Integrated Dell Remote Access Controller 9
User's Guide
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。
Chapter 1: iDRAC の概要

iDRAC With Lifecycle Controller を使用するメリット..........................................................16
主な機能.......................................................................................................................................17
New features added .....................................................................................................................19
ファームウェア バージョン 4.20.20.20..................................................................................19
ファームウェア バージョン 4.10.10.10..................................................................................20
ファームウェア バージョン 4.00.00.00..................................................................................20
本ガイドの使用方法..................................................................................................................21
対応ウェブブラウザ...................................................................................................................21
サポートされる OS とハイパーバイラ...
### Chapter 3: 管理下システムのセットアップ

<table>
<thead>
<tr>
<th>内容</th>
<th>ページ</th>
</tr>
</thead>
<tbody>
<tr>
<td>iDRAC IPアドレスのセットアップ</td>
<td>48</td>
</tr>
<tr>
<td>iDRAC設定ユーティリティを使用したiDRAC IPのセットアップ</td>
<td>49</td>
</tr>
<tr>
<td>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</td>
<td>52</td>
</tr>
<tr>
<td>自動検出</td>
<td>52</td>
</tr>
<tr>
<td>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</td>
<td>54</td>
</tr>
<tr>
<td>セキュリティ向上のためのパスワードの使用</td>
<td>59</td>
</tr>
<tr>
<td>ローカル管理者アカウント設定の変更</td>
<td>61</td>
</tr>
<tr>
<td>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</td>
<td>61</td>
</tr>
<tr>
<td>RACADMを使用した管理下システムの場所のセットアップ</td>
<td>61</td>
</tr>
<tr>
<td>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</td>
<td>61</td>
</tr>
<tr>
<td>システムバフォーマンスと電力消費の最適化</td>
<td>62</td>
</tr>
<tr>
<td>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</td>
<td>62</td>
</tr>
<tr>
<td>RACADMを使用した温度設定の変更</td>
<td>64</td>
</tr>
<tr>
<td>iDRAC設定ユーティリティを使用したサーマル設定の変更</td>
<td>67</td>
</tr>
<tr>
<td>iDRAC Webインタフェースを使用したPCleエアフレー設定の変更</td>
<td>68</td>
</tr>
<tr>
<td>管理ステーションのセットアップ</td>
<td>68</td>
</tr>
<tr>
<td>iDRACへのリモートアクセス</td>
<td>69</td>
</tr>
<tr>
<td>対応ウェブブラウザの設定</td>
<td>69</td>
</tr>
<tr>
<td>Internet Explorerの設定</td>
<td>69</td>
</tr>
<tr>
<td>Mozilla Firefoxの設定</td>
<td>70</td>
</tr>
<tr>
<td>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</td>
<td>71</td>
</tr>
<tr>
<td>ウェブインタフェースのローカライズパージョンの表示</td>
<td>74</td>
</tr>
<tr>
<td>デバイスファームウェアのアップデート</td>
<td>74</td>
</tr>
<tr>
<td>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</td>
<td>77</td>
</tr>
<tr>
<td>自動ファームウェアアップデートのスケジュール設定</td>
<td>78</td>
</tr>
<tr>
<td>RACADMを使用したデバイスファームウェアのアップデート</td>
<td>79</td>
</tr>
<tr>
<td>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</td>
<td>80</td>
</tr>
<tr>
<td>DUPを使用したファームウェアのアップデート</td>
<td>80</td>
</tr>
<tr>
<td>リモートRACADMを使用したファームウェアのアップデート</td>
<td>81</td>
</tr>
<tr>
<td>Lifecycle Controller Remote Servicesを使用したファームウェアのアップデート</td>
<td>81</td>
</tr>
<tr>
<td>iDRACからのCMCファームウェアのアップデート</td>
<td>81</td>
</tr>
<tr>
<td>ステージングされたアップデートの表示と管理</td>
<td>82</td>
</tr>
<tr>
<td>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</td>
<td>82</td>
</tr>
<tr>
<td>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</td>
<td>82</td>
</tr>
<tr>
<td>デバイスファームウェアのロールバック</td>
<td>82</td>
</tr>
<tr>
<td>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</td>
<td>83</td>
</tr>
<tr>
<td>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</td>
<td>84</td>
</tr>
<tr>
<td>RACADMを使用したファームウェアのロールバック</td>
<td>84</td>
</tr>
<tr>
<td>Lifecycle Controllerを使用したファームウェアのロールバック</td>
<td>84</td>
</tr>
<tr>
<td>Lifecycle Controller-Remote Servicesを使用したファームウェアのロールバック</td>
<td>84</td>
</tr>
</tbody>
</table>
RACADM を使用した最初の起動デバイスの設定..............................104
仮想コンソールを使用した最初の起動デバイスの設定........................104
前回のクラッシュ画面の有効化......................................................... 105
OS から iDRAC へのパススルーの有効化または無効化................105
OS から iDRAC へのパススルー用の対応カード............................106
USB NIC 対応のオペレーティングシステム......................................106
Web インターフェイスを使用した OS to iDRAC パススルーの有効化または無効化 107
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 108
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 108
証明書の取得.................................................................................. 108
SSL サーバー証明書...................................................................... 109
新しい証明書署名要求の生成..........................................................110
自動証明書登録............................................................................ 110
サーバー証明書のアップロード...........................................................111
サーバー証明書の表示.....................................................................111
カスタム署名証明書のアップロード...................................................112
カスタムSSL証明書署名証明書のダウンロード.................................112
カスタムSSL証明書署名証明書の削除...............................................113
RACADM を使用した複数の iDRAC の設定.......................................113
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 114

Chapter 5: iDRAC と管理下システム情報の表示................................. 115
管理下システムの正常性とプロパティの表示......................................115
アセット追跡の設定........................................................................ 115
システムインベントリの表示.............................................................115
センター情報の表示........................................................................ 116
CPU、メモリ、および入出力モジュールのパフォーマンスインデックスの監視 118
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 119
RACADM を使用した CPU、メモリ、入出力モジュールのパフォーマンスインデックスの監視 119
アイドル サーバーの検出................................................................119
GPU（アクセラレーター）の管理.......................................................120
システムの Fresh Air 対応性のチェック...........................................121
温度の履歴データの表示.................................................................121
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................121
RACADM を使用した温度の履歴データの表示.....................................122
吸気口温度の警告しきい値の設定....................................................122
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..............................122
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 123
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 123
FlexAddress メザニンカードのファブリック接続の表示.........................123
iDRAC セッションの表示または終了................................................124
ウェブインタフェースを使用した iDRAC セッションの終了..................124

Chapter 6: iDRAC 通信のセットアップ............................................... 125
DB9 ケーブルを使用したシリアル接続による iDRAC との通信................126
BIOS のシリアル接続用設定............................................................ 126
RAC シリアル接続の有効化............................................................... 127
IPMI シリアル接続のペースシックモードおよびターミナルモードの有効化 127
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 129
Kerberos Keytabファイルの生成.................................................................169
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.................................................169
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..........................................................170
管理ステーションの設定........................................................................170
スマートカードログインの有効化または無効化..........................................170
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.................................................................170
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.........171
iDRAC設定ルータ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..............................................................171
スマートカードログインの設定................................................................171
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 ........................................................................171
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..............171
スマートカードを使用したログイン................................................................172

Chapter 10: アラートを送信するためのiDRACの設定.......................................174
アラートの有効化または無効化..................................................................174
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.............174
RACADMを使用したアラートの有効化または無効化..............................175
iDRAC設定ルータリティを使用したアラートの有効化または無効化........175
アラートのフィルタ..................................................................................175
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....................175
RACADMを使用したアラートのフィルタ..................................................175
イベントアラートの設定.........................................................................176
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..........................176
RACADMを使用したイベントアラートの設定..........................................176
アラート反復イベントの設定....................................................................177
RACADMを使用したアラート反復イベントの設定.....................................177
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........177
イベント処置の設定................................................................................177
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......................177
RACADMを使用したイベントアクションの設定.......................................177
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......178
IPアラート送信先の設定........................................................................178
電子メールアラートの設定......................................................................180
WSEventingの設定................................................................................182
RedfishEventingの設定.........................................................................182
シャーシイベントの監視..........................................................................182
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...............182
RACADMを使用したシャーシイベントの監視..........................................183
アラートメッセージID..........................................................................183

Chapter 11: iDRAC 9グループマネージャ..................................................186
グループマネージャ................................................................................186
サマリビュー.........................................................................................187
ネットワーク設定の要件........................................................................187
ログインの管理......................................................................................188
新規ユーザーの追加................................................................................188
ユーザーパスワードの変更....................................................................189
ユーザーの削除......................................................................................189
アラートの設定......................................................................................189
Chapter 14: ネットワークデバイスのインベントリ、監視、および設定............................................................................. 204
ネットワークデバイスのインベントリと監視.............................................................. 204
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................................... 204
RACADM を使用したネットワークデバイスの監視.................................................. 204
接続ビュー............................................................................................................. 205
対応ストレ RAID
物理ディスクの管理
FC HBA
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
I/O アイデンティティ最適化対応のカード
I/O アイデンティティ最適化向けにサポートされている NIC ファームウェアバージョン
iDRAC ガリモト割り当てアドレス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見
たはリモート割り当てアドレスと永続性ポリシーの動作
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
仮想ディスクの作成
仮想ディスクの暗号
仮想ディスクの初期化
仮想ディスク整合性のチェック
仮想ディスクの削除
仮想ディスクキャッシュポリシーの編集
仮想ディスクの再構成
仮想ディスク整性のチェック
仮想ディスクの初期化
仮想ディスクの暗号化
専用ネットスペアの割り当てまたは割り当て解除
ウェブインタフェースを使用した仮想ディスクの管理
RACADM を使用した仮想ディスクの管理
RAID 設定機能
コントローラーの管理

Chapter 15: Managing storage devices ................................................................. 220
RAID の概念について .................................................................................. 221
RAID とは .................................................................................................. 222
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 .................. 223
RAID レベルの選択 .................................................................................. 223
RAID レベルパフォーマンスの比較 .............................................................. 229
対応コントローラー ................................................................................... 230
対応エンクロージャ .................................................................................. 231
Summary of supported features for storage devices .................................... 231
ストレージデバイスのインベントリと監視 .................................................. 235
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 ......................... 235
RACADM を使用したストレージデバイスの監視 ......................................... 236
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 ......................... 236
ストレージデバイスのトポロジの表示 ......................................................... 236
物理ディスクの管理 .................................................................................. 236
グローバルネ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 ................................................................................................. 237
物理ディスクの RAID または非 RAID モードへの変換 ................................. 238
物理ディスクの削去 .................................................................................. 239
SED デバイスデータの削去 ...................................................................... 239
物理ディスクの再構成 ................................................................................ 240
仮想ディスクの管理 .................................................................................... 241
仮想ディスクの作成 .................................................................................... 241
仮想ディスクキャッシュポリシーの編集 ....................................................... 243
仮想ディスクの削除 .................................................................................... 243
仮想ディスク整合性のチェック .................................................................... 244
仮想ディスクの初期化 ................................................................................ 244
仮想ディスクの暗号化 ................................................................................ 245
専用ネットスペアの割り当てまたは割り当て解除 ....................................... 245
ウェブインタフェースを使用した仮想ディスクの管理 .................................. 247
RACADM を使用した仮想ディスクの管理 .................................................... 248
RAID 設定機能 ......................................................................................... 249
コントローラーの管理 ................................................................................ 250
Chapter 17: 仮想コンソールの設定と使用

対応画面解像度とリフレッシュレート......................................................... 275
仮想コンソールの設定........................................................................ 276
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.......................... 276
RACADMを使用した仮想コンソールの設定........................................ 276
仮想コンソールのプレビュー................................................................. 276
仮想コンソールの起動........................................................................ 277
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.......................... 277
URLを使用した仮想コンソールの起動.................................................. 277
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......................................................... 278
仮想コンソールビューの使用................................................................. 278
HTML5ベースの仮想コンソール................................................................ 278
マウスポイントの同期......................................................................... 281
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........... 281
章23: SMCLPの使用

SMCLPを使ったシステム管理機能
SMCLPコマンドの実行
iDRAC SMCLP構文
MAPアドレス領域のナビゲーション
show命令の使用
-displayオプションの使用
-levelオプションの使用
-outputオプションの使用
使用例
サーバー電源管理
SEL管理
MAPターゲットナビゲーション

章24: オペレーティングシステムの導入

リモートファイル共有を用い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の管理
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
RACADMを使用したリモートファイル共有の設定
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
複数のディスクからオペレーティングシステムのインストール
SDカードの内蔵オペレーティングシステムの導入
BIOSでのSDモジュールと冗長性の有効化

章25: iDRACを使った管理下システムのトラブルシューティング

診断コンソールの使用
iDRACのリセットとIDRACのデフォルトへのリセット
自動リモート診断のスケジュール
RACADMを使用した自動リモート診断のスケジュール
Postコードの表示
起動キャプチャとクラッシュキャプチャデータの表示
ビデオキャプチャの設定
ログの表示
前回のシステムクラッシュ画面の表示
システムステータスの表示
システムの前面パネルLCDステータスの表示
システムの前面パネルLEDステータスの表示
ハードウェア問題の兆候
システム正常性の表示
サーバーステータス画面でのエラーメッセージの確認.................................................................................335
iDRAC の再起動............................................................................................................................335
iDRAC ウェブインタフェースを使用した iDRAC のリセット............................................................335
RACADM を使用した iDRAC のリセット.......................................................................................335
システムおよびユーザーデータの消去..........................................................................................335
工場出荷時のデフォルト設定への iDRAC のリセット...............................................................336
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......336
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......336

Chapter 26: iDRAC への SupportAssist の統合..................................................................................337
SupportAssist 登録......................................................................................................................337
サービスモジュールのインストール............................................................................................338
サーバーオペレーティングシステムのフロントエンドインストール........................................338
SupportAssist.............................................................................................................................338
サポートリクエストポータル......................................................................................................338
収集ログ.....................................................................................................................................338
SupportAssist コレクションの生成.............................................................................................338
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..................339
設定..........................................................................................................................................340
収集の設定..................................................................................................................................340
連絡先情報..................................................................................................................................340

Chapter 27: よくあるお問い合わせ (FAQ) .........................................................................................341
システムイベントログ..................................................................................................................341
iDRAC アラート用のカスタム送信者 E メールの設定.................................................................342
ネットワークセキュリティ...........................................................................................................342
デレクトリーコストリーミング.....................................................................................................342
Active Directory........................................................................................................................343
シングルサインオン.....................................................................................................................344
スマートカードログイン............................................................................................................345
仮想コンソール................................................................................................................................345
仮想メディア..................................................................................................................................348
vFlash SD カード.......................................................................................................................350
SNMP 認証...................................................................................................................................350
ストレージデバイス....................................................................................................................351
GPU (アクセラレーター) ..............................................................................................................351
iDRAC サービスモジュール.........................................................................................................351
RACADM.....................................................................................................................................351
デフォルトのパスワードを永続的に calvin に設定する...............................................................354
その他.......................................................................................................................................354

Chapter 28: 使用事例シナリオ.........................................................................................................360
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.......................................................360
システム情報の取得とシステム正常性の評価..............................................................................360
アラートのセットアップと電子メールアラートの設定................................................................361
システムイベントログと Lifecycle ログの表示とエクスポート................................................361
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..............................................361
正常なシャットダウンの実行.......................................................................................................361
新しい管理者ユーザーアカウントの作成...................................................................................361
サーバのリモートコンソールの起動と USB ドライブのマウント................................................................. 362
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.......................... 362
ラック密度の管理........................................................................................................................................ 362
新しい電子ライセンスのインストール............................................................................................................. 362
一度のホストシステム再起動における複数ネットワークカードへの I/O アイデンティティ構成設定の適用........................................... 362
iDRAC は、サーバ管理者の生産性を向上させ、デルサーバの総合的な可用性を高めるように設計されています。iDRAC は、システム障害に関するアラートの送信、リモートシステム管理の実施の支援、およびシステムへの物理的なアクセスの必要性の軽減を行います。

iDRAC テクノロジーは、より大きなデータセンターを管理する一部であり、ビジネスに不可欠なアプリケーションとワークロードをいつでも使用できる状態にすることができます。このテクノロジーを利用することで、エージェントやオペレーティングシステムを使用することなく、あらゆる場所からデルサーバを導入、監視、管理、設定、アップデート、トラブルシューティングすることが可能になります。

iDRAC および Lifecycle Controller は、いくつかの製品と連携して IT 業務の簡素化および能率化を図ります。次に、いくつかのツールを示します。

- Dell VMware vCenter
- Dell Repository Manager
- Dell OpenManage Enterprise
- Dell OpenManage Power Center

iDRAC には次のタイプが用意されています。

- iDRAC Basic — 200 ～ 500 シリーズのサーバではデフォルトで使用可能です。
- iDRAC Express — 600 以上のシリーズのラックまたはタワーサーバ、およびすべてのプレードサーバではデフォルトで使用可能
- iDRAC Enterprise — すべてのサーバモジュールで使用可能
- iDRAC Datacenter — すべてのサーバモジュールで使用可能

トピック：
- iDRAC With Lifecycle Controller を使用するメリット
- 主な機能
- New features added
- 本ガイドの使用方法
- 対応ウェブブラウザ
- iDRAC ライセンス
- Licensed features in IDRC9
- iDRAC にアクセスするためのエラーメッセージとプロトコル
- iDRAC ポート情報
- その他の必要マニュアル
- デルへのお問い合わせ
- デルサポートサイトからの文書へのアクセス

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。

- 可能性の向上 — 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経済的コスト（TCO）の削減 — 遠隔地に多数存在するサーバーへの管理の管理範囲を拡大し、交通費などの運行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 — ローカルの導入の場合は Lifecycle Controller GUI をして導入および簡単な保守を行い、リモートな導入の場合は Dell OpenManage Essentials およびパートナーコンソールと統合された Remote Services （WSMan）インタフェースを使用します。
主な機能

iDRAC の主要機能は次のとおりです。

ライフサイクルコントローラ GUI の詳細については Lifecycle Controller ユーザーガイド を、リモートサービスについては www.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。

インベントリと監視

• グローバルホットスペアのインベントリおよび監視。
• ホストコントローラおよび仮想メディアの設定と使用。

• 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と仮想メディアを使用して、ホストウェブインタフェースを起動し、OpenManage Enterprise (OME) Modular の情報と WWN/MAC アドレスを確認します。

• メモ: CMC は、M1000E シャーシ LCD パネルおよびローカルコントロールパネルを介して、iDRAC へのアクセスを提供します。詳細については、「Chassis Management Controller ユーザーガイド」は、www.dell.com/cmcmanual にあります。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。

• iDRAC9 は、強化された監視および管理機能を Quick Sync 2 に提供します。Android または iOS モバイルデバイスに OpenManage Mobile アプリがセットされている必要があります。

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と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。

• 自動検出の有効化。

• RACADM、WSMan、および Redfish を介した XML または JSON 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設定の実行。詳細については、「Dell Lifecycle Controller Remote Services クイックスタートガイド」は、www.dell.com/idracmanuals にあります。を参照してください。

• 仮想アドレス、イニシャル化、およびストレージアリガメン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。
iDRACの概要

- 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ベントトラックとリモート監視。
  - PCIe SSD の取り外し準備。
  - データのセキュリティ消去。
- 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クアップするための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。
- 営のファームウェアイメージを使用した iDRAC システムおよび Lifecycle Controller ファームウェアのアップデートまたはリセット。
- ストレ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ブロックを使用した 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 に依存しないサーバーの設定。
- イベントのログ：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 ログ、および v3 の設定。
- 前回のシステムクラッシュイジェクスのキャプチャ。
- 起動キャッシュディオおよびクラッシュキャッシュディオの表示。
- CPU、メモリー、I/O モジュールのパフォーマンスインデックスのアウトオブバンドでの監視および通知。
- 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写。
  - システムの自動リカバリーオプション。
  - PSUs を除くすべてのシステムコンポーネントのフロップリサイクルのステータスを有効または無効にする。
  - iDRAC をリモートでハードウェアリセットする。
  - インタフェースを 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 Collection との統合。この機能は iDRAC サービスマージューバージョン 2.0 以降がインストールされている場合のみ利用可能です。
- 次の方法による SupportAssist コレクション、生成：
  - 自動 — OS Collector ソースを自動で呼び出す iDRAC サービスモジュールを使用します。

iDRAC に関するデバイスのシステムグレイシス
- Dell iDRAC は、個々の管理ネットワーク上の配置することを目的としています。インターネットに直接配置すること、または接続すること、その設計や目的に反します。そうすることにより、接続されたシステムの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、デルの安全なリスクに対して一切の責任を負いません。
- Dell EMC では、ラックおよびドウロサーバーで利用可能な、専用ギガビットイーサネットポートの使用を推奨しています。このイーサネットポートを、ホストオペレーティングシステムと共有され、管理トラフィックを個別の物理ネットワークにルーティングするために、アプリケーションターフィックの分離が可能になります。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の LOM または NIC ポートとは個別のルーティングします。専用オプションを使用すると、ホストの LOM または NIC に割り当てられている IP アドレスと比較した上で、同じサブネットまたは異なるサブネットから、iDRAC に IP アドレスを割り当てることができます。
- 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 へのアクセスを制御するため接続されたサーバー管理者に限定する必要があります。
- Dell EMC では、256 ビットの暗号化強度と、TLS 1.2 以上の使用も推奨しています。
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。
- 番号付け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アカウントの管理。
- サードパーティログイン機能を使用した 2 要素認証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。
  - 番号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アカウントの管理。

メモ: セキュアな接続を確保するため、デルでは TLS 1.2 以上の使用をお勧めしています。

- 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 による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。

New features added

This section provides the list of new features added in the following releases:

- ファームウェア バージョン 4.20.20.20 on page 19
- ファームウェア バージョン 4.10.10.10 on page 20
- ファームウェア バージョン 4.00.00.00 on page 20

ファームウェア バージョン 4.20.20.20

本リリースで追加された機能は次のとおりです。

電源供給ユニット（PSU）

- 1100W～48W DC PSU をサポート。
- 4S PSU の制限を削除。

NIC

- (4x 10/25 SFP28) OCP 3.0 デル バーツ ナンバー JTK7F (Broadcom) のサポート。
- (4x10/25) MX Mezz、デル バーツ ナンバー DCWFP (Broadcom および MX 25G クワッド ポート (MX プラットフォーム上で) のサポート。
- R340 への Broadcom 10GbE NIC カードの追加のサポート。

アクセラレーターおよび CPU

- Precision 7920 ラック (Navi10DT/W5700、Navi14DT/W5500) での 2 つの新しい GPU カードのサポート。
PowerEdge での Nvidia V100S のサポート。
新しい Intel プロセッサー 6250 および 6256 のサポート。

NVMe
- Samsung PM 1735 および PM 1733 NVMe PCIe ストレージのサポート。

オートメーション/スクリプト作成/テレメトリー
- Redfish 2018R3、2019R1、および 2019R2 機能のサポート。
- POST コード取得 CLI メソッドのサポート。
- Power Manager プラグインにおけるテレメトリー CUPS のレポート期間制限の 1 分から 1 時間への増加をサポート。
- テレメトリーのサポート（メトリック レポートの有効化/無効化）。
- SSH を用いたユーザーログ強化のサポート。
- PCI Add IPMI コマンドへの階層指定フラグの追加をサポート。

ファームウェア バージョン 4.10.10.10
本リリースで追加された機能は次のとおりです。

デフォルトライセンスでのサポート機能
- BIOS のリカバリーや Root of Trust (RoT)

Enterprise ライセンスでのサポート機能
- Secure Enterprise Key Management (SEKM)：Vormetric Data Security Manager のサポートが追加されました。

Datacenter ライセンスでのサポート機能
- BIOS ライブ スキャン：AMD システムでのみ使用できます。

ファームウェア バージョン 4.00.00.00
本リリースには、以前のリリースのすべての機能が含まれています。本リリースで追加された新機能は次のとおりです。

メモ: 対応システムについて詳しくは、https://www.dell.com/support/article/sln308699 にある各バージョンのリリースノートを参照してください。

Datacenter ライセンスでのサポート機能
- テレメトリー ストリーミング：分析ツールにストリーミングされる指標レポート
- GPU インベントリーと監視
- 熱管理：電力および冷却の高度な機能
- 自動証明書登録および更新：SSL 証明書用
- 仮想クリップボード：リモート仮想コンソール デスクトップへのテキスト文字列の切り取りおよび貼り付けをサポート
- SFP トランシーバー：入力/出力の監視
- SMART ログ：ストレスドライプ
- システム シリアル データバッファーキャップチャ
アイドル サーバーの検出

Enterprise または Datacenter ライセンスでのサポート機能

- E メールによる多要素認証
- エージェントフリークラッシュビデオキャプチャ（Windows のみ）
- LLDP 転送の接続ビュー
- System Lockdown モード：任意のページから利用可能なヘッダーの新しいアイコン
- グループマネージャ：250 ノードのサポート
- Secure Enterprise Key Management（SEKM）サポートの拡張

デフォルトライセンスでのサポート機能（iDRAC Basic または iDRAC Express）

- GUI 拡張機能
  - ダッシュボードの [タスク サマリー] セクション
  - ヘッダーの [検索] ボックス
  - SupportAssist Collection ビューア：iDRAC GUI 出力を表示
- API、CLI、SCP
  - サーバー構成プロファイル（SCP）によるオペレーティング システムの導入
  - SCP および RACADM への起動順序制御を有効または無効にする機能
  - Redfish API の新しいスキーマ
  - SCP で起動ソースの状態を変更するオプション
  - RACADM でのコマンド/属性自動完了の自動化
- アラートと監視
  - SMTP 設定での E メール アラート用のカスタム送信者電子メール アドレス
  - SMTP でのクラウドベース E メール サーバー
  - ハード ドライブおよび PCIe SSD デバイスの SupportAssist ログ収集の SMART ログ
  - アラート メッセージに故障したコンポーネントのパラ テルを含む
- セキュリティ
  - RACADM コマンドのみを使用した複数の IP フィルタリング範囲
  - 最大長が 40 文字に拡張された iDRAC ユーザー パスワード
  - SCP 経由の SSH 公開キー
  - SSH ログイン用のカスタマイズ可能なセキュリティ パネル
  - ログインのための強制パスワード変更（FCP）
- ストレージおよびストレージコントローラー
  - PERC を有効にして SEKM 暗号化モードへの切り替え

本ガイドの使用方法

本ユーザーズガイドでは、以下を使用したさまざまなタスクの実行方法を説明します。

- iDRAC ウェブインタフェース：本書では、タスク関連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 コマンド：本書では、使用する必要のある 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、『iDRAC RACADM CLI ガイド』は、www.dell.com/idracmanuals にあります。を参照してください。
- iDRAC 設定ユーティリティ：本書では、タスク関連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の詳細については、『iDRAC 設定ユーティリティ』は、iDRAC オンラインヘルプを参照してください。
- Redfish — 本書では、タスク関連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の詳細については、「iDRAC Redfish API ガイド」は、www.dell.com/idracmanuals にあります。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。
対応バージョンのリストについては、『iDRAC リリースノート』は、www.dell.com/idracmanuals にあります。を参照してください。

サポートされる OS とハイパーパイザ

iDRAC は、ハイパーパイザの以下の OS でサポートされています。

- Microsoft Windows Server および Windows PE
- VMware ESXi
- Redhat Enterprise Linux
- SUSE Linux Enterprise Server

メモ：対応バージョンのリストについては、『iDRAC リリースノート』は、www.dell.com/idracmanuals にあります。を参照してください。

iDRAC ライセンス

iDRAC の機能は、ライセンスの種類に応じて利用可能になります。システムモデルによって異なりますが、iDRAC Basic または iDRAC Express ライセンスは、デフォルトでインストールされています。iDRAC Enterprise ライセンス、iDRAC Datacenter ライセンス、および iDRAC SEKM ライセンスは、アップグレードとして提供されており、いつでも購入できます。iDRAC を設定または使用できるインタフェースでは、ライセンス機能のみを使用できます。詳細については、「iDRAC のライセンス機能」を参照してください。

ライセンスのタイプ

iDRAC Basic または iDRAC Express は、システム上でデフォルトで使用できる標準ライセンスです。iDRAC の Enterprise ライセンスと Datacenter ライセンスには、ライセンス対象の機能がすべて含まれており、随時購入できます。Enterprise ライセンスには、次のタイプがあります。

- 30 日間評価 - 評価版ライセンスは期間ベースであり、システムの電源を入れるとタイマーが始動します。このライセンスは延長できません。
- 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。

次の表は、第 14 世代サーバで使用可能なデフォルトライセンスのリストです。

表 1. デフォルトライセンス

<table>
<thead>
<tr>
<th>iDRAC Express ライセンス</th>
<th>iDRAC Enterprise ライセンス</th>
<th>iDRAC Datacenter ライセンス</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerEdge C41XX</td>
<td>全プラットフォーム、アップグレードオプション付き</td>
<td>全プラットフォーム、アップグレードオプション付き</td>
</tr>
<tr>
<td>PowerEdge FC6XX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PowerEdge R6XX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PowerEdge R64XX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PowerEdge R7XX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PowerEdge R74XXd</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PowerEdge R74XX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PowerEdge R8XX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PowerEdge R9XX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PowerEdge T6XX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dell Precision Rack R7920</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

メモ：PowerEdge C64XX システムで使用できるデフォルトライセンスは Basic Plus です。Basic Plus ライセンスは、C64XX システム用にカスタマイズされました。

メモ：ブレード用 Express ライセンスは、PowerEdge M6XX および MXXXX システムのデフォルトのライセンスです。
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。

- Dell Digital Locker - Dell Digital Locker では、製品、ソフトウェア、ライセンス情報を1つの場所で表示して管理できます。Dell Digital Lockerへのリンクは DRAC Web インターフェイスにあります。【設定】＞【ライセンス】の順にアクセスしてください。

memo: Dell Digital Locker の詳細については、Web サイトの FAQ を参照してください。

- 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。
- 販売時 — システムの発注時にライセンスを取得します。

memo: ライセンスの管理、または新しいライセンスの購入を行うには、Dell Digital Locker に移動します。

Dell Digital Locker からライセンスキーを取得する
アカウントからライセンスキーを取得するには、注文確認 Eメールで送付される登録コードを使用して製品を登録する必要があります。このコードは、Dell Digital Locker にログインした後に、【製品登録】タブで入力する必要があります。

左ペインで、【製品】または【注文履歴】タブをクリックして、製品のリストを表示します。サブスクリプションベースの製品は、【請求先アカウント】タブに表示されます。

ライセンスキーを Dell Digital Locker アカウントからダウンロードするには、次の手順を実行します。
1. Dell Digital Locker アカウントにサインインします。
2. 左ペインで、【製品】をクリックします。
3. 表示する製品をクリックします。
4. 製品名をクリックします。
5. 【製品管理】ページで、【キーの取得】をクリックします。
6. 画面の指示に従って、ライセンスキーを取得します。

memo: Dell Digital Locker アカウントを持っていない場合は、購入時に提供された Eメールアドレスを使用してアカウントを作成します。

memo: 新規購入用に複数のライセンスキーを生成するには、【ツール】＞【ライセンスのアクティブ化】＞【非アクティブ化ライセンス】の下にある指示に従ってください。

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いてください。詳細についてはライセンスの取得方法を参照してください。

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

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

- 表示 — 現在のライセンス情報を表示します。
- インポート - ライセンスの取得後、ライセンスをローカルストレージに保存し、サポートされているいずれかのインタフェースを使用して 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。

memo: 工場出荷時にインストールされているライセンスをエクスポートすることはできませんが、インポートすることはできます。このライセンスをインポートするためには、Digital Locker から同等のライセンスをダウンロードするか、ライセンスの購入時に受信した Eメールから取得します。

memo: ライセンスをインポートしたら、iDRAC に再ログインする必要があります。これは、iDRAC ウェブインタフェースにのみ適用されます。

- エクスポート — インストールされているライセンスをエクスポートします。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。
- 削除 - ライセンスを削除します。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。
- 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。
詳細オプションで正しいページが表示されるようにするため、セキュリティ設定の信頼しているサイトのリストには*.dell.comを追加するようにしてください。詳細については、Internet Explorerのヘルプマニュアルを参照してください。

一対多のライセンス展開には、Dell License Managerを使用できます。詳細については、「Dell License Managerユーザーズガイド」は、www.dell.com/esmmanualsにあります。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、Configuration(設定)＞Licenses(ライセンス)の順に移動します。

Licensing(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、または削除の詳細については、「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。詳細については、以下を参照してください('iDRAC RACADM CLIガイド」は、www.dell.com/idracmanualsにあります。).

