRAC の USB ポートをタイプ A/A ケーブルで接続します。
   管理 LED（ある場合）が緑色になり、2 秒間点灯します。
4. ノートブックに 169.254.0.4、iDRAC に 169.254.0.3 の IP アドレスが割り当てられるまで待ちます。これには数秒かかることがあります。
5. ウェブインタフェース、RACADM、WS-Man などの iDRAC ネットワークインタフェースの使用を開始します。

6. iDRAC が USB ポートを使用しているときは、LED が点滅してアクティブであることを示します。LED は 1 秒間に 4 回点滅します。
7. 使用後、ケーブルを切断します。
   LED が消灯します。

USB デバイスのサーバー設定プロファイルを使用した iDRAC の設定

新しい iDRAC ダイレクト機能を使用すると、サーバーレベルの iDRAC 設定を行うことができます。まず、iDRAC で USB 管理ポートを設定し、サーバー設定プロファイルが保存された USB デバイスを挿入し、その後 USB デバイスから iDRAC にサーバー設定をインポートします。

メモ: サーバーに DRAC デバイスが接続されていない場合にのみ、DRAC インタフェースを使用して USB 管理ポートを設定できます。

メモ: LCD および LED パネルが装備されていない PowerEdge サーバーは、USB キーをサポートしません。

関連概念

USB 管理ポートの設定 、p. 272

関連タスク

USB デバイスからのサーバー設定プロファイルのインポート 、p. 274

USB 管理ポートの設定

iDRAC で USB ポートを設定することができます。

- BIOS セットアップを使用して、サーバーの USB ポートを有効または無効にします。[すべてのポートを無効にする] または [前面ポートを無効にする] のいずれかに設定した場合、iDRAC の管理下にある USB ポートも無効になります。ポートのステータスは iDRAC インタフェースを使用して表示できます。ステータスが無効の場合は、以下の状態になります。
  - iDRAC は、管理下 USB ポートに接続されている USB デバイスまたはホストを処理しません。
  - 管理下 USB 設定を変更することはできますが、前面パネルの USB ポートが BIOS で有効になるまで、変更後の設定は反映されません。
- USB 管理ポートモードを設定します。USB ポートが iDRAC によって使用されているかどうかを決定する、またはサーバー OS :
  - 自動 (デフォルト): iDRAC でサポートされていない USB デバイス、またはサーバの構成プロファイルを、デバイスに存在しない場合は、USB ポートを iDRAC との関連付けは解除されます。サーバに接続されている場合は、からデバイスが削除されると、そのポートの設定がリセットされると、iDRAC によって使用されます。
  - 標準 OS 使用 : USB デバイスは、常に、オペレーティングシステムで使用されます。
  - iDRAC ダイレクト限定 : USB デバイスは、常に、iDRAC によって使用されます。

USB 管理ポートを設定するには、サーバー制御権限を持っている必要があります。

USB デバイスが接続されている場合は、システムインベントリ ページの ハードウェアインベントリ セクションの下に、その USB デバイスの情報が表示されます。

以下の場合は、イベントが Lifecycle Controller ログに記録されます。

- USB デバイスが自動または iDRAC モードのときに、デバイスが挿入されたか取り外された。
- USB 管理ポートのモードが変更された。
- デバイスが iDRAC から OS に自動的に切り替えられます。
- デバイスは iDRAC または OS から除外されました

デバイスが USB 仕様で許可されている電源要件を超えると、デバイスは切り離され、次のプロパティを含む過電流イベントが生成されます。

- カテゴリ : システム正常性
- タイプ : USB デバイス
- 重大度 : 警告
- 通知許可 : 電子メール、SNMP トラップ、リモート syslog および WS-Eventing
- アクション : なし

エラーメッセージが表示され、次のような場合には Lifecycle Controller ログに記録されます。

- サーバー制御ユーザの権限なしで、USB 管理ポートを設定しようとした場合。
- USB デバイスが iDRAC で使用されており、USB 管理ポートのモードを変更しようとした場合。
- USB デバイスが iDRAC で使用されているときにデバイスを取り外した。

ウェブインタフェースを使用した USB 管理ポートの設定

USB ポートを設定するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、[概要] > [ハードウェア] > [USB 管理ポート] と移動します。
   [USB 管理ポートの設定] ページが表示されます。
2. [USB 管理ポートモード] ドロップダウンメニューから、次のいずれかのオプションを選択します。
   - [自動] — USB ポートは、iDRAC またはサーバーのオペレーティングシステムによって使用されます。
   - [標準 OS 使用] — USB ポートはサーバーの OS で使用されます。
   - [iDRAC ダイレクトのみ] — USB ポートは iDRAC によって使用されます。
3. iDRAC 管理対象 : USB XML 設定 ドロップダウンメニューでオプションを選択し、USB ドライブに保存されている XML 設定ファイルをインポートしてサーバーを設定します。
   - [無効]
   - [サーバーにデフォルト資格情報があるときにのみ有効]
   - [Enabled (有効)]

   フィールドについては、『iDRAC オンラインヘルプ』を参照してください。
4. 設定を適用するには、[適用] をクリックします。

RACADM を使用した USB 管理ポートの設定

USB 管理ポートを設定するには、次の RACADM サブコマンドおよびオブジェクトを使用します。

- USB ポートのステータスを表示するには、次のコマンドを使用します。

```
racadm get iDRAC.USB.ManagementPortStatus
```

- USB ポートの設定を表示するには、次のコマンドを使用します。

```
racadm get iDRAC.USB.ManagementPortMode
```

- USB ポートの設定を変更するには、次のコマンドを使用します。

```
racadm set iDRAC.USB.ManagementPortMode <Automatic|Standard OS Use|iDRAC|>
```

  メモ: RACADM set コマンドを使用する際は、必ず Standard OS Use 属性を一重引用符で囲んでください。

- USB デバイスのインベントリを表示するには、次のコマンドを使用します。

```
racadm hwinventory
```

- 現在のアラート設定をセットアップするには、次のコマンドを使用します。

```
racadm eventfilters
```

詳細については、**dell.com/esmmanuals** にある『iDRAC RACADM コマンドラインインタフェース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 USB 管理ポートの設定

USB ポートを設定するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、[メディアおよび USB ポートの設定] に移動します。
   [iDRAC 設定 : メディアおよび USB ポートの設定] ページが表示されます。
2. [USB 管理ポートモード] ドロップダウンメニューで、次の操作を実行します。
   - [自動] — USB ポートは、iDRAC またはサーバーのオペレーティングシステムによって使用されます。
   - [標準 OS 使用] — USB ポートはサーバーの OS で使用されます。

- [iDRAC ダイレクトのみ] — USB ポートは iDRAC によって使用されます。

3. [iDRAC ダイレクト : USB 設定 XML] ドロップダウンメニューからオプションを選択し、USB ドライブ上に保存されているサーバー設定プロファイルをインポートしてサーバーを設定します。
   - [無効]
   - [サーバーにデフォルト資格情報があるときにのみ有効]
   - [Enabled (有効)]

   各フィールドについては、『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] をクリックして設定を適用します。

USB デバイスからのサーバー設定プロファイルのインポート

必ず USB デバイスのルートに `System_Configuration_XML` というディレクトリを作成し、`config.xml` と `control.xml` の両方のファイルを含めます。

- サーバー設定プロファイルは、USB デバイスのルートディレクトリの下にある `System_Configuration_XML` サブディレクトリにあります。このファイルには、サーバーのすべての属性 - 値ペアが含まれています。これには iDRAC、PERC、RAID、BIOS の属性も含まれます。このファイルを編集し、サーバーに任意の属性を設定することができます。ファイル名は `<servicetag>-config.xml`、`<modelnumber>-config.xml`、または `config.xml` のいずれかです。
- コントロール XML ファイルには、インポート操作を制御するためのパラメータが含まれ、iDRAC またはシステム内のその他のコンポーネントの属性は含まれていません。このコントロールファイルには、以下の 3 つのパラメータが含まれています。
  - ShutdownType – 正常、強制、再起動なし
  - TimeToWait (秒) – 最小 300、最大 3,600
  - EndHostPowerState – オンまたはオフ

`control.xml` ファイルの例を次に示します。

```
<InstructionTable>       <InstructionRow>                 <InstructionType>Configuration XML
import Host control Instruction</InstructionType>                 <Instruction>ShutdownType</
Instruction>                 <Value>NoReboot</Value>
<ValuePossibilities>Graceful,Forced,NoReboot</ValuePossibilities>       </
InstructionRow>       <InstructionRow>                 <InstructionType>Configuration XML
import Host control Instruction</InstructionType>                 <Instruction>TimeToWait</
Instruction>                 <Value>300</Value>                 <ValuePossibilities>Minimum
value is 300 -Maximum value is 3600 seconds.</ValuePossibilities>       </
InstructionRow>       <InstructionRow>                 <InstructionType>Configuration XML
import Host control Instruction</InstructionType>
<Instruction>EndHostPowerState</Instruction>                 <Value>On</
Value>                 <ValuePossibilities>On,Off</ValuePossibilities>       </
InstructionRow></InstructionTable>
```

この操作を実行するには、サーバー制御の権限を持っている必要があります。

メモ: サーバー設定プロファイルのインポート中、USB 管理設定を XML ファイル内で変更すると、ジョブに失敗するか、ジョブがエラーで完了します。XML 内のエラーを回避するには、属性からコメントを追加します。

USB デバイスから iDRAC にサーバー設定プロファイルをインポートするには、次の手順を実行します。

1. USB 管理ポートを設定します。
   - [USB 管理ポートモード] を [自動] または [iDRAC] に設定します。
   - [iDRAC 管理対象 : USB XML 設定] を [デフォルト資格情報付きで有効] または [無効] に設定します。
2. `configuration.xml` および `control.xml` ファイルが保存されている USB キーを iDRAC USB ポートに挿入します。
3. サーバー設定プロファイルは、USB デバイスのルートディレクトリの下にある `System_Configuration_XML` サブディレクトリにあります。次のシーケンスで確認できます。
   - `<servicetag>-config.xml`
   - `<modelnum>-config.xml`
   - `config.xml`
4. サーバー設定プロファイルのインポートジョブが開始されます。

   プロファイルが検出されない場合、処理は停止します。

   [iDRAC 管理対象 : USB XML 設定] が [デフォルト資格情報付きで有効] に設定され、BIOS セットアップパスワードが null でない場合、またはいずれかの iDRAC ユーザーアカウントが変更されている場合、エラーメッセージが表示され、処理が停止します。

5. LCD パネルと LED (ある場合) に、インポートジョブが開始されたことを示すステータスが表示されます。
6. ステージングする必要のある設定があり、コントロールファイルで [シャットダウンタイプ] に [再起動なし] が指定されている場合、設定を行うにはサーバーを再起動する必要があります。それ以外の場合は、サーバーが再起動されて設定が適用されます。ただしサーバーがすでにシャットダウンしている場合は、[再起動なし] が指定されていても、ステージングされた設定が適用されます。
7. インポートジョブが完了すると、LCD/LED でジョブが完了したことが示されます。再起動が必要な場合は、LCD にステータスが「再起動の待機中」として表示されます。
8. USB デバイスがサーバーに挿入されたままの場合、インポート操作の結果は USB デバイスの `results.xml` ファイルに記録されます。

LCD メッセージ

LCD パネルが使用可能な場合、パネルには次のメッセージが順次表示されます。
1. インポート中 – USB デバイスからサーバー設定プロファイルがコピーされています。
2. 適用中 — ジョブが進行中です。
3. 完了 — ジョブが正常に完了しました。
4. エラーで完了 — ジョブは完了しましたがエラーが発生しました。
5. 失敗 — ジョブが失敗しました。

詳細については、USB デバイスの結果ファイルを参照してください。

LED の点滅動作

USB LED がある場合は、次のことを示します。
- 緑色の点灯 – USB デバイスからサーバー設定プロファイルがコピーされている。
- 緑色の点滅 – ジョブが進行中である。
- 緑色の点灯 – ジョブが正常に完了した。

ログと結果ファイル

インポート操作に関する次の情報がログに記録されます。
- USB からの自動インポートが Lifecycle Controller ログファイルに記録されます。
- USB デバイスが挿入されたままの場合、ジョブの結果は USB キーに保存されている結果ファイルに記録されます。

次の情報を使用して、サブディレクトリで `Results.xml` という名前の結果ファイルが更新または作成されます。
- サービスタグ – インポート処理でジョブ ID またはエラーが返された後、データが記録されます。
- ジョブ ID - インポート処理でジョブ ID が返された後、データが記録されます。
- ジョブの開始日時 - インポート処理でジョブ ID が返された後、データが記録されます。
- ステータス – インポート処理でエラーが返された場合、またはジョブの結果が使用可能な場合、データが記録されます。

21

iDRAC Quick Sync の使用

デルの第 13 世代 PowerEdge サーバーの一部には、Quick Sync 機能をサポートする Quick Sync ベゼルが搭載されています。この機能を使用すると、モバイルデバイスでサーバーレベルの管理が可能になります。これにより、モバイルデバイスを使用して、インベントリや監視情報を表示し、基本的な iDRAC 設定 (ルート資格情報や 1 番目の起動デバイスの設定など) を指定することができます。

モバイルデバイス (たとえば OpenManage Mobile) のための iDRAC Quick Sync アクセスは、i DRAC で設定できます。iDRAC Quick Sync インタフェースを使用してサーバーを管理するには、モバイルデバイスに OpenManage Mobile アプリケーションをインストールする必要があります。

メモ: この機能は現在、Android オペレーティングシステムを搭載したモバイルデバイスでサポートされています。

現在のリリースでは、この機能は Dell PowerEdge R730、R730xd、および R630 ラックサーバーのみで使用できます。これらのサーバー用に、オプションのベゼルを購入することができます。つまりこれはハードウェアの上位オプションであり、その機能は iDRAC ソフトウェアライセンスとは関係ありません。

iDRAC Quick Sync ハードウェアには以下が含まれます。

- アクティベーション ボタン – このボタンを押して Quick Sync インタフェースをアクティブにします。ラック密度が高い環境では、通信の対象とするサーバーを特定して起動する際にこのボタンが役立ちます。Quick Sync 機能は、設定可能な時間 (デフォルトは 30 秒) 中アイドル状態であった後、または非アクティブ化ボタンが押されると、非アクティブになります。
- アクティビティ LED – Quick Sync が無効になると、LED は数回点滅した後、消灯します。設定可能な非アクティブタイマーがトリガされた場合も LED が消灯し、インタフェースが非アクティブになります。

iDRAC での iDRAC Quick Sync の設定後、モバイルデバイスをサーバーから 2 センチ未満の距離に近づけてサーバーについての関連情報を読み取り、iDRAC 設定を実行します。

OpenManage Mobile を使用すると、以下の操作を実行することができます。

- インベントリ情報の表示
- 監視情報の表示
- 基本的な iDRAC ネットワーク設定

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

関連概念

iDRAC Quick Sync の設定 、p. 276
モバイルデバイスを使用した iDRAC 情報の表示 、p. 277

トピック：

- iDRAC Quick Sync の設定
- モバイルデバイスを使用した iDRAC 情報の表示

iDRAC Quick Sync の設定

iDRAC ウェブインタフェースまたは RACADM を使用して、iDRAC Quick Sync 機能を設定し、モバイルデバイスにアクセスを許可することができます。