Licensed features in iDRAC9

The following table lists iDRAC9 features that are enabled based on the license purchased:

Table 2. Licensed features in iDRAC9

<table>
<thead>
<tr>
<th>Feature</th>
<th>iDRAC9 Basic</th>
<th>iDRAC9 Express</th>
<th>iDRAC9 Express for Blades</th>
<th>iDRAC9 Enterprise</th>
<th>iDRAC9 Datacenter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interfaces / Standards</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iDRAC RESTful API and Redfish</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IPMI 2.0</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DCMI 1.5</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Web-based GUI</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RACADM command line (local/remote)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SMASH-CLP (SSH-only)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Telnet</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SSH</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Serial Redirection</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>WSMAn</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Time Protocol</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Connectivity</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shared NIC (LOM)</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dedicated NIC</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>VLAN tagging</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IPv4</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IPv6</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DHCP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Feature</td>
<td>iDRAC9 Basic</td>
<td>iDRAC9 Express</td>
<td>iDRAC9 Express for Blades</td>
<td>iDRAC9 Enterprise</td>
<td>iDRAC9 Datacenter</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------</td>
<td>----------------</td>
<td>---------------------------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>DHCP with zero touch</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dynamic DNS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OS pass-through</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>iDRAC Direct - Front panel USB</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Connection View</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Connection View - LLDP transmit</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Role-based authority</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Local users</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SSL encryption</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Secure Enterprise Key Manager</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes (with SEKM license)</td>
<td>Yes (with SEKM license)</td>
</tr>
<tr>
<td>IP blocking</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Directory services (AD, LDAP)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Two-factor authentication (smart card)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Single sign-On</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PK authentication (for SSH)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FIPS 140-2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Secure UEFI boot - certificate management</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Lock down mode</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Unique iDRAC default password</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Customizable Security Policy Banner - login page</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Easy Multi Factor Authentication</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Auto Certificate Enrollment (SSL Certs)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>iDRAC Quick Sync 2 - optional auth for read operations</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>iDRAC Quick Sync 2 - add mobile device number to LCL</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>System Erase of internal storage devices</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Remote Presence**
Table 2. Licensed features in iDRAC9 (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>iDRAC9 Basic</th>
<th>iDRAC9 Express</th>
<th>iDRAC9 Express for Blades</th>
<th>iDRAC9 Enterprise</th>
<th>iDRAC9 Datacenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power control</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Boot control</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Serial-over-LAN</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual Media</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual Folders</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote File Share</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HTML5 access to Virtual Console</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual Console</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>VNC connection to OS</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Quality/bandwidth control</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual Console collaboration (up to six simultaneous users)</td>
<td>No</td>
<td>No</td>
<td>No (One user only)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual Console chat</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual Flash partitions</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>NOTE:</strong> vFlash is not available in iDRAC9 for PowerEdge Rx5xx/Cx5xx.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group Manager</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HTTP / HTTPS support along with NFS/CIFS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Power and Thermal**

<p>| Real-time power meter                       | Yes          | Yes            | Yes                       | Yes               | Yes               |
| Power thresholds and alerts                 | No           | Yes            | Yes                       | Yes               | Yes               |
| Real-time power graphing                    | No           | Yes            | Yes                       | Yes               | Yes               |
| Historical power counters                   | No           | Yes            | Yes                       | Yes               | Yes               |
| Power capping                               | No           | No             | No                        | Yes               | Yes               |
| Power Center integration                    | No           | No             | No                        | Yes               | Yes               |
| Temperature monitoring                      | Yes          | Yes            | Yes                       | Yes               | Yes               |
| Temperature graphing                        | No           | Yes            | Yes                       | Yes               | Yes               |
| PCIe airflow customization (LFM)            | No           | No             | No                        | No                | Yes               |
| Custom Exhaust Control                      | No           | No             | No                        | No                | Yes               |
| Custom Delta-T control                      | No           | No             | No                        | No                | Yes               |
| System Airflow Consumption                  | No           | No             | No                        | No                | Yes               |
| Custom PCIe inlet temperature               | No           | No             | No                        | No                | Yes               |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>iDRAC9 Basic</th>
<th>iDRAC9 Express</th>
<th>iDRAC9 Express for Blades</th>
<th>iDRAC9 Enterprise</th>
<th>iDRAC9 Datacenter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Health Monitoring</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full agent-free monitoring</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Predictive failure monitoring</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SNMPv1, v2, and v3 (traps and gets)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Email Alerting</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configurable thresholds</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Fan monitoring</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Power Supply monitoring</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Memory monitoring</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CPU monitoring</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RAID monitoring</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NIC monitoring</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HD monitoring (enclosure)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Out of Band Performance Monitoring</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Alerts for excessive SSD wear</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Customizable settings for exhaust temperature</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Serial Console Logs</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SMART logs for Storage Drives</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Idle server detection</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Telemetry Streaming</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Update</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote agent-free update</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Embedded update tools</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Update from repository (Auto-Update)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Schedule update from repository</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Improved PSU firmware updates</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Feature</td>
<td>IDRAC9 Basic</td>
<td>IDRAC9 Express</td>
<td>IDRAC9 Express for Blades</td>
<td>IDRAC9 Enterprise</td>
<td>IDRAC9 Datacenter</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------</td>
<td>----------------</td>
<td>--------------------------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td><strong>Deployment and Configuration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local configuration via F10</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Embedded OS deployment tools</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Embedded configuration tools</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Auto-Discovery</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote OS deployment</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Embedded driver pack</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Full configuration inventory</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Inventory export</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote configuration</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Zero-touch configuration</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>System Retire/Repurpose</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Server Configuration Profile in GUI</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Add BIOS configuration to IDRAC GUI</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Diagnostics, Service, and Logging</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Embedded diagnostic tools</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Part Replacement</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**NOTE:** After performing part replacement on RAID hardware, and the process is complete for replacing firmware and configuration, Lifecycle Logs reports double part replacement entries which is expected behavior.

<table>
<thead>
<tr>
<th>Feature</th>
<th>IDRAC9 Basic</th>
<th>IDRAC9 Express</th>
<th>IDRAC9 Express for Blades</th>
<th>IDRAC9 Enterprise</th>
<th>IDRAC9 Datacenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Configuration Backup</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Easy Restore (system configuration)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Server Configuration Restore</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Easy Restore Auto Timeout</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**NOTE:** Server Backup and Restore features are not available in iDRAC9 for PowerEdge R5xx/Cx5xx.

<table>
<thead>
<tr>
<th>Feature</th>
<th>IDRAC9 Basic</th>
<th>IDRAC9 Express</th>
<th>IDRAC9 Express for Blades</th>
<th>IDRAC9 Enterprise</th>
<th>IDRAC9 Datacenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>LED Health status indicators</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LCD screen (iDRAC9 requires optional)</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table 2. Licensed features in iDRAC9 (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>iDRAC9 Basic</th>
<th>iDRAC9 Express</th>
<th>iDRAC9 Express for Blades</th>
<th>iDRAC9 Enterprise</th>
<th>iDRAC9 Datacenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Sync (require NFC bezel, 13G only)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>iDRAC Quick Sync 2 (BLE/Wi-Fi hardware)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>iDRAC Direct (front USB management port)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>iDRAC Service Module (ISM) embedded</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ISM to in-band alert forwarding to consoles</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SupportAssist Collection (embedded)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Crash screen capture</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Crash video capture¹</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Agent Free Crash Video Capture (Windows only)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Boot capture</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manual reset for iDRAC (LCD ID button)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote reset for iDRAC (requires ISM)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual NMI</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OS watchdog</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>System Event Log</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Lifecycle Log</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Enhanced Logging in Lifecycle Controller Log</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Work notes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote Syslog</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>License management</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Improved Customer Experience**

<table>
<thead>
<tr>
<th>Feature</th>
<th>iDRAC9 Basic</th>
<th>iDRAC9 Express</th>
<th>iDRAC9 Enterprise</th>
<th>iDRAC9 Datacenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>iDRAC - Faster processor, more memory</td>
<td>N/A</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>GUI rendered in HTML5</td>
<td>N/A</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Add BIOS configuration to iDRAC GUI</td>
<td>N/A</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table 2. Licensed features in iDRAC9 (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>iDRAC9 Basic</th>
<th>iDRAC9 Express</th>
<th>iDRAC9 Express for Blades</th>
<th>iDRAC9 Enterprise</th>
<th>iDRAC9 Datacenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>iDRAC support for SW RAID licensing</td>
<td>N/A</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

[1] Requires iSM or OMSA agent on target server.

### 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

<table>
<thead>
<tr>
<th>インタフェースまたはプロトコル</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>iDRAC設定ユーティリティ（F2）</td>
<td>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。Lifecycle Controllerにアクセスするには、起動中にF10を押します。詳細に関しては、www.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。</td>
</tr>
<tr>
<td>Lifecycle Controller （F10）</td>
<td>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を押します。詳細に関しては、www.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。</td>
</tr>
<tr>
<td>iDRACウェブインタフェース</td>
<td>iDRACウェブインタフェースを使用して、iDRACを管理し、管理対象のシステムをモニタします。ブラウザは、HTTPSポートを介してウェブサーバに接続します。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ポートを介接した場合、HTTPSにリダイレクトされます。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、ウェブサーバのセキュリティを確保できます。デフォルトのHTTPおよびHTTPSポートは変更できます。ユーザーアクセスはユーザ権限に基づきます。</td>
</tr>
<tr>
<td>OpenManage Enterprise (OME) Modular Webインタフェース</td>
<td>メモ: このインタフェースは、MXプラットフォームの場合のみ利用できます。シャーシの監視と管理のほか、OME-Modular Web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詳細については、「PowerEdge MX7000シャーシ向けOME-Modularユーザーズガイド」は、www.dell.com/openmanagemanualsにあります。を参照してください。</td>
</tr>
<tr>
<td>CMC Webインタフェース</td>
<td>メモ: このインタフェースは、MXプラットフォームでは使用できません。シャーシの監視と管理のほか、CMC Web 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</td>
</tr>
</tbody>
</table>
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）

<table>
<thead>
<tr>
<th>インタフェースまたはプロトコル</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>• iDRAC ウェブインタフェースへのログイン</td>
<td></td>
</tr>
<tr>
<td>• 管理下システムの開始、停止、またはリセット</td>
<td></td>
</tr>
<tr>
<td>• BIOS、PERC、および対応ネットワークアダプタのアップデート</td>
<td></td>
</tr>
</tbody>
</table>

**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

プレードサーバーでは、LCD にシャーシの前面パネルにあり、すべてのプ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。

**メモ:** LCD パネルは、前面ベゼルをサポートするラックシステムまたはタワーシステムでのみ使用できます。プレードサーバーでは、LCD はシャーシの前面パネルにあり、すべてのプレード間で共有されています。

**RACADM**
このコマンドラインユーティリティを使用して、iDRAC およびサーバの管理を実行します。RACADMを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ている管理下システムで実行されます。ローカル RACADM は、帯域外 IPMI ホストインタフェースを介して iDRAC と通信します。このユーティリティはローカルの管理下システムで送信されています。これを実行するためには、ユーザーは完全な Administrator 権限を持っているか、root 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 ケーブルも使用します。"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 には、SSH または telnet を使用して iDRAC にログインすることでアクセスできます。iDRAC IP、ユーザー名、またはパスワードを指定期定にファームウェア RACADM コマンドを実行することができます。
- 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 プロントの起動後、racadm プリファックスを付けずに直接コマンドを実行することができます。

**iDRAC RESTful API および Redfish**
Redfish スケーラブルプラットフォーム管理 API は、Distributed Management Task Force (DMTF) によって定義された標準です。Redfish は、次世代のシステム管理インタフェース標準で、スケーラブルかつセキュアでオープンなサーバ管理を可能にします。これは、帯域外システム管理を実行するためにモデルフォーマットで定義されたデータに、RESTful インタフェースのセマンティックを用いてアクセスする新しいインタフェースです。スタンドアロンサーバからラックマウントサーバやプレードサーバといった広範囲のサーバ環境、および大規模クラウド環境に適しています。
Redfishには、既存のサーバの管理方法に比べて次の利点があります。
- 簡便性と利便性が向上
- 高いデータセキュリティ
- 容易にスクリプト作成できるプログラマブルインタフェース
- 広く使用されている標準に準拠
詳細については、「iDRAC Redfish API ガイド」は、www.dell.com/idracmanuals にあります。を参照してください。

**WSMan**
WSMan は、WSMan 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。
WSMan スーパーサービス機能を使用するには、WinRM クライアント (Windows) または OpenWSMan クライアント (Linux) などの WSMan クライアントを使用する必要があります。PowerShell または Python を使用して、WSMan インターフェイスに対してスクリプトを実行することもできます。
### iDRAC ポート情報

次の表に、ファイアウォール経由でiDRACにリモートでアクセスするために必要なポートを示します。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。ポートを変更するには、サービスの設定、p. 97を参照してください。

<table>
<thead>
<tr>
<th>ポート番号</th>
<th>タイプ</th>
<th>機能</th>
<th>設定可能なポート</th>
<th>最大暗号化レベル</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>SSH</td>
<td>はい</td>
<td>256 ビット SSL</td>
</tr>
</tbody>
</table>
表 4. iDRAC が接続についてリッスンするポート (続き)

<table>
<thead>
<tr>
<th>ポート番号</th>
<th>タイプ</th>
<th>機能</th>
<th>設定可能なポート</th>
<th>最大暗号化レベル</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>TCP</td>
<td>TELNET</td>
<td>はい</td>
<td>なし</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>HTTP</td>
<td>はい</td>
<td>なし</td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>SNMP エージェント</td>
<td>はい</td>
<td>なし</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
<td>はい</td>
<td>256 ビット SSL</td>
</tr>
<tr>
<td>623</td>
<td>UDP</td>
<td>RMCP/RMCP+</td>
<td>いいえ</td>
<td>128 ビット SSL</td>
</tr>
<tr>
<td>5000</td>
<td>TCP</td>
<td>iDRAC から iSM</td>
<td>いいえ</td>
<td>256 ビット SSL</td>
</tr>
</tbody>
</table>

注: iSM 3.4 以降と iDRAC ファームウェア 3.30.30.30 以降の両方がインストールされている場合、最大暗号化レベルは 256 ビット SSL です。

<table>
<thead>
<tr>
<th>ポート番号</th>
<th>タイプ</th>
<th>ポート番号</th>
<th>タイプ</th>
<th>機能</th>
<th>設定可能なポート</th>
<th>最大暗号化レベル</th>
</tr>
</thead>
<tbody>
<tr>
<td>5900</td>
<td>TCP</td>
<td>TELNET</td>
<td>はい</td>
<td>128 ビット SSL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5901</td>
<td>TCP</td>
<td>VNC</td>
<td>はい</td>
<td>128 ビット SSL</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

注: ポート 5901 は、VNC機能が有効になっている場合に開きます。

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

<table>
<thead>
<tr>
<th>ポート番号</th>
<th>タイプ</th>
<th>機能</th>
<th>設定可能なポート</th>
<th>最大暗号化レベル</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>TCP</td>
<td>SMTP</td>
<td>はい</td>
<td>なし</td>
</tr>
<tr>
<td>53</td>
<td>UDP</td>
<td>DNS</td>
<td>いいえ</td>
<td>なし</td>
</tr>
<tr>
<td>68</td>
<td>UDP</td>
<td>DHCP で割り当てた IP アドレス</td>
<td>いいえ</td>
<td>なし</td>
</tr>
<tr>
<td>69</td>
<td>TFTP</td>
<td>TFTP</td>
<td>いいえ</td>
<td>なし</td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td>ネットワークタイムプロトコル (NTP)</td>
<td>いいえ</td>
<td>なし</td>
</tr>
<tr>
<td>162</td>
<td>UDP</td>
<td>SNMP トラブル</td>
<td>はい</td>
<td>なし</td>
</tr>
<tr>
<td>445</td>
<td>TCP</td>
<td>共通インターネットファイルシステム (CIFS)</td>
<td>いいえ</td>
<td>なし</td>
</tr>
<tr>
<td>636</td>
<td>TCP</td>
<td>LDAP Over SSL (LDAPS)</td>
<td>いいえ</td>
<td>256 ビット SSL</td>
</tr>
<tr>
<td>2049</td>
<td>TCP</td>
<td>ネットワークファイルシステム (NFS)</td>
<td>いいえ</td>
<td>なし</td>
</tr>
<tr>
<td>3269</td>
<td>TCP</td>
<td>グローバルカタログ (GC) 用 LDAPS</td>
<td>いいえ</td>
<td>256 ビット SSL</td>
</tr>
<tr>
<td>5353</td>
<td>UDP</td>
<td>mDNS</td>
<td>いいえ</td>
<td>なし</td>
</tr>
</tbody>
</table>

注: 開始ノード検出かグループマネージャーが有効になっていれば、iDRAC は mDNS を使用してポート 5353 経由で通信します。両方とも無効になっていると、ポート 5353 は iDRAC の内部ファイアウォールによってブロックされ、ポートスキャンでは開いているまたはフィルタリングされたポートとして表示されます。

<table>
<thead>
<tr>
<th>ポート番号</th>
<th>タイプ</th>
<th>機能</th>
<th>設定可能なポート</th>
<th>最大暗号化レベル</th>
</tr>
</thead>
<tbody>
<tr>
<td>514</td>
<td>UDP</td>
<td>リモート Syslog</td>
<td>はい</td>
<td>なし</td>
</tr>
</tbody>
</table>

その他の必要マニュアル

一部の iDRAC インタフェースには、オンラインヘルプドキュメントが組み込まれており、ヘルプ (?) アイコンをクリックするとアクセスできます。オンラインヘルプには、ウェブインタフェースで使用できるフィールドの詳細情報やウェブインタフェースの説明が記載されています。さらに、デルサポートウェブサイト (dell.com/support) から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 Redfish API ガイドには Redfish API に関する説明があります。
- iDRAC RACADM CLI ガイドは RACADM サブコマンド、サポート対象インタフェース、iDRAC プロパティデータベースグループ、オブジェクト定義に関する情報があります。
- Systems Management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さまざまなソフトウェアについての簡単な説明があります。
- 「Dell Remote Access 設定ツールユーティリティ」は、ツールを使用してネットワーク内の iDRAC 機能を検出し、1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の説明があります。
- 「Dell システム経済性サポートマニュアル」は、各 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。
- 「Dell サービスモジュールユーティリティ」は、iDRAC サービスモジュールをインストールする方法の情報が記載されています。
- 「Dell OpenManage Server Administrator イントールガイド」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 イントールガイド」では、Dell OpenManage Management Station Software（ペースボード管理ユーティリティ、iDRAC ソール、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」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情報を提供します。

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、別途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。
- スタートガイドには、システム機能、システムのセットアップ、技術仕様の概要が記載されています。
- 設置およびサービスマニュアルでは、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、システムコンポーネントのインストールやリプレースメントの方法について説明しています。

デルへのお問い合わせ

この製品へのお問い合わせをご希望の際は、次のいずれかの方法で行います。
- デルサポートサイトからの文書へのアクセス

必要なドキュメントにアクセスするには、次のいずれかの方法で行います。
- 次のリンクを使用します。
  - すべてのエンドユーザーのシステム管理および OpenManage Connections のドキュメント - www.dell.com/esmmanuals
  - OpenManage のマニュアル - www.dell.com/openmanagemanuals
  - IDRAC および Lifecycle Controller のマニュアル - www.dell.com/idracmanuals
  - Serviceability Tools のドキュメント - https://www.dell.com/serviceabilitytools
  - Client Command Suite システム管理のドキュメント - www.dell.com/omconnectionsclient

製品検索を使用したマニュアルへのアクセス

1. https://www.dell.com/support にアクセスします。
2. サービスタグ、シリアル番号を入力...検索ボックスに製品名を入力します。たとえば、「PowerEdge」または「iDRAC」などで検索します。
3. 一致した製品のリストが表示されます。
4. 目標の製品を選択し、検索アイコンをクリックするか、Enter を押します。
5. DOCUMENTATION をクリックします。
5. マニュアルおよび文書をクリックします。

製品セレクタを使用したマニュアルへのアクセス

お使いの製品を選択してドキュメントにアクセスすることもできます。

1. https://www.dell.com/support にアクセスします。
2. すべての製品を参照 をクリックします。
3. サーバ、ソフトウェア、ストレージなど、目的の製品カテゴリをクリックします。
4. 目的の製品をクリックし、必要に応じて対象のバージョンをクリックします。
   ☢ メモ: 一部の製品では、さらにサブカテゴリを選択していく必要があります。
5. DOCUMENTATION をクリックします。
6. マニュアルおよび文書をクリックします。
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LDAP（Lightweight Directory Access Protocol）ユーザーとしてログインできます。また、OpenID接続と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。

セキュリティ強化のため、各システムにはiDRAC固有のパスワードが付属しています。これはシステム情報タグに記載されています。デフォルトのユーザー名はrootです。

システムを注文する際に、以前のパスワード「calvin」をデフォルトのパスワードとして保持することができます。以前のパスワードを保持する場合は、システム情報タグのパスワードを使用できません。

このバージョンでは、DHCPはデフォルトで有効になっており、iDRACのIPアドレスが動的に割り当てられます。

メモ:
• iDRACへのログインするには、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: ユーザー名とパスワードで推奨される文字の詳細については、「ユーザーレ名およびパスワードで推奨される文字」、p. 145を参照してください。

OpenID接続

Dell EMC OpenManage Enterprise（OME）- Modularなどの他のWebコンソールの認証情報を使用して、iDRACにログインできます。この機能を有効にすると、コンソールがiDRACのユーザー権限の管理を開始します。iDRACは、ユーザーセッションにコンソールで指定されているすべての権限を提供します。

メモ: ロックダウンモードが有効になっている場合、OpenID ConnectログインオプションはiDRACログインページには表示されません。

iDRACにログインせずに、詳細なヘルプにアクセスできます。iDRACログインページのリンクを使用して、ヘルプとバージョン情報、ドライバとダウンロード、マニュアルとTechCenterにアクセスします。

トピック:

• パスワードの強制変更（FCP）
• OpenID Connectを使用したiDRACへのログイン
• ローカルユーザー、Active Directoryユーザー、またはLDAPユーザーとしてのiDRACへのログイン
• マルチ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
• シンプルな2要素認証（シンプル2FA）
• システム正常性の表示
• 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
パスワードの強制変更（FCP）

[パスワードの強制変更] は、デバイスの工場出荷時のデフォルトパスワードを変更するように要求する機能です。この機能は、工場出荷時の設定の一部として有効することができます。

FCP 画面はユーザー認証が成功した後に表示されます。スキップすることはできません。ユーザーがパスワードを入力した後にのみ、通常のアクセスと操作が許可されます。この属性の状態は、設定のデフォルトへのリセット操作の影響を受けません。

メモ: FCP 属性を設定またはリセットするには、ログイン権限とユーザー設定権限が必要です。

メモ: FCP が有効になっている場合、デフォルトユーザーパスワードを変更すると[デフォルトパスワード警告]設定が無効になります。

メモ: root ユーザーが公開キー認証（PKA）によりログインするときは、FCP はスキップされます。

FCP が有効になっている場合、以下の操作は許可されません。

• CLI とでデフォルトのユーザー資格情報を使用するIPMIpover-LANインターフェイスを除いた、任意のUIでiDRACにログインする。
• Quick Sync-2 を使用してOMMアプリからiDRACにログインする。
• グループマネージャでメンバーiDRACを追加する。

OpenID Connect を使用した iDRAC へのログイン

メモ: この機能は MX プラットフォームでのみ使用できます。

OpenID Connect 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. 対応ウェブブラウザで、https://[iDRAC-IP-address]と入力し、Enterを押します。
   サービスページが表示されます。
2. 次を使用してログイン: メニューでOME Modularを選択します。
   コンソールログインページが表示されます。
3. コンソールのユーザー名とパスワードを入力します。
4. ログインをクリックします。
   コンソールユーザー権限でiDRACにログインされます。
   ロックダウンモードが有効になっている場合、OpenID ConnectログインオプションはiDRACログインページには表示されません。

ローカルユーザー、Active Directoryユーザー、または LDAPユーザーとしての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、必要な権限が付与されたユーザーアカウントが作成されているようにしてください。

メモ: Active Directoryユーザーの場合、ユーザー名では大文字と小文字は区別されません。パスワードはどのユーザーも数、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。

iDRACへのログイン 37
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. **Address (アドレス) フィールドにhttps://[iDRAC-IP-address]と入力して、<Enter>を押します。**

   **memo:** デフォルトのHTTPSポート番号（ポート443）が変更された場合は、https://[iDRAC-IP-address]:[port-number]と入力します。ここで、[iDRAC-IP-address]はiDRACのIPv4またはIPv6アドレス、[port-number]はHTTPSのポート番号です。

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、User name（ユーザー名）とPassword（パスワード）フィールドに、Active Directoryのユーザー名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This iDRAC（このiDRAC）を選択します。ユーザー名の形式は、ドメイン名><ユーザー名>、または<ユーザー名>@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、Username（ユーザー名）フィールドとPassword（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This iDRAC（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。

---

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、次の手順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。
- ユーザーの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インページを表示します。

**memo:** 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。

   **memo:** デフォルトのHTTPSポート番号（ポート443）が変更された場合は、https://[IP address]:[port-number]と入力します。ここで、[IP address]はiDRACのIPv4アドレス、[port-number]はHTTPSのポート番号です。

2. スマートカードをリーダーに挿入してLogin（ログイン）をクリックします。

   スマートカードのPINのプロンプトが表示されます。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。

   **memo:** Enable CRL check for Smart Card Logon（スマートカードログオンのCRLチェックを有効にする）が有効になっているローカルユーザーの場合は、iDRACは証明書失効リスト（CRL）のダウンロードを試行し、ユーザーの証明書の
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、次の手順を実行しておく必要があります。

1. 信頼済み認証局 (CA) 証明書 (CA 規定付き Active Directory 証明書) を iDRAC にアップロードします。
2. DNS サーバーを設定します。
3. Active Directory ログインを有効にします。
4. 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ことは、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。
   - スマートカードの PIN のプロンプトが示されます。
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。

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。

iDRAC ウェブインタフェースを使用した iDRAC SSO 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. Web ブラウザに、https://[FQDN address] と入力します。
   - 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://[FQDN address]:[port number] と入力します。ここで、[FQDN address] は iDRAC FQDN (iDRACdnsname.domain.name)、[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

| メモ: この機能は MX プラットフォームでは使用できません。 |

SSO 機能を使用すると、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 を起動するための CMC ユーザー権限があります。CMC に表示されるユーザーアカウントが iDRAC には表示されない場合でも、ユーザーは CMC から iDRAC を起動することができます。

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アクセスになります。

詳細については、「Chassis Management Controller ユーザーズ マニュアル」は、www.dell.com/cmcmanual にあります。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。

詳細については、「iDRAC RACADM CLI ユーザーズ マニュアル」は、www.dell.com/idracmanuals にあります。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、iDRAC がセキュアセッションを確立するために 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、または自己署名されます。どちらの場合でも、管理ステーションが CA または署名機関を認識しない場合、警告が表示されます。 |

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 [yourdownloadedformatcert.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、RHEL 5.6 ビットの場合は /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 にアクセスする方法については、「iDRAC RACADM CLI マニュアル」は、www.dell.com/idracmanuals にあります。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。詳細については、「iDRAC RACADM CLI マニュアル」は、www.dell.com/idracmanuals にあります。を参照してください。
シンプルな2要素認証 (シンプル2FA)

iDRACには、ログイン時のローカルユーザーのセキュリティを強化する、シンプルな2要素認証オプションが用意されています。前回のログイン時とは異なるソースIPアドレスからログインした場合、2番目の要素認証の詳細を入力するように求められます。シンプルな2要素認証は、次の2つの認証ステップで構成されています。

- iDRACのユーザー名とパスワード
- ユーザーにEメール送信されるシンプルな6桁のコード。この6桁のコードは、ログイン時のプロンプト表示に対して入力する必要があります。

MEMO:
- 6桁のコードを受信するには、「カスタム送信者アドレス」を設定する必要があり、SMTPを正しく設定する必要があります。
- 2FAコードは10分間で期限切れになりますが、その前でも使用した段階で無効になります。
- グループ管理者によりアカウントのiDRACへのログイン権限が追加されます。

メモ：iDRACからのRACADM、Redfish、WSMAN、IPMI LAN、CSVリリース、CLIなどは、iDRAC GUI、SSH、Telnetなどのサポートされているインターフェイスからのログインに成功した後でのみ機能します。

システム正常性の表示

タスクを実行またはイベントをトリガーする前に、RACADMを使用してシステムが適切な状態であるかどうかをチェックできます。RACADMからリモートサービスステータスを表示するには、getremoteservicesstatusコマンドを使用します。

表6. システムステータスに可能な値

<table>
<thead>
<tr>
<th>ホストシステム</th>
<th>Lifecycle Controller (LC)</th>
<th>リアルタイムステータス</th>
<th>全般的ステータス</th>
</tr>
</thead>
<tbody>
<tr>
<td>電源オフ</td>
<td>準備完了</td>
<td>準備完了</td>
<td>準備完了</td>
</tr>
<tr>
<td>POST中</td>
<td>初期化されていない</td>
<td>準備できていない</td>
<td>準備できていない</td>
</tr>
<tr>
<td>POST完了</td>
<td>データのリロード中</td>
<td>リカバリ中</td>
<td></td>
</tr>
<tr>
<td>システムインベントリの収集</td>
<td>無効</td>
<td>使用中</td>
<td></td>
</tr>
<tr>
<td>自動タスク実行</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lifecycle Controller Unified Server Configurator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>POSTエラーのため、サーバがF1/F2エラーメッセージがブロントで停止した</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>起動可能なデバイスがないため、サーバがF1/F2/F11ブロントで停止した</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>サーバがF2セットアップメニューに移行した</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>サーバがF11ブートマネージャメニューに移行した</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. 読み取り/書き込み：読み取り専用
2. ユーザー権限：ログインユーザー
3. 必要なライセンス：iDRAC ExpressまたはiDRAC Enterprise
4. 依存関係：なし
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 にログインすることができます。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することもできます。コマンドが完了してからセッションが終了するため、コマンドラインオプションはリモート RACADM と同様に動作します。