- アクセス — 次のいずれかのオプションを指定して、iDRAC Quick Sync 機能のアクセス状況を設定できます。
  - 読み取り / 書き込み — デフォルトステータスです。
  - 読み取り / 書き込みアクセス – 基本的な iDRAC 設定を指定できます。
  - 読み取り専用アクセス - インベントリと監視情報を表示できます。
  - 無効アクセス – 情報の表示、設定の指定はできません。
- タイムアウト — iDRAC Quick Sync 非アクティブタイマーを有効または無効にすることができます。
  - 有効になっている場合、Quick Sync モードがオフになるまでの時間を指定できます。オンにするには、アクティブ化ボタンを再度押します。

    ○ 無効になっている場合、タイマーはタイムアウト時間の入力を許可しません。
- タイムアウト制限 — Quick Sync モードが無効になる時間を指定できます。デフォルト値は 30 秒です。

設定を行うには、サーバー制御権限を持っている必要があります。設定を有効にするためにサーバーを再起動する必要はありません。

設定が変更された場合は、Lifecycle Controller ログにエントリが記録されます。

ウェブインタフェースを使用した iDRAC Quick Sync の設定

iDRAC Quick Sync を設定するには、次の手順を実行します。

1. iDRAC 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. [iDRAC Quick Sync] セクションで、[アクセス] ドロップダウンメニューから次のいずれかを選択し、Android モバイルデバイスにアクセスできるようにします。
    - 読み取り / 書き込み
    - 読み取り専用
    - 無効
3. タイマーを有効にします。
4. タイムアウト値を指定します。
    上記のフィールドの詳細については、『iDRAC オンラインヘルプ』を参照してください。
5. 設定を適用するには、[適用] をクリックします。

RACADM を使用した iDRAC Quick Sync の設定

iDRAC Quick Sync を設定するには、**System.QuickSync** グループの racadm オブジェクトを使用します。詳細については、**dell.com/esmmanuals** にある『iDRAC RACADM コマンドライン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 iDRAC Quick Sync の設定

iDRAC Quick Sync 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、[前面パネルセキュリティ] に移動します。
    [iDRAC 設定 : 前面パネルセキュリティ] ページが表示されます。
2. [iDRAC Quick Sync] セクションで、次の手順を実行します。
    - アクセスレベルを指定します。
    - タイムアウトを有効にします。
    - ユーザー定義のタイムアウト制限を指定します (15 ~ 3,600 秒)。

    上記のフィールドの詳細については、『iDRAC 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。
    この設定が適用されます。

モバイルデバイスを使用した iDRAC 情報の表示

モバイルデバイスで iDRAC 情報を表示するには、**dell.com/support/manuals** にある『OpenManage Mobile ユーザーズガイド』の手順を参照してください。

22

オペレーティングシステムの導入

管理下システムへのオペレーティングシステムの導入には、次のいずれかのユーティリティを使用できます。
- リモートファイル共有
- 仮想メディアコンソール

関連タスク

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導入、p. 278
仮想メディアを使用したオペレーティングシステムの導入、p. 280

トピック：

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導入

リモートファイル共有（RFS）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。
- iDRAC に対する ［設定］［ユーザー］ および ［仮想メディアへのアクセス］ 権限が、そのユーザーに対して有効である。
- 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起動可能イメージファイルが **.img** または **.iso** などの業界標準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、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。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確実に同じ展開手順から起動し、実行するようにします。

RFS を使用してオペレーティングシステムを導入するには、次の手順を実行します。

1. リモートファイル共有（RFS）を使用し、NFS または CIFS 経由で管理下システムに ISO または IMG イメージファイルをマウントします。
2. ［概要］ > ［セットアップ］ > ［最初の起動デバイス］へと進みます。
3. 起動順序を、［最初の起動デバイス］ ドロップダウンリストで設定して、フロッピー、CD、DVD、または ISO などの仮想メディアを選択します。
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。

関連概念

リモートファイル共有の管理、p. 278
最初の起動デバイスの設定、p. 88

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。RFS はライセンスが必要な機能です。

メモ: CIFS は IPv4 と IPv6 の両方のアドレス、NFS は IPv4 アドレスのみをサポートします。

リモートファイル共有では、**.img** および **.iso** イメージファイルフォーマット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、RFS 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 と仮想メディアの機能は相互排他的です。

- 仮想メディアクライアントがアクティブではない場合に、RFS 接続の確立を試行すると、接続が確立され、リモートイメージがホストのオペレーティングシステムで使用可能になります。
- 仮想メディアクライアントがアクティブである場合に RFS 接続の確立を試行すると、次のエラーメッセージが表示されます。

  Virtual Media is detached or redirected for the selected virtual drive. (仮想メディアが分離された、または選択した仮想ドライブにリダイレクトされました。)

RFS の接続ステータスは iDRAC ログで提供されます。接続されると、RFS マウントされた仮想ドライブは、iDRAC からログアウトしても切断されません。iDRAC 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 接続を終了させるには、CMC および iDRAC 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、iDRAC の既存の RFS マウントよりも常に優先されます。

メモ: iDRAC VFlash 機能と RFS には、関連性がありません。

アクティブな RFS 接続があり、仮想メディアの接続モードの設定が [連結] または [自動連結] になっているときに iDRAC ファームウェアバージョンを 1.30.30 から 1.50.50 ファームウェアにアップデートする場合、iDRAC は、ファームウェアのアップグレードが完了して iDRAC が再起動した後で RFS 接続の再確立を試みます。

アクティブな RFS 接続があり仮想メディアの接続モードの設定が [分離] になっているときに iDRAC ファームウェアバージョンを 1.30.30 から 1.50.50 ファームウェアにアップデートする場合、iDRAC は、ファームウェアのアップグレードが完了して iDRAC が再起動した後に RFS 接続の再確立を試みません。

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. iDRAC の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. [連結されたメディア] の下で、[連結] または [自動連結] を選択します。
3. [リモートファイル共有] で、イメージファイルパス、ドメイン名、ユーザー名、およびパスワードを指定します。フィールドの詳細については、『iDRAC オンラインヘルプ』を参照してください。

   次にイメージファイルパスの例を挙げます。

   - CIFS — //<CIFS ファイルシステムの接続先 IP アドレス>/<ファイルパス>/<イメージ名>
   - NFS — <NFS ファイルシステムの接続先 IP アドレス>:/<ファイルパス>/<イメージ名>

   メモ: ファイルパスには、「/」と「\」のどちらの文字も使用できます。

   CIFS は IPv4 と IPv6 の両方のアドレスをサポートしていますが、NFS は IPv4 アドレスのみをサポートします。

   NFS 共有を使用する場合、大文字と小文字が区別されるため、<ファイルパス> と <イメージ名> を正確に入力するようにしてください。

   メモ: ユーザー名およびパスワードの推奨文字に関する詳細は、ユーザー名およびパスワードで推奨される文字、p. 126 を参照してください。

   メモ: ネットワーク共有設定を指定する場合は、ユーザー名とパスワードに特殊記号を使用しないようにするか、特殊文字をパーセントエンコードすることが推奨されます。

4. [適用] をクリックして、[接続] をクリックします。
   接続が確立された後、[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 <options>`

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>：ネットワーク上のイメージの場所。場所の両側に二重引用符を使用します。「Web 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」の項でイメージファイルパスの例を参照してください

`-s`：現在のステータスを表示

メモ: ユーザー名、パスワード、および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を使用できますが、'（一重引用符）、"（二重引用符）、,（コンマ）、<（小なり記号）、>（大なり記号）は使用できません。

仮想メディアを使用したオペレーティングシステムの導入

仮想メディア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。

- 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起動可能イメージファイルが **.img** または **.iso** などの業界標準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導入するには、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。
   - iDRAC 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導入を完了します。

関連概念

仮想メディアの設定 、p. 235
最初の起動デバイスの設定 、p. 88

関連タスク

iDRAC の設定 、p. 78

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導入

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導入し、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。

関連概念

IDSDM について 、p. 281

関連タスク

BIOS での SD モジュールと冗長性の有効化 、p. 281

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。

iDRAC 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。

関連概念

センサー情報の表示 、p. 101

23

iDRAC 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
- Lifecycle 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

関連タスク

トピック：

診断コンソールの使用

iDRAC では、Microsoft Windows または Linux ベースのシステムに装備されているツールに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。ネットワーク診断ツールには、iDRAC 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. iDRAC 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。コマンドの詳細については、『iDRAC 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。

自動リモート診断のスケジュール

1 回限りのイベントとして、サーバー上で、リモートのオフライン診断を呼び出して結果を返すことができます。診断で再起動が必要な場合、すぐに再起動するか、次回の再起動またはメンテナンス期間までステージングすることができます (アップデートを実行する場合と同様)。診断を実行すると、結果が収集され、内部 iDRAC ストレージに保存されます。この後、`diagnostics export` racadm コマンドを使用して結果を NFS または CIFS ネットワーク共有にエクスポートできます。診断の実行は、適切な WSMAN コマンドを使用しても行うことができます。詳細に関しては、WSMAN のマニュアルを参照してください。

自動リモート診断を使用するには、iDRAC Express ライセンスが必要です。

診断をすぐに実行する、または特定の日付と時刻をスケジュールしたり、診断タイプおよび再起動のタイプを指定することができます。

スケジュールに関しては、以下を指定することができます。

- 開始時刻 - 将来の日付と時刻に診断を実行します。TIME NOW を指定すると、診断は、次回の再起動時に実行されます。
- 終了時刻 - 開始時刻より後、診断がその時まで実行される日付と時刻です。終了時刻までに診断が終了しない場合、有効期限切れで失敗としてマークされます。TIME NA を指定すると、待機時間は適用されません。

診断テストの種類は次のとおりです。

- 拡張テスト
- エクスプレステスト
- 両方のテストを順に実行

再起動の種類は次のとおりです。

- システムのパワーサイクル
- 正常なシャットダウン (オペレーティングシステムの電源をオフ、またはシステムを再起動を待機)
- 強制シャットダウン (オペレーティングシステムに電源オフの信号を送り 10 分待機。オペレーティングシステムの電源が切れない場合、iDRAC が電源サイクルを実行します)

スケジュール可能な診断ジョブ、または一度に実行可能なジョブは 1 つのみです。診断ジョブを実行すると、正常に完了、エラーで終了、または不成功、のいずれかになります。結果を含む診断イベントは Lifecycle Controller ログに記録されます。リモート RACADM、または WSMAN を使用して最近実行した診断の結果を取得することができます。

リモートでスケジュールされた診断テストのうち、最新の診断結果を、CIFS または NFS などのネットワーク共有にエクスポートできます。最大ファイルサイズは 5 MB です。

ジョブのステータスが未スケジュールまたはスケジュール済みの場合、診断ジョブをキャンセルできます。診断を実行中の場合は、ジョブをキャンセルするにはシステムを再起動します。

リモート診断を実行する前に次を確認します。

- Lifecycle Controller が有効化されている。
- ログインおよびサーバー制御権限がある。

RACADM を使用した自動リモート診断のスケジュール

- リモート診断を実行して、結果をローカルシステムに保存するには、次のコマンドを使用します。

  ```
  racadm diagnostics run -m <Mode> -r <reboot type> -s <Start Time> -e <Expiration Time>
  ```

- 最後に実行されたリモート診断結果をエクスポートするには、次のコマンドを使用します。

  ```
  racadm diagnostics export -f <file name> -l <NFS / CIFS share> -u <username> -p <password>
  ```

各オプションの詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

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。

iDRAC 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、iDRAC 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。
- iDRAC GUI ビデオプレーヤーに表示されるビデオキャプチャ時間が、他のビデオプレーヤーに表示されるビデオキャプチャ時間と異なる場合があります。他のすべてのビデオプレーヤーがそれぞれのオペレーティングシステムのタイムゾーンの時刻を表示する一方で、iDRAC GUI ビデオプレーヤーは iDRAC のタイムゾーンの時刻を表示します。

[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。詳細については、『iDRAC オンラインヘルプ』を参照してください。

ビデオキャプチャの設定

ビデオキャプチャを設定するには、次の手順を実行します。

1. iDRAC 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。
   [ビデオキャプチャ] ページが表示されます。
2. [ビデオキャプチャ設定] ドロップダウンメニューから、次のいずれかのオプションを選択します。
   - [無効] — 起動キャプチャは無効です。
   - [バッファが満杯になるまでキャプチャ] — バッファサイズに達するまで起動シーケンスがキャプチャされます。
   - [POST の最後までキャプチャ] — POST の最後まで起動シーケンスがキャプチャされます。
3. 設定を適用するには、[適用] をクリックします。

ログの表示

システムイベントログ (SEL) および Lifecycle ログを表示できます。詳細については、「システムイベントログの表示」および「Lifecycle 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、iDRAC 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. iDRAC 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。

関連概念

前回のクラッシュ画面の有効化 、p. 89

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

適切なラックサーバおよびタワーサーバの LCD 前面パネルステータスを表示するには、iDRAC 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。

ⓘ **メモ:** ラックサーバおよびタワーサーバでのみエラーを非表示または再表示できます。

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` グループのオブジェクトを使用します。詳細に関しては、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

関連概念

LCD の設定 、p. 86

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、iDRAC 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 [エラーを再表示する] の両方がグレー表示されます。ラックサーバおよびタワーサーバについてのみエラーの非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。

詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

関連概念

システム ID LED の設定 、p. 87

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

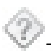
iDRAC および CMC (ブレードサーバーの場合) ウェブインタフェースには、次のアイテムのステータスが表示されます。

- バッテリ
- シャーシコントローラ状態
- 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

iDRAC 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 の正常性を表示するには、[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。

SupportAssist コレクションの生成

サーバーの問題についてテクニカルサポートとの作業が必要であるが、セキュリティポリシーによってインターネットへの直接接続が制限されているという場合、デルからソフトウェアをインストールしたりツールをダウンロードする、またはサーバーオペレーティングシステムや iDRAC からのインターネットへのアクセスを必要とすることなく、テクニカルサポートに必要なデータを提供して問題のトラブルシューティングを円滑に進めることができます。代替のシステムからデータを送信し、テクニカルサポートへの転送中に、お使いのサーバーから収集されたデータが許可を持たないユーザーによって閲覧されないことを確実にすることができます。

サーバーの正常性レポートを生成し、レポートを管理ステーション（ローカル）上の場所または、共有インターネットファイルシステム（CIFS）やネットワークファイル共有（NFS）といったネットワーク上の共有の場所で共有することができます。その後、このレポートをテクニカルサポートと直接共有することができます。CIFS や NFS といったネットワーク共有の場所にエクスポートするには、iDRAC 共有への直接ネットワーク接続、または専用のネットワークポートが必要です。