例えば次のようにします。

**ログイン：**

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

または

```plaintext
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：**

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

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

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 iDRAC セッション数を示します。

<table>
<thead>
<tr>
<th>インタフェース</th>
<th>セッション数</th>
</tr>
</thead>
<tbody>
<tr>
<td>iDRAC ウェブインタフェース</td>
<td>8</td>
</tr>
<tr>
<td>リモート RACADM</td>
<td>4</td>
</tr>
<tr>
<td>ファームウェア RACADM/SMCLP</td>
<td>SSH - 4</td>
</tr>
<tr>
<td></td>
<td>Telnet - 2</td>
</tr>
<tr>
<td></td>
<td>シリアル - 1</td>
</tr>
</tbody>
</table>

セキュアなデフォルトパスワード

システムの発注時に設定パスワードに `calvin` を選択しない限り、すべてのサポート対象システムは、iDRAC に固有なデフォルトパスワードを設定して出荷されます。固有のパスワードは、iDRAC とサーバのセキュリティ強化に有効です。セキュリティをさらに強化するには、デフォルトパスワードを変更することをお勧めします。

システム固有のパスワードは、システム情報タグで確認できます。タグの場所については、https://www.dell.com/support にあるサーバのドキュメントを参照してください。

**メモ：** PowerEdge C6420、M640、FC640 の場合、デフォルトパスワードは `calvin` です。

**メモ：** iDRAC を出荷時のデフォルト設定にリセットすると、デフォルトパスワードはサーバ出荷時のパスワードに戻ります。

パスワードを忘れてシステム情報タグにアクセスできない場合は、ローカルまたはリモートでパスワードをリセットする方法がいくつかあります。

**デフォルトの iDRAC パスワードのローカルでのリセット**

システムに物理的にアクセスできる場合は、次の方法でパスワードをリセットできます。
iDRAC 設定ユーティリティを使用したデフォルトパスワードのリセット

サーバのセットアップユーティリティを使用してiDRAC設定ユーティリティにアクセスできます。iDRACを使用してすべての機能をデフォルトにリセットする場合、iDRACのログイン資格情報もデフォルトにリセットできます。

警告: iDRACをすべてデフォルトにリセットすると、iDRACは出荷時のデフォルトにリセットされます。

iDRAC設定ユーティリティを使用してiDRACをリセットするには、次の手順を実行します。
1. サーバを再起動し、<F2>を押します。
2. セットアップユーティリティページでiDRAC設定をクリックします。
3. iDRAC設定をすべてデフォルトにリセットをクリックします。
4. はいをクリックして確認し、次に戻るをクリックします。
5. 終了をクリックします。

すべてのiDRAC設定がデフォルトに設定されると、サーバが再起動されます。

ローカル RACADM を使用したデフォルトパスワードのリセット

1. システムにインストールされているホストOSにログインします。
2. ローカル RACADM インタフェースにアクセスします。
3. 「RACADMを使用したデフォルトログインパスワードの変更、p.44」の手順に従ってください。

OpenManage Mobile を使用したデフォルトパスワードのリセット

OpenManage Mobile（OMM）を使用してログインし、デフォルトのパスワードを変更できます。OMMを使用してiDRACにログインするには、システム情報タグのQRコードをスキャンします。OMMの使用に関する詳細については、「PowerEdge MX7000シャーシ向けOME-Modularユーザーズガイド」は、www.dell.com/openmanagemanualsにあります。でOMMのドキュメントを参照してください。

Memo: QRコードをスキャンした場合、デフォルトの資格情報がデフォルト値である場合に限り、iDRACにログインできます。値をデフォルト値から変更した場合は、アップデートされた資格情報を入力してください。

サーバ管理のUSBポートを使用したデフォルトパスワードのリセット

Memo: これらの手順の前に、USB管理ボートの有効化と設定が済んでいる必要があります。

サーバ設定プロファイルファイルの使用

デフォルトアカウントの新しいパスワードを使用してサーバ設定プロファイル(SCP)ファイルを作成し、それをメモリキュー上に置き、サーバ上のサーバ管理USBポートを使用してSCPファイルをアップロードします。ファイル作成の詳細については、「サーバー管理USBポートの使用、p.294」を参照してください。

ラップトップを使用したiDRACへのアクセス

ラップトップをサーバ管理のUSBポートに接続し、iDRACにアクセスしてパスワードを変更します。詳細については、「直接USB接続を介したiDRACインタフェースへのアクセス、p.294」を参照してください。

USB-NICを使用したデフォルトパスワードの変更

キーボード、マウス、およびディスプレイデバイスにアクセスできる場合は、USB-NICを使用してサーバに接続し、iDRACインタフェースにアクセスしてデフォルトのパスワードを変更します。
1. デバイスをシステムに接続します。
2. サポートされているブラウザを使用して、iDRACIPを使用してiDRACインタフェースにアクセスします。
3. 「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、p.44」の手順に従ってください。
デフォルトの iDRAC パスワードのリモートでのリセット

システムに物理的にアクセスできない場合は、デフォルトのパスワードをリモートでリセットすることができます。

リモート - プロビジョニングされたシステム

オペレーティングシステムがシステムにインストールされている場合は、リモートデスクトップクライアントを使用してサーバにログインします。サーバにログインしたら、RACADM やウェブインタフェースなどのローカルインタフェースを使用してパスワードを変更します。

リモート - プロビジョニングされていないシステム

サーバにオペレーティングシステムがインストールされておらず、PXE セットアップが使用可能な場合は、PXE を使用してから RACADM を使用してパスワードをリセットします。

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。
- デフォルトの iDRAC ユーザーレコードにパスワードがシステム情報タグに記載されている。

警告メッセージは、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にも表示されます。ウェブインタフェース、SSH、および Telnet の場合は、セッションごとに単一の警告メッセージが表示されます。リモート RACADM の場合は、コマンドごとに警告メッセージが表示されます。

メモ: ユーザーレコードおよびパスワードの推奨文字に関する詳細は、「ユーザーレコードおよびパスワードで推奨される文字、p.145」を参照してください。

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、Default Password Warning (デフォルトパスワード警告) ページが表示された場合、パスワードを変更できます。この操作を行うには、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: ユーザーレコードおよびパスワードの推奨文字に関する詳細は、「ユーザーレコードおよびパスワードで推奨される文字、p.145」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. Continue (続行) をクリックします。

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。

```bash
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> は新しいユーザーディロ義パスワードです。

メモ: デフォルトアカウントの索引は 2 です。
詳細については、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。 を参照してください。

1. メモ: ユーザー名とパスワードに推奨される文字の詳細については、「ユーザー名およびパスワードで推奨される文字、 p. 145」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. 145」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。

Password Strength Policy

Using iDRAC interface, you can check the password strength policy and check any errors if the policy is not met. The password policy cannot be applied to previously saved passwords, Server Configuration Profiles (SCP) copied from other servers, and embedded passwords in the profile.

To access Password settings, go to iDRAC Settings > Users > Password Settings.

Following fields are available in this section:

- **Minimum Score** — Specifies the minimum password strength policy score. The values in this field are:
  - 0 — Password is accepted
  - 1 — Upper case letter is not provided
  - 3 — Number is not provided
  - 7 — Symbol is not provided
  - 15 — Minimum length is not met
  - 31 — Minimum score is not met
  - 63 — Regular Expression is not matched
  - 255 — Internal error / Timeout

- **Simple Policy** — Specifies the required characters in a secure password. It has the following options:
  - Upper Case Letters
  - Numbers
  - Symbols
  - Minimum Length

- **Regular Expression** — The Regular expression along with the Minimum score is used for password enforcement. The values are 1-4.

iDRACへのログイン

IP ブロック

IP ブロックを用いると、特定の IP アドレスからのログインの失敗が過剰に発生していないかを動的に判断し、事前に選択されたタイムスパンの間、そのアドレスが iDRAC9 にログインするのをブロックまたは防止することができます。IP ブロックは以下の要件で構築されます。
ログイン失敗の許容回数。
・ 一連の失敗と見なすのに必要な時間枠（秒単位）。
・ 失敗の合計数が許容回数を超過した後に、対象のIPアドレスによるセッション確立を防止させる時間（秒単位）。
特定のIPアドレスからのログインが何度か連続して失敗し続けている場合、その回数は内部カウンターによって追跡されます。正常にログインできた場合、障害履歴はクリアされ、内部カウンター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連続して拒否されること、一部のSSHクライアントでは、次のようないく
メッセージが表示されることがあります

ssh exchange identification: Connection closed by remote host

メモ: IPブロック機能は、最大5つのIP範囲をサポートします。これらの表示と設定はRACADMを介してのみ行えます。

表8. ログイン再試行の制限プロパティ

<table>
<thead>
<tr>
<th>プロパティ</th>
<th>定義</th>
</tr>
</thead>
<tbody>
<tr>
<td>iDRAC.IPBlocking.BlockEnable</td>
<td>IPブロック機能を有効にします。連続した失敗が</td>
</tr>
<tr>
<td></td>
<td>iDRAC.IPBlocking.FailCount</td>
</tr>
<tr>
<td></td>
<td>単一のIPアドレスから特定の時間内に発生している場合</td>
</tr>
<tr>
<td></td>
<td>iDRAC.IPBlocking.FailWindow</td>
</tr>
<tr>
<td></td>
<td>当該アドレスからのセッション確立の試行は特定の期間中すべて拒否されます</td>
</tr>
<tr>
<td></td>
<td>iDRAC.IPBlocking.PenaltyTime</td>
</tr>
<tr>
<td></td>
<td>過剰に失敗したIPアドレスに対し、そのログイン試行をすべて拒否させるタイムスパン（秒単位）の指定。</td>
</tr>
</tbody>
</table>

Web インターフェイスを使用したOS to iDRACパススルーの有効化または無効化

Webインタフェイスを使用して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. [iDRAC設定] > [接続] > [ネットワーク] > [OSからiDRACへのパススルー]に移動します。
2. 状態を有効に変更します。
3. パススルーモードには、次のいずれかのオプションを選択します。
   - 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。
   1メモ: パススルーモードをLOMに設定した場合は、次のことを確認します。
   - OSとiDRACが同じサブネット上にある
   - ネットワーク設定でNICの選択がLOMに設定されている
4. 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。
メモ：VLAN が iDRAC で有効になっている場合は、LOM パススルーは VLAN タグ機能がホストで設定されている共有 LOM モードでのみ機能します。

メモ：
・ LOM がパススルー モードに設定されていると、コールド プート後にホスト OS から iDRAC を起動することはできません。
・ 専用モード機能で、意図的に LOM パススルーを削除してあります。

5. パススルー設定として USB NIC を選択した場合は、USB NIC の IP アドレスを入力します。
デフォルト値は 169.254.1.1 です。デフォルトの IP アドレスを使用することをお勧めします。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。
IP 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 ケーブル使用時前面パネルの USB NIC ポート用に予約されています。
メモ：IPv6 が望ましい場合、デフォルトのアドレスは fde1:53ba:e9a0:de11::1です。このアドレスは、必要に応じて idrac.OS-BMC.UsbNicULA 設定で変更できます。IPv6 を USB-NIC で使用したくない場合は、アドレスを「::」に変更することで無効化できます。

6. 適用 をクリックします。

7. 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。

```bash
racadm set iDRAC.IPMIIFan.AlertEnable <n>
```

n=0 — 無効
n=1 — 有効
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 の詳細については、『OpenManage Server Administrator コーダーズガイド』は、www.dell.com/openmanagemanuals にあります。を参照してください。

トピック:
- iDRAC IP アドレスのセットアップ
- ローカール管理者アカウント設定の変更
- 管理下システムの場所のセットアップ
- システムパフォーマンスと電力消費の最適化
- 管理ステーションのセットアップ
- 対応ウェブブラウザの設定
- デバイスファームウェアのアップデート
- 宇宙管理されたアップデートの表示と管理
- デバイスファームウェアのロールバック
- その他のシステム管理ツールを使用した iDRAC の監視
- サーバ設定プロファイルのサポート - インポーとエクスポート
- BIOS 設定または F2 からのセキュアなプート設定
- サーバ設定プロファイルのサポート - インポートおよびエクスポート
- システム管理ドキュメントおよびツールDVD または https://www.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

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ためには、お使いのネットワークインフラストラッ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。IP アドレスを設定するには、次のいずれかのインタフェースを使用します。

- iDRAC 機設ユーティリティ
- Lifecycle Controller（Lifecycle Controller ユーザーズガイドを参照）
- Dell Deployment Toolkit（Dell OpenManage Deployment Toolkit コーダーズガイドを参照）

メモ：ブレード サーバーの場合、CMC の初期設定中のみ、シャーシの LCD パネルを使用してネットワーク設定を構成できます。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 Web インターフェイス（MX プラットフォームには非該当）（Chassis Management Controller コーダーズガイドを参照）
- 収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 のネ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。

- デフォルトのユーザー名とパスワードを変更するようにしてください。
- 次のいずれかのインタフェースで 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
  - SSH サーバー（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、クライアントは必要ありません。）
  - 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（『システム管理ドキュメントおよびツール』DVD または https://www.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）
**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。

**ネットワークの設定**

ネットワーク設定を行うには、次の手順を実行します。

1. NIC の有効化 で、有効 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ー (RAC) 上で利用可能な専用ネットワークインタフェイスを使用できるようにします。このインターフェイスは、ホストオペレーティングシステムと共有されず、管理トラフィックを個別の物理ネットワークにルーティングするために、アプリケーショントラフィックの分離が可能になります。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の LOM または NIC ポートとは個別にルーティングします。専用オプションを使用すると、iDRAC で、ネットワークトラフィックを管理するためにホスト LOM または NIC に割り当てられている IP アドレスと比較して、同じサブネットまたは別のサブネットから IP アドレスを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
3. NIC の選択 ドロップダウンメニューから、システムにリモートでアクセスするポートを選択します。オプションは次のとおりです。
   - メモ: これらの機能は、MX プラットフォームでは使用できません。
メモ: 専用のネットワークインタフェースカードまたはクアッドポートまたはデュアルポートのメザニカードで使用可能なLOMのリストから選択できます。

- シャーシ（専用）:このオプションにより、セキュアアクセスデバイスはセキュアアクセスコントロール (RAC) 上の専用ネットワークインタフェースを使用できます。このインタフェースは、ホストオペレーティングシステムと共有されず、管理トラフィックを個別の物理ネットワークにルーティングするため、アプリケーションのトライフィックの分離が可能になります。

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のLOMまたはNICポートとは個別にルーティングされます。専用オプションを使用すると、iDRACでネットワークトラフィックを管理するためにホストLOMまたはNICに割り当てられているIPアドレスと比較して、同じサブネットまたは別のサブネットからIPアドレスを割り当てることができます。

- クアッドポートカードの場合 - LOM1~LOM16
- デュアルポートカードの場合 - LOM1、LOM2、LOM5、LOM6、LOM9、LOM10、LOM13、LOM14

4. [フェー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1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: このオプションは、[NICの選択]が[専用]に設定されている場合は、無効になります。

メモ: フェールオーバーネットワーク設定を使用する場合は、すべてのLOMポートを同じネットワークに接続することが推奨されます。

5. 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。有効になると、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1000Mbpsに設定します。

6. ネットワーク速度で、10Mbpsまたは100Mbps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1000Mbps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。

7. 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]が[有効]に設定されている場合、このオプションは無効になります。

メモ: ネットワークトライフィックが同じネットワークアダプタをNICの選択として使用してホストOSで設定されている場合は、次にフェールオーバーネットワークも設定する必要があります。NICの選択とフェールオーバーネットワークでは、ネットワークトライフィックの一部として設定されているポートを使用する必要があります。3つ以上のポートがネットワークトライフィックの一部として使用されている場合、フェールオーバーネットワークの選択は「すべて」である必要があります。

8. [NICMTU]で、NICの最大転送単位を入力します。

メモ: NICでのMTUのデフォルトおよび最大値は1500に制限されており、最小値は576です。IPv6が有効になっている場合、1280以上のMTU値が必要です。

### 共通設定
ネットワークインフラストラクチャにDNSサーバが存在する場合は、DNSにiDRACを登録します。これは、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を有効にするための初期設定要求です。

iDRACを登録するには、次の手順を実行します。

1. DNSにiDRACを登録する
2. DNS DRAC名を入力します。
3. Auto Config Domain Name（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 Domain Name（DNSドメイン名）を入力します。

### IPV4の設定
IPV4の設定を行うには、次の手順を実行します。
IPv6設定の構成

1. Enable IPv4 (IPv4 の有効化) で、Enabled (有効) オプションを選択します。
   - メモ: 第14世代のPowerEdgeサーバでは、DHCPがデフォルトで有効です。

2. Enable DHCP (DHCP の有効化) で、Enabled (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なります。または、Disabled (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、Use DHCP to obtain DNS server address (DHCPを使用してDNSサーバアドレスを取得する) を有効にし、DHCPがStatic Preferred DNS Server (静的優先DNSサーバ) およびStatic Alternate DNS Server (静的代替DNSサーバ) を割り当てることができるようになります。または、Static Preferred DNS Server (静的優先DNSサーバ) およびStatic Alternate DNS Server (静的代替DNSサーバ) のIPアドレスを入力します。

IPv6設定の構成

IPv6アドレスプロトコルを、インフラストラクチャセットアップに基づいて使用することができます。

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、およびサブネットマスクを割り当てるようにするには、自動設定の有効で有効オプションを選択します。
   - メモ: 固定IPおよびDHCPIPの両方を同時に設定することができます。
3. [固定IPアドレス]ボックスに、固定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: 固定IPを構成する場合、現在のIPアドレス1には固定IPが表示され、IPアドレス2には動的IPが表示されません。固定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サーバーのアドレスを取得します。必要に応じて、次の設定を行えます。
   - 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。

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の値数を入力して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

Chassis Management Controller（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。CMCオプションは、ブレードサーバにしか適用できません。

1. CMCウェブインタフェースにログインします。
2. iDRAC設定設定CMCの順に移動します。
   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ーを要件に従って選択します。詳細については、CMCオンラインヘルプを参照してください。
4. 各ブレードサーバ固有の追加のネットワーク設定には、サーバの概要>サーバ名>と移動します。
   サーバ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、iDRAC設定接続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
   - 詳細ネットワーク設定

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。
   詳細については、「Chassis Management Controllerユーザーズガイド」は、www.dell.com/cmcmanualにあります。を参照してください。

自動検出

自動検出機能を使用すると、新しくインストールされたサーバーによって、プロビジョニングサーバーをホストするリモート管理コンソールが自動的に検出されます。プロビジョニングサーバーは、カスタム管理ユーザーアカウントを持つシステム管理者 priest_idracに登録され、それが利用できるように設定されます。プロビジョニングサーバーの詳細については、「Dell Lifecycle Controller Remote Servicesクイックスタートガイド」は、www.dell.com/idracmanualsにあります。を参照してください。

プロビジョニングサーバーは固定IPアドレスで動作します。iDRACの自動検出機能は、DHCP/ユニキャストDNS/mDNSを用いたプロビジョニングサーバーの検出に使用されます。
- iDRACがコントロールアドレスを有している場合は、自身のサービススタグ、IPアドレス、Redfishポート番号、Web証明書などを送信します。
- この情報を、定期的にコントロールサーバーに対して公開されます。

DHCPサーバ名、DNSサーバ名、デフォルトDNSホスト名により、プロビジョニングサーバーを検出します。DNSが指定されている場合、プロビジョニングサーバーIPがDNSから取得され、DHCP設定は不要になります。プロビジョニングサーバーが検出されていない場合、検出はスキップされ、DHCPもDNSも不要になります。

自動検出は、次の方法で有効にできます。
1. iDRACGUIを使用する：[iDRAC設定]＞[接続]＞[iDRAC自動検出]
2. RACADMを使用する：
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]＞[Remote Enablement]の順に選択します。
   [iDRAC設定のRemote Enablement]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コンポーネントの設定

自動設定機能により、サーバのすべてのコンポーネントを1回の操作で設定し、プロビジョニングできます。これらのコンポーネントには、BIOS、iDRAC、PERCがあります。自動設定では、すべての設定可能なバラメーターを含むサーバ設定プロファイル(SCP)のXMLファイルまたはJSONファイルが自動的にインポートされます。IPアドレスを割り当てるとDHCPサーバーも、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により作成されます。この設定は、DHCPや設定中のサーバのiDRACによりアクセス可能、共有のNFS、CIFS、HTTP、またはHTTPSのネットワーク共有にエクスポートされます。SCPファイル名は、サーバーのサーバスタンダードまたはモデル番号に基づく名前、または一般的な名前を指定することができます。DHCPサーバー、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、iDRACはSCPを使用してサーバのデバイスを設定します。自動設定は、iDRACがそのIPアドレスをDHCPサーバから取得した後でなければ呼び出されません。DHCPサーバからの応答がなかったりIPアドレスを取得できなかった場合、自動設定は呼び出されません。

HTTPおよびHTTPSファイル共有オプションは、iDRACファームウェア3.00.00.00以降でサポートされています。HTTPまたはHTTPSアドレスの詳細を提供する必要があります。サーバでブロギが有効になっている場合は、HTTPまたはHTTPSを使用して情報を転送するために、さらにブロギ設定を提供する必要があります。

表9. 異なる共有タイプとパスイン値

<table>
<thead>
<tr>
<th>共有タイプ</th>
<th>パスイン</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS</td>
<td>0またはnfs</td>
</tr>
<tr>
<td>CIFS</td>
<td>2またはcifs</td>
</tr>
<tr>
<td>HTTP</td>
<td>5またはhttp</td>
</tr>
<tr>
<td>HTTPS</td>
<td>6またはhttps</td>
</tr>
</tbody>
</table>

メモ: HTTPS証明書は自動設定ではサポートされません。自動設定では、証明書の警告を無視します。

次のリストでは、文字列の値をパスインするために必要なバラメーターと、オプションのバラメーターについて説明します。
- f (Filename): エクスポートされたサーバ設定プロファイルの名前。これは、iDRACファームウェアのバージョンが2.20.20.20より前の場合に必要です。
- n (Sharename): ネットワーク共有の名前。これは、NFSまたはCIFSに必要です。
- s (ShareType): NFSの場合は0、CIFSの場合は2、HTTPの場合は5、HTTPSの場合は6のいずれかをパスイン。これは、iDRACファームウェアのバージョン3.00.00.00の必須フィールドです。
基本の設定ファイル: config.xml
- "<servicestag>-config.xml" 例: CDVH7R1-config.xml
- "<モード番号>-config.xml" 例: R640-config.xml
- "config.xml"
- "<servicestag>-config.json" 例: CDVH7R1-config.json
- "<モード番号>-config.json" 例: R630-config.json
- "config.json"

 Memo: HTTP の詳細については、https://www.dell.com/support にあるホワイトペー「Lifecycle Controller インタフェース搭載 iDRAC9 での HTTP および HTTPS の 14G サポート」を参照してください。

Memo:
- 自動設定を有効化できるのは、DHCPV4 および IPv4 の有効化オプションが有効になっ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。自動検出を無効にして、自動設定を有効にしてください。
- サーバ設定を自動で行うために、自動設定機能が有効になります。

Memo: iDRAC サーバ設定エージェントは、サーバのサービススタグ、モデル番号、またはデフォルトのファイル名 config.xml を使用して設定ファイル名を自動的に生成します。

Memo: 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設定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。

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の共有の場所に、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. IP アドレスを取得中の iDRAC はベンダクラス識別子をアドバタイズします。（オプション 60）
5. DHCP サーバーは、ベンダーセルを選択できます。dhcpd.conf ファイル内のベンダーのオプションと一致させ、SCP サポートを提供した場合を除きます。
6. iDRAC は、SCP サポートを有効にします。

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 クライアントにバスできます。各パラメータは、DHCP オプションと呼ばれます。各オプションは、1byte 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、テキストとして定義されます。このテキストは、SCP サポートの場所および SCP サポート名（指定されている場合）を iDRAC に送信します。

DHCP サーバーは、SCP サポートを処理し、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 V6 は、グローバルに定義された多数のパラメータを DHCP クライアントにバスできます。各パラメータは、DHCP オプションと呼ばれます。各オプションは、1byte 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 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 サーバでは、iDRAC が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 サーバで新規範囲のオプションを有効にする必要があります。

Windowsでのオプション 43 の設定

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。
4. 「範囲のオプション ダイアログボックス」が表示されます。
5. DHCP サーバーで、043 ベンダー固有の情報を選択します。
6. Data Entry(データ入力) フィールドで ASCII の下の任意の場所をクリックし、SCP サポートのパスを含む共有の場所を持つサーバーの IP アドレスを入力します。
7. 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

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. 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。
5. 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:
6. 表示名: フィールドで、iDRAC と入力します。
7. 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。
16. 060でiDRAC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のに役立ちます。
   - Filename (-f) - エクスポートしたサーバ設定プロファイール(SCP)ファイルの名前を示します。
   - Sharename (-n) - ネットワーク共有の名前を示します。
   - ShareType (-s) - NFSおよびCIFSベースのファイル共有をサポートするほか、iDRACファームウェア3.00.00.00以上では、HTTPおよびHTTPSを使用してプロファイルファイルへのアクセスもサポートされています。-sオプションフラグは、次のように更新されます。
     - s (ShareType): NFSの場合はnfsまたは0、CIFSの場合はcifsまたは2、HTTPの場合はhttpまたは5、HTTPSの場合はhttpsまたは6を入力します（必須）。
   - IPAddress (-i) - ファイル共有のIPアドレスを示します。
   - Username (-u) - ネットワーク共有にアクセスするために必要なユーザー名を示します。この情報は、CIFSにのみ必要です。
   - Password (-p) - ネットワーク共有にアクセスするために必要なパスワードを示します。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は強制シャットダウンを示します。
   - TimeToWait (-t) - ホストシステムがシャットダウンするまで待機する時間を示します。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。

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。

```plaintext
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パラメータは次のとおりです。

- **Filename (-f)** - エクスポートしたサーバ設定プロファイルファイルの名前を示します。
  
  - **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、5 は HTTP を示し、6 は HTTPS を示します。
  - **IPAddress (-i)** - ファイル共有の IP アドレスを示します。
  - **Username (-u)** - ネットワーク共有へのアクセスにユーザーネーム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 は強制シャットダウンを示します。
  - **TimeToWait (-t)** - ホストサブ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。

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

```plaintext
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";
}
```
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。
- サポートされるネットワーク共有（NFS、CIFS、HTTPおよびHTTPS）は、iDRACおよびDHCPサーバと同じサブネット上にあります。ネットワーク共有をテストし、アクセス可能であること、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、SCCファイルに必要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がサーバーに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。

DHCPv4およびIPv4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。

自動設定機能を有効化するには、次の手順を実行します。
1. iDRACウェブインタフェースで、iDRAC Settings（iDRAC設定）＞Connectivity（接続性）＞Network（ネットワーク）＞Auto Config（自動設定）と動きます。
   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。
   - Enable Once （一回のみ有効）：DHCPサーバによって参照されるSCP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。
   - Enable once after reset（リセット後一回のみ有効）：iDRACのリセット後、DHCPサーバによって参照されるSCP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。
   - 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、『iDRAC RACADM CLIガイド』は、www.dell.com/idracmanualsにあります。を参照してください。

自動設定機能の詳細に関しては、https://www.dell.com/supportにあるホワイトペーパー「Dell EMC iDRACを使用した、LifecycleControllerの自動設定機能でのゼロタッチベアメタルサーバプロビジョニング」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

iDRACバージョン3.00.00.00搭載のPowerEdgeサーバでは、一方向ハッシュ形式を使用してユーザーパスワードおよび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）、パスワードをブ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です。
- 独自のSHA256ハッシュを生成してiDRACユーザーアカウントとBIOSパスワードを設定できます。これにより、サーバ構成プロファイル、RACADM、およびWSMまたは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。
- メモ：リモートRACADMまたはWSMまたはRedfishでは、iDRACのパスワードの設定/交換には使用できません。リモートRACADMまたはWSMまたはRedfishでのハッシュパスワードの設定/交換にはSCPを使用できません。
- 現在のブ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およびIPMI認証に必要なハッシュ値が含まれています。このプロファイルをもとにした後、最新のDellIPMIツールを使用する必要があります。古いツールを使用すると、ハッシュ化されたパスワードが設定されているユーザーのIPMI認証が失敗します。
- iDRACGUIなど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。
SHA256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、MD5v3Key、またはIPMIKey)を使用していない場合、SNMPv3およびIPMI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

#### メモ: SHA256PasswordおよびSHA256PasswordSaltフィールドはXMLインポート用に予約されているため、コマンドラインツールでは設定しないでください。いずれかのフィールドを設定すると、現在のユーザーがiDRACにログインできなくなる可能性があります。SHA256Passwordを使用してパスワードをインポートする場合、iDRACはパスワード長チェックを強制しません。

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/HTTP/HTTPS 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マンド解除できます。両方がコマンド解除されると、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

ハッシュパスワードは、ソルトあり/なしで、SNMPv3およびIPMI認証なしで生成できます。いずれの場合もSHA256が必要です。

ソルトありでハッシュパスワードを生成するには、次の手順に従います。

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と、16バイトのバイナリ文字列が付加されます。ソルトが提供されている場合は16バイト長である必要があります。付加されると、32文字の文字列になります。形式は次のように、「パスワード」+「ソルト」となります。

パスワード = SOMEPASSWORD

ソルト = ALITTLEBITOF_SALT - 16文字が付加されます。

2. 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。

   ```
   Generate Hash -> echo -n SOMEPASSWORDALITTLEBITOF_SALT|sha256sum -> <HASH>
   Generate Hex Representation of Salt -> echo -n ALITTLEBITOF_SALT | xxd -p -> <HEX-SALT>
   ```

   ```
   set iDRAC.Users.4.SHA256Password <HASH>
   ```

   ```
   set iDRAC.Users.4.SHA256PasswordSalt <HEX-SALT>
   ```

3. インポートされたサーバ設定プロファイル、RACADMコマンド、Redfish、またはWSManでハッシュ値とソルトを提供します。
メモ: 以前にソルト化したパスワードをクリアしたい場合は、次のように、パスワード+ソルトを明示的に空の文字列に設定してください。