このレポートは、標準の ZIP フォーマットで生成されます。このレポートに含まれる情報は DSET レポートにある情報と似ています。以下に例を示します。

- すべてのコンポーネントのハードウェアインベントリ
- システム、Lifecycle Controller、およびコンポーネントの属性
- オペレーティングシステムおよびアプリケーションの情報
- アクティブ Lifecycle Controller ログ（アーカイブされたエントリは含まない）
- PCIe SSD ログ
- ストレージコントローラログ

メモ: SupportAssist 機能を使用した PCIe SSD のための TTYLog コレクションは、デルの第 12 世代 PowerEdge サーバーではサポートされません。

データの生成後、このデータを表示することができます。データには複数の XML ファイルとログファイルが含まれています。このデータは、問題のトラブルシューティングのためにテクニカルサポートと共有する必要があります。

データ収集が実行されるたびに、イベントが Lifecycle Controller ログに記録されます。イベントには、使用されたインタフェース、エクスポートの日時、iDRAC ユーザー名などの情報が含まれます。

次の 2 つの方法で、OS アプリケーションおよびログレポートを生成できます。

- 自動 — OS Collector ツールを自動で呼び出す iDRAC サービスモジュールを使用します。
- 手動 — 実行可能な OS Collector をサーバー OS から手動で実行します。iDRAC は、実行可能な OS Collector を、DRACRW ラベルが付いた USB デバイスとしてサーバー OS に表示します。

メモ:

- OS Collector ツールは、Dell Precision PR7910 システムには適用されません。
- OS ログ収集機能は、CentOS オペレーティングシステムではサポートされていません。
- Windows 2016 Nano エディションを実行しているサーバでは、HardwareEvent.evtx ビューアのログは OS コントローラツールによって生成されません。HardwareEvent.evtx ビューアのログを生成するには、OS コントローラツールを実行する前に ~New-Item -Path HKLM:\SYSTEM\ControlSet001\Services\EventLog\HardwareEvents~ コマンドを実行します。

正常性レポートを生成する前に、次を確認します。

- Lifecycle Controller が有効化されている。
- Collect System Inventory On Reboot（CSIOR）が有効になっている。
- ログインおよびサーバー制御権限がある。

関連概念

SupportAssist コレクションの自動生成、p. 288
SupportAssist コレクションの手動生成、p. 289

SupportAssist コレクションの自動生成

iDRAC サービスモジュールがインストールされ、実行されている場合は、SupportAssist コレクションを自動的に生成できます。iDRAC サービスモジュールは、ホストオペレーティングシステムで適切な OS Collector ファイルを呼び出してデータを収集し、それを iDRAC に転送します。その後、データを必要な場所に保存できます。

iDRAC ウェブインタフェースを使用した SupportAssist コレクションの自動生成

SupportAssist コレクションを自動的に生成するには、次の手順を実行します。

1. iDRAC 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] > [SupportAssist] と移動します。
   [SupportAssist] ページが表示されます。
2. データを収集するためのオプションを選択します。
   - [ハードウェア]
   - [OS およびアプリケーションデータ]

     メモ: ネットワーク共有設定を指定する場合は、ユーザー名とパスワードに特殊記号を使用しないようにするか、特殊文字をパーセントエンコードすることが推奨されます。
   - [詳細エクスポートオプション] をクリックして、次の追加オプションを選択します。
     - [RAID コントローラログ]
     - [OS およびアプリケーションデータ] の [レポートのフィルタ処理を有効にする]

   選択したオプションに基づいて、データの収集にかかった時間が、これらのオプションの隣に表示されます。
3. [SupportAssist によるこの情報の使用に同意する] オプションを選択し、[エクスポート] をクリックします。
4. iDRAC サービスモジュールが OS およびアプリケーションデータを iDRAC に転送すると、それらのデータがハードウェアデータと共にパッケージ化され、最終的なレポートが生成されます。レポートを保存するよう促すメッセージが表示されます。
5. SupportAssist コレクションの保存場所を指定します。

SupportAssist コレクションの手動生成

iSM がインストールされていない場合、OS Collector ツールを手動で実行して SupportAssist コレクションを生成することができます。OS およびアプリケーションデータをエクスポートするには、サーバー OS で OS Collector ツールを実行する必要があります。DRACRW というラベルが付いた仮想 USB デバイスがサーバーオペレーティングシステムに表示されます。このデバイスには、ホストオペレーティングシステムに固有の OS Collector ファイルが含まれています。サーバー OS からオペレーティングシステムに固有のファイルを実行し、データを iDRAC へ転送します。その後、データをローカルまたはネットワーク共有の場所へエクスポートできます。

デルの第 13 世代 PowerEdge サーバーでは、OS Collector DUP が工場出荷時にインストールされています。ただし、OS Collector が iDRAC に存在しないことが確認された場合は、デルのサポートサイトから DUP ファイルをダウンロードし、ファームウェアアップデート処理を使用してそのファイルを iDRAC にアップロードすることができます。

OS Collector ツールを使用して SupportAssist Collection を手動で生成する前に、ホストのオペレーティングシステムで次の操作を実行します。

- Linux オペレーティングシステム : IPMI サービスが実行されているかどうかを確認します。実行されていない場合は、このサービスを手動で開始する必要があります。次の表に、各 Linux OS で IPMI サービスステータスの確認とサービスの開始 (必要な場合) に使用できるコマンドを示します。

LINUX オペレーティングシステム	IPMI サービスステータスを確認するコマンド	IPMI サービスを開始するコマンド
Red Hat Enterprise Linux 5 64 ビット Red Hat Enterprise Linux 6 SUSE Linux Enterprise Server 11 CentOS 6 Oracle VM Oracle Linux 6.4	`$ service ipmi status`	`$ service ipmi start`
Red Hat Enterprise Linux 7	`$ systemctl status ipmi.service`	`$ systemctl start ipmi.service`

メモ:
- CentOS は iDRAC サービスモジュール 2.0 以降でのみサポートされています。
- IPMI モジュールが存在しない場合は、OS 配布メディアから対応するモジュールをインストールできます。インストールが完了すると、サービスが開始されます。

- Windows オペレーティングシステム：
  - WMI サービスが実行されているかどうかを確認します。
    - WMI が停止している場合、OS Collector は自動的に WMI を起動し、収集を続行します。
    - WMI が無効になると、OS Collector は収集を停止し、エラーメッセージが表示されます。
  - 適切な権限レベルを確認し、レジストリやソフトウェアデータの取得を妨げているファイアウォールまたはセキュリティ設定がないことを確認します。

iDRAC ウェブインタフェースを使用した SupportAssist コレクションの手動生成

SupportAssist コレクションを手動で生成するには、次の手順を実行します。

1. iDRAC 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] > [SupportAssist] と移動します。[SupportAssist] ページが表示されます。
2. データを収集するためのオプションを選択します。
   - レポートをローカルシステム上の場所にエクスポートする場合は [ハードウェア] を選択します。
   - レポートをネットワーク共有にエクスポートし、ネットワーク設定を指定するには、[OS およびアプリケーションデータ] を選択します。

     メモ: ネットワーク共有設定を指定する場合は、ユーザー名とパスワードに特殊記号を使用しないようにするか、特殊文字をパーセントエンコードすることが推奨されます。
   - [詳細エクスポートオプション] をクリックして、次の追加オプションを選択します。
     - [RAID コントローラログ]
     - [OS およびアプリケーションデータ] の [レポートのフィルタ処理を有効にする]

   選択したオプションに基づいて、データの収集にかかった時間が、これらのオプションの隣に表示されます。

   OS Collector ツールがシステム上で実行されていなかった場合、OS およびアプリケーションデータ オプションはグレー表示になり、選択することができません。OS およびアプリケーションデータ (タイムスタンプ : なし) というメッセージが表示されます。

   以前 OS Collector がシステム上で実行されていた場合、オペレーティングシステムおよびアプリケーションデータが最後に収集された時のタイムスタンプ 最後のコレクション : <timestamp> が表示されます。
3. [OS Collector の連結] をクリックします。
   ホスト OS にアクセスするように指示されます。仮想コンソールの起動を促すメッセージが表示されます。
4. 仮想コンソールを起動したら、ポップアップメッセージをクリックし、OS Collector ツールを使用してデータを収集します。
5. DRACRW 仮想 USB デバイスに移動します。このデバイスは、iDRAC によってシステムに提供されます。
6. ホストのオペレーティングシステムに適した OS Collector ファイルを呼び出します。
   - Windows の場合、**Windows_OSCollector_Startup.bat** を実行します。
   - Linux の場合、**Linux_OSCollector_Startup.exe** を実行します。
7. OS Collector が iDRAC へのデータ転送を完了したら、iDRAC によって USB デバイスが自動的に削除されます。
8. [SupportAssist] ページに戻り、[更新] アイコンをクリックして新しいタイムスタンプを反映させます。
9. データをエクスポートするには、[書き出し場所] で [ローカル] または [ネットワーク] を選択します。
10. [ネットワーク] を選択した場合は、ネットワークの詳細な場所を入力します。
11. [SupportAssist によるこの情報の使用に同意する] オプションを選択してから、[エクスポート] をクリックして、指定した場所にデータをエクスポートします。

RACADM を使用した SupportAssist コレクションの手動生成

RACADM を使用して SupportAssist コレクションを生成するには、**techsupreport** サブコマンドを使用します。詳細については、**dell.com/esmmanuals** にある『*iDRAC RACADM コマンドラインリファレンスガイド*』を参照してください。

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。

iDRAC の再起動

サーバーの電源を切らずに、iDRAC 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 — iDRAC ウェブインタフェースまたは RACADM を使用します。

iDRAC ウェブインタフェースを使用した iDRAC のリセット

iDRAC を再起動するには、iDRAC ウェブインタフェースで次のいずれかの操作を実行します。

- [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 iDRAC のリセット

iDRAC を再起動するには、[racreset] コマンドを使用します。詳細については、**dell.com/support/manuals** にある『iDRAC 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。

システムおよびユーザーデータの消去

システムコンポーネントおよびユーザーデータを削除できます。システムコンポーネントには以下が含まれます。

- Lifecycle Controller のデータ
- 内蔵診断機能
- 組み込み OS ドライバパック
- デフォルトへの BIOS リセット
- デフォルトへの iDRAC リセット

システム消去を実行する前に、以下を確認します。

- iDRAC サーバー制御権限がある。
- Lifecycle Controller が有効化されている。

Lifecycle Controller のデータ オプションでは、LC ログ、設定データベース、ロールバックのファームウェア、工場出荷時のログ、FP SPI (または管理ライザ) からの設定情報などのコンテンツが削除されます。

メモ: Lifecycle Controller ログには、システム消去の要求に関する情報と、iDRAC の再起動時に生成された情報が含まれます。以前の情報はすべて削除されます。

SystemErase コマンドを使用して、1 つまたは複数のシステムコンポーネントを削除できます。

```
racadm systemErase <BIOS | DIAG | DRVPACK | LCDATA | IDRAC >
```

ここで、

- BIOS — デフォルトへの BIOS のリセット
- DIAG — 内蔵診断機能
- DRVPACK — 組み込み OS ドライバパック
- LCDATA — Lifecycle Controller データの消去
- iDRAC — デフォルトへの iDRAC のリセット

詳細については、**dell.com/esmmanuals** にある『iDRAC RACADM コマンドラインリファレンスガイド』を参照してください。

メモ: デルテックセンターのリンクはデルブランドのシステムの iDRAC GUI に表示されます。WS-Man コマンドを使用してシステムデータを消去し、リンクをもう一度表示する場合は、ホストを手動で再起動し CSIOR が実行するまで待機します。

工場出荷時のデフォルト設定への iDRAC のリセット

iDRAC 設定ユーティリティまたは iDRAC ウェブインタフェースを使用して iDRAC を工場出荷時のデフォルト設定にリセットできます。

iDRAC ウェブインタフェースを使用した iDRAC の工場出荷時デフォルト設定へのリセット

iDRAC ウェブインタフェースを使用して iDRAC を工場出荷時のデフォルト設定にリセットするには、次の手順を実行します。

1. ［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。
   ［診断コンソール］ページが表示されます。
2. ［iDRAC をデフォルト設定にリセット］をクリックします。
   完了ステータスはパーセントで表示されます。iDRAC が再起動し、工場出荷時のデフォルト設定が復元されます。iDRAC IP はリセットされ、アクセスできなくなります。IP は前面パネルまたは BIOS を使用して設定できます。

iDRAC 設定ユーティリティを使用した iDRAC の工場出荷時デフォルト設定へのリセット

iDRAC 設定ユーティリティを使用して iDRAC 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 設定のデフォルトへのリセット］に移動します。
   ［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。

24

よくあるお問い合わせ（FAQ）

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
- ネットワークセキュリティ
- Active Directory
- シングルサインオン
- スマートカードログイン
- 仮想コンソール
- 仮想メディア
- vFlash SD カード
- SNMP 認証
- ストレージデバイス
- iDRAC サービスモジュール
- RACADM
- その他

トピック：

システムイベントログ

Internet Explorer で iDRAC 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、iDRAC 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、［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: iDRAC 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

iDRAC 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。

iDRAC にはデフォルトの iDRAC 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 iDRAC サーバー証明書をアップロードします。

DNS サーバーが iDRAC 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 iDRAC 名しか登録しません。

iDRAC 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 iDRAC 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。

iDRAC にはデフォルトの iDRAC 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、iDRAC に発行されたデフォルトの証明書が iDRAC 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 iDRAC ホスト名に対して発行された iDRAC 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 iDRAC 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 iDRAC の登録名（証明書が iDRAC 登録名に対して発行された場合）を一致させます。

CSR が DNS iDRAC 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. iDRAC 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 iDRAC 名を入力します。
3. [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 iDRAC 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 iDRAC 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 有効] オプションが選択されている。
  - [iDRAC 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 iDRAC 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。
  - ユーザーと iDRAC オブジェクトが別のドメイン内にある場合は、[ログインからのユーザードメイン] オプションを選択しないでください。代わりに、[ドメインを指定する] オプションを選択し、iDRAC オブジェクトが属するドメイン名を入力します。
- ドメインコントローラの SSL 証明書で、iDRAC 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?

```
ERROR: Can't contact LDAP server, error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check the correct
Certificate Authority (CA) certificate has been uploaded to iDRAC. Please also check if the
iDRAC date is within the valid period of the certificates and if the Domain Controller
Address configured in iDRAC matches the subject of the Directory Server Certificate.
```

証明書の検証が有効な場合、iDRAC はディレクトリサーバーとの SSL 接続を確立すると、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。

- iDRAC 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。iDRAC の日付と証明書の有効期間を確認してください。
- iDRAC 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、iDRAC 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。
- iDRAC 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、iDRAC 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。

iDRAC 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、iDRAC 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。

iDRAC 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、iDRAC 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。

iDRAC 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?

iDRAC は、iDRAC 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。

iDRAC 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 iDRAC 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。iDRAC 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 iDRAC 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を目的としたものです。

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 iDRAC にアップロードします。

これで、SSO を使用して iDRAC 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 iDRAC 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] > [システム] > [CurrentControlSet] > [制御] > [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 iDRAC にログインできます。

iDRAC 用に SSO を有効にし、Internet Explorer を使って iDRAC 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?