```bash
set iDRAC.Users.4.SHA256Password
cia74e5fe75654735d3b8d04a7bdf5dcd06f1c6c2a215171a24e5a9dc82e7a2
```

4. パスワードの設定後に、通常のブレーンテキストパスワード認証は機能しますが、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SNMPv3およびIPMI認証は失敗します。

### 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、ユーザーや2）を変更できます。これらの操作を行うには、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、データセンタ内で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、System（システム）>Details（詳細）>System Details（システムの詳細）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、データセンタ内で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、「iDRAC RACADM CLIガイド」は、www.dell.com/idracmanualsにあります。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. データセンタ内で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。
システムパフォーマンスと電力消費の最適化

サーバを冷却するために必要な電力は、システム全体の電力の大きな部分を占めます。熱制御は、ファン速度およびシステム電源の管理によりシステム冷却をアクティブに管理します。これにより、システムの電力消費、エアフロ、システム音響出力を最小限に抑えつつ、システムの信頼性を確保します。熱制御設定を調整し、システムパフォーマンスおよびワット当たりのパフォーマンス要件に合わせて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

熱管理の機能のリストを以下に示します。

- システムエアフロ消費量：リアルタイムのシステムエアフロ消費量（CFM単位）を表示し、ラックレベルおよびデータセンターレベルでのエアフローのバランス調整を可能にします。
- カスタムDelta-T：吸気から排気までの温度差を制限し、インフラストラクチャレベルの冷却を最適化します。
- ターク温度制御：データセンターレベルでの設定で、サーバから排出される気温の温度制限を指定します。
- カスタムPCle吸気温度：サーバーのパフォーマンスに適合する適切な入力吸気温度を選択します。
- PCIeエアフロ設定：サーバーについて包括的なPCIeデバイス冷却ビューを提供し、サーバーパーティーカードの冷却のカスタマイズを可能にします。

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、[設定] > [システム設定] > [ハードウェア設定] > 冷却設定の順に移動します。
2. 以下を指定します。
   - 温度プロファイル最適化 — 温度プロファイルを選択します。
     - デフォルトの温度プロファイル設定（最小電力） — 温度アルゴリズムがシステムBIOSに設定図定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。
     - 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スロットの確認を削減。
       - サーバーのアクティビティの確率を増加。
       - 一般的に、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。
     - サウンドキャップ — サウンドキャップは、パフォーマンスの一部を犠牲にして、サーバからの音響の出力を軽減します。サウンドキャップを有効にすると、有効されている領域でサーバーの一部時的なノイズまたは評価が含まれることがあります。現在のデフォルトはパフォーマンス重視のアプリケーション向けに使用しないでください。
   - 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。

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を変更する必要があります。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設定が上書きされます。

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えるように、システムのファン速度を変更させることができるになります。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働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と、サーバーに冷却機能を追加できます。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える速度に、オフセット%値に従って上昇します。以下の値があります。

- 低ファン速度 - ファン速度を緩やかに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 - ファン速度を最高速度近くまで上昇させます。
- ファン最大速 - ファン速度を最高速度まで上昇させます。
- [オフ] — ファン速度オフセットがオフに設定されています。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。逆に、最大設定では、すべてのファンが最高速度で回転します。

ファン速度オフセットは動的で、システムに基づいています。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では、システムファン速度を4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、この機能を使用して、他の目的のためにシステムの冷却を向上させることができます。

しきい値

- PCIe吸気口最大温度制限 — デフォルト値は摂氏55度です。吸気口温度を低めにする必要があるサーバーパーティ製PCIeカードの場合、45℃の低温を選びます。
- 排気温度制限 — 次の値を変更することで、排気温度制限を設定できます。
  - 最大排気温度制限の設定
  - エア温度上昇制限の設定
- PWMでの最小ファン速度（最大の割合） — 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。このオプションを使用すると、他のシステムファン速度オプションで必要なファン速度が得られない場合に、ベースラインのシステムファン速度を高く設定したり、システムファン速度を上げることができます。
  - 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 - 変更するファン速度のパーセントを入力します。範囲は9～100です。
  
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動的に変化します。最初の値がアイドル時の速度であり、2番目の値は、設定速度最低速度（システムの設定によっては、最高速度は100%までとなることがある）です。システムのファンは、システムの熱要件に従ってこの速度よりも高い速度で動作することができますが、定義されている最小速度よりも低い速度で動作することはできません。たとえば、最小ファン速度を35%に設定すると、ファン速度は35%PWM未満に低下することはありません。

メモ: 0%PWMはファンがオフであることを示すものではありません。これは、ファンが達成できる最低ファン速度です。

設定は永続的です。つまり、一度設定して適用すると、システムの再起動、電源の再投入、iDRAC、またはBIOSのアップデート中にデフォルト設定に自動的に変更されることはありません。カスタム冷却オプションは、すべてのサーバーでサポートされているわけではありません。オプションがサポートされていない場合は、表示されないか、カスタム値を指定できません。

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.

4. 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 10. 温度設定

<table>
<thead>
<tr>
<th>オブジェクト</th>
<th>説明</th>
<th>使用状況</th>
<th>例</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirExhaustTemp</td>
<td>最大排気温度制限を設定することができます。</td>
<td>次の値のいずれかに設定します（システムに基づく）。</td>
<td>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。</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 0 — 40°C を示します。</td>
<td>racadm get system.thermalsettings.AirExhaustTemp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 1 — 45°C を示します。</td>
<td>気は次のとおりです。</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 2 — 50°C を示します。</td>
<td>AirExhaustTemp=70</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 3 — 55°C を示します。</td>
<td>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。</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 4 — 60°C を示します。</td>
<td>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。</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 255 - 70 °C を示します（デフォルト）。</td>
<td>racadm set system.thermalsettings.AirExhaustTemp 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>出力は次のとおりです。</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Object value modified successfully.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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。</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>racadm set system.thermalsettings.AirExhaustTemp 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>次のエラーメッセージが表示されます。</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ERROR: RAC947: Invalid object value specified.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>オブジェクトのタイプに基づいて値を指定してください。</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>詳細に関しては、RACADM のヘルプを参照してください。</td>
</tr>
</tbody>
</table>

64 管理下システムのセットアップ
### 表10. 温度設定（続き）

<table>
<thead>
<tr>
<th>オブジェクト</th>
<th>説明</th>
<th>使用状況</th>
<th>例</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 値と 100 値の範囲の設定値 0～100 の値</td>
<td>使用状況</td>
<td>例</td>
<td>例</td>
</tr>
<tr>
<td><strong>FanSpeedHighOffsetVal</strong></td>
<td>この変数を取得すると、高速ファン速度オフセット設定値（%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。</td>
<td>例</td>
<td>例</td>
</tr>
<tr>
<td><strong>FanSpeedLowOffsetVal</strong></td>
<td>この変数を取得すると、低速ファン速度オフセット設定値（%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。</td>
<td>例</td>
<td>例</td>
</tr>
<tr>
<td><strong>FanSpeedMaxOffsetVal</strong></td>
<td>この変数を取得すると、最速ファン速度オフセット設定値（%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 3 でこの値を設定します。</td>
<td>例</td>
<td>例</td>
</tr>
</tbody>
</table>

**例**

<table>
<thead>
<tr>
<th>コマンド</th>
<th>例</th>
</tr>
</thead>
<tbody>
<tr>
<td>racadm set</td>
<td>system.thermalsettings.AirExhaustTemp 255</td>
</tr>
<tr>
<td>racadm set</td>
<td>system.thermalsettings.FanSpeedHighOffsetVal 66</td>
</tr>
<tr>
<td>racadm set</td>
<td>system.thermalsettings.FanSpeedLowOffsetVal 23</td>
</tr>
<tr>
<td>racadm set</td>
<td>system.thermalsettings.FanSpeedMaxOffsetVal 100</td>
</tr>
</tbody>
</table>

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。

**例**

<table>
<thead>
<tr>
<th>コマンド</th>
<th>例</th>
</tr>
</thead>
<tbody>
<tr>
<td>racadm set</td>
<td>system.thermalsettings.FanSpeedMaxOffsetVal 100</td>
</tr>
</tbody>
</table>

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（フルスピードのとき、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に達した場合に設定されます。
### 表10. 温度設定（続き）

<table>
<thead>
<tr>
<th>オブジェクト</th>
<th>説明</th>
<th>使用状況</th>
<th>例</th>
</tr>
</thead>
<tbody>
<tr>
<td>FanSpeedMediumOffsetVal</td>
<td>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。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。</td>
<td>0~100の値</td>
<td>racadm get system.thermalsettings FanSpeedMediumOffsetVal これにより、「47」などの値が返されます。これは、次のコマンドを使用したときに、ベースラインファン速度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</td>
</tr>
<tr>
<td>FanSpeedOffset</td>
<td>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。</td>
<td>値：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</td>
<td>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</td>
</tr>
<tr>
<td>MFSMaximumLimit</td>
<td>MFSの最大制限の読み取り</td>
<td>1~100の値</td>
<td>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</td>
</tr>
</tbody>
</table>
表10. 温度設定（続き）

<table>
<thead>
<tr>
<th>オブジェクト</th>
<th>説明</th>
<th>使用状況</th>
<th>例</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFSMinimumLimit</td>
<td>MFSの最低制限の読み取り操作を実行します。</td>
<td>0～MFSMaximumLimitの値の範囲内に設定する。</td>
<td>MinimumFanSpeedオブジェクトを使用して設定できる最小値を表示するには、次のコマンドを使用します。</td>
</tr>
<tr>
<td>MinimumFanSpeed</td>
<td>• 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。</td>
<td>MFSMinimumLimit～MFSMaximumLimitの値を設定します。</td>
<td>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。</td>
</tr>
<tr>
<td>ThermalProfile</td>
<td>• 温度ベースアルゴリズムを指定することができます。</td>
<td>既存の温度プロファイル設定を表示するには、次のコマンドを使用します。</td>
<td>racadm get system.thermalsettings.ThermalProfile</td>
</tr>
<tr>
<td>ThirdPartyPCIFanResponse</td>
<td>• サードパーティPCIカード用サーマルオーバーライド。</td>
<td>既出されたサーマル設定を無効にするには、次のコマンドを使用します。</td>
<td>racadm set system.thermalsettings.ThirdPartyPCIFanResponse 0</td>
</tr>
</tbody>
</table>

iDRAC設定ユーティリティ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設定ユーティリティで、サーマルメニュに移動します。
2. 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

これらの設定は永続的です。つまり、一度設定して適用すると、システムの再起動、電源サイクリング、iDRAC、または BIOS のアップデート中にも、これらの設定が自動的にデフォルト設定に変更されることはありません。一部の Dell サーバでは、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全部がサポートされる場合とされない場合があります。オプションがサポートされない場合は、そのオプションが表示されないか、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。

iDRAC Web インターフェースを使用した PCIe エアフロー設定の変更

カスタム高出力 PCIe カード用に熱マージンの増加が必要なときに、PCIe エアフロー設定を使用します。

memo: PCIe エアフロー設定は、MX プラットフォームでは使用できません。

PCIe エアフロー設定を変更するには、次の手順を実行します。

1. iDRAC Web インターフェースで、設定 > [システム設定] > [ハードウェア設定] > [冷却設定] の順に移動します。
   ・ ファン設定セクションの右下に [PCIe エアフロー設定] ページが表示されます。

2. 以下の手順を実行します。
   • [LFM モード] - [カスタム] モードを選択して、カスタム LFM オプションを有効にします。
   • [カスタム LFM] - LFM 値を入力します。

3. 設定を適用するには、適用をクリックします。
   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。

memo: 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。

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 インター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. サポートされているウェブブラウザをインストールして設定します。詳細については、リリースノートを参照してください。
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）。

memo: この機能を使用して IPv6 ネットワーク上で iDRAC 仮想コンソールを起動するには、Java 8 以降が必要です。

4. 「Dell Systems Management Tools and Documentation」DVD から、SYSGMT フォルダーにあるリモート 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、「iDRAC RACADM CLI 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
### 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。たとえば、次のとおりです。

- プレードサーバー - 管理ステーションは、CMC および OME Modular と同じネットワークに存在する必要があります。管理対象システムのネットワークから CMC ネットワークを分離する方法の詳細については、『Chassis Management Controller ユーザーズガイド』は、www.dell.com/cmcmanual にあります。を参照してください。

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。

**対応ウェブブラウザの設定**

[jep: 対応ブラウザとバージョンの詳細については、www.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に、これらのブラウザのデフォルト設定でアクセスできます。一部の機能を使用するには、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あります。

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 Web インターフェイ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 Web ブラウザを設定します。

[jep: 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設定を行う必要がある場合があります。その他のサポート対象ブラウザは、デフォルト設定で使用できます。]

[jep: 空のプロキシ設定はプロキシがないと認識されます。]

### Internet Explorer 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。設定には以下が含まれます。

- 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
- IE セキュリティ強化の構成の無効化

#### 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. セキュリティオプション セキュリティ ローカルネットワークまたは ローカルインタナネット をクリックします。
3. カスタムレベルをクリックして中低を選択し、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、Refresh (更新) をクリックすると、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推奨します。

[jep: 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. システム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、ローカルインター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（インターネット）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. Advanced（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. 閉じをクリックしてOKを2回クリックします。

Internet Explorerセキュリティ強化構成の無効化

ウェブインタフェースを使用してログファイルやその他のローカル要素をダウンロードできるようにするには、Windowsの機能からInternet Explorerセキュリティ強化の構成を無効にすることをお勧めします。お使いのWindowsのバージョンでこの機能を無効にする方法については、Microsoftのマニュアルを参照してください。

Mozilla Firefoxの設定

このセクションでは、iDRAC Web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説明します。これらの設定には、次のものが含まれます。
- 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

メモ: Mozilla Firefoxブラウザーには、iDRACオンラインヘルプページ用のスクロールバーがない場合があります。

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のサイトごとにプラグインをインストールするためのユーザー権限が必要な「ホワイトリスト」機能があります。このホワイトリスト機能を有効にする場合は、ビューのバージョンが同一であっても、アクセスするiDRACごとに仮想コンソールビューをインストールする必要があります。

ホワイトリスト機能を無効にし、不要なプラグインインストールを避けるには、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を見つけつけてダブルクリックします。

   Preference Name（プリファレンス名）、Status（ステータス）、Type（タイプ）、およびValue（値）の値が太字のテキストに変更されます。Status（ステータス）の値はユーザーセットに変更され、Value（値）はfalseに変更されます。
4. プリファレンス名列で、xpininstall.enabledを見つけます。

   Value（値）がtrueであることを確認します。そうでない場合は、xpininstall.enabledをダブルクリックしてValue（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. Filter（フィルター）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）。

70 管理下システムのセットアップ
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、www.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ビューは、Internet Explorerでのみサポートされます。
   HTML5またはJavaビューは、どのブラウザでもサポートされています。

   メモ: この機能を使用してIPv6ネットワーク上でiDRAC仮想コンソールを起動するには、Java8以降が必要です。

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、ユーティリティ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。

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テクノロジを使用して作成されます。HTML5テクノロジの利点は次のとおりです。

• 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。
• 互換性はプ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。ブラウザの設定を行うには、次の手順を実行します。

1. ポップアップブロックを無効にします。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ベースのプラグイン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、インストール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:feff:2fe9]/ to https://fe80--d267-e5ff-feff-2fe9.ipv6-literal.net/```

   • IPv6アドレスを使用したIEでのDirectHTML5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:feff:2fe9]/console to https://fe80--d267-e5ff-feff-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クラシックの順に移動します。

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

HTML5ベースの仮想コンソールおよび仮想メディアアプリケーションを起動および実行する前に、Edgeの設定を行う必要があります。ブラウザの設定を行うには、次の手順を実行します。

1. [設定]＞[詳細設定を表示]をクリックし、[ポップアップをブロックする]オプションを無効にします。
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。

ActiveX プラグインを使用するための IE の設定

ActiveX プラグインのタイプがテキストにダウンロードされます。ActiveX プラグインは、32 ビットまたは 64 ビット版のブラウザにプラグインをインストールできます。

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。

ActiveX プラグインを使用するための IE の設定

ActiveX プラグインのタイプがテキストにダウンロードされる場合、仮想コンソールでプラグインのタイプが Native-ActiveX タイプに設定されている場合、仮想コンソールで起動すると、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 プラグインの仮想コンソールが起動します。Internet Explorer で ActiveX プラグインのダウンロード、インストール、実行を行うには設定が必要です。

64 ビットのオペレーティングシステムでは、32 ビット版または 64 ビット版の Internet Explorer をインストールできます。32 ビット版または 64 ビット版のどちらかを使用できますが、対応するプラグインをインストールする必要があります。たとえば、64 ビット版ブラウザにプラグインをインストールしてから、32 ビット版ブラウザでビューアを開く場合、プラグインを再度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のセキュリティ強化モードを必ず無効にしてください。

Windows 7、Windows 2008、および Windows 10 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. プ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 Local Internet site (ローカルインターネットサイト) リストに追加します。
3. カスタム設定を中等にリセットするか、設定を変更して最適な ActiveX プラグインのインストールを許可します。
4. プラウザの暗号化されたコンテンツのダウンロードを有効にして、サーバー製のプラウザ拡張を有効にしてください。これを行うには、Tools (ツール) > Internet Options (インターネットオプション) > Advanced (詳細設定) の順に移動し、Do not save encrypted pages to disk (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、Enable third-party browser extensions (サードパーティ製のプラウザ拡張を有効にする) オプションを選択します。

メモ: サードパーティのプラウザ拡張を有効にする設定を反映させるために、Internet Explorer を再起動します。

5. ツール > インターネットオプション > セキュリティと進み、アプリケーションを実行するゾーンを選択します。
6. Custom level (レベルのカスタマイズ) をクリックします。Security Settings (セキュリティ設定) ウィンドウで、次のいずれかを実行します。
   - 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。
   - 場合によって 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開じます。
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開じます。

メモ: Internet Explorer 11 を搭載したシステムでは、Tools (ツール) > Compatibility View settings (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。

IPv6 アドレスを次のように変更します。

https://2607:f2b1:f083:147::1eb.ipv6:literal.net/restgui to https://2607-f2b1-f083-147--1eb.ipv6-literal.net/restgui
メモ:

- Internet Explorer のさまざまなバージョン、Internet Options（インターネットオプション）を共有します。したがって、サーバーのあるブラウザの信頼済みサイトのリストに追加した後、別のブラウザが同じ設定を使用します。
- ActiveX コントロールをインストールする前に、Internet Explorer にセキュリティ警告が表示される場合があります。ActiveX コントロールのインストール手順を完了するには、Internet Explorer がセキュリティ警告を発しても ActiveX コントロールを許可します。
- 仮想コンソールの起動中に、不明な発行元のエラーが発生する場合、コードサインング証明書のバスの変更が原因である場合があります。このエラーを解決するには、追加のキーをダウンロードする必要があります。検索エンジンを使用して、Symantec SO16958 を検索し、検索結果にある Symantec Web サイトの指示に従います。

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. タスカーマネージャー > セキュリティ > 保護モードを有効にするオプションを有効にします。
3. 信頼を行うサイトに対して Enable Protected Mode (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、インター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。インター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。

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 キャッシュビューが表示されます。
2. iDRAC 仮想コンソール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を起動すると、証明書の検証用プロンプトが表示されます。カスタム Web サーバー証明書がある場合は、CA 証明書を Java または ActiveX の信頼済み証明書ストアにインポートすることで、これらのプロンプトを回避できます。

自動証明書登録（ACE）の詳細については、次のセクションを参照：自動証明書登録、 p.110

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、OKをクリックします。Java Control Panel（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）を使用して証明書に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 1.0.0 以降では、デフォルトで SHA を使用しているため、これを使用することを推奨します。CA 証明書は、Base64 でエンコードされた PEM フォーマットである必要があります。これは、各 CA 証明書をインポートするワンタイムプロセスです。

CA 証明書を ActiveX の信頼済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。
3. CA 証明書の名前を出力ファイルの名前に変更し、「.0」という拡張子を付けます。たとえば、cacert.pem の場合は、431db322.0 です。
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。例えば、C:¥Documents and Settings¥<ユーザー> ¥ディレクトリです。

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)

かっこ内の 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必要があります。

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。これら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。

注意: 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
- ポート
- 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
- 電源供給ユニット (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 コンソール

注意: PSU ファームウェアのアップデートは、システム構成と PSU モデルによっては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と、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ミングされ、次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。

**メモ:**
- コントローラーでSEKMモードが有効になっている場合、SEKM対応のiDRACバージョンからSEKM非対応のiDRACバージョンに切り替えようとすると、iDRACファームウェアのダウングレード/アップグレードが失敗します。SEKM対応したバージョンで実行した場合は、iDRACファームウェアのアップグレード/ダウングレードが成功します。
- SEKMが有効になっている場合、PERCファームウェアのダウングレードが失敗します。
- SEKMが有効になっている場合、SEKM対応したバージョン同士で実行した場合は、iDRACファームウェアのアップグレード/ダウングレードが成功します。
- SEKMが有効になっている場合、PERCファームウェアのダウングレードが失敗します。
- SEKMが有効になっている場合、PERCファームウェアのダウングレードが失敗します。

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)。このイメージファイルタイプを使用するには、制御および設定権限が必要です。
- .d9—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。
- .d9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、次的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、HTTPまたはHTTPS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。
- カスタムリポジトリはDell Repository Managerを使って作成できます。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。そのリポジトリに含まれる該当アップデートのすべてがシステムに適用されます。この機能はiDRAC Enterpriseライセンスで使用可能です。
- 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。次表は、iDRACファームウェアに於ける適用度です。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11 イメージファイルのタイプと依存関係**

<table>
<thead>
<tr>
<th>インタフェース</th>
<th>.D9 イメージ</th>
<th>iDRAC DUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMCFW64.exe ユーティリティ</td>
<td>有</td>
<td>無</td>
</tr>
<tr>
<td>Racadm FWUpdate (古い)</td>
<td>有</td>
<td>無</td>
</tr>
<tr>
<td>Racadm Update (新しい)</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>iDRAC UI</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>WSMAN</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>インバンド OS DUP</td>
<td>無</td>
<td>該当なし</td>
</tr>
</tbody>
</table>

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。
複数のファームウェアのアップデートを域外方式で適用する場合、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12. ファームウェアアップデート — 対応コンポーネント

<table>
<thead>
<tr>
<th>コンポーネント名</th>
<th>ファームウェアのロールバックのサポート（有または無）</th>
<th>帯域外 — システム再起動の必要性</th>
<th>インバンド — システム再起動の必要性</th>
<th>Lifecycle Controller GUI — 再起動の必要性</th>
</tr>
</thead>
<tbody>
<tr>
<td>診断</td>
<td>無</td>
<td>無</td>
<td>無</td>
<td>無</td>
</tr>
<tr>
<td>オペレーティングシステムのドライバパック</td>
<td>無</td>
<td>無</td>
<td>無</td>
<td>無</td>
</tr>
<tr>
<td>iDRAC</td>
<td>有</td>
<td>無</td>
<td>なし*</td>
<td>有</td>
</tr>
<tr>
<td>BIOS</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>RAID コントローラ</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>BOSS</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>NVDIMM</td>
<td>無</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>バックプレーン</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>エンクロージャ</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>NIC</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>電源供給ユニット</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>CPLD</td>
<td>無</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
</tbody>
</table>

メモ: CPLD ファームウェアのアップデートが完了すると、iDRAC は自動的に再起動します。

<table>
<thead>
<tr>
<th>コンポーネント名</th>
<th>ファームウェアのロールバックのサポート（有または無）</th>
<th>帯域外 — システム再起動の必要性</th>
<th>インバンド — システム再起動の必要性</th>
<th>Lifecycle Controller GUI — 再起動の必要性</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC カード</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>NVMe PCIe SSD ドライバ</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>SAS/SATA ハードドライバ</td>
<td>無</td>
<td>有</td>
<td>有</td>
<td>無</td>
</tr>
<tr>
<td>OS コレクタ</td>
<td>無</td>
<td>無</td>
<td>無</td>
<td>無</td>
</tr>
<tr>
<td>CMC (PowerEdge FX2 サーバー)</td>
<td>無</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
</tbody>
</table>

メモ: MX プラットフォームでサポートされるコンポーネントの詳細については、表13を参照してください。

### 表13. ファームウェアアップデート — MX プラットフォームでサポートされているコンポーネント

<table>
<thead>
<tr>
<th>コンポーネント名</th>
<th>ファームウェアのロールバックのサポート（有または無）</th>
<th>帯域外 — システム再起動の必要性</th>
<th>インバンド — システム再起動の必要性</th>
<th>Lifecycle Controller GUI — 再起動の必要性</th>
</tr>
</thead>
<tbody>
<tr>
<td>診断</td>
<td>無</td>
<td>無</td>
<td>無</td>
<td>無</td>
</tr>
<tr>
<td>オペレーティングシステムのドライバパック</td>
<td>無</td>
<td>無</td>
<td>無</td>
<td>無</td>
</tr>
<tr>
<td>iDRAC</td>
<td>有</td>
<td>無</td>
<td>なし*</td>
<td>有</td>
</tr>
<tr>
<td>BIOS</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>RAID コントローラ</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>BOSS</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>NVDIMM</td>
<td>無</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>バックプレーン</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>エンクロージャ</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
</tbody>
</table>
### 表13. ファームウェアアップデート—MXプラットフォームでサポートされているコンポーネント（続き）

<table>
<thead>
<tr>
<th>コンポーネント名</th>
<th>ファームウェアのロールバックのサポート（有または無）</th>
<th>帯域外—システム再起動の必要性</th>
<th>インバンド—システム再起動の必要性</th>
<th>Lifecycle Controller GUI —再起動の必要性</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIC</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>電源供給ユニット</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>CPLD</td>
<td>無</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>FC カード</td>
<td>有</td>
<td>有</td>
<td>有</td>
<td>有</td>
</tr>
<tr>
<td>NVMe PCIe SSD ドライブ</td>
<td>有</td>
<td>無</td>
<td>無</td>
<td>無</td>
</tr>
<tr>
<td>SAS/SATA ハードドライブ</td>
<td>無</td>
<td>有</td>
<td>有</td>
<td>無</td>
</tr>
<tr>
<td>OS コレクタ</td>
<td>無</td>
<td>無</td>
<td>無</td>
<td>無</td>
</tr>
</tbody>
</table>

*は、システムの再起動は必要でなくても、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

ローカルシステムで使用可能なファームウェアイメージを使用して、ネットワーク共有（CIFS、NFS、HTTP、またはHTTPS）のリポジトリから、またはFTPからデバイスファームウェアをアップデートできます。

#### 単一デバイスのファームウェアのアップデート

单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。

1. [メンテナンス] > [システムアップデート] に移動します。
   - ファームウェアのアップデートページが表示されます。
   - メモ：ローカルを選択する場合は、ローカルシステムの場所にファームウェアイメージをダウンロードしてください。アップデートのためにiDRACにステージするファイルを1つ選択してください。iDRACへのアップロードには、1度に1ファイルずつ追加ファイルを選択することができます。ファイルはiDRACの一時スペースにアップロードされ、この最大容量は約300MBです。
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で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、正常にアップロードされた場合は、[内容]列のファームウェアイメージファイル名の横にプラスアイコン（+）が表示されます。名前を拡張して、[デバイス名]、[現在]、および[使用可能なファームウェアバージョン]情報が確認します。
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イメージの場合は、[インストール]をクリックします。たとえば、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。

管理下システムのセットアップ
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のスケジュール設定

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。

1. IDRCウェブインタフェースで、Maintenance（メンテナンス） > System Update（システムアップデート） > Automatic Update（自動アップデート）と移動します。

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。

6. Network（ネットワーク）—ネットワーク共有（CIFS、NFS、HTTPまたはHTTPS、TFTP）からのカタログファイルを使用します。ネットワーク共有設定詳細を入力してください。

7. FTP—FTPサイトからのカタログファイルを使用します。FTPサイト詳細を入力します。

8. HTTPまたはHTTPS—カタログファイルのストリーミング、via HTTPとvia HTTPSのファイル転送が可能です。

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。

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リに作成されます。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:
  ```bash
  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:
  ```bash
  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:
  ```bash
  ```

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:
  ```bash
  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:
  ```bash
  ```

- 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:
  ```bash
  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:
  ```bash
  racadm set lifecycleController.lcattributes.AutoUpdate.Enable 0
  ```

- スケジュールの詳細をクリアする:
  ```bash
  racadm AutoUpdateScheduler clear
  ```

- HTTP 共有からアップリモートデータファイルをアップロードする:
  ```bash
  racadm update -f <updatefile> -u admin -p mypass -l http://1.2.3.4/share
  ```

- HTTPS 共有からアップリモートデータファイルをアップロードする:
  ```bash
  racadm update -f <updatefile> -u admin -p mypass -l https://1.2.3.4/share
  ```

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。詳細については、www.dell.com/idracmanuals にある iDRAC RACADM CLI 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:
  ```bash
  racadm update -f catalog.xml -l //192.168.1.1 -u test -p passwd --verycatalog
  ```
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. iDRAC Settings (iDRAC 設定) > Settings (設定) > CMC の順に移動します。
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。

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、次の手順をおこなってください。

- 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おきます。

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 というようなエラー・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 ハイパーバイザー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 usbbarbretor stop` コマンドを使用して「usbbarbretor」サービスを停止されていることを確認します。

DUP の一部のバージョンは、相互に競合が生じるような方式で構築されています。これは、時間の経過とともにソフトウェアの

新バージョンが追加されることが一般的です。新バージョンのソフトウェアでは、レガシー・デバイスのサポートが放棄される

場合があります。新しいデバイスのサポートが追加される場合もあります。例として 2 つの DUP の、

`Network_Firmware_NDT09_WN64_21.60.50.EXE` や `Network_Firmware_8J1P7_WN64_21.60.27.50.EXE` を考えてみましょう。これらの DUP でサポートされているデバイスは、5 つのグループに分けられます。

- グループ A はレガシー・デバイスで、NTD09 でのみサポートされています。
- グループ B は、NTD09 および 8J1P7 の両方でサポートされているデバイスです。
- グループ C は新しいデバイスで、8J1P7 でのみサポートされています。

グループ A、B、C に属するデバイスを、それぞれ 1 つまたは複数持っているサーバーを考えてみましょう。DUP が一度に 1 つずつ使

用されている場合、その処理は成功するはずです。NTD09 を単独で使用しているところ、グループ A とグループ B のデバイスは更新

されます。8J1P7 を単独で使用していれば、グループ B とグループ C のデバイスは更新されます。しかしながら、同時に両方の
DUP を使用しようとするとき、グループ B のデバイスに対しては、2 つのアップデート作成が同時に試みられるかもしれません。

そのためこのデバイスのジョブはすでに存在しますというメッセージが表示される可能性があります。同じデバイスに対して同時に 2
つの正しいアップデートを試みようとする 2 つの有効な DUP の競合は、両方のデバイスがサポートされていません。この競合は、デバイスでのロールバック実行
時に発生します。ベストプラクティスとしては、各 DUP を個別に使用することが推奨されます。

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.d9 です。
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.d9 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.d9 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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。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方法の詳細については、「Dell Lifecycle Controller Remote Services クイック スタートガイド」は、www.dell.com/idracmanuals にあります。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 のないシャーシは「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 のないシャーシは 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、シャーシ出力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. iDRAC Settings (iDRAC 設定) > Settings (設定) > CMC の順に移動します。
iDRAC の導入ページが表示されます。

3. Chassis Management at Server Mode (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、Manage and Monitor (管理および監視) を選択して、Apply (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 Settings (iDRAC 設定) > Settings (設定) > CMC の順に移動します。
2. Chassis Management Controller Firmware Update (Chassis Management Controller ファームウェアアップデート) をクリックします。
3. 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。

**ステーディ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、ライセンス付きの機能です。次回の起動時に実行するためにキーに入っているすべてのジョブを削除できます。

**iDRAC ウェブインタフェースを使用したステーディ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、Maintenance (メンテナンス) > Job Queue (ジョブキュー) の順に移動します。Job Queue (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。

ジョブを削除するには、ジョブを選択して Delete (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 の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、(状態が「実行中」または「ダウンロード中」になっているジョブ) は削除できません。

ジョブの削除には、サーバー制御の特権が必要です。

**RACADM を使用したステーディングされたアップデートの表示と管理**

RACADM を使用してステーディングアップデートを表示するには、jobqueue サブコマンドを使用します。詳細については、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。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**

以前に別のインタフェースを使用してアップグレードした場合でも、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を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は、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できます。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することができます。

単一の iDRAC および Lifecycle Controller ファームウェアを持つ Dell 第 14 世代の 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。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 コントローラー
・ 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、次のこと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 LOB 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 Web インタフェース（MX プラットフォームでは未サポート）
・ OME-Modular Web インタフェース（MX プラットフォームでは未サポート）
・ iDRAC RACADM CLI
・ Lifecycle Controller GUI
・ Lifecycle Controller-Remote Services

### 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、Maintenance（メンテナンス）> System Update（システムアップデート）> Rollback（ロールバック）に移動します。
   Rollback（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確認できます。
2. ファームウェアをロールバックするデバイスを選択します。
3. 選択したデバイスに基づいて、Install and Reboot（インストールおよび再起動）または Install Next Reboot（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、Install（インストール）をクリックします。
   インストールおよび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すると、「ジョブキューページが表示されます。
4. ジョブキューをクリックします。
   ステージされているファームウェアアップデートを表示および管理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中にステージされているか、またはすぐに実行状況である。

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. iDRAC Settings (iDRAC 設定) > Settings (設定) > CMC の順に移動します。
iDRAC の導入ページが表示されます。
3. Launch iDRAC (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、p. 83」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 swinvetory コマンドで、ロールバックのステータスおよび FQDD をチェックします。
   ```
racadm swinvetory
   ```
   ファームウェアをロールバックするデバイスの場合、Rollback Version が Available になっている必要があります。また、FQDD をメモに書き留めてください。
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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。 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

詳細については、「Lifecycle Controller ユーザーズガイド」は、www.dell.com/idracmanuals にあります。 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

詳細については、「Dell Lifecycle Controller Remote Services クイックスタートガイド」は、www.dell.com/idracmanuals にあります。 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の背面と、ブレードサーバの前面にあります)。
- 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 EX3 でフォーマットします。
- firmimg.d9 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.d9 を読み取り、iDRAC を再プログラムし、iDRAC を再起動します。
サーバープロファイルのバックアップ

BIOS、RAID、NIC、iDRAC、Lifecycle Controller、ネットワークドーターーカード（NDC）など、さまざまなコンポーネントにインストールされたファームウェアイメージ、およびこれらのコンポーネントの設定を含むシステム設定をバックアップできます。バックアップ操作には、ハードディスク構成データ、マザーボード、および交換済み部品も含まれます。バックアップは、vFlash SDカードまたはネットワーク共有（CIFS、NFS、HTTP、またはHTTPS）に保存できる1つのファイルを作成します。

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。

メモ：サーバープロファイルのバックアップまたは復元操作の進行中は、iDRACをリセットしないことをお勧めします。

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。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。

1. Collect System Inventory On Reboot（CSIOR）が有効になっている。

CSIORが無効になっているときにバック操作を開始すると、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

2. 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。

   a. vFlash SDカードが挿入され、有効化および初期化されました。
   b. 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100MB以上の空き容量があります。

   バックアップイベントがLifecycleログに記録されます。

メモ：Windows 10オペレーティングシステムでNFSを使用してサーバープロファイルをエクスポートし、エクスポートされたサーバープロファイルにアクセスする際に問題が発生した場合は、Windows機能でClient for NFSを有効にします。

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、次の手順を行います。

1. iDRAC Settings（iDRAC設定）＞Settings（設定）＞Backup and Export Server Profile（サーバープロファイルのバックアップとエクスポート）の順に移動します。

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。

   a. Network Share（ネットワーク共有）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。
   b. HTTP（HTTP）またはHTTPS（HTTPS）を選択して、バックアップファイルイメージをHTTP/HTTPSファイル転送介してローカルファイルに保存。

メモ：NFS共有をマウントしたら、iDRAC内ではroot以外のユーザーは共有への書き込みができなくなります。これはiDRACのセキュリティを向上するためです。

3. バックアップについて、FileName（ファイル名）、Backup File Passphrase（バックアップファイルのパスフレーズ）（オプション）、Confirm Passphrase（パスフレーズの確認）の詳細を入力します。

4. ファイルの場所としてNetwork（ネットワーク）を選択した場合は、該当の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ディング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。

RACADMを使用したサーバープロファイルのバックアップ

RACADM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、systemconfig backupコマンドを使用します。詳細については、「iDRAC RACADM CLIガイド」は、www.dell.com/idracmanualsにあります。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、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る。

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、iDRAC Settings (iDRAC 設定) > Settings (設定) > Backup and Export Server Profile (サーバープロファイルのバックアップとエクスポート) の順に移動します。
2. 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。
3. 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。
   - HTTP または HTTPS を選択して、バックアップファイルイメージを HTTP/S ファイル転送を使用して保存。
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。
5. Backup Now (今すぐバックアップ) をクリックします。

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リング

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：