iDRAC 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 iDRAC 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。iDRAC 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

iDRAC ウェブインタフェースからログアウトしても、仮想コンソールセッションがアクティブです。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 iDRAC 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。

iDRAC ユーザーがローカルサーバービデオをオン / オフにするために必要な権限は何ですか?

iDRAC 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。

`iDRAC.VirtualConsole.AttachState` オブジェクトのステータスを表示するには、次のコマンドを使用します。

```
racadm get idrac.virtualconsole.attachstate
```

または、Telnet、SSH、リモートセッションから次のコマンドを使用します。

```
racadm -r (iDrac IP) -u (username) -p (password) get iDRAC.VirtualConsole.AttachState
```

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、iDRAC 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。

Lifecycle 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。［マウスアクセラレーション］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。

iDRAC 仮想コンソールクライアントで、iDRAC 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に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には、オペレーティングシステムをリモートインストールする前に、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?

iDRAC からアクセスした場合、管理ステーションの Num Lock インジケータは、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、iDRAC 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、iDRAC 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や帯域幅などの物理的制限によってパラメータの最大範囲が設定されます。

iDRAC 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?

iDRAC 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 iDRAC 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 iDRAC の IP アドレスまたは DNS 名を入力します。
3. ［Add（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。iDRAC 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。iDRAC 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 1 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 iDRAC 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 iDRAC 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 iDRAC 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、iDRAC 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 iDRAC 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、iDRAC 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、iDRAC 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 iDRAC ウェブインタフェースまたはローカル RACADM コマンドを使用して変更した場合、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』(Dell システム管理ツールおよびマニュアル DVD) を使用して Windows オペレーティングシステムをインストールするときに、ネットワーク接続の速度が遅い場合、ネットワーク遅延が原因で、iDRAC 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表示されません。

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?

iDRAC 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?

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。

iDRAC 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 iDRAC 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、iDRAC 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デバイス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 iDRAC 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、iDRAC 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、iDRAC 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、iDRAC 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 iDRAC 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?

iDRAC 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。

iDRAC サービスモジュール

iDRAC サービスモジュールをインストールまたは実行する前に、OpenManage Server Administrator をアンインストールする必要がありますか?

いいえ。Server Administrator をアンインストールする必要はありません。iDRAC サービスモジュールをインストールまたは実行する前に、iDRAC サービスモジュールの Server Administrator の機能を停止してください。

ホストオペレーティングシステムに iDRAC サービスモジュールがインストールされていることを確認する方法を教えてください。

iDRAC サービスモジュールがインストールされているかどうかを確認するには、次の手順を実行します。

- Windows を実行しているシステムの場合：

  コントロールパネル を開いて、表示されるインストール済みプログラムのリストに、iDRAC サービスモジュールがあるかどうかを確認します。

- Linux を実行しているシステムの場合

  コマンド `rpm —qi dcism` を実行します。iDRAC サービスモジュールがインストールされている場合、表示されるステータスは **installed** となります。

メモ: iDRAC サービスモジュールが Red Hat Enterprise Linux 7 にインストールされているかどうか確認するには、`init.d` コマンドではなく `systemctl status dcismeng.service` コマンドを使用します。

システムにインストールされている iDRAC サービスモジュールのバージョン番号を確認する方法を教えてください。

iDRAC サービスモジュールのバージョンを確認するには、次の手順のいずれかを実行します。

- ［スタート］>［コントロールパネル］>［プログラムと機能］の順にクリックします。インストールされている iDRAC サービスモジュールのバージョンが［バージョン］タブに一覧表示されます。
- ［マイコンピュータ］>［プログラムのアンインストールと変更］に移動します。

iDRAC サービスモジュールをインストールするために必要な最低許可レベルは何ですか？

iDRAC サービスモジュールをインストールするには、管理者レベルの権限を持っている必要があります。

iDRAC サービスモジュールのバージョン 2.0 およびそれ以前のバージョンでは、iDRAC サービスモジュールのインストール中に「これはサポートされているサーバはありません。」というエラーメッセージが表示されます。サポートされているサーバの詳細については、ユーザーガイドを参照してください。エラーを解決する方法は次のとおりです。

iDRAC サービスモジュールをインストールする前に、サーバーが第 12 世代以降の PowerEdge サーバーであることを確認してください。また、64 ビットシステムを使用していることも確認してください。

USBNIC 経由の OS to iDRAC パススルーが正しく設定されていても、OS のログに次のメッセージが表示されます。なぜですか?

iDRAC サービスモジュールは、OS to iDRAC パススルーチャネルを使用して、iDRAC と通信できません

iDRAC サービスモジュールは、OS to iDRAC パススルー機能を使用して、USB NIC 経由で iDRAC との通信を確立します。正しい IP エンドポイントを使用して USB NIC インタフェースが設定されていても、場合によっては通信が確立されないことがあります。この状況は、ホストのオペレーティングシステムのルーティングテーブルで、同じ宛先マスクに対して複数のエントリが設定されているため、USB NIC の宛先がルーティング順序の 1 番目に指定されない場合に発生することがあります。

Destination（送信先）	ゲートウェイ	Genmask	フラグ	メトリック	参照	使用インタフェース
デフォルト	10.94.148.1	0.0.0.0	UG	1024	0	0 em1
10.94.148.0	0.0.0.0	255.255.255.0	U	0	0	0 em1

Destination（送信先）	ゲートウェイ	Genmask	フラグ	メトリック	参照	使用インタフェース
link-local	0.0.0.0	255.255.255.0	U	0	0	0 em1
link-local	0.0.0.0	255.255.255.0	U	0	0	0 enp0s20u12u3

この例で、**enp0s20u12u3** は USB NIC インタフェースです。リンクローカル宛先マスクが繰り返され、USB NIC は順序の一番目になっていません。その結果、OS to iDRAC パススルーで iDRAC サービスモジュールと iDRAC の間に接続の問題が発生します。この接続問題を解決するには、iDRAC USBNIC IPv4 アドレス（デフォルトでは 169.254.0.1）がホストのオペレーティングシステムから到達可能であることを確認します。

到達可能でない場合は、次の手順を実行します。

- 一意の宛先マスクで iDRAC USBNIC アドレスを変更します。
- ルーティングテーブルから不要なエントリを削除して、ホストが iDRAC USB NIC IPv4 アドレスと通信する際には USB NIC が経路で選択されるようにします。

iDRAC サービスモジュールバージョン 2.0 またはそれ以前のバージョンでは、VMware ESXi サーバーから iDRAC サービスモジュールをアンインストールするときに、vSphere クライアントで仮想スイッチが vSwitchiDRACvusb、ポートグループが iDRAC ネットワークと命名されます。これらを削除する方法を教えてください。

VMware ESXi サーバーに iDRAC サービスモジュール VIB をインストールすると、iDRAC サービスモジュールは仮想スイッチとポートグループを作成し、OS to iDRAC パススルーを介して USB NIC モードで iDRAC と通信できるようにします。サービスモジュールをアンインストールしても、仮想スイッチ［vSwitchiDRACvusb］とポートグループ［iDRAC Network］は削除されません。これらを手動で削除するには、次の手順のいずれかを実行します。

- vSphere クライアント設定ウィザードに移動し、エントリを削除します。
- Esxcli に移動し、次のコマンドを入力します。
  - ポートグループを削除する場合：`esxcfg-vmknic -d -p "iDRAC Network"`
  - 仮想スイッチを削除する場合：`esxcfg-vswitch -d vSwitchiDRACvusb`

  メモ: サーバーの機能に問題があるわけではないので、VMware ESXi サーバーに iDRAC サービスモジュールを再インストールすることができます。

複製された Lifecycle ログはオペレーティングシステムのどこにありますか?