```
```

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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。を参照してください。

**サーバー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。

memo: 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、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。

**簡易な復元**

お使いのサーバーのマザーボードを交換後、簡易復元により、以下のデータを自動的に復元できます:

• System Service Tag (システムサービスタグ)
• 資産タグ
• 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

簡易復元では、簡易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。マザーボードを交換し、システムの電源を入れると、BIOS により iDRAC のクエリが行われ、バックアップデータを復元するように求められます。最初の BIOS 画面では、サービスタグ、ライセンス、UEFI 診断アプリケーションを復元するように求められます。2 番目の BIOS 画面では、システム構成の設定を復元するように求められます。最初の BIOS 画面でデータの復元を行わないことを選択し、かつ、別的方法によってサービスタグを設定しない場合、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。

memo:

• システム構成の設定は、CSIOR が有効になっている場合にのみバックアップされます。Lifecycle Controller および 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、簡易復元フラッシュメモリのデータは消去されません。
• 簡易復元では、ファームウェアイメージ、vFlash 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。

**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. [iDRAC 設定] > [設定] > [サーバープロファイルのインポート] の順に移動します。
   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。
ネットワーク共有を選択して、バックアップファイルイメージをCIFSまたはNFS共有に保存します。

HTTP/HTTPSを選択して、バックアップファイルイメージをHTTP/Sファイル転送を介してローカルファイルに保存します。

3. バックアップのファイル名、バックアップファイルのパスフレーズ（オプション）、およびパスフレーズの確認の詳細を入力します。

4. バックアップのファイル名および復号化パスフレーズを入力します（オプション）。

5. 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：ネットワーク共有の設定の際には、ユーザー名およびパスワードでの特殊文字の使用、および特殊文字のパーセントエンコーディングは避けることをお勧めします。

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。  

6. 仮想ディスク設定とハードディスクデータの保存—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。

7. 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。

7. 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。

6. IDRACを使用したサーバープロファイルのインポート

RACADM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、systemconfig restoreコマンドを使用します。詳細については、「iDRAC RACADM CLIガイド」は、www.dell.com/idracmanualsにあります。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あります。詳細については、それぞれのユーザーガイドを参照してください。

サーバ設定プロファイルのサポート - インポートおよびエクスポート

サーバ設定プロファイル（SCP）によって、サーバ設定ファイルをインポートおよびエクスポートできます。

メモ: SCPタスクのエクスポートとインポートを実行するには、管理者権限が必要です。

ローカルの管理ステーション、およびCIFS、NFS、HTTP、HTTPSのいずれかを介したネットワーク共有から、インポートおよびエクスポートができます。SCPを使用して、BIOS、NIC、RAIDのコンポーネントレベルの設定を選択し、インポートまたはエクスポートすることができます。SCPは、ローカル管理ステーションまたはネットワーク共有（CIFS、NFS、HTTP、またはHTTPS）
にインポートおよびエクスポートできます。iDRAC、BIOS、NIC、およびRAIDのプロファイルを個々にインポートおよびエクスポートすることも、それぞれすべてを1つのファイルとしてインポートおよびエクスポートすることもできます。
SCPのインポートまたはエクスポートのレビューを指定できます。ここではジョブが実行され、設定結果が生成されますが、いずれの設定も適用されません。
インポートまたはエクスポートがGUIを介して開始されると、ジョブが作成されます。ジョブ状態は、ジョブキーページで観ることができます。

1. メモ: ホスト名またはIPアドレスのみが送信先アドレスとして受け入れられます。
2. メモ: 特定の場所を参照してサーバ設定ファイルをインポートすることもできます。インポートするサーバ設定ファイルを正確に選択する必要があります。たとえば、import.xmlです。
3. メモ: エクスポートした（選択した）ファイル形式によっては、拡張子が自動的に追加されます。たとえば、
   export_system_config.xmlとします。
4. メモ: SCPは、再起動を最小数に抑えて、1つのジョブで完全な設定を適用します。ただし、システム構成によっては、属性の一部は、デバイスの動作モードを変更したり、新しい属性のサブデバイスを作成したりすることがあります。このようなことが発生した場合、SCPは1つのジョブですべての設定を適用できない場合があります。保留中の構成の設定を解決するには、ジョブのConfigResultエントリを確認します。
SCPを使用すると、1つのxml/jsonファイルで数のシステムにOSの導入(OSD)が行えます。また、構成やリポジトリのアップデートなどの従来の操作の一括処理も可能です。
SCPでは、すべてのIDRACユーザーのSSH公開キーのエクスポートおよびインポートも可能です。すべてのユーザーに関するSSH公開キーは4つ存在します。
SCPを使用したOS展開の手順は次のとおりです。
1. SCPファイルをエクスポートする
2. SCPファイルには、OSDに必要な抑制属性がすべて入っています。
3. OSD属性を編集/アップデートしてから、インポート操作を実行します。
4. このOSD属性は、SCPオーケストレーターによって検証されます。
5. SCPオーケストレーターは、SCPファイルに指定された構成およびリポジトリのアップデートを実行します。
6. 構成とアップデートが完了すると、ホストOSはシャットダウンされます。
7. メモ: OSメディアのホスティングでサポートされているのは、CIFSおよびNFS共有のみです。
SCPオーケストレーターは、選択したオペレーティングシステムのドライバを接続することでOSDを開始し、NFS/共有にあるOSメディアに対して1回限りの起動を開始します。
SCPの使用で、ジョブの進行状況が表示されます。
BIOSによるOSメディアからの起動が行われると、SCPジョブの完了が表示されます。
接続されていたメディアおよびOSメディアは、65535秒またはOSD.1#ExposeDuration属性に指定された期間の経過後、自動的に接続解除されます。

iDRACウェブインタフェースを使用したサーバ設定プロファイイルのインポート
サーバ設定プロファイアルをインポートするには、次の手順を実行します。
1. 設定>サーバ設定プロファイアルに移動します。
   サーバ設定プロファイアルページが表示されます。
2. 次のいずれかを選択して、場所のタイプを指定します。
   - ローカルを選択すると、ローカルドライブに保存された設定ファイルをインポートします。
   - ネットワーク共有を選択すると、CIFSまたはNFS共有から設定ファイルをインポートします。
   - HTTPまたはHTTPSを選択すると、HTTP/HTTPSファイル転送を使用してローカルファイルから設定ファイルをインポートします。
3. インポートコンポーネントオプションにリストされているコンポーネントを選択します。
4. シャットダウンタイプを選択します。
5. 最大待機時間を選択して、インポート完了後にシステムがシャットダウンするまでの待機時間を指定します。
6. インポートをクリックします。

### iDRAC ウェブインタフェースを使用したサーバ設定プロファイルのエクスポート

サーバ設定プロファイルをエクスポートするには、次の手続きを実行します。

1. 設定 > サーバ設定プロファイルに移動します。
2. サーバ設定プロファイルページを表示させます。
3. エクスポートをクリックします。

次のいずれかを選択して、場所のタイプを指定します。

- ローカルを選択すると、設定ファイルはローカルドライブに保存されます。
- ネットワーク共有を選択すると、設定ファイルはCIFSまたはNFS共有に保存されます。
- HTTPまたはHTTPSを選択すると、設定ファイルはHTTP/HTTPSファイル転送を使用してローカルファイルに保存されます。

**メモ**: 場所のタイプに応じて、ネットワーク設定またはHTTP/HTTPS設定を入力する必要があります。HTTP/HTTPS用にプロキシが設定されている場合は、プロキシ設定も必要です。

7. 追加のエクスポートアイテムを選択します。
8. エクスポートをクリックします。

### BIOS 設定またはF2からのセキュアなブート設定

UEFIセキュアブートは、UEFIファームウェアとUEFIオペレーティングシステム（OS）間のハンドオフ中に発生する可能性がある重大なセキュリティの無効を排除するテクノロジーです。UEFIセキュアブートでは、特定の証明書に対してチェーン内の各コンポーネントの検証と承認が行われるか、ロードまたは実行が許可されます。セキュアブートでは、ブートプラットフォームのファームウェア、オプションカード、およびOS BootLoaderのすべての起動ステップを確認し、脅威を排除してソフトウェアIDを提供します。

Unified Extensible Firmware Interface (UEFI)フォーラム：プレブートソフトウェアの基準を整備する業界団体で、UEFI仕様にセキュアブートを定義しています。コンピュータシステムベンダー、拡張カードベンダー、およびオペレーティングシステムプロバイダーが、相互運用性を促進するためにこの仕様に協力しています。UEFIの仕様の一部として、セキュアブートはプレブート環境のセキュリティに関連する業界標準を表しています。

### 使用可能なファイロフォーマット

セキュアブートポリシにはPKに1つのキーだけが含まれていますが、複数のキーがKEKに存在する場合があります。ブートフォームの製造元またはプレブートフォームの所有者のどちらかが、キーパックPKに対応する秘密キーを保持するのが理想的です。サードパーティ（OSプロバイダやデバイスプロバイダなど）は、KEKの公開キーに対応する秘密キーを保持します。この方法では、プレブートフォームの所有者またはサードパーティが、特定のシステムのdbまたはdbxのエントリを追加または削除することができます。

セキュアブートポリシは、dbとdbxを使用して、ブートイメージファイルの実行を許可します。イメージファイルを実行するには、dbではキーまたはハッシュ値に関連付ける必要があり、dbxではキーまたはハッシュ値に関連付けません。dbまたはdbx
の内容をアップデートする際は、プライベート PK または KEK による署名が必要です。PK または KEK の内容をアップデートする際は、プライベート PK による署名が必要です。

表 14. 使用可能なファイルフォーマット

<table>
<thead>
<tr>
<th>ポリシーコンポーネント</th>
<th>使用可能なファイルフォーマット</th>
<th>使用可能なファイル拡張子</th>
<th>最大レコード数</th>
</tr>
</thead>
<tbody>
<tr>
<td>PK</td>
<td>X.509 証明書（バーチャル DER 形式のみ）</td>
<td>.cer</td>
<td>1回</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.der</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>.crt</td>
<td></td>
</tr>
<tr>
<td>KEK</td>
<td>X.509 証明書（バーチャル DER 形式のみ）</td>
<td>.cer</td>
<td>1回以上</td>
</tr>
<tr>
<td></td>
<td>公開キーストア</td>
<td>.der</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>.crt</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>.pbk</td>
<td></td>
</tr>
<tr>
<td>DB および DBX</td>
<td>X.509 証明書（バーチャル DER 形式のみ）</td>
<td>.cer</td>
<td>1回以上</td>
</tr>
<tr>
<td></td>
<td>EFI イメージ（システム BIOS がイメージダイジェストを計算してインポートします）</td>
<td>.der</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>.crt</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>.efi</td>
<td></td>
</tr>
</tbody>
</table>

セキュアブート設定機能にアクセスするには、システム BIOS 設定の下にあるシステムセキュリティをクリックします。システム BIOS 設定に移動するには、POST 中に会社のロゴが表示されたら、F2 キーを押します。

- デフォルトでは、セキュアブートは無効、セキュアブートポリシーは標準に設定されています。セキュアブートポリシーを設定するには、セキュアブートを有効にする必要があります。
- セキュアブートモードが標準に設定されている場合、システムにはデフォルトの証明書、イメージダイジェスト、または工場出荷時のハッシュがあることを示しています。これは、標準のファームウェア、ドライバ、オプション ROM、ブートローダのセキュリティに対応しています。
- サーバーに新しいドライバまたはファームウェアをサポートするには、セキュアブート証明書ストアの DB にそれぞれの証明書を登録する必要があります。したがって、セキュアブートポリシーをカスタムに設定する必要があります。

セキュアブートポリシーがカスタムに設定されている場合は、デフォルトでシステムにロードされている、変更可能な標準の証明書とイメージダイジェストを紹介しています。カスタムに設定されているセキュアブートポリシーでは、表示、エクスポート、インポート、削除、すべて削除、リスト、すべてリストなどの操作を実行できます。これらの操作を使用して、セキュアブートポリシーを設定することができます。

セキュアブートポリシーをカスタムに設定すると、エクスポート、インポート、削除、すべて削除、リスト、すべてリストなどのアクションを使用して、証明書ストアを管理するためのオプションを有効にできます。変更するポリシー（PK/KEK/DB/DBX）を検索し、それぞれのリンクをクリックすると、適切なアクションを実行することができます。各セクションには、インポート、エクスポート、削除、およびリスト操作を実行するためのリンクがあります。設定の時点で適用可能なものに基づいて、リンクが有効になっています。すべて削除およびすべてリストは、すべてのポリシーに影響を与える操作です。すべて削除は、カスタムポリシー内のすべての証明書およびイメージダイジェストを削除し、すべてリストは、標準またはデフォルトの証明書ストアからすべての証明書およびイメージダイジェストを復元します。

BIOS recovery

BIOS recovery 機能を使用すると、格納されたイメージから BIOS を手動でリカバリできます。BIOS は、システムの電源投入時にチェックされ、破損した BIOS または不具合がある BIOS が検出されると、エラーメッセージが表示されます。BIOS のリカバリプロセスは RACADM から開始できます。手動で BIOS をリカバリするには、www.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 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、必要なライセンスをアップデートされているようにしてください。iDRAC でのライセンス可能機能の詳細については、iDRAC ライセンス、p. 22 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 バススルーに設定します。

トピック:

• iDRAC 情報の表示
• ネットワーク設定の変更
• 暗号スイートの選択
• FIPS モード
• サービスの設定
• TLS 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、iDRAC Settings (iDRAC 設定) > Overview (概要) に移動し、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。

iDRAC の詳細情報
- デバイスタイプ
- ハードウェアバージョン
- Firmware Version (ファームウェアバージョン)
- ファームウェアアップデート
- RAC 時間
- IPMI バージョン
- 可能なセッション数
- 現在のセッション数
- IPMI バージョン

iDRAC サービスモジュール
- ステータス

接続ビュー
- 状態
- スイッチ接続 ID
- スイッチポート接続 ID

現在のネットワーク設定
- iDRAC MAC アドレス
- アクティブ NIC インタフェース
- DNS ドメイン名

現在の IPv4 設定
- IPv4 有効
- DHCP
- 現在の IP アドレス
- 現在のサブネットマスク
- 現在のゲートウェイ
- DHCP を使用して DNS サーバアドレスを取得
- 現在の優先 DNS サーバー
- 現在の代替 DNS サーバー

現在の IPv6 設定
- IPv6 有効
- 自動設定
- 現在の IP アドレス
- 現在の IP ゲートウェイ
- リンクのローカルアドレス
- DHCPv6 を使用して DNS を取得する
- 現在の優先 DNS サーバー
- 現在の代替 DNS サーバー
RACADMを使用したiDRAC情報の表示

RACADMを使用してiDRAC情報を表示する場合は、「iDRAC RACADM CLIガイド」は、www.dell.com/idracmanualsにあります。に記載されているgetsysinfoまたはgetサブコマンドの詳細情報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構成した後も、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。

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、iDRAC Settings（iDRAC設定）＞Connectivity（接続）＞Network（ネットワーク）＞Network Settings（ネットワーク設定）の順に移動します。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。

ネットワークページ（ネットワーク設定）でAuto Dedicated NIC（自動専用NIC）を選択した場合、iDRACのNIC選択が共有LOM（1、2、3、または4）になっている場合、iDRAC専用NICでリンクが検出されると、iDRACはNIC選択を変更して専用NICを使用します。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WSMan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。

```bash
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。

```bash
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。

```bash
racadm set iDRAC.Nic.Enable 1
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 にアクセスできるクライアントの IP アドレス範囲を限定します。IP フィルタは、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リクエストはすべて拒否されます。
- 特定 IP アドレスからのログインが繰り返し失敗した場合、事前に選択された期間、そのアドレスからは iDRAC にログインできません。ログインに最大で 2 回失敗すると、30 秒後でないと再度のログインは許可されません。2 回以上ログインに失敗すると、60 秒後でないと再度のログインは許可されません。

memo: この機能は最大 5 つの IP 範囲をサポートします。この機能は、RACADM および Redfish で表示/設定できます。

特定の IP アドレスからのログインが何度か失敗している場合、その回数は内部カウンターによって記録されています。正常にログインできた場合、障害履歴はクリアされ、内部カウンターがリセットされます。

memo: 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 exchange identification: Connection closed by remote host」というメッセージが一部の SSH クライアントに表示されることがあります。

memo: Dell Deployment Toolkit (DTK) を使用する場合は、権限について、『OpenManage Deployment Toolkit ユーザーズガイド』は、www.dell.com/openmanagemanuals にあります。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、iDRAC 設定接続ネットワークネットワーク設定詳細ネットワーク設定の順に移動します。ネットワークページが表示されます。
2. 詳細ネットワーク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 範囲のアドレスと IP 範囲のサブネットマスクを使用して、IP フィルタリング設定を指定します。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。

連邦情報処理標準（FIPS）は、米国政府機関および請負業者で使用される基準一式です。FIPS モードは、FIPS 140-2 レベル 1 の要件を満たすことが意図されています。FIPS の詳細については、「FIPS User Guide for iDRAC, and CMC for non MX platforms」（FIPS iDRAC and CMC 非 MX プラットフォーム用ユーザーズガイド）を参照してください。

memo: FIPS モードを無効にするには、iDRAC をデフォルト設定にリセットする必要があります。

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、着信 IP アドレスと RangeAddr プロパティの両方に適用されます。結果が同一である場合、着信ログインリクエストは iDRAC へのアクセスを許可されます。この範囲に含まれていない IP アドレスからログインすると、エラーが発生します。

memo: IP フィルタリングの構成では、最大 5 つの IP 範囲がサポートされます。

次の式の値がゼロに等しい場合は、ログインに進みます。

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

&

数量のビット積

iDRAC の設定 95
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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。を参照してください。

暗号スイートの選択

暗号スイートの選択により、iDRAC またはクライアント通信に使用される暗号を制限して、通信の安全性の程度を決定することができます。使用されている有効な TLS 暗号スイートについて、異なるレベルのフィルタリングを利用できます。設定には、iDRAC ウェブインタフェース、RACADM、WSMan コマンドラインインタフェースを使用できます。

iDRAC ウェブインタフェースを使用した暗号スイート選択の設定

注意: OpenSSL 暗号コマンドで、文字列の解析に無効な構文を使用すると、予期しないエラーが発生する可能性があります。

メモ: これは、詳細セキュリティオプションです。このオプションを設定する前に、次のような知識が十分にあることを確認してください。

• OpenSSL の暗号文字列の構文とその使用方法。
• 期待と要件に合致する結果を得るために、結果として生じた暗号スイートの設定を有効化するためのツールと手順。

メモ: TLS 暗号スイートの詳細設定を設定する前に、サポートされているウェブブラウザを使用していることを確認します。

カスタムの暗号文字列を追加するには、次の手順を実行します。
1. iDRAC Web インタフェースで、[iDRAC 設定] [ サービス ] [Web サーバー] の順に移動します。
2. カスタム暗号文字列 オプションの下に 暗号文字列選択 をクリックします。
[カスタム暗号文字列の設定] ページが表示されます。
3. [ カスタム暗号文字列] フィールドに有効な文字列を入力し、[ 暗号文字列の設定] をクリックします。

メモ: 暗号文字列の詳細については、www.openssl.org/docs/man1.0.2/man1/ciphers.html を参照してください。

4. 適用 をクリックします。
カスタム暗号文字列を設定すると、現在の iDRAC セッションが終了します。しばらく待ってから、新しい iDRAC セッションを開いてください。

RACADM を使用した暗号スイート選択の設定

RACADM を使用して暗号スイート選択を設定するには、次のコマンドのいずれかを使用してください。

```
· racadm set idrac.webServer.cipherString ALL:!DHE-RSA-AES256-GCM-SHA384:!DHE-RSA-AES256-GCM-SHA256
· racadm set idrac.webServer.cipherString ALL:-DHE-RSA-CAMELLIA256-SHA
```
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ー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こと、iDRAC の全バージョンで検証済みであるわけではないことをご理解ください。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ー構成プロファイル（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 ウェブインタフェースで、iDRAC Settings（iDRAC 設定）＞Connectivity（接続）＞Network（ネットワーク）＞Network Settings（ネットワーク設定）＞Advanced Network Settings（ネットワークの詳細設定）の順に移動します。
2. FIPS モードで、有効を選択して適用をクリックします。

メモ: FIPS モードを有効にすると、iDRAC はデフォルト設定にリセットされます。

メモ: FIPS モードで、iDRAC が FIPS モードで再起動します。iDRAC に再起動するまでに少なくとも 60 秒間待機します。

メモ: 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。

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サーバー
iDRACWebインタフェースへのアクセスを有効にします。Web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サーバーとリモートRACADMを再び有効にします。

SEKM設定
クライアントサーバー-クライアントを使用して、iDRACでセキュアなエントープライズキー管理機能を有効にします。

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。

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。

Redfish
RedfishRESTfulAPIのサポートを有効にします。

VNCサーバー
SSL暗号化あり、または無しでVNCサーバーを有効にします。

Webインタフェースを使用したサービスの設定
iDRACWeb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 Webインタフェースで、[iDRAC設定]＞[サービス]の順に移動します。

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：このページで追加ダイアログを作成しないチェックボックスをオンにしないでください。このオプションを選択すると、サービスを設定できなくなるます。

[iDRAC設定]ページからSEKMを設定できます。[iDRAC設定]、[サービス]、[SEKM設定]の順にクリックします。

メモ：SEKMの設定手順の詳細については、「iDRACオンラインヘルプ」を参照してください。


KeySecureサーバーで[クライアント証明書]セクションの[ユーザーステート名]フィールドの値を変更した場合（[共通名(CN)]を[ユーザーアイデンティファイア(ID)]に変更した場合など）、次の内容を確認してください。

a. 既存のアカウントを使用している場合：

iDRAC SSL証明書で、[ユーザーステート名]フィールド（[共通名]フィールドではなく）とKMSの既存ユーザーネームが一致していることを確認します。一致していない場合、[ユーザーステート名]フィールドの設定、SSL証明書の再生成、KMSへのインストール、iDRACへの再アップロードを順に実行する必要があります。

メモ：この事前設定の詳細については、「iDRACオンラインヘルプ」を参照してください。

b. 新しいユーザーアカウントを使用している場合：

iDRAC SSL証明書の[ユーザーステート名]フィールドが一致していることを確認します。

メモ：この事前設定の詳細については、「iDRACオンラインヘルプ」を参照してください。

Vormetric Data Security ManagerをKMSとして使用する場合は、iDRAC SSL証明書の[共通名(CN)]フィールドが、Vormetric Data Security Managerに追加されたホスト名と一致していることを確認します。そうでない場合、証明書が正常にインストールされないことがあります。

メモ：racadm sekm getstatusを実行して「失敗」と通知された場合、[再キー]オプションは無効になります。
メモ: SEKM は、クライアント証明書の [ユーザー名] キールドに指定された「共通名」、「ユーザー ID」、または「部門名」のみをサポートします。

メモ: サードパーティ CA を iDRAC CSR への署名に使用している場合、サードパーティ CA がクライアント証明書の [ユーザー名] キールドの値に指定された UID をサポートしていることを確認してください。サポートされていない場合、[ユーザー名] キールドの値として共通名を使用してください。

メモ: [ユーザー名] キールドと [パスワード] キールドを使用している場合は、KMS サーバーでそれらの属性がサポートされていることを確認してください。

**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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。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。デフォルトで有効になっています。この設定を有効にするには、iDRAC からログアウトして再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ています。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. iDRAC Settings (iDRAC 設定) > Services (サービス) に移動します。
2. サービス タブをクリックし、Web サービスをクリックします。
3. TLS 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を停止させたとき、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、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、ディスプレイ、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。

2 つの VNC クライアントセッションを同時にアクティブ化することができます。2 つのヒャブは読み取り専用モードです。

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。再生化が無効になっている場合、VNC クライアントは RFB ハンドシェイクを直接開始し、SSL ハンドシェイクは必要ありません。VNC クライアントハンドシェイク (RFB または SSL) 中、別の VNC セッションがアクティブであるか、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。最初のハンドシェイクが完了すると、VNC サーバーは仮想コンソールを無効にし、仮想メディアの読み取り専用モードになります。

VNC セッションが終了すると、VNC サーバーは仮想コンソールの元の状態を復元します (有効または無効)。

メモ:
- VNC セッションの起動中に RFB プロトコルエラーが発生した場合は、VNC クライアント設定を高品質に変更してから、セッションを再起動します。
- iDRAC NIC が共有モードで、ホストシステムの電源を入れ直すと、ネットワーク接続は数秒間失われます。この間、アクティブな VNC クライアントで操作を実行すると、VNC セッションは閉じることがあります。タイムアウト (iDRAC Web...
インターフェイスの [ サービス ] ページの VNC サーバー設定で設定された値）を持ってから、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 60 秒以上最小化されていると、クライアントウィンドウは閉じます。新しい VNC セッショングを開く必要があります。VNC クライアントウィンドウを 60秒以内に最大化すると、引き続き使用できます。

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、Configuration (設定) > Virtual Console (仮想コンソール) の順に移動します。
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。

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 のオブジェクトで set コマンドを使用します。
詳細については、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。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 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。

注: 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。たとえば、127.0.0.1:5930 です。
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。たとえば、192.168.0.120:5901 です。
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 サーバと接続します。iDRAC で VNC サーバーを設定するときに SSL 暗号化オプションが無効になっている場合、VNC ビューアと接続するには、以下の手順を実行します。

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 サーバフィールドに入力します。
的形式は、<iDRAC IP address;VNC port number> です。
たとえば、iDRAC IP アドレスが 192.168.0.120、VNC ポート番号が 5901 の場合は、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IDLEDのみです。

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、Configurations（設定）＞System Settings（システム設定）＞Hardware Settings（ハードウェア設定）＞Front Panel configuration（前面パネル設定）の順に移動します。

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）
   - 資産タグ
   - 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
   - システムのモデル
   - 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）。有効になると、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Live Front Panel Feed（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という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

サーバーの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、「iDRAC RACADM CLIガイド」は、www.dell.com/idracmanualsにあります。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。

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、Configuration (設定) > System Settings (システム設定) > Hardware Settings (ハードウェア設定) > Front Panel configuration (フロントパネル設定) の順に移動します。System ID LED Settings (システムID LED 設定) 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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。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. iDRAC Settings (iDRAC 設定) > Settings (設定) > Time zone and NTP Settings (タイムゾーンおよび NTP 設定) の順に移動します。
   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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。を参照してください。

iDRAC の設定 103
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に、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
- Lifecycle Controller
- BIOS 起動マネージャ
- UEFI デバイスバス
- UEFI HTTP

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。

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. Configuration (設定) > System Settings (システム設定) > Hardware Settings (ハードウェアの設定) > First Boot Device (最初の起動デバイス) に移動します。
   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. 選択されたデバイスから次回の起動時に一回のみ起動するには、Boot Once (一回のみ起動) を選択します。それ以降は、システムはBIOS起動順序の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、「iDRAC RACADM CLIガイド」は、www.dell.com/idracmanualsにあります。参照してくださ。

仮想コンソールを使用した最初の起動デバイスの設定

サーバが起動時のシーケンスを実行する前、サーバが仮想コンソールビューで表示される際に、起動するデバイスを選択できます。

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、「OpenManageインストールガイド」は、www.dell.com/openmanual.htmlにあります。を参照してください。

この機能を使用するホストシステムでは、Windowsオペレーティングシステムが必要です。

メモ:
・この機能は、Linuxシステムには適用されません。
・これはエージェントや属性とは無関係な機能です。

OSからiDRACへのパススルーワ全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LANOnMotherboard(LOM)デバイスがあるサーバでは、OSからiDRACへのパススルーワ全機能を有効にできます。この機能は、共有LOM、専用NIC、またはUSBNIC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、www.dell.com/idracservicemoduleにある「iDRACServiceModuleUser'sGuide」(iDRACサービスモジュールユーザーズガイド)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。ブレードサーバの専用NICは、ChassisManagementController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WSMan(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へのパススルーワ全機能を有効化する前に、少なくとも10秒間待つ必要があります。

RACADM、WSMan、またはRedfishを介してサーバ設定プロファイルを使用してサーバを設定していて、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へのパススルーワ全機能を有効化する、またはOSホストIPアドレスを設定するにあたっては、15秒間待つ必要があります。

OSからiDRACへのパススルーワ全機能を有効化する前に、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へのパススルーワ全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のパススルーワ全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 アドレスと異なる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: USB NIC が無効状態のときに iDRAC サービス シリーズを起動すると、iDRAC サービス モジュールは、USB NIC IP アドレスを 169.254.0.1 に変更します。

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。

メモ: NIC チーニングが有効になっている場合、LOM バススルーを起動するホストサーバから iDRAC にアクセスすることはできません。iDRAC には、iDRAC USB NIC を使用してホストサーバ OS から、または iDRAC 専用 NIC 経由で外部ネットワークからアクセスできます。

OS から iDRAC へのパススルー用の対応カード
次表には、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対応するカードのリストが示されています。

表 15. LOM を使用した OS から iDRAC へのパススルー - 対応カード

<table>
<thead>
<tr>
<th>カテゴリ</th>
<th>製造元</th>
<th>タイプ</th>
</tr>
</thead>
<tbody>
<tr>
<td>NDC</td>
<td>Broadcom</td>
<td>5720 QP rNDC 1G BASE-T</td>
</tr>
<tr>
<td></td>
<td>Intel</td>
<td>x520/350 QP rNDC 1G BASE-T</td>
</tr>
</tbody>
</table>

組込み型 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。

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。

- Server 2012 R2 Foundation Edition
- Server 2012 R2 Essentials Edition
- Server 2012 R2 Standard Edition
- Server 2012 R2 Datacenter Edition
- Server 2012 for Embedded Systems ( Base および R2 w/ SP1 )
- Server 2016 Essentials Edition
- Server 2016 Standard Edition
- Server 2016 Datacenter Edition
- RHEL 7.3
- RHEL 6.9
- SLES 12 SP2
- ESXi 6.0 U3
- vSphere 2016
- XenServer 7.1

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。
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。

メモ: Linux オペレーティングシステムまたは XenServer で USB NIC を DHCP に設定するには、オペレーティングシステムまたは Hypervisor のドキュメントを参照してください。

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、以下の手順を実行します。

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。

```bash
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、esxcfg-vmknic -l コマンドを実行します。

出力はusb0 エントリを表示します。

---

**Web インターフェイスを使用した OS to iDRAC パススルーノの有効化または無効化**

Web インターフェイスを使用して 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. [iDRAC 設定] > [接続] > [ネットワーク] > [OS から iDRAC へのパススルー] に移動します。

OS to iDRAC パススルー ページが表示されます。

2. 状態を有効に変更します。

3. パススルーモードには、次のいずれかのオプションを選択します。

   - 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 パス経由で確立されます。

   **メモ:** パススルーモードを LOM に設定した場合は、次のことを確認します。

   - OS と iDRAC が同じサブネット上にある
   - ネットワーク設定で NIC の選択が LOM に設定されている

4. 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有効化されます。

   **メモ:** VLAN が iDRAC で有効になっている場合は、LOM パススルーは VLAN タグ機能がホストで設定されている共有 LOM モードでのみ機能します。

   **メモ:**
   - LOM がパススルーモードに設定されていると、コールド プート後にホスト OS から iDRAC を起動することはできません。
   - 専用モード機能で、意図的に LOM パススルーを削除してあります。

5. パススルーモードとして USB NIC を選択した場合は、USB NIC の IP アドレスを入力します。

   デフォルト値は 192.168.1.1 です。デフォルトの IP アドレスを使用することをお勧めします。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。

   IP 192.168.4.0 と 192.168.4.0 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。

   **メモ:** IPv6 が望ましい場合、デフォルトのアドレスは fde1:53ba:e9a0:de11::1 です。このアドレスは、必要に応じて idrac.OS-BMC.UsbNicULA 設定で変更できます。IPv6 を USB-NIC で使用したくない場合は、アドレスを「::」に変更することで無効化できます。

6. 適用 をクリックします。

7. 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 グループ内のオブジェクトを使用します。
詳細については、「iDRAC 属性レジストリ」は、www.dell.com/idracmanuals にあります。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。
   - 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 パス経由で確立されます。

   メモ: パススルーモードを LOM に設定した場合は、次のことを確認します。
          • OS と iDRAC が同じサブネット上にある
          • ネットワーク設定で NIC の選択が LOM に設定されている

   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。

4. パススルー設定として USB NIC を選択した場合は、USB NIC の IP アドレスを入力します。
   デフォルト値は 169.254.1.1 です。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。IPv6 は不要です。IPv6 のアドレスは fde1:53ba:e9a0:de11::1: です。このアドレスは、必要に応じて idrac.OS-BMC.UsbNicULA 設定で変更できます。IPv6 を USB-NIC で使用したくない場合は、アドレスを「::」に変更することで無効化できます。

   メモ: IPv6 が望ましい場合、デフォルトのアドレスは fde1:53ba:e9a0:de11::1 です。このようなアドレスは、必要に応じて idrac.OS-BMC.UsbNicULA 設定で変更できます。IPv6 を USB-NIC で使用したくない場合は、アドレスを「::」に変更することで無効化できます。

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16. ログインタイプに基づいた証明書のタイプ

<table>
<thead>
<tr>
<th>ログインタイプ</th>
<th>証明書タイプ</th>
<th>取得方法</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory を使用したシングルサインオン</td>
<td>信頼済み CA 証明書</td>
<td>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。</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ローカルログインタイプまたは Active Directory ユーザーとしてのスマートカードログイン</th>
<th>証明書タイプ</th>
<th>取得方法</th>
</tr>
</thead>
</table>
| 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アカウントを Base64 でエンコードされたファイルとしてエクスポートします。 
信頼済み 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。 |
| 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。 |
| 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。 |

### 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ウェブサーバーが含まれています。SSL 暗号化オプションは、脆弱な暗号を無効にするために用意されています。非対称暗号テクノロジーを基盤とする SSL は、クライアントとサーバ間の通信を認証および暗号化して、ネットワーク全体の盗聴を防止するために広く受け入れられています。

SSL 対応システムは、次のタスクを実行できます。
- SSL 対応クライアントに自らを認証する
- 2 つのシステムに暗号化接続の確立を許可する

**メモ:** SSL 暗号化が 256 ビット以上および 168 ビット以上に設定されている場合、仮想マシン環境 (JVM、IcedTea) に対する暗号化設定には、vConsole のような iDRAC プラグインの使用がそのような高いレベルの暗号化で許可されるように、Unlimited Strength Java Cryptography Extension ポリシーサイズのインストールが必要になる場合があります。ポリシーのインストールの詳細については、Java のマニュアルを参照してください。

iDRAC ウェブサーバーには、デルの自己署名固有的 SSL デジタル証明書がデフォルトで含まれています。デフォルトの SSL 証明書は、よく知られた認証局 (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。認証局は、情報テクノロジー業界において、信頼のおける審査、識別、およびその他の重要なセキュリティ基準の高い水準を満たしていると認識された事業体です。CA の例としては Thawte や VeriSign が挙げられます。CA 署名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。その後、生成した CSR を VeriSign や Thawte などの CA に送信します。CA は、ルート CA または中間 CA となります。CA 署名 SSL 証明書を受信したら、これを 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、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、サポートされるブラウザは、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。

この機能のデフォルト署名証明書に頼らずに、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できます。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と、カスタム署名証明書を使用するすべての iDRAC が信頼
新刊の証明書を自動登録します。この機能を有効にすると、iDRAC Web サーバーの新規の証明書を自動でデプロイすることができる。既存の証明書のみを削除することもできます。自動証明書登録を有効にするときには、Web サーバーの設定を必要とします。

1. iDRAC Web インターフェイスを使用して、新規の証明書を登録します。新規の証明書は、証明書署名要求 (CSR) の生成時に共通名 (CN) の一部としてアスタリスク (*) をサポートします（たとえば、*qa.comや*company.qa.com）。これは、ワイルドカード証明書で呼ばれます。iDRAC ウェブインタフェースでのワイルドカード CSR は、1つの共通名を含む CSR で複数の iDRAC アドレスにアップロードすることできます。すべての iDRAC はサポートされているブラウザによって信頼されます。ワイルドカード証明書をサポートしているブラウザを使用して iDRAC ウェブインタフェースの接続に接続すると、iDRAC はブラウザによって信頼されます。仮想ルータを起動すると、iDRAC はビューワの設定により信頼されます。

新しい証明書署名要求の生成

CSR は、SSL サーバ証明書の認証局 (CA) へのデジタル要求です。SSL サーバ証明書によって、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可能にします。

1. iDRAC Web インターフェイスで、「[iDRAC 設定] > [サービス] > [Web サーバー] > [SSL 証明書]'の順に移動し、「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 の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。新規の CSR は新しい証明書として生成されます。管理ステーションに保存されます。

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、『iDRAC RACADM CLI ガイド』は、www.dell.com/idracmanuals にあります。参照してください。

自動証明書登録

iDRAC では自動証明書登録機能を使用して、Web サーバーで用いられる TLS 証明書の自動インストールと更新を行うことができます。この機能は有効にすると、既存の Web サーバー証明書が新しい証明書に置き換えられます。

メモ
- 自動証明書登録はライセンスが必要な機能で、Datacenter ライセンスが必要です。
- サーバー証明書を発行するには、有効な NDES（ネットワーク デバイス登録サービス）のセットアップが必要です。

自動証明書登録の構成パラメーターは次のとおりです。
- 有効化/無効化
- SCEP サーバー URL
- チャレンジ・パスワード
これらのパラメータの詳細については、iDRACのオンラインヘルプを参照してください。

自動証明書登録のステータスは次のとおりです。

- 登録済み：自動証明書登録が有効になっています。証明書は監視され、有効期限が切れる前に新しい証明書が発行されます。
- 登録中：自動証明書登録が有効になった後の中間状態。
- エラー：iDRAC サーバーで問題が発生しました。
- なし：デフォルト。

自動証明書登録を有効にすると、Web サーバーが再起動され、既存の Web セッションはすべてログアウトされます。

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。

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、iDRAC Settings (iDRAC 設定) > Connectivity (接続) > SSL > SSL certificate (SSL 証明書) の順に移動し、Upload Server Certificate (サーバー証明書のアップロード) を選択して Next (次へ) をクリックします。
2. 証明書アップロードページが表示されます。
3. ファイルパスで参照をクリックして、管理ステーションの証明書を選択します。
4. 適用をクリックします。

証明書アップロードの完成時、証明書が iDRAC に登録されます。

注意: SSL サーバー証明書が iDRAC にアップロードされます。

サードパーティ使用したサーバー証明書のアップロード

SSL サーバー証明書をアップロードするには、sslcertupload コマンドを使用します。詳細については、「iDRAC RACADM CLI レファレンス」を参照してください。

注意: SSL サーバー証明書が iDRAC にアップロードされます。

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. CSR を既知のルート CA に送信します。CA が CSR に署名すると、CSR は証明書として有効になります。
2. リモート racadm sslkeyupload コマンドで、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 コマンドで、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 のリセットを要求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。

注意: 新しい証明書が発行され、リセット中、iDRAC は数分間使用できません。

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。
Web インターフェイスを使用したサーバー証明書の表示

iDRAC ウェブ インターフェイスで、[iDRAC 設定] > [サービス] > [Web サーバー] > [SSL 証明書] の順に移動します。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、「iDRAC RACADM CLI ユーザーズガイド」は、www.dell.com/idracmanuals にあります。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

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

カスタム署名証明書をアップロードして SSL 譼明書に署名することができます。SHA-2 譼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

1. iDRAC ウェブ インター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。
   SSL ページが表示されます。

2. Custom SSL Certificate Signing Certificate (カスタム SSL 証明書署名証明書) で、Upload Signing Certificate (署名証明書のアップロード) 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. Choose File (ファイルの選択) 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、Reset iDRAC (iDRAC をリセット) または iReset iDRAC Later (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。
詳細については、「iDRAC RACADM CLI ユーザーズガイド」は、www.dell.com/idracmanuals にあります。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

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

1. iDRAC ウェブ インター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。
   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。
   選択した場合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

iDRAC ウェブ インターフェースまたは 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。

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

RACADM 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、sslcertdownload サブコマンドを使用します。詳細については、「iDRAC RACADM CLI ユーザーズガイド」は、www.dell.com/idracmanuals にあります。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

1. iDRAC Settings (iDRAC 設定) > Connectivity (接続) > SSL の順に移動します。
   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、Reset iDRAC (iDRAC をリセット) または iReset iDRAC Later (iDRAC を後でリセット) をクリックします。

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 コマンドで iDRAC をリセットします。

詳細については、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。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、同じプロパティで1つまたは複数の iDRAC を設定できます。グループ ID とオブジェクト ID を使用して特定の iDRAC のクエリを実行すると、RACADM は取得した情報から設定ファイルを作成します。他の iDRAC にファイルをインポートして、同様にこれらを設定します。

メモ:
• 設定ファイルには、特定のサーバーに適用される情報が入っています。この情報は、さまざまなオブジェクトグループの下で管理されています。
• 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。

またシステム設定プロファイル (SCP) では、RACADM を使用して複数の iDRAC を設定することもできます。SCP ファイルには、コンポーネント設定情報が入っています。このファイルをターゲットシステムにインポートすると、BIOS、iDRAC、RAID、NIC の設定が適用されます。詳細については、www.dell.com/manuals 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。

```bash
racadm get -f <file_name>.xml -t xml -c iDRAC.Embedded.1
```

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、グルーブ内のある設定プロパティ（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: このファイルは、単純なテキストエディタで編集することをお勧めします。RACADM ユーザーリリースは、ASCII テキストパーサを使用します。何らかの書式設定によってパーサが混乱すると、RACADM データベースが破損す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
```

情報が他の iDRAC にロードされます。set コマンドで、ユーザーやパスワードのデータベースを Server Administrator と同期させます。

4. racadm racreset コマンドで、ターゲットの iDRAC をリセットします。

### 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、これらの設定を表示することができます。この操作を行うには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、iDRAC Settings (iDRAC 設定) > Services (サービス) > Local Configurations (ローカル構成) の順に移動します。

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 構成を実行できません。ただし、IPMI Over LAN は使用できます。
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ー、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。プレードサーバーの場合、FlexAddress またはリモート割り当てアドレス（MX プラットフォームにのみ該当）も表示できます。

トピック:
- 管理下システムの正常性とプロパティの表示
- アセット追跡の設定
- システムインベントリの表示
- センサー情報の表示
- CPU、メモリ、および入出力モジュールのパフォーマンスインデックスの監視
- アイドルサーバーの検出
- GPU（アクセラレータ）の管理
- システムの Fresh Air 対応性のチェック
- 温度の履歴データの表示
- 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
- FlexAddress メザニンカードのファブリック接続の表示
- iDRAC と管理下システム情報の表示
- iDRAC セッションの表示または終了

管理下システムの正常性とプロパティの表示

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ー、センサーの正常性を表示できます。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。プレードサーバーの場合、FlexAddress またはリモート割り当てアドレス（MX プラットフォームにのみ該当）も表示できます。

アセット追跡の設定

iDRAC でのアセット追跡機能を使用すると、サーバーに関連するさまざまな属性を設定できます。これは、取得、保証、サービスなどの情報が含まれます。

アセット追跡を設定するには、次の手順を実行します。

1. iDRAC インターフェイスで [設定] > [アセット追跡] の順に移動します。
2. [カスタムアセットの追加] をクリックして、このページでデフォルトで設定されていない属性を追加します。
3. サーバーアセットのすべての関連情報を入力し、[適用] をクリックします。
4. アセット追跡レポートを表示するには、[詳細] > [アセット追跡] の順に移動します。

システムインベントリの表示

このページには、管理対象システムにインストールされているハードウェアおよびファームウェアコンポーネントの情報が表示されます。これを行うには、iDRAC Web インターフェイスで [システム] > [インベントリ] の順に移動します。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。
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
- バッテリー
- 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
- バッテリー
- 物理ディスク
- 電源ユニット
- NIC
- ファイバチャネル
- 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には、ファームウェアバージョンとリリース日情報の末尾 4 バイトのみが表示されます。たとえばファームウェアバージョンが FLVDL06 の場合、ファームウェアインベントリには DL06 と表示されます。
- Redfish インターフェイスを使用してソフトウェアのインベントリを収集する場合、リリース日情報は、ロールバックをサポートするコンポーネントについてのみ表示されます。

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

メモ: iDRAC ユーザインタフェースでインベントリを取得する（CSIOR）オプションを有効にして、再起動時にシステムインベントリを収集します。しばらく待って iDRAC にログインし、システムインベントリページに移動すると、詳細が表示されます。サーバーにインストールされているハードウェアによっては、情報の表示には 5 分ほど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。

センター情報の表示

次のセンターは、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 ボード 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パー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 — 管理対象システムに搭載された CPU の正常性と状態を示します。また、プロセッサ自動スロットルおよび予測障害をレポートします。

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。

- インターネットサーバー情報の表示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パーの場合のみ利用可能）— 電源装置と電源装置の冗長性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 の冗長性が有効になっている場合は、「IDSDM 冗長性ステータス、IDSDM SD1、IDSDM SD2」という IDSDM センサステータスが表示されます。冗長性が無効になっている場合は、IDSDM SD1のみ表示されます。
- 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 の冗長性が有効になっていて、IDSDM 内 2 枚の SD カードが入っているにもかかわらず、1 枚の SD カードのステータスがオンラインで、もう 1 枚の SD カードのステータスがオフラインになっている場合、IDSDM 内 2 枚の SD カード間の冗長性が復元するには、システムを再起動する必要があります。冗長性が復元されると、IDSDM に入っている両方の SD カードのステータスがオンラインになります。
- IDSDM に存在する 2 枚の 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 の再構築中にホストシステムを再起動すると、iDRAC には IDSDM 情報が表示されなくなります。この問題を解決するには、IDSDM を再構築するか、iDRAC をリセットしてください。

メモ: iDRAC ファームウェアが 3.30.30.30 より以前のバージョンからアップデートされた場合、Server Administrator のプラットフォームイベントフィルターに IDSDM 設定を表示させるには iDRAC をデフォルトにリセットする必要があります。

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 17. Web インタフェイスと RACADM を使用したセンサー情報

<table>
<thead>
<tr>
<th>情報を表示するセンサー</th>
<th>Web インタフェイス使用</th>
<th>RACADM 使用</th>
</tr>
</thead>
<tbody>
<tr>
<td>バッテリー</td>
<td>ダッシュボード &gt; システム正常性 &gt; バッテリー</td>
<td>getsensorinfo コマンドを使用します。</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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。</td>
</tr>
<tr>
<td></td>
<td></td>
<td>詳細については、「『IDRAC RACADM CLI ガイド』」は、www.dell.com/idracmanuals にあります。を参照してください。</td>
</tr>
<tr>
<td>ファン</td>
<td>ダッシュボード &gt; システム正常性 &gt; ファン</td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>ダッシュボード &gt; システム正常性 &gt; CPU</td>
<td></td>
</tr>
<tr>
<td>メモリ</td>
<td>ダッシュボード &gt; システム正常性 &gt; メモリ</td>
<td></td>
</tr>
</tbody>
</table>
表17. Web インターフェイスと RACADM を使用したセンサ情報（続き）

<table>
<thead>
<tr>
<th>情報を表示するセンサ</th>
<th>Web インターフェイス使用</th>
<th>RACADM 使用</th>
</tr>
</thead>
<tbody>
<tr>
<td>イントルージョン</td>
<td>ダッシュボード &gt; システム正常性 &gt; イントルージョン</td>
<td></td>
</tr>
<tr>
<td>電源装置</td>
<td>ハードウェア &gt; 電源装置</td>
<td></td>
</tr>
<tr>
<td>リムーバブルフラッシュメディア</td>
<td>ダッシュボード &gt; システム正常性 &gt; リムーバブルフラッシュメディア</td>
<td></td>
</tr>
<tr>
<td>温度</td>
<td>ダッシュボード &gt; システム正常性 &gt; 電源/温度</td>
<td></td>
</tr>
<tr>
<td>電圧</td>
<td>ダッシュボード &gt; システム正常性 &gt; 電源/温度</td>
<td></td>
</tr>
</tbody>
</table>

CPU、メモリ、および入出力モジュールのパフォーマンスインディックスの監視

デルの第14世代 Dell PowerEdge サーバでは、Intel ME は Compute Usage Per Second（CUPS）機能をサポートしています。CUPS機能は、システムに搭載された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ィックスのリアルタイム監視を行います。Intel MEは帯域外（OB）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使用率インディックスの瞬間的な値も監視します。

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積算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、帯域外システムエンタファ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ィックス値の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積算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** - 各メモリチャネルまたはメモリコンポーネント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、またはそこへ到達する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え慮した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ラ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ラムが存在します。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インデックスが小さい場合、大きい計算ヘッドラムが存在すること、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し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視点を提供することができるため、ライブネットワークデータセンターリ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は瞬間的な値を示します。
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、System(システム）＞Performance(パフォーマンス）に移動します。
- 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インデックスを表示します。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。Reset Historical Peak（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。
- パフォーマンスマトリックスセクション：
  - 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設定または指定します。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。

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CPU、メモリ、入出力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、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、SystemPerfStatisticsサブコマンドを使用します。詳細については、「iDRAC RACADM CLIガイド」を参照してください。

アイドルサーバーの検出

iDRACには、CPU、メモリー、I/Oなどのサーバーコンポーネントのアウトオブバンドのパフォーマンス監視インデックスが表示されます。

サーバーレベルのCUPSインデックスの履歴データは、サーバーが長時間使用されているか、アイドル状態であるかを監視するために使用されます。定義間隔（時間単位）でサーバー利用が一定のしきい値を下回っていると、サーバーはアイドルサーバーとして報告されます。

この機能は、CUPS機能を備えたインテルプラットフォームでのみサポートされています。CUPS機能のないAMDおよびインテルプラットフォームでは、この機能はサポートされていません。

1 メモ:
- この機能にはDatacenterライセンスが必要です。
- アイドルサーバー設定パラメーターの設定を読み取るには、ログイン権限が必要であり、iDRAC設定権限が必要なパラメーターを変更する必要があります。

パラメーターを表示または変更するには、設定＞システム設定の順にアクセスします。

アイドルサーバーの検出は、次のパラメーターに基づいて報告されます。
- アイドルサーバーしきい値（%）- デフォルトで20%に設定されており、0〜50%の間で設定できます。リセット操作をするとき、しきい値が20%に設定されます。
アイドルサーバー スキャン間隔（時間単位） - アイドルサーバーを特定するために、1時間ごとにサンプルが収集される期間です。デフォルトでは240時間に設定されており、1~9000時間の範囲で設定できます。リセット操作をすると、間隔が240時間に設定されます。

- サーバー使用率（%） - 使用率の値は80~100%に設定できます。デフォルト値は80%です。時刻ごとのサンプルの80%が使用率のしきい値を下回ると、アイドルサーバーと見なされます。

RACADM を使用したアイドルサーバー検出パラメーターの変更

```bash
racadm get system.idleServerDetection
```

Redfish を使用したアイドルサーバー検出パラメーターの変更

```url
https://<iDRAC IP>/redfish/v1/Managers/System.Embedded.1/Attributes
```

WSMAN を使用したアイドルサーバー検出パラメーターの変更

```cmd
```

メモ: iDRAC GUI では、属性の表示または変更はサポートされていません。

GPU (アクセラレーター) の管理

Dell PowerEdge サーバーには、グラフィックス プロセッシング ユニット (GPU) が装備されています。GPUの管理により、システムに接続されているさまざまなGPUを表示したり、GPUの電源、温度、およびサーマル情報を監視することができます。

メモ: これはライセンスが必要な機能で、iDRAC Datacenterライセンスでのみ利用できます。

メモ: 内蔵GPUカードのGPUプロパティはリストされず、ステータスは不明とマークされます。

コマンドがデータをフェッチする前に、GPUが準備完了状態になっている必要があります。イベントリの [GPU ステータス]フィールドには、GPUの可用性と、GPUデバイスが応答しているかどうかが表示されます。GPU ステータスが準備完了の場合は [GPU ステータス] に [OK] と表示され、それ以外の場合は、ステータスに [使用不可] と表示されます。

GPUには複数の正常性パラメーターがあり、NVIDIA コントローラの SMBPBIンタフェイスを介して取得できます。この機能は NVIDIA カードに限定されています。以下の正常性パラメーターがGPUデバイスから取得されます。

- 電源
- 温度
- サーマル

メモ: この機能は NVIDIA カードに限定されています。この情報、サーバーがサポートしていてもその他のGPUでは利用できません。PBIでGPUカードをポーリングする間隔は5秒です。

電力消費、GPU タタゲ温度、最小GPU 減速温度、GPU シャットダウン温度、最大メモリー動作温度、最大 GPU 動作温度の各機能を使用するには、ホストシステムに NVIDIA ドライバーがインストールされ、実行中である必要があります。GPU ドライバーバがインストールされていない場合、これらの値は [該当なし]と表示されます。

Linuxでは、カードが使用されていないときはドライバがカードの機能縮小とアンロードを行い、電力を節約します。このような場合、電力消費、GPU タタゲ温度、最小GPU 減速温度、GPU シャットダウン温度、最大メモリー動作温度、最大 GPU 動作温度の各機能は利用できません。アンロードを回避するには、デバイスで持続モードを有効にする必要があります。これを有効にするには、nvidia-smi ソールのコマンド nvidia-smi -pm 1 を使用します。
テレメトリを使用してGPUレポートを生成できます。テレメトリ機能の詳細については、次を参照：テレメトリーストリミング、p.208

メモ: RACADM では、値が空白のデミー GPU エントリが表示される場合があります。これは、iDRAC が GPU デバイスに情報を問い合わせたときにデバイスが応答する準備ができていない場合に発生します。この問題を解決するには、iDRAC でraccrest操作を実行します。

システムの Fresh Air 対応性のチェック

Fresh Air による冷却は、外部から直接使用してデータセンタ内のシステムを冷却します。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°C（113°F）まで）。

メモ: 一部のサーバまたは特定のサーバの設定は、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、[システム] > [概要] > [冷却] > [温度の概要] の順に移動します。
   Temperature overview (温度の概要) ページが表示されます。
2. サーバが 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フレッシュエア温度しきい値を超える周囲温度で動作する時間の割合を、監視することができます。この値は、システムが工場出荷されてから初めて電源投入されたときに設定されます。データ収集は、システム基板の温度センサーやの読み取り値を基に、システムが工場出荷されてから初めて電源投入されたときから開始されます。データ収集は、システムの電源がオンになっている間に収集、表示されます。過去7年間の監視温度を追跡し、保存できます。

メモ: Fresh Air 対応ではないシステムでも、温度履歴を追跡することができます。ただし、しきい値制限と生成されたフレッシュエアに関する警告は、フレッシュエア制限値に基づきます。制限値は、42℃で警告、47℃で重大です。これらの値は、2℃の精度マージンを持った40℃と45℃のフレッシュエア制限値に等価です。

フレッシュエア制限に関連付けられた次の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℃）より高温で動作した時間からなる。システムが警告領域で動作している割合は、過去12ヶ月で10％です。
- 重大領域: システムが温度センサーの重大しきい値（47℃）より高温で動作した時間からなる。システムが重要領域で動作している割合は、過去12ヶ月で1％です。

収集されたデータはグラフ形式で表示され、10%と1%のレベルを追跡できます。記録された温度データは、工場出荷前のもの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働を続けると、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）の場合は、Lifecycleログにイベントが記録され、該当SNMPトラブルが生成されます。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働時間のうち8％以上あった場合
- 重大イベント: 温度が過去12ヶ月に重大しきい値を超過した状態が全稼働時間のうち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働時間のうち0.8％以上あった場合
- 重大イベント: 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働時間のうち1％以上あった場合

追加のイベントを生成するよう、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、p.177」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 Web インターフェースで、[システム] > [概要] > [冷却] > [温度の概要] の順にアクセスします。
   [温度の概要] 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データ」の項を参照してください。

iDRAC と管理下システム情報の表示

121
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、『iDRAC RACADM CLIガイド』は、www.dell.com/idracmanualsにあります。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変更できます。デフォルトの動作にリセットすると、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、次のように実行します。
1. iDRAC Webインタフェースで、システム > 概要 > 冷却 > 温度の概要の順にアクセスします。
2. 温度の概要セクションのシステム基板吸気口温度に、警告しきい値の最小値と最大値を入力します。
   摂氏で値を入力した場合は、システムが華氏の値を自動的に計算して表示します。同様に、華氏で入力した場合は、摂氏で値が表示されます。
3. 適用をクリックします。

値が設定されます。

メモ：デフォルトしきい値への変更は、チャートの範囲が外気制限値のみに対応しているため、履歴データチャートには反映されません。カスタムしきい値超過の警告は、外気しきい値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サーバアドレス、およびDHCPサーバ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。
- iDRAC Settings (iDRAC設定) > Overview (概要) > iDRAC Service Module (DRAC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IPv6DHCP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. System (システム) > Host OS (ホスト OS) > Network Interfaces (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 FGDD 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 FGDD 列から、ネットワークデバイスリンクをクリックします。

Hardware (ハードウェア) > Network Devices (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ジが表示されます。このペジでは、デバイス詳細の表示が可能です。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。

4. アイコンをクリックして、詳細を表示します。

同様に、Hardware (ハードウェア) > Network Devices (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の情報を表示できます。View Host OS Network Interfaces (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マットで表示されます。

/Linux-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利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 コマンドを実行します。詳細については、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals であります。 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、「Chassis Management Controller ユーザーズガイド」は、www.dell.com/omcmanual であります。 を参照してください。

メモ：管理下システムに電源を投入できなくな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。

iDRAC の 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 でアドレス割り当ての MAC アドレスの保存をサポートします。iDRAC が起動時に、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。

- システム詳細 iDRAC の詳細
- システムサーバ WWN/MAC
- iDRAC 設定 > 概要 > 現在のネットワーク設定

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ガ、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、以下の手順を実行します。

1. iDRAC ウェブインタフェースで、iDRAC Settings (iDRAC 設定) > User (ユーザー) > Sessions (セッション) の順に移動します。
   Sessions (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。
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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。を参照してください。
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

Memo: ローカル RACADM のインポートコマンドまたはエクスポートコマンドを正しく機能させるには、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るようしてください。USB ストレージホストを有効にする方法については、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 18. 通信モード—サマリ

<table>
<thead>
<tr>
<th>通信のモード</th>
<th>対応プロトコル</th>
<th>対応コマンド</th>
<th>前提条件</th>
</tr>
</thead>
<tbody>
<tr>
<td>iDRAC ウェブインタフェース</td>
<td>インターネットプロトコル（https）</td>
<td>該当なし</td>
<td>Web サーバ</td>
</tr>
<tr>
<td>ヌルモデム DB9 ブループロトコルを使用したシリアル</td>
<td>シリアルプロトコル</td>
<td>RACADM, SMCLP, IPMI</td>
<td>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</td>
</tr>
<tr>
<td>IPMI シリアルオーバー LAN</td>
<td>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</td>
<td>IPMI</td>
<td>IPMITool がインストール済みで、IPMI シリアルオーバー LAN が有効</td>
</tr>
<tr>
<td>IPMI over LAN</td>
<td>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</td>
<td>IPMI</td>
<td>IPMITool がインストール済みで、IPMI の設定が有効</td>
</tr>
<tr>
<td>リモート RACADM</td>
<td>https</td>
<td>リモート RACADM</td>
<td>リモート RACADM がインストール済みで、有効</td>
</tr>
<tr>
<td>ファームウェア RACADM</td>
<td>SSH, Telnet</td>
<td>ファームウェア RACADM</td>
<td>ファームウェア RACADM がインストール済みで、有効</td>
</tr>
<tr>
<td>ローカル RACADM</td>
<td>IPMI</td>
<td>ローカル RACADM</td>
<td>ローカル RACADM がインストール済み</td>
</tr>
<tr>
<td>リモートサービス ①</td>
<td>WSMan</td>
<td>WinRM（Windows） OpenWSMan（Linux）</td>
<td>WinRM（Windows）または OpenWSMan（Linux） がインストール済み</td>
</tr>
<tr>
<td></td>
<td>Redfish</td>
<td>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</td>
<td>ブラグイン、CURL、Python モジュールがインストール済み</td>
</tr>
</tbody>
</table>

① 詳細については、『Lifecycle Controller ユーザーズ ガイド』は、www.dell.com/idracmanuals にあります。を参照してください。
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、「Chassis Management Controller ユーザーズガイド」は、www.dell.com/cmcmanual にあります。（MX プラットフォームには該当しない）「PowerEdge MX7000 シャーシ向け OME - Modular ユーザーズガイド」は、www.dell.com/openmanagemanuals にあります。（MX プラットフォームに該当する）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。

メモ: ポーレートを変更した場合、vConsole または GUI からサーバー電源を入れ直す必要があります。

メモ: iDRAC シリアル接続認証が無効の場合、ポーレートの変更には iDRAC の racreset が必要です。

3. 次のいずれかを使用して、管理ステーションのターミナルエミュレーションソフトウェアがシリアル接続用に設定されていることを確認します。
   - Xterm の Linux Minicom
   - Hilgraeve の HyperTerminal Private Edition（バージョン 6.3）

管理対象システムの起動プロセスに応じて、POST 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 の場合は SAC、Linux の場合は Linux ターミナルモード画面のように、設定に基づいて表示されます。

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。

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 スerial 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、再起動をクリックします。
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。

126 iDRAC 通信のセットアップ
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、iDRAC Settings (iDRAC 設定) > Network (ネットワーク) > Serial (シリアル) に移動します。
2. シリアル ページが表示されます。
3. 適用をクリックします。

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: これには、ラックおよびタワーサーバー上の iDRAC 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 <username> -p <password> sel get

メモ: デフォルトの iDRAC ユーザー名とパスワードはシステムマニュアルに記載されています。

- 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。このモードでは、限られた数のコマンド（電源制御を含む）と、16 文字の ASCII 文字として入力される未処理の 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 でのオペレーティングシステムの起動順序を表示できます。IPMI ターミナルからログアウトする場合は、[sys pwd -x] を使用します。次に、IPMI ターミナルモードコマンドの例を示します。
  ○ [sys tmode]
  ○ [sys pwd -u root calvin]
  ○ [sys health query -v]
  ○ [18 00 01]
  ○ [sys pwd -x]

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、iDRAC Settings (iDRAC 設定) > Connectivity (接続) > Serial (シリアル) に移動します。
2. IPMI Serial (IPMI シリアル) で、各属性の値を設定します。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。
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 シリアルポートを設定します。

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

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>指定可能な値（bps）</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;baud_rate&gt;</td>
<td>9600、19200、57600、115200</td>
</tr>
</tbody>
</table>

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>
```

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>権限レベル</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;level&gt; = 2</td>
<td>ユーザー</td>
</tr>
<tr>
<td>&lt;level&gt; = 3</td>
<td>オペレータ</td>
</tr>
<tr>
<td>&lt;level&gt; = 4</td>
<td>管理者</td>
</tr>
</tbody>
</table>

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、iDRAC Settings (iDRAC 設定) > Connectivity (接続) > Serial (シリアル) に移動します。
   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
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。

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ログインポータル（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）を使用すると、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管理ネットワーク経由でリダイレクトできます。SOLを使用して以下を行うことができます。

• 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EmergencyManagementServices（EMS）またはSpecialAdministratorConsole（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。

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
   • ウエブレセーフポーレート — 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Redirection After Boot（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、iDRAC Settings(iDRAC設定)→Connectivity(接続)→Serial Over LAN(シリアルオーバーLAN)に移動します。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。
3. iDRAC SOL設定が設定されます。
4. 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。
5. 各属性の値を指定し、適用をクリックします。
   - iDRAC 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。

   ```bash
   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。

   ```bash
   racadm set iDRAC.IPMISol.MinPrivilege <level>
   ```
<table>
<thead>
<tr>
<th>パラメータ</th>
<th>権限レベル</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;level&gt; = 2</td>
<td>ユーザー</td>
</tr>
<tr>
<td>&lt;level&gt; = 3</td>
<td>オペレーター</td>
</tr>
<tr>
<td>&lt;level&gt; = 4</td>
<td>管理者</td>
</tr>
</tbody>
</table>

メモ: IMPI SOL をアクティブにするには、IMPI SOL で定義された最小特権が必要です。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 IMPI SOL のポーレートをアップデートします。

```bash
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 ポーレートが管理下システムのポーレートと同じであることを確認してください。

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;baud_rate&gt;</td>
<td>指定可能な値 (bps)</td>
</tr>
<tr>
<td>9600</td>
<td></td>
</tr>
<tr>
<td>19200</td>
<td></td>
</tr>
<tr>
<td>57600</td>
<td></td>
</tr>
<tr>
<td>115200</td>
<td></td>
</tr>
</tbody>
</table>

4. コマンドを使用して SOL を有効にします。

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

メモ: シリアルコンソールを LAN 経由でリダイレクトするには、SOL ポーレートが管理下システムのポ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、iDRAC Settings (iDRAC 設定) > Services (サービス) の順に移動し、SSH または Telnet に対しても Enabled (有効) を選択します。

IPMI を有効にするには、iDRAC Settings (iDRAC 設定) > Connectivity (接続) の順に移動し、IMPI Settings (IMPI 設定) 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

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

- SSH

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

SSH ポートを変更するには

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

次のようなソールを使用できます。
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、認証された認証、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 への RMCP+ 接続は、暗号化キーを使用して暗号化する必要があります（キーベースのキー）。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、暗号化キーを設定できます。

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。

1. 必要に応じて、iDRAC に SSH サービスを選択して、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。
   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。

      ```bash
      ipmitool -H <iDRAC-ip-address> -l 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。

SSH または Telnet プロトコルを使用した SOL

SSH または 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。これからのインタフェースのいずれかを介して、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 は Telnet よりもセキュリティが強化されています。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、これがデフォルトで有効になっています。iDRAC は同時に、最大 2〜4 の SSH セッションと 2 つの Telnet セッションをサポートします。Telnet はセキュアプロトコルではないため、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ラな場合にのみ使用するようにしてください。

SSH または Telnet を使用してiDRAC と通信する前には、次の作業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。

Windows での PuTTY からの SOL の使用

1. 必要に応じて、iDRAC Settings（iDRAC 設定）> Services（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 iDRAC を開始するには、次の手順を実行します。

1. 以下を入力します。
   ```
   putty.exe [-ssh | -telnet] <login name>@<iDRAC-ip-address> <port number>
   ```

   メモ: ボート番号はオプションです。ボ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。

   Windows では、ポートの再割り当て後に、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。SOI セッションを終了し、ターミナルを開じて、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。

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。

1. 必要に応じて、iDRAC Setting（iDRAC 設定）> Services（サービス）で、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> <login name>
   - Telnet の場合: telnet <iDRAC-ip-address>

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を利用できなくなります。エスケープキーを正しく実行し、iDRAC コマンドラインコンソールを開きます。エスケープキーは、SOL セッションが接続されるとすぐに画面にも表示されます。管理下システムがオフの場合、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。サーバー再起動して接続を確立します。com2コマンドは、キーボードからの入力またはコンソール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。

**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＞リモートサーバーの種類＞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、アプリケーションを25行×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>
```

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;IP address&gt;</td>
<td>IDRAのIPアドレスです</td>
</tr>
<tr>
<td>&lt;port number&gt;</td>
<td>Telnetのポート番号です（新しいポートを使用している場合）</td>
</tr>
</tbody>
</table>

**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をエコーディングする場合があります。ただし、ほとんどのMicrosoftおよびLinuxTelnetクライアントは、<Backspace>キーを使用するように設定できます。

LinuxTelnet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。

MicrosoftTelnetクライアントで<Backspace>キーを使う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>+<c>`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セッションが終了します。
- LinuxでTelnetからのSOLセッションを終了するには、<Ctrl>+<c>を長押しします。
  
  Telnetプロンプトが表示されます。`quit`と入力して、Telnetを終了します。

ユーティリティでの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、「iDRAC Settings（iDRAC設定）＞Connectivity（接続）＞Serial Over LAN（シリアルオーバーLAN）」を選択し、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 サーバと通信することができません。

**メモ**: IPMI は Linux 基幹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

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

**メモ**: IPMI は Linux 基幹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。

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

1. iDRAC 設定ユーティリティで、iDRAC Settings (iDRAC 設定) > Connectivity (接続) 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。

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**: この設定で、LAN インタフェース経由での IPMI を使用して実行される IPMI コマンドを決定します。詳細については、intel.com にある IPMI 2.0 の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>
```

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>権限レベル</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;level&gt; = 2</td>
<td>ユーザー</td>
</tr>
<tr>
<td>&lt;level&gt; = 3</td>
<td>オペレータ</td>
</tr>
<tr>
<td>&lt;level&gt; = 4</td>
<td>管理者</td>
</tr>
</tbody>
</table>

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>
```

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;key&gt;</td>
<td>有効な 16 進形式の 20 文字の暗号化キー</td>
</tr>
</tbody>
</table>
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、iDRAC Settings (DRAC 設定) > Services (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: ローカル RACADM またはファームウェア RACADM を使用して、これらのコマンドを実行することを推奨します。

- 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。無効にするには、「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」、p.114 を参照してください。

管理下システムでの IPMI の有効化

管理対象システムで、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、『OpenManage Server Administrator ユーザーズ ガイド』、www.dell.com/openmanagemanuals を参照してください。

RHEL 6 での起動中の 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。
   ```bash
   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。
   ```bash
   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。

```bash
# 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/sdal hd=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/sdal 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。
   ```bash
   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:** プロトローグ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 Redirection After Boot (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。

```bash
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.
s1:sysinit:/etc/rc.d/rc.sysinit
10:0:wait:/etc/rc.d/rc 0
11:1:wait:/etc/rc.d/rc 1
12:2:wait:/etc/rc.d/rc 2
13:3:wait:/etc/rc.d/rc 3
14:4:wait:/etc/rc.d/rc 4
15:5:wait:/etc/rc.d/rc 5
16:6: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。

```
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
```

メモ: IPMIツールを使用するシリアルコンソールでは、ブレーキキーチェーン (~B) を使用して、Linux Magic SysRq キー命令を実行します。
RHEL 7 でのシリアルターミナルの設定

RHEL 7 でシリアルターミナルを設定するには:

1. /etc/default/grub に次の行を追加または更新します。

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8"
   GRUB_TERMINAL="console serial"
   GRUB_SERIAL_COMMAND="serial --speed=115200 --unit=0 --word=8 --parity=no --stop=1"
   ```

   GRUB_CMDLINE_LINUX_DEFAULT は、この設定をデフォルトのメニュー項目のみに適用し、GRUB_CMDLINE_LINUX を
   使用してすべてのメニュー項目に適用します。

   各行は、/etc/default/grub 内に1回だけ存在します。その行がすでに存在する場合は、変更して別のコピーを回避しま
   す。そのため、GRUB_CMDLINE_LINUX_DEFAULT は、1行だけ許可されています。

2. 次のように grub2-mkconfig -o コマンドを実行して /boot/grub2/grub.cfg 設定ファイルを再構築します。
   - BIOS ベースのシステムの場合:
     ```
     ~]# grub2-mkconfig -o /boot/grub2/grub.cfg
     ```
   - UEFI ベースのシステムの場合:
     ```
     ~]# grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
     ```

詳細に関しては、redhat.com にある RHEL 7 のシステム管理者ガイドを参照してください。

シリアルコンソールからの GRUB の制御

VGA コンソールではなく、シリアルコンソールを使用するように GRUB を設定できます。これにより、起動プロセスを中断し、
別カーネルを選択したり、カーネルのパラメータを追加したりできます。たとえば、シングルユーザーモードで起動します。
シリアルコンソールを使用するように GRUB を設定するには、スプラッシュイメージをコメントアウトし、grub.conf に serial と terminal のオプションを追加します。

```bash
[root@localhost ~]# cat /boot/grub/grub.conf
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You have a /boot partition. This means that
# all kernel and initrd paths are relative to /boot/, eg.
#
# root (hd0,0)
#
# kernel /vmlinuz-version ro root=/dev/hda2
#
# initrd/initrd-version.img
#
#boot=/dev/hda

default=0
timeout=10

#splashimage=(hd0,0)/grub/splash.xpm.gz
serial --unit=0 --speed=115200
```

メモ: 設定を有効にするためにシステムを再起動します。

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 19. SSH 暗号化スキーム

<table>
<thead>
<tr>
<th>スキームの種類</th>
<th>アルゴリズム</th>
</tr>
</thead>
<tbody>
<tr>
<td>非対称暗号化</td>
<td>ssh-rsa</td>
</tr>
<tr>
<td></td>
<td>ecdsa-sha2-nistp256</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>対称暗号化</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>キー交換</td>
<td><a href="mailto:curve25519-sha256@libssh.org">curve25519-sha256@libssh.org</a></td>
</tr>
<tr>
<td></td>
<td>ecdh-sha2-nistp256</td>
</tr>
<tr>
<td></td>
<td>ecdh-sha2-nistp384</td>
</tr>
<tr>
<td></td>
<td>ecdh-sha2-nistp521</td>
</tr>
<tr>
<td></td>
<td>diffie-hellman-group-exchange-sha256</td>
</tr>
</tbody>
</table>

iDRAC 通信のセットアップ
### 表 19. SSH 暗号化スキーム（続き）

<table>
<thead>
<tr>
<th>スキームの種類</th>
<th>アルゴリズム</th>
</tr>
</thead>
<tbody>
<tr>
<td>暗号化</td>
<td>diffie-hellman-group14-sha1</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:chacha20-poly1305@openssh.com">chacha20-poly1305@openssh.com</a></td>
</tr>
<tr>
<td></td>
<td>aes128-ctr</td>
</tr>
<tr>
<td></td>
<td>aes192-ctr</td>
</tr>
<tr>
<td></td>
<td>aes256-ctr</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:aes128-gcm@openssh.com">aes128-gcm@openssh.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:aes256-gcm@openssh.com">aes256-gcm@openssh.com</a></td>
</tr>
<tr>
<td>MAC</td>
<td>hmac-sha1</td>
</tr>
<tr>
<td></td>
<td>hmac-ripemd160</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:umac-64@openssh.com">umac-64@openssh.com</a></td>
</tr>
<tr>
<td>Compression (圧縮)</td>
<td>なし</td>
</tr>
</tbody>
</table>

**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 経由の公開キー認証 (PKA) をサポートします。これは、ライセンス付きの機能です。SSH 経由の PKA を正しくセットアップして使用すると、iDRAC にログインする際にユーザー名の入力が求められます。これは、さまざまな機能を実行する自動化スクリプトをセットアップする場合に役立ちます。アップロードされるキーは、RFC 4716 または OpenSSH 形式である必要があります。これ以外の場合は、キーを RFC 4716 または OpenSSH 形式に変換する必要があります。

どのシナリオでも、秘密キーと公開キーのペアを管理ステーションで生成する必要があります。管理ステーションと iDRAC 間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:** この権限は、通常、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用に予約されています。ただし、「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可能。この特権を持つユーザーは、あらゆるユーザー設定を変更できます。これには、ユーザーの作成や削除、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、「ユーザーセットアップ」ユーザーコントロールに基づいています。この権限により、ユーザーは他のユーザーの SSH キー設定できます。この権限は慎重に割り当てることが重要。

### 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。このビット数は 2048 ~ 4096 ビットにすることがあります。
3. 生成をクリックし、指示に従ってマウスボ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. キーの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ペ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

```bash
ssh-keygen -t rsa -b 2048 -C testing
```

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ます。キー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つまで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。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、iDRAC Settings (iDRAC 設定) > Users (ユーザー) > Local Users (ローカルユーザー) の順に移動します。
2. Local Groups (ローカルグループ) ページが表示されます。
3. ユーザー ID 列で、ユーザー ID 番号をクリックします。
4. 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。
5. SSH キーのアップロードページが表示されます。
6. 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。
7. 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:
  ```bash
  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:
  ```bash
  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。

```bash
$ 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、iDRAC Settings (iDRAC 設定) > User (ユーザー) の順に移動します。
2. ユーザー ID 列で、ユーザー ID 番号をクリックします。
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。

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、iDRAC Settings (iDRAC 設定) > User (ユーザー) の順に移動します。
2. ID 列で、ユーザー ID 番号を選択し、Edit (編集) をクリックします。
3. SSH Key Configurations (SSH キー設定) で、SSH キーを選択し、Edit (編集) をクリックします。
   SSH Key (SSH キー) ページには、Edit From (編集元) の詳細が表示されます。
4. 削除するキーに対して Remove (削除) を選択し、Apply (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 to 16> -d -k <1 to 4>
- すべてのキー - racadm sshpkauth -i <2 to 16> -d -k all
ユーザーアカウントと権限の設定

特定の権限（役割ベースの認証）を持つユーザーアカウントをセットアップすることで、iDRACを用いたシステムの管理およびシステムセキュリティの維持ができます。デフォルトでのiDRACの構成は、ローカル管理者アカウントで行われます。デフォルトのiDRACユーザー名とパスワードは、システムバッジで提供されます。管理に必要なユーザーアカウントのセットアップでは、他のユーザーがiDRACにアクセスできるように設定できます。詳細については、サーバーのドキュメントを参照してください。

ローカルユーザーのセットアップおよび、Microsoft Active DirectoryやLDAPなどのディレクトリサービスを使用したユーザーアカウントのセットアップも行えます。ディレクトリサービスを使用することで、認証されたユーザーアカウントの一元的な管理ができます。

iDRACでは、関連した権限セットに基づいた役割ベースのユーザーアクセスがサポートされています。役割には、「管理者」、「オペレーター」、「読み取り専用」、「なし」があります。この役割によって、各自の使用可能な最大権限が定義されます。

トピック:
- iDRACユーザーの役割と特権
- ユーザーの設定
- 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

### iDRACユーザーの役割と特権

iDRACの役割名と特権名は前の世代のサーバから変更しました。役割名は次のとおりです。

<table>
<thead>
<tr>
<th>表20. iDRACの役割</th>
<th>現在の世代</th>
<th>以前の世代</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>システム管理者</td>
<td>システム管理者</td>
<td>ログイン、設定、ユーザーの設定、ログ、システム制御、仮想コントールへのアクセス、仮想メディアへのアクセス、システム操作、デバッグ</td>
<td></td>
</tr>
<tr>
<td>オペレーター</td>
<td>電力ユーザー</td>
<td>ログイン、設定、システム制御、仮想コントールへのアクセス、仮想メディアへのアクセス、システム操作、デバッグ</td>
<td></td>
</tr>
<tr>
<td>読み取り専用</td>
<td>ゲストユーザー</td>
<td>ログイン</td>
<td></td>
</tr>
<tr>
<td>なし</td>
<td>なし</td>
<td>なし</td>
<td></td>
</tr>
</tbody>
</table>

次の表では、ユーザーログインについて説明します。

<table>
<thead>
<tr>
<th>表21. iDRACユーザーログイン</th>
<th>現在の世代</th>
<th>以前の世代</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>ログイン</td>
<td>IDRACへのログイン</td>
<td>ユーザーによるiDRACへのログインを可能にします。</td>
<td></td>
</tr>
<tr>
<td>設定</td>
<td>IDRACの設定</td>
<td>ユーザーによるiDRACの設定を可能にします。この権限を持つユーザーは、電源管理、仮想コントロール、仮想メディア、ライセンス、システム設定、ストレージデバイス、BIOS設定、SCPなどを設定することもできます。</td>
<td></td>
</tr>
</tbody>
</table>

**メモ**：管理者の役割は、BIOSセットアップパスワードなどの他のコンポーネントのすべての権限を上書きします。

| 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。 |

144 ユーザーアカウントと権限の設定
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。

### メモ
パスワードには、大文字と小文字、数字、特殊文字を1文字ずつ含める必要があります。

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:

<table>
<thead>
<tr>
<th>文字</th>
<th>長さ</th>
</tr>
</thead>
<tbody>
<tr>
<td>0～9</td>
<td>1～16</td>
</tr>
<tr>
<td>A～Z</td>
<td></td>
</tr>
<tr>
<td>a～z</td>
<td></td>
</tr>
<tr>
<td>- !#$%&amp;()*:/?@[]^_`{</td>
<td>}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>文字</th>
<th>長さ</th>
</tr>
</thead>
<tbody>
<tr>
<td>0～9</td>
<td>1～40</td>
</tr>
<tr>
<td>A～Z</td>
<td></td>
</tr>
<tr>
<td>a～z</td>
<td></td>
</tr>
<tr>
<td>- !#$%&amp;()*:/?@[]^_`{</td>
<td>}</td>
</tr>
</tbody>
</table>

### メモ
その他の文字を含むユーザー名とパスワードも作成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に、ここに記載されている文字のみを使用することをお勧めします。

### メモ
ネットワーク共有のユーザー名とパスワードに許可される文字は、ネットワーク共有のタイプによって定義されます。
iDRACでは、共有のタイプによって定義されるネットワーク共有資格情報の有効な文字をサポートします。ただし、<、>、(コンマ)を除きます。

### メモ
セキュリティを向上させるため、小文字の英字、大文字の英字、数字、特殊文字を含んだ、8文字以上の複雑なパスワードを使用することをお勧めします。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。

ユーザーaカウントと権限の設定 145
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 ユーザを追加し、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、iDRAC Settings（iDRAC 設定）> User（ユーザー）の順に移動します。
   Local Groups（ローカルグループ）ページが表示されます。
2. ユーザー ID 列で、ユーザー ID 番号を選択し、Edit（編集）をクリックします。
   メモ: ユーザー ID 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。
3. User Configuration（ユーザー設定）ページが表示されます。
4. User Account Settings（ユーザーアカウントの設定）と Advanced Settings（詳細設定）に詳細情報を追加してユーザーアカウントを設定します。
   メモ: ユーザー ID を有効にして、そのユーザーのユーザ名、パスワード、およびユーザー役割（アクセス権限）を指定します。LAN 特権レベル、シリアルポート特権レベル、シリアルオーバー LAN ステータス、SNMPv3 認証、認証タイプ、およびユーザーのプライバシーレベル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. Save（保存）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
RACADM を使用して単一または複数の iDRAC ユーザを設定できます。

同様設定で複数の iDRAC ユーザを設定するには、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batchファイルを作成し、各管理下システムでbatchファイルを実行します。
・ iDRAC 設定ファイルを作成し、同様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。

新しい iDRAC を設定する場合またはracadm racresetcfg コマンドを使用した場合は、システムパッケージに記載されたデフォルトの iDRAC ユーザー名とパスワードを確認してください。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: 時間の経過とともに、ユーザーの有効/無効を切り替えることができます。その結果、ユーザーには、各 iDRAC で異なる索引番号が割り当てられ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。

```bash
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、その索引番号が使用されています。

メモ: ユーザーは

```bash
racadm get -f <myfile.cfg>
```
ファイルを表示または編集できます。このファイルにはすべての iDRAC 設定パラメーターが含まれています。

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。
   ```bash
racadm set iDRAC.users.<index>.username <user_name>
```

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;index&gt;</td>
<td>ユーザー固有のインデックス</td>
</tr>
<tr>
<td>&lt;user_name&gt;</td>
<td>ユーザー名</td>
</tr>
</tbody>
</table>

2. パスワードを設定します。
   ```bash
   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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。を参照してください。

4. ユーザーを有効にします。
   ```bash
   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。
```bash
racadm get idrac.users.<index>
```
詳細については、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。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。
   ```bash
   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。
   ```bash
   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、これはユーザーの権限が有効になっていないことを示します。特定のユーザー権限に対して有効なビットマスク値のリストについては、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。を参照してください。
Active Directory ユーザーの設定

会社で Microsoft Active Directory 軟体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、ライセンス付きの機能です。

Active Directory を介してユーザー認証を設定して、iDRAC にログインできます。また、ロールベースの権限を付与することで、管理者は各ユーザーに特定の権限を設定することもできます。

Memo: MX テンプレートを介して行われたすべての導入においてテンプレート内で CA 検証が有効になっている場合は、ユーザーニによる CA 証明書のアップロードを、最初のログイン時または、認証サービスを LDAP から Active Directory に（またはその逆）変更する前に実施する必要があります。

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、次の確認を行ってください。

- Active Directory インフラストラクチャが展開済み。詳細については、Microsoft 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 へのセキュリティ認証を行います。詳細については、Microsoft のウェブサイトを参照してください。
- すべてのドメインコントローラで認証するために、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。

ドメインコントローラでの SSL の有効化

IDRAC は、Active Directory のドメインコントローラでユーザーを認証すると、そのドメインコントローラと SSL セッションを開始します。このとき、ドメインコントローラは認証局 (CA) によって署名された証明書を公開する必要があり、そのルート証明書は IDRAC へもアップロードされます。IDRAC が在籍のドメインコントローラ (ルートドメインコントローラまたは子ドメインコントローラに関係なく) を認証するにあたっては、そのドメインコントローラにはドメインの CA によって署名された SSL 対応の証明書が必要です。

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。

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. スタート > 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。
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

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] (または [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. スタートアドオンスナップイン 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ンドウで次へを選択し、いいえ、秘密キーはエクスポートしないを選択します。
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)を選ぶ。
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：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 1 -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選択するか、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上さまざまな権限レベルを持つユーザーアクセスを設定できる最大限の柔軟性が実現します。

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

Active Directory では、1つの標準グループ オブジェクトが1つの役割グループとして使用されます。iDRAC のアクセス権を持つユーザーは、役割グループのメンバになります。このユーザーに特定の iDRAC へのアクセス権を与えるには、役割グループ名およびそのドメイン名を、当該 iDRAC で設定する必要があります。役割と権限レベルの定義は、Active Directory ではなく個々の iDRAC で行います。各 iDRAC には最大 15 の役割グループを設定できます。表に記載された番号は、デフォルトの役割グループの権限を示します。

表 24. デフォルトの役割グループ権限

<table>
<thead>
<tr>
<th>役割グループ</th>
<th>デフォルトの権限レベル</th>
<th>許可する権限</th>
<th>ビットマスク</th>
</tr>
</thead>
<tbody>
<tr>
<td>役割グループ 1</td>
<td>なし</td>
<td>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</td>
<td>0x0000001ff</td>
</tr>
<tr>
<td>役割グループ 2</td>
<td>なし</td>
<td>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</td>
<td>0x000000f9</td>
</tr>
<tr>
<td>役割グループ 3</td>
<td>なし</td>
<td>iDRAC へのログイン</td>
<td>0x00000001</td>
</tr>
<tr>
<td>役割グループ 4</td>
<td>なし</td>
<td>権限の割り当てなし</td>
<td>0x00000000</td>
</tr>
<tr>
<td>役割グループ 5</td>
<td>なし</td>
<td>権限の割り当てなし</td>
<td>0x00000000</td>
</tr>
</tbody>
</table>

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

標準スキーマ Active Directory を設定する前に、次のことを確認します。

- iDRAC Enterprise のライセンスを所有している。
- 設定はドメインコントローラとして使用されているサーバで実行されている。
- サーバの日、時刻、およびタイムゾーンが正しい。
- iDRAC ネットワーク設定が設定されているか、iDRAC ウェブインタフェースで iDRAC 設定 > 接続方法 > ネットワーク > 共通設定の順に移動して、ネットワーク設定を設定する。

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. iDRAC グループとユーザーを作成します。
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。

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、iDRAC Settings（iDRAC 設定）> User（ユーザー）> Directory Services（ディレクトリサービス）の順に移動します。
   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、Edit（編集）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。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。そのため、ネットワーク設定で DNS を正しく設定する必要があります。
5. Next（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 からの認証を待機する時間を指定します。
   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 iDRAC Settings（iDRAC 設定）> Network（ネットワーク）で確認してください。
7. Next（次へ）をクリックします。Active Directory Configuration and Management Step 3 of 4（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は、ユーザーアカウントと役割グループが異なるドメインにある標準スキーマの場合のみ必要です。複数のドメインにある場合は、ユニバーサルグループのみを使用できます。
- 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 Overview (概要) > iDRAC Settings (iDRAC 設定) > Network (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 1 -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化している場合は、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。

拡張スキーマは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、属性とクラスの分散データベースです。Active Directory スキーマには、データベースに追加または含めることができるデータのタイプを決定する規則が含まれています。データベースに格納されているクラスの1つの例がユーザーグループで、ユーザーのクラスの属性の例には、ユーザーの名、姓、電話番号などがあります。特定の要件に合わせて独自の属性やクラスを追加することで、Active Directory データベースを拡張できます。Dell では、Active Directory を使用したリモート管理の認証と承認をサポートするのに必要な変更を含むように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を保持するために、Microsoft は Active Directory オブジェクト識別子（OID）のデータベースを保持しているため、企業がスキーマに拡張機能を追加したときに、それらが固有で互いに競合しないことが保証されます。Microsoft の Active Directory でスキーマ拡張するためには、Dell はディレクトリサービスに追加される属性とクラスに対して、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 to 12079

iDRAC スキーマ拡張の概要

スキーマは、Association（関連づけ）、Device（デバイス）および Privilege（権限）のプロパティを含むよう、拡張されていま
す。Association（関連づけ）プロパティは、1つまたは複数のiDRAC デバイスに特定の権限セットを持つユーザーまたはグループをリンクするために使用されます。このモデルは、管理者が、ネットワーク上のユーザー、iDRAC 権限、iDRAC デバイスの様々なコンピューションについて、複雑な手間を要することなく最大限の柔軟性を提供します。

認証と許可のための Active Directory に統合するネットワーク上の各物理iDRAC デバイスには、少なくとも1つの関連オブジェクトと1つ以上のiDRAC デバイスに特定の権限セットを持つユーザーまたはグループをリンクするために使用されます。このモデルは、管理者が、ネットワーク上のユーザー、iDRAC 権限、iDRAC デバイスの様々なコンピューションについて、複雑な手間を要することなく最大限の柔軟性を提供します。

ただし、iDRAC オブジェクト（または、ユーザー、ユーザーグループ、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できません。この例では、管理者が必要に応じてiDRAC 権限で各ユーザーの権限をコントロールできます。

iDRAC デバイスオブジェクトは、認証と許可を Active Directory に照会するための 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る際に、ユーザーが Active Directory で認証と許可を実行できるように、管理者はiDRAC とそのデバイスオブジェクトを Active Directory 名で設定する必要があります。さらに、管理者は、ユーザーが認証できるように、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、認証と許可を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絡します。

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絡しません。

任意のドメインのユーザー、ユーザーグループ、またはネッ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。拡張スキーマリビジョンは、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を蓄積します。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。

Active Directory スキーマの拡張

Active Directory スキーマを拡張すると、Active Directory ユーザーとコンピュータスナップインに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ー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: この製品のスキーマ拡張は、以前の世代と異なります。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ユーティリティを正常に機能させるために、このファイルの名前は変更しないでください。

1. ようこそ画面で、次へをクリックします。
2. 警告を読み、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って選択するか、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。

スキーマ拡張が完了します。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、p.156が存在することを確認します。MMCおよび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、Microsoftのマニュアルを参照してください。
クラスと属性

表 25. Active Directory スキーマに追加されたクラスのクラス定義

<table>
<thead>
<tr>
<th>クラス名</th>
<th>割り当てられたオブジェクト識別番号 (OID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>delliDRACDevice</td>
<td>1.2.840.113556.1.8000.1280.1.7.1.1</td>
</tr>
<tr>
<td>delliDRACAssociation</td>
<td>1.2.840.113556.1.8000.1280.1.7.1.2</td>
</tr>
<tr>
<td>delliRAC4Privileges</td>
<td>1.2.840.113556.1.8000.1280.1.1.1.3</td>
</tr>
<tr>
<td>delliPrivileges</td>
<td>1.2.840.113556.1.8000.1280.1.1.1.4</td>
</tr>
<tr>
<td>delliProduct</td>
<td>1.2.840.113556.1.8000.1280.1.1.1.5</td>
</tr>
</tbody>
</table>

表 26. DelliDRACdevice クラス

<table>
<thead>
<tr>
<th>OID</th>
<th>1.2.840.113556.1.8000.1280.1.7.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>説明</td>
<td>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。</td>
</tr>
<tr>
<td>クラスの種類</td>
<td>構造体クラス</td>
</tr>
<tr>
<td>SuperClasses</td>
<td>delliProduct</td>
</tr>
<tr>
<td>属性</td>
<td>delliSchemaVersion</td>
</tr>
<tr>
<td></td>
<td>delliRacType</td>
</tr>
</tbody>
</table>

表 27. delliDRACAssociationObject クラス

<table>
<thead>
<tr>
<th>OID</th>
<th>1.2.840.113556.1.8000.1280.1.7.1.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>説明</td>
<td>Dell 関連オブジェクトを表します。この関連オブジェクトは、ユーザーとデバイス間の接続を行います。</td>
</tr>
<tr>
<td>クラスの種類</td>
<td>構造体クラス</td>
</tr>
<tr>
<td>SuperClasses</td>
<td>グループ</td>
</tr>
<tr>
<td>属性</td>
<td>delliProductMembers</td>
</tr>
<tr>
<td></td>
<td>delliPrivilegeMember</td>
</tr>
</tbody>
</table>

表 28. delliRAC4Privileges クラス

<table>
<thead>
<tr>
<th>OID</th>
<th>1.2.840.113556.1.8000.1280.1.1.1.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>説明</td>
<td>iDRAC の権限（許可権限）を定義します。</td>
</tr>
<tr>
<td>クラスの種類</td>
<td>補助クラス</td>
</tr>
<tr>
<td>SuperClasses</td>
<td>なし</td>
</tr>
<tr>
<td>属性</td>
<td>delliIsLoginUser</td>
</tr>
<tr>
<td></td>
<td>delliIsCardConfigAdmin</td>
</tr>
<tr>
<td></td>
<td>delliIsUserConfigAdmin</td>
</tr>
</tbody>
</table>
表 28. dellRAC4Privileges クラス（続き）

<table>
<thead>
<tr>
<th>OID</th>
<th>1.2.840.113556.1.8000.1280.1.1.1.3</th>
</tr>
</thead>
</table>
|     | dellIsLogClearAdmin  
|     | dellIsServerResetUser  
|     | dellIsConsoleRedirectUser  
|     | dellIsVirtualMediaUser  
|     | dellIsTestAlertUser  
|     | dellIsDebugCommandAdmin |

表 29. dellPrivileges クラス

<table>
<thead>
<tr>
<th>OID</th>
<th>1.2.840.113556.1.8000.1280.1.1.1.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>説明</td>
<td>デルの権限（許可権限）のコンテナクラスとして使用されます。</td>
</tr>
<tr>
<td>クラスの種類</td>
<td>構造体クラス</td>
</tr>
<tr>
<td>SuperClasses</td>
<td>ユーザー</td>
</tr>
<tr>
<td>属性</td>
<td>dellRAC4Privileges</td>
</tr>
</tbody>
</table>

表 30. dellProduct クラス

<table>
<thead>
<tr>
<th>OID</th>
<th>1.2.840.113556.1.8000.1280.1.1.1.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>説明</td>
<td>すべての Dell 製品が派生するメインクラス。</td>
</tr>
<tr>
<td>クラスの種類</td>
<td>構造体クラス</td>
</tr>
<tr>
<td>SuperClasses</td>
<td>コンピュータ</td>
</tr>
<tr>
<td>属性</td>
<td>dellAssociationMembers</td>
</tr>
</tbody>
</table>

表 31. Active Directory スキーマに追加された属性のリスト

<table>
<thead>
<tr>
<th>属性名 / 説明</th>
<th>割り当てられた OID/構文オブジェクト識別子</th>
<th>単一値</th>
</tr>
</thead>
<tbody>
<tr>
<td>dellPrivilegeMember</td>
<td>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）</td>
<td>FALSE</td>
</tr>
<tr>
<td>dellProductMembers</td>
<td>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）</td>
<td>FALSE</td>
</tr>
<tr>
<td>dellIsLoginUser</td>
<td>1.2.840.113556.1.8000.1280.1.1.2.3布尔（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）</td>
<td>TRUE</td>
</tr>
<tr>
<td>dellIsCardConfigAdmin</td>
<td>1.2.840.113556.1.8000.1280.1.1.2.4</td>
<td>TRUE</td>
</tr>
</tbody>
</table>
### 表 31. Active Directory スキーマに追加された属性のリスト（続き）

<table>
<thead>
<tr>
<th>属性名</th>
<th>説明</th>
<th>割り当てられたオID/構文オブジェクト識別子</th>
<th>単一値</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ユーザーにデバイスのカード設定権限がある場合は TRUE。</td>
<td>1.2.840.113556.1.8000.1280.1.1.2.5</td>
<td>TRUE</td>
</tr>
<tr>
<td>dellIsUserConfigAdmin</td>
<td>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。</td>
<td>1.2.840.113556.1.8000.1280.1.1.2.6</td>
<td>TRUE</td>
</tr>
<tr>
<td>dellIsLogClearAdmin</td>
<td>ユーザーにデバイスのログクリア権限がある場合は TRUE。</td>
<td>1.2.840.113556.1.8000.1280.1.1.2.7</td>
<td>TRUE</td>
</tr>
<tr>
<td>dellIsServerResetUser</td>
<td>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。</td>
<td>1.2.840.113556.1.8000.1280.1.1.2.8</td>
<td>TRUE</td>
</tr>
<tr>
<td>dellIsVirtualMediaUser</td>
<td>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。</td>
<td>1.2.840.113556.1.8000.1280.1.1.2.9</td>
<td>TRUE</td>
</tr>
<tr>
<td>dellIsTestAlertUser</td>
<td>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。</td>
<td>1.2.840.113556.1.8000.1280.1.1.2.10</td>
<td>TRUE</td>
</tr>
<tr>
<td>dellIsDebugCommandAdmin</td>
<td>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。</td>
<td>1.2.840.113556.1.8000.1280.1.1.2.11</td>
<td>TRUE</td>
</tr>
<tr>
<td>dellSchemaVersion</td>
<td>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。</td>
<td>1.2.840.113556.1.8000.1280.1.1.2.12</td>
<td>TRUE</td>
</tr>
<tr>
<td>dellRacType</td>
<td>この属性は dellDRACDevice オブジェクトの現在の RAC タイプで dellAssociationObjectMembers オブジェクトへのバックワードリンクです。</td>
<td>1.2.840.113556.1.8000.1280.1.1.2.13</td>
<td>TRUE</td>
</tr>
<tr>
<td>dellAssociationMembers</td>
<td>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。</td>
<td>1.2.840.113556.1.8000.1280.1.1.2.14</td>
<td>FALSE</td>
</tr>
<tr>
<td></td>
<td>リンク ID：12071</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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は、インストール時に Active Directory Users and Computers Snap-in (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ルは次の場所にある。

<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

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。
3. 新規オブジェクト ウィンドウで表示されます。
4. 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。
5. 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。

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。
3. 新規オブジェクト ウィンドウで表示されます。
4. 新しいオブジェクトの名前を入力します。
5. 権限オブジェクトを選択し、OKをクリックします。
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。

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。
3. 新規オブジェクト ウィンドウで表示されます。
4. 関連オブジェクト の名前を入力し、関連オブジェクトを選択します。
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. Administrative Tools (管理ツール) > ADSI Edit (ADSIエディタ) の順に移動します。ADSI Edit (ADSIエディタ)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、Check Names (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Groups and user names（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、ユーザーやユーザーグループ、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。

ユーザーやiDRACデバイスグループを追加できます。

権限の追加

権限を追加するには、次の手順を実行します。

Privilege Object（権限オブジェクト）タブをクリックして、iDRACデバイスの認証時にユーザーやユーザーグループの権限を定義する関連付け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. Privilege Object（権限オブジェクト）タブをクリックして、iDRACデバイスの認証時にユーザーやユーザーグループの権限を定義する関連付け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. Products（製品）タブをクリックして、定義されたユーザーや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iDRAC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、iDRAC Settings（iDRAC設定）> Users（ユーザー）> Directory Services（ディレクトリサービス）> Microsoft Active Directoryに移動します。Edit（編集）をクリックします。
2. Active Directory設定と管理手順4の1ページが開きます。
3. 次へ（次へ）をクリックします。
4. Active Directoryタブ設定と管理手順4の2ページが開きます。
4. Active Directory（AD）サーバとユーザーアカウントの場所の情報を指定します。また、ログイン処理中にiDRACがADからの応答を受け取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 FQDN を指定します。DNS が正しく設定されていることを iDRAC Settings (iDRAC 設定) > Network (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、User Domain from Login (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、Specify a Domain (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。

5. Next (次へ) をクリックします。Active Directory Configuration and Management Step 3 of 4 (Active Directory 設定と管理 4 の 3) ページが開きます。

6. 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。

7. 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。

```bash
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 デバイスが存在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。

```bash
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）。

```bash
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。

```bash
racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
```

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のアドレスおよび FQDN を指定します。DNS が iDRAC 設定 > ネットワーク で正しく設定されていることを確認します。

次の RACADM コマンドの使用はオプションです。

```bash
racadm sslcertdownload -t 1 -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。

```bash
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、iDRAC Settings (iDRAC 設定) > Users (ユーザー) > Directory Services (ディレクトリサービス) > Microsoft Active Directory の順に移動し、Test (テスト) をクリックします。Test Active Directory Settings (Active Directory 設定のテスト) ページが表示されます。
2. 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）とパスワードを入力し、Start Test (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。

#### 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、「iDRAC RACADM CLI ガイド」は www.dell.com/idracmanuals にあります。参照してください。

### 汎用 LDAP ユーザーの設定
iDRAC には 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があります。この機能は、ディレクトリサービス上のスキーマ拡張を必要としません。

iDRAC LDAP の実装を汎用にするために、異なるディレクトリサービス間の共通性を利用してユーザーをグループ化し、ユーザーグループの関係をマップします。これにより、ディレクトリサービス特有の処置がスキーマです。たとえば、グループ、ユーザー、およびユーザーグループの関係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。

#### 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、iDRAC設定＞Users（ユーザー）＞Directory Services（ディレクトリサービス）＞Generic LDAP Directory Service（汎用LDAPディレクトリサービス）の順に移動し、Edit（編集）をクリックします。

Generic LDAP Configuration and Management Step 1 of 3（汎用LDAPの設定と管理-手順1/3）ページに、現在の汎用LDAP設定が表示されます。

2. 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。サポートされているのはLDAP over SSLのみです。

3. Next（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。

4. 汎用LDAP認証を有効にして、汎用LDAPサーバーとユーザー認証の場所情報を指定します。

   メモ: 本リリースでは、ネストされたグループはサポートされていません。ファームウェアでは、ユーザーDNに一致するグループのメンバーを検索します。また、シングルドメインのみがサポートされています。クロスドメインのサポートされていません。

5. Next（次へ）をクリックします。

   汎用LDAP設定と管理手順3の2aページが表示されます。

6. 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2bページが表示されます。

7. 役割グループの設定が保存されます。Generic LDAP Configuration and Management Step 3a of 3（汎用LDAPの設定と管理-ステップ3a/3）ページに、役割グループの設定が表示されます。

8. 追加の役割グループを設定する場合は、手順7と8を繰り替えます。

9. 終了をクリックします。汎用LDAPディレクトリサービス設定が表示されます。

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、「iDRAC RACADM CLIガイド」は、www.dell.com/idracmanualsにあります。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、設定の有効性を確認したり、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、iDRAC設定＞Users（ユーザー）＞Directory Services（ディレクトリサービス）＞Generic LDAP Directory Service（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. 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。フォーマットは、使用されているユーザーアカウントの属性によって異なり、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: Enable Certificate Validation（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 サーバが IP アドレスで識別されている場合、iDRAC が LDAP サーバと通信できないため、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としてユーザ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、「iDRAC RACADM CLI ガイド」を参照してください。
システムロックダウンモード

システムロックダウンモードは、システムのプロビジョニング後に意図しない変更を防止するために役立ちます。この機能を使用すると、意図しない変更または悪意のある変更からシステムを保護することができます。ロックダウンモードは、設定とファームウェアのアップデートの両方に適用されます。システムがロックダウンされている場合、システム設定を変更しようとすると、プロックされます。重要なシステム設定を変更しようとした場合、エラーメッセージが表示されます。

ロックダウンモードは、次のインタフェースを使用して有効または無効にすることができます。

- iDRAC ウェブインタフェース
- RACADM
- WSMAN
- SCP（システム設定プロファイル）
- Redfish
- POST 中に F2 を使用して iDRAC 設定を選択する

メモ：ロックダウンモードを有効にするには、iDRAC Enterprise または Datacenter ライセンスおよび、制御とシステム設定の権限が必要です。

システムがロックダウンモードの場合でも、次のタスクは実行できます。

- 電力上限設定
- システム電源の操作（電源オン/オフ、リセット）
- 電源の優先度
- 操作の識別（シャーシまたは PERC）
- 部品交換
- 診断プログラムの実行
- モジュラーデバイスを直接アクセスするすべてのベンダートール（FlexAddress またはリモート割り当てアドレス）
- Group Manager パスコード

メモ：システムがロックダウンモードのときに vMedia にアクセスできますが、リモートファイル共有の設定は有効になっていません。

次の表は、ロックダウンモードの影響を受ける機能および機能以外の特性、インターフェイス、およびユーティリティーのリストです。

メモ：ロックダウンモードが有効になっている場合は、iDRAC を使用した起動順序の変更はサポートされていません。ただし、vConsole メニューでは、起動制御オプションを使用できます。これは、iDRAC がロックダウンモードでは有効ではありません。

表 32. ロックダウンモードの影響を受けるアイテム

<table>
<thead>
<tr>
<th>無効</th>
<th>引き続き機能するもの</th>
</tr>
</thead>
<tbody>
<tr>
<td>OMSA/OMSS</td>
<td>デバイスに直接アクセスするすべてのベンダーソフト</td>
</tr>
<tr>
<td>IPMI</td>
<td>PERC</td>
</tr>
<tr>
<td>DRAC/LC</td>
<td>○ PERC CLI</td>
</tr>
<tr>
<td>DTK-Syscfg</td>
<td>○ DTK-RAIDCFG</td>
</tr>
<tr>
<td>Redfish</td>
<td>○ F2/Ctrl+R</td>
</tr>
<tr>
<td>OpenManage Essentials</td>
<td>NVMe</td>
</tr>
<tr>
<td>BIOS（F2 設定は読み取り専用になります）</td>
<td>○ DTK-RAIDCFG</td>
</tr>
<tr>
<td></td>
<td>○ F2/Ctrl+R</td>
</tr>
<tr>
<td></td>
<td>BOSS-S1</td>
</tr>
</tbody>
</table>
表 32. ロックダウンモードの影響を受けるアイテム

<table>
<thead>
<tr>
<th>無効</th>
<th>引き続き機能するもの</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>○ Marvell CLI</td>
</tr>
<tr>
<td></td>
<td>○ F2/Ctrl+R</td>
</tr>
<tr>
<td>部品交換、簡易復元、システム基板の交換</td>
<td>電力制限</td>
</tr>
<tr>
<td></td>
<td>システムの電源制御操作（電源のオン/オフ、リセット）</td>
</tr>
<tr>
<td></td>
<td>デバイスの識別（シャーシまたは PERC）</td>
</tr>
<tr>
<td>ISM/OMSA の設定（OS BMC の有効、watchdog ping、OS 名、OS バージョン）</td>
<td>モジュラー操作（FlexAddress またはリモート割り当てアドレス）</td>
</tr>
<tr>
<td></td>
<td>Group Manager パスコード</td>
</tr>
</tbody>
</table>

メモ: ロックダウンモードが有効になっている場合、OpenID Connect ログインオプションは iDRAC ログインページには表示されません。

166 システムロックダウンモード
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）に用いる iDRAC を設定するための情報を記載します。SSO および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、Kerberos ベースの Active Directory 認証をサポートしており、スマートカードおよび SSO ログインに対応しています。Kerberos の詳細については、Microsoft の Web サイトを参照してください。

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 ユーザーのための iDRAC SSO ログインの設定
- シングルサインオン用に、デバイスの設定
- マシンネームを使用したログイン

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 の時刻が Active Directory ドメインコントローラの時刻と同期します。同期しない場合、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、「タイムゾーンおよび NTP の設定」、p. 103」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 Delegation (委任) タブで Trust this user for delegation to any service (Kerberos only) (任意のサービスへの委任についてこのユーザーを信用する (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にのみ使用できます。
- 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ゾーンを設定します。
  
  なお: ネームは 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。
- SSO ログインをサポートするようにブラウザを設定します。詳細については、「シングルサインオン、p. 344」を参照してください。
  
  なお: 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。

iDRAC のドメイン名システムへの登録

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. [iDRAC 設定] > [接続] > [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。
2. IP 設定に基づいて [IPv4 設定] または [IPv6 設定] を選択できます。
3. 有効な[優先/代替 DNS サーバ]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。
4. iDRAC の DNSへの登録を選択します。
5. 有効な DNS ドメイン名を入力します。
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 のオンライン ヘルプを参照してください。

Active Directory オブジェクトの作成と権限の付与

Active Directory 標準スキーマ ベース SSO へのログイン

Active Directory 標準スキーマベース SSO ログイン用に、次の手順を実行します。
1. ユーザー グループを作成します。
2. 標準スキーマのユーザーを作成します。  

メモ: 既存の AD ユーザー グループと AD ユーザーを使用します。

Active Directory 拡張スキーマ ベース SSO へのログイン

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. 作成した権限オブジェクトにアクセス権限を設定します。  

メモ: 一部のセキュリティチェックがバイパスされる可能性があるため、管理者権限を提供しないことをお勧めします。
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、一部のユーザーグループに与えます。

Active Directory SSO へのログイン

Active Directory SSO ログイン用に、次の手順を実行します。
1. キー タブファイルの作成に使用する Kerberos キーをアカウント作成します。

メモ: すべての iDRAC IP に対して新しい KERBROS キーを作成します。

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。

SSO 用の Active Directory でのユーザーの作成

SSO 用の Active Directory にユーザーを作成するには、次の手順を実行します。
1. 組織ユニットに新しいユーザーを作成します。
2. [Kerberos ユーザー]、[プロパティ]、[アカウント]、[このアカウントに Kerberos DES 暗号化タイプを使用する] の順に移動します。
3. 次のコマンドを使用して、Active Directory サーバーで Kerberos キーを生成します。

C:\> ktpass.exe -princ HTTP/idrac7name.domainname.com@DOMAINDOMAINNAME.COM -mapuser DOMAINNAME \username -mapOp set -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass [password] -out c:\krbkeytab

拡張スキーマに関する注意事項

- Kerberos ユーザーの委任設定を変更します。
- Kerberos ユーザーの[委任]、[委任]、[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)] の順に移動します。

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
前述の設定を変更した後、管理ステーションの Active Directory ユーザーからログオフしてログインします。

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、iDRAC では、Windows Kerberos ネットワーク上で自身を Kerberos 化されたサービスとして有効にする構成がサポートされています。iDRAC での Kerberos の設定手順では、Windows Server Active Directory での Windows Server 以外の Kerberos サービスをセキュリティブリンシルとして設定する場合と同様の手順を実行します。

ktpass は、サーバーのインストール CD/DVD の一部としてマイクロソフトから入手可能で、stdin からの Active Directory ユーザーのログイン情報を入力して、UTF-8 にエンコードされた Kerberos Keytab ファイルを作成し、Active Directory の KDC サーバーにアップロードします。

ktpass は、Kerberos Keytab ファイルの生成、Active Directory の Kerberos 認証をサポートするため、Windows Server Active Directory での Windows Server 以外の Kerberos サービスをセキュリティブリンシルとして設定する場合に使用します。

Kerberos認証に使用する Active Directory のユーザーアカウントを作成するために、ktpass コマンドを使用します。このコマンドは、Active Directory ユーザーアカウントを設定するために、Kerberos Keytab ファイルを作成し、そのファイルを iDRAC DNS 名にアップロードします。

Keytabファイルを生成する場合、事前に ktpass コマンドの -mapuser オプションで用いる Active Directory ユーザーアカウントを作成しておく必要があります。この名前は、生成した Keytab ファイルのアップロード先となる iDRAC DNS 名と同じにする必要があります。

Keytabファイルを生成するには、次の手順を実行します。

1. 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。サービスブリンシ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 256 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。

Keytabファイルを生成する場合、前に ktpass コマンドの -mapuser オプションで用いる Active Directory ユーザーアカウントを作成しておく必要があります。この名前は、生成した Keytab ファイルのアップロード先となる iDRAC DNS 名と同じ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 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。

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 Web インタフェースで、「[iDRAC 設定]」＞[ネットワーク]＞[共有設定]」の順に移動し、「DNS iDRAC 名」プロパティを調べます。

2. 標準スケーマまたは拡張スケ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
```

管理ステーションの設定
Active DirectoryユーザーサのSSOログインを設定した後、次の手順を実行します。

1. ネットワークのDNSサーバーIPプロパティを設定し、優先DNSサーバーIPを指定します。
2. [マイコンピューター]に移動して、*domain.tldドメインを追加します。
3. 管理者にActive Directoryユーザーサーを追加するには、[マイコンピューター]＞[管理]＞[ローカルユーザーとグループ]＞[グループ]＞[管理者]の順に移動し、Active Directoryユーザーを追加します。
4. システムからログオフし、Active Directoryユーザー認証情報を使用してログインします。
5. Internet Explorerの設定で、*domain.tldドメインを以下のように追加します。
   a. [ツール]＞[インターネットオプション]＞[セキュリティ]＞[ローカルインターネット]＞[サイト]の順に選択し、[インターネットのネットワークを自動的に検出する]設定の選択をクリアします。残りの3つのオプションを選択し、[詳細設定]をクリックして*domain.tldを追加します。
   b. IEで新しいウィンドウを開き、iDRACホスト名を使用してiDRAC GUIを起動します。
6. Mozilla Firefoxの設定で、*domain.tldドメインを追加します。
   a. Firefoxブラウザを起動し、URLに「about:config」と入力します。
   b. [フィルター]テキストボックスで[ネゴシエート]を使用します。auth.trusted.urisで構成される結果をダブルクリックします。ドメインを入力して設定を保存し、ブラウザを閉じます。
   c. Firefoxで新しいウィンドウを開き、iDRACホスト名を使用してiDRAC GUIを起動します。

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、インターフェースは自動で有効にはなりません。

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イ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のウェブインタフェースで、iDRAC Settings (iDRAC設定) ＞ Users (ユーザー) ＞ Smart Card (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. Configure Smart Card Logon (スマートカードログインの設定)ドロップダウンメニューから、Enabled (有効)を選択してスマートカードログインを有効化するか、Enabled With Remote RACADM (リモートRACADMで有効化)を選択します。それ以外の場合は、Disabled (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イン試行では、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、「iDRAC RACADM CLI ユーザーレファレンス」ウェブサイトにあります。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イン機能を有効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インを有効にするには、Enabled（有効）を選択します。それ以外の場合は、Disabled（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イン機能が有効または無効化されます。

スマートカードログインの設定

メモ: 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にあたり、Active Directory を設定している際に、「Active Directory の設定と管理手順」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 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。

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

ローカルユーザーのための iDRAC スマートカードログインができるように 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。

スマートカードユーザー証明書のアップロード

ユーザーアカウントの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アカウントが 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。

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アカウントの証明書をアップロードするには、次の手順を実行します。

シャ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
スマートカードログイン機能を使用するには、ローカルおよび/または Active Directory ユーザー証明書の設定が必要です。

スマートカードログインの設定] で、[リモート RACADM で有効化] を選択して設定を有効にします。
3. [スマートカードログインの CRL チェックを有効にする] にオプションを設定します。
4. 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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。参照してください。

スマートカード登録のために証明書を要求する
スマートカード登録用の証明書を要求するには、次の手順を実行します。
1. クライアントシステムにスマートカードを接続し、必要なドライバとソフトウェアをインストールします。
2. デバイスマネージャーでドライバのステータスを確認します。
3. プラウザーでスマートカード登録エージェントを起動します。
5. [証明書の要求] をクリックします。
6. [証明書の要求の詳細設定] をクリックします。
7. スマートカード証明書登録ステーションを使用して、別のユーザーの代わりにスマートカードの [証明書の要求] をクリックします。
8. [ユーザーの選択] ボタンをクリックして、登録するユーザーを選択します。
9. [登録] をクリックし、スマートカード証明情報を入力します。
10. スマートカード PIN を入力し、[送信] をクリックします。

ウェブインタフェースを使用したスマートカード用の証明書 CA 証明書のアップロード
ウェブインタフェースを使用したスマートカード用の証明書 CA 証明書のアップロードには、次の手順を実行します。
1. iDRAC ウェブインタフェースで、iDRAC Settings（iDRAC 設定） > Network（ネットワーク） > User Authentication（ユーザーオーロット（ID 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。
3. スマートカード設定で、証明書 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。
4. 証明書 CA 証明書のアップロードページが表示されます。
5. 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証明書 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証明書 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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。参照してください。

スマートカードを使用したログイン
スマートカードログインは、Internet Explorer でのみサポートされています。
スマートカードを有効にした後、iDRAC GUI からログアウトします。
3. スマートカードログインのダウンロード後に、[インストール] をクリックします。
4. スマートカード PIN を入力し、[送信] をクリックします。
5. iDRAC にスマート カードを使用して正常にログインします。
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状態が事前に定義した条件を超えると発生します。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 トラブル、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）を生成しようとしている場合、アラートが 1 つ、または複数の設定済みの宛先に送信されます。また、同じイベントフィルタが処置（システムの再起動、電源のオフ、またはパワーサイクル）を実行するように設定されている場合は、その処置が実行されます。処置はイベントごとに 1 つだけ設定できます。

アラートを送信するための iDRAC の設定

1. アラートを有効化します。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。
2. 電子メールアラート、SNMP トラブル、リモートシステムログ、Redfish イベント、および WS イベントを設定します。
3. 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 トラブル、リモートシステムログ、Redfish イベント、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。

### トピック:
- アラートの有効化または無効化
- アラートのフィルタ
- イベントアラートの設定
- アラート反復イベントの設定
- イベント処置の設定
- 電子メールアラート、SNMP トラブル、または IPMI トラブル設定の設定
- WS Eventing の設定
- Redfish Eventing の設定
- シャーシイベントの監視
- アラートメッセージ ID

### アラートの有効化または無効化

設定された宛先にアラートを送信する、またはイベント処置を実行するには、グローバルアラートオプションを有効に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。

### 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 Web インタフェースで、【設定】 > 【システム設定】 > 【アラート設定】の順に移動します。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。
クイックアラートの設定
アラートを一括設定するには、次の手順を実行します。
1. [アラート設定] ページの [クイックアラートの設定] に移動します。
2. [クイックアラートの設定] セクションで、次の手順を実行します。
   - アラートカテゴリを選択します。
   - 問題の重大度通知を選択します。
   - これらの通知を受信する場所を選択します。
3. 適用をクリックして設定を保存します。
   - メモ: 設定を適用するには、カテゴリ、重大度、宛先のタイプをそれぞれ少なくとも1つ選択する必要があります。
設定されているすべてのアラートは、[アラート設定サマリー] に合計表示されます。

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.IPMLan.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. Platform Events（プラットフォームイベント）で、Enabled（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。それ以外の場合は、Disabled（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。

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、Configuration（設定）> System Settings（システム設定）> Alerts and Remote System Log Configuration（アラートとリモートシステムログ設定）に移動します。
2. Alerts and Remote System Log Configuration（アラートとリモートシステムログ設定）セクションで、Filter（フィルタ）を選択します。
   - システムの正常性 - System Health（システムの正常性）カテゴリには、システムシャーシ内のハードウェアに関連するアラートがすべて表示されます。たとえば、温度エラー、電圧エラー、ディバイスエラーなどです。
   - Storage Health（ストレージの正常性） — Storage Health（ストレージの正常性）カテゴリは、ストレージサブシステムに関連した警告を表します。たとえば、コントローラのエラー、物理ディスクエラー、仮想ディスクエラーなどです。
   - 設定 - Configuration（設定）カテゴリには、ハードウェア、ファームウェア、およびソフトウェアの設定変更に関連するアラートが表示されます。たとえば、PCI-Eカードの追加/取り外し、RAID設定の変更、iDRACライセンスの変更などです。
- 監査 - Audit（監査）カテゴリには、監査ログが表示されます。たとえば、ユーザログイン/ログアウト情報、パスワード認証エラー、セッション情報、電源状況などです。
- アップデート - Update(アップデート)カテゴリには、ファームウェア/ドライバのアップグレード/ダウングレードで発生したアラートが表示されます。

 Memo: これは、ファームウェアイベントを表すものではありません。

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、『iDRAC RACADM CLIガイド』は、www.dell.com/idracmanuals にあります。 を参照してください。

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. iDRACウェブインタフェースで、設定⇒システム設定⇒アラートおよびリモートシステムログの設定 の順に選択します。
3. カテゴリで、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
   - SNMP トラップ
   - IPMI アラート
   - リモートシステムログ
   - WS イベント
   - OS ログ
   - Redfish イベント
4. アクションを選択します。
   設定が保存されます。
5. 必要に応じて、テストイベントを送信できます。イベントをテストするメッセージIDフィールドに、アラートが生成されるかどうかをテストするメッセージIDを入力し、テスト をクリックします。システムファームウェアや、システムコンポーネントを監視するエージェントによって生成されたイベントメッセージおよびエラーメッセージについては、iDRACmanuals にある『イベントおよびエラーメッセージリファレンスガイド』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。詳細については、『iDRAC RACADM CLIガイド』は、www.dell.com/idracmanuals にあります。 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移動し続けた場合に、iDRACが追加のイベントを特定の間隔で生成するよう設定できます。デフォルトの間隔は30日です。有効な範囲は、0～365日です。値が「0」の場合は、イベントの反復がないことを示します。

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。

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、「iDRAC RACADM CLIガイド」は、www.dell.com/idracmanualsにあります。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、Configuration(設定)＞System Settings(システム設定)＞Alert Recurrence(アラート反復)と移動します。
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。

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。

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、Configuration(設定)＞System Settings(システム設定)＞Alert and Remote System Log Configuration(アラートとリモートシステムログ設定)の順に移動します。
2. Actions(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。
   - 再起動する
   - 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、「iDRAC RACADM CLIガイド」は、www.dell.com/idracmanualsにあります。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 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は、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。SNMP v1、v2、および v3 形式がサポートされています。

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 トラップの送信元となる 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。

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 によるサーバ監視を必要とする iDRAC MIB については、「Dell EMC OpenManage SNMP リファレンス ガイド」は、www.dell.com/openmanagemanuals にあります。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. iDRAC ウェブインタフェースで、「Configuration (設定) > System Settings (システム設定) > SNMP and E-mail Settings (SNMP および電子メールの設定)」の順に移動します。

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 個の送信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、iDRAC 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 Trap Format (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 Trap Format (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

トラブル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>

アラートを送信するための iDRAC の設定
### 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宛先 (IPv4, IPv6, または FQDN) を設定できます。この操作を行うには、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. Trap Settings (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。

---

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;index&gt;</td>
<td>宛先索引。有効な値は 1～8 です。</td>
</tr>
<tr>
<td>&lt;n&gt;=0</td>
<td>トラックの無効化</td>
</tr>
<tr>
<td>&lt;n&gt;=1</td>
<td>トラックの有効化</td>
</tr>
</tbody>
</table>

2. トラック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>

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;index&gt;</td>
<td>宛先索引。有効な値は 1～8 です。</td>
</tr>
<tr>
<td>&lt;Address&gt;</td>
<td>有効な IPv4、IPv6、または FQDN アドレスです。</td>
</tr>
</tbody>
</table>

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>

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;community_name&gt;</td>
<td>SNMP コミュニティ名です。</td>
</tr>
</tbody>
</table>

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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。参照してください。
電子メールアラートの設定

送信者のEメールアドレスと、Eメールアラートを受信する受信者（宛先）のEメールアドレスを設定できます。SMTPサーバー アドレスも設定してください。

メモ: Eメールアラートは、IPv4アドレスとIPv6アドレスの両方をサポートします。IPv6を使用する場合は、iDRAC DNS ドメイン名を指定する必要があります。

メモ: 外部SMTPサーバーを使用している場合は、iDRACがそのサーバーと通信できることを確認してください。サーバーが到達不能な場合は、テストメールの送信中にエラーRAC0225が表示されます。

Web インターフェイスを使用したEメールアラートの設定

Webインターフェイスを使用してE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. iDRAC Web インターフェイスで、[設定] > [システム設定] > [SMTP( Eメール)設定]の順に進移動します。

2. 有効なEメールアドレスを入力します。

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。

5. [SMTP( Eメール)サーバー設定]については、次の詳細を入力します。
   - SMTP(電子メール)サーバーIPアドレスまたはFQDN/DNS名
   - [カスタム送信者アドレス]—このフィールドには、次のオプションがあります。
     - [デフォルト]—アドレスフィールドは編集できません。
     - [カスタム]—Eメールアラート送信用のEメールIDを入力できます。
   - SMTPメッセージ件名プレフィックス:—このフィールドには次のオプションがあります。
     - [デフォルト]—デフォルトメッセージは編集できません。
     - [カスタム]—Eメール件名行に表示させるメッセージを選択できます。
   - SMTPポート番号:—接続は暗号化が可能で、Eメールを安全なポートを介して送信することができます。
     - [暗号化なし]—ポート25(デフォルト)
     - [StartTLS]—ポート587
     - [TLS/SSL]—ポート465
   - [接続の暗号化]—手元の施設内にEメールサーバーがない場合は、クラウドベースのEメールサーバーまたはSMTPリレーを使用できます。クラウドEメールサーバーを設定する場合、この機能を以下のいずれかの値にドロップダウンで設定します。
     - [なし]—SMTPサーバーへの接続を暗号化しません。これはデフォルト値です。
     - [SSL/TLS]—SMTPプロトコルをSSL/TLSに変換する
     - [STARTTLS]—暗号化なしのSMTP接続で開始し、SMTP STARTTLSコマンドを用いてSSL/TLSに切り替えます。

メモ:
○この機能はグループマネージャーを介して構成することはできません。
○これはライセンスが必要な機能で、iDRAC Basicライセンスでは利用できません。
○この機能を利用するには、iDRAC設定権限が必要です。

6. 適用をクリックします。オプションの詳細については、iDRACのオンラインヘルプを参照してください。

RACADMを使用した電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]
2. 電子メール設定を行う:

```
racadm set iDRAC.EmailAlert.Address.[index] [email-address]
```

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>メールの宛先索引です。有効な値は1～4です。</td>
</tr>
<tr>
<td>n=0</td>
<td>電子メールアラートを無効にします。</td>
</tr>
<tr>
<td>n=1</td>
<td>電子メールアラートを有効にします。</td>
</tr>
</tbody>
</table>

3. 送信者のEメール設定を行う:

```
racadm set iDRAC.RemoteHosts.[index] [email-address]
```

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>送信者のEメールの索引です。</td>
</tr>
<tr>
<td>email-address</td>
<td>プラットフォームイベントアラートを送信する送信者のEメールアドレスです。</td>
</tr>
</tbody>
</table>

4. カスタムメッセージを設定する:

```
racadm set iDRAC.EmailAlert.CustomMsg.[index] [custom-message]
```

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>メールの宛先索引です。有効な値は1～4です。</td>
</tr>
<tr>
<td>custom-message</td>
<td>カスタムメッセージ</td>
</tr>
</tbody>
</table>

5. 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]
```

<table>
<thead>
<tr>
<th>パラメータ</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>テスト対象のメールの