複製された Lifecycle ログを表示するには、次の手順を実行します。

オペレーティングシステム	場所
Microsoft Windows	［イベントビューア］>［Windows ログ］>［システム］と移動します。iDRAC サービスモジュールのすべての Lifecycle ログは、［iDRAC Service Module］というソース名の下で複製されます。 **メモ:** iSM バージョン 2.1 以降では、Lifecycle Controller ログのソース名の下に Lifecycle ログが複製されます。iSM バージョン 2.0 およびそれ以前のバージョンでは、ログは iDRAC サービスモジュールのソース名の下に複製されます。 **メモ:** Lifecycle ログの場所は、iDRAC サービスモジュールインストーラを使用して設定できます。iDRAC サービスモジュールのインストール中またはインストーラの変更中に場所を設定できます。
Red Hat Enterprise Linux、SUSE Linux、CentOS、および Citrix XenServer	`/var/log/messages`
VMware ESXi	`/var/log/syslog.log`

Linux のインストール中に、インストールに使用できる Linux 依存パッケージまたは実行可能プログラムとは何ですか?

Linux 依存パッケージのリストを表示するには、『iDRAC サービスモジュールインストールガイド』で「Linux の依存関係」の項を参照してください。

RACADM

iDRAC 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?

```
ERROR: Unable to connect to RAC at specified IP address
```

このメッセージは、別のコマンドを発行する前に、iDRAC 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。

iDRAC 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 iDRAC 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 < filename >
```

`filename` は openssl または libopenssl rpm パッケージファイルです。

たとえば、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?

iDRAC ウェブサーバのリセット後は、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。

iDRAC ウェブサーバは、次の場合にリセットされます。

- iDRAC 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。
- `racadm set -f <config file>`が変更する場合を含め、iDRAC.Webserver.HttpsPort property が変更された。
- `racresetcfg` コマンドが使用された。
- iDRAC 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

ブレードサーバの iDRAC IP アドレスを検索するには、どうすればよいですか?

- **CMC ウェブインタフェースを使用する場合**：

  ［シャーシ］ > ［サーバ］ > ［セットアップ］ > ［導入］と移動します。表示された表にサーバの IP アドレスを表示します。

- **仮想コンソールを使用する場合**：POST 中にサーバを再起動して iDRAC IP アドレスを表示します。OSCAR の「Dell CMC」コンソールを選択して、ローカルシリアル接続から CMC にログインします。CMC RACADM コマンドはこの接続から送信できます。

CMC RACADM コマンドの詳細については、**dell.com/esmmanuals** にある『*CMC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

iDRAC RACADM コマンドの詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

- **ローカル RACADM を使用する場合**

  `racadm getsysinfo` のコマンドを使用します。例：

```
$ racadm getniccfg -m server-1
DHCP Enabled = 1
IP Address    = 192.168.0.1
Subnet Mask  = 255.255.255.0
Gateway       = 192.168.0.1
```

- **LCD を使用する場合**：

  メインメニューで、サーバ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?

- **iDRAC ウェブインタフェースから次の操作を行います。**

  [概要] > [iDRAC 設定] > [CMC] と移動します。[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次の操作を行います。**

  OSCAR の「Dell CMC」コンソールを選択して、ローカルシリアル接続から CMC にログインします。CMC RACADM コマンドはこの接続から発行できます。

```
$ 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。

CMC RACADM コマンドの詳細については、**dell.com/esmmanuals** にある『*CMC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

iDRAC RACADM コマンドの詳細については、**dell.com/idracmanuals** にある『*iDRAC RACADM コマンドラインインタフェースリファレンスガイド*』を参照してください。

ラックおよびタワーサーバーの iDRAC IP アドレスはどのように検索すればよいですか?

- **iDRAC ウェブインタフェースから次の操作を行います。**

  [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 iDRAC IP アドレスが表示されます。

- **ローカル RACADM から次の操作を行います。**

  `racadm getsysinfo` のコマンドを使用します。

- **LCD から次の操作を行います。**

物理サーバで、LCD パネルのナビゲーションボタンを使用して iDRAC 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 から次の操作を行います。**

  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。

iDRAC 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。
- NIC の設定、IPv4 および 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。

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。

- iDRAC 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。

iDRAC 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?

iDRAC 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 iDRAC 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 iDRAC 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。

iDRAC がアップグレード可能なコンポーネントとして表示されているかどうかを 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、iDRAC ウェブインタフェースを使用するか、サーバーの LCD で、iDRAC ログのエラーメッセージを確認します。

25

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。

トピック：

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、iDRAC 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
- iDRAC 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 Lifecycle 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。
- テクニカルサポートレポートの生成および収集したデータの表示。
- iDRAC サービスモジュールによって提供される監視機能の使用

関連タスク

仮想コンソールのプレビュー 、p. 226
起動キャプチャとクラッシュキャプチャビデオの表示 、p. 285

システム正常性の表示、p. 287
ログの表示、p. 285
SupportAssist コレクションの生成、p. 288
ストレージデバイスのインベントリと監視、p. 196
iDRAC サービスモジュールの使用、p. 262

システム情報の取得と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。

- iDRAC 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。
- iDRAC サービスモジュールが取り付けられている場合は、オペレーティングシステムのホスト情報が表示されます。

関連タスク

システム正常性の表示、p. 287
iDRAC サービスモジュールの使用、p. 262
SupportAssist コレクションの生成、p. 288

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. アラートを有効化します。
2. 電子メールアラートを設定し、ポートを確認します。
3. 管理下システムの再起動、電源オフ、またはパワーサイクルを実行する。
4. テストアラートを送信します。

Lifecycle ログとシステムイベントログの表示とエクスポート

Lifecycle 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. iDRAC 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] > [Lifecycle ログ] と移動して Lifecycle ログを表示します。

   メモ: SEL は Lifecycle 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 Lifecycle 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、Lifecycle 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。
3. iDRAC サービスモジュールを使用している場合は、Lifecycle ログを OS ログにエクスポートします。詳細については、「iDRAC サービスモジュールの使用、p. 262」を参照してください。

iDRAC ファームウェアをアップデートする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。

- iDRAC ウェブインタフェース
- RACADM CLI (iDRAC 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、iDRAC 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］>［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］>［ 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。

メモ: すべての［電源］オプションは、ホストオペレーティングシステムによって異なります。オプションが正常に機能するには、オペレーティングシステムで変更を行う必要があります。たとえば、RHEL 7.2 の Gnome-tweak-tool などです。

詳細については、『*iDRAC 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、iDRAC 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］>［ 仮想コンソール ］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

2 台のサーバーがラックに取り付けられているとします。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、電力上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。

一度のホストシステム再起動での複数ネットワークカードのための I/O アイデンティティ構成設定の適用

サーバー内に SAN（Storage Area Network）環境の一部である複数のネットワークカードがあり、これらのカードに異なる仮想アドレス、イニシエータ、およびターゲットの構成設定を適用したい場合は、I/O アイデンティティ最適化機能を使用して、設定の構成に要する時間を削減することができます。

1. BIOS、iDRAC、ネットワークカードが最新のファームウェア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。
2. IO アイデンティティ最適化を有効化します。
3. XML 設定ファイルを iDRAC からエクスポートします。
4. I/O アイデンティティ最適化設定を XML ファイルで編集します。
5. XML 設定ファイルを iDRAC にインポートします。

関連概念

デバイスファームウェアのアップデート 、p. 62
I/O アイデンティティ最適化の有効化または無効化 、p. 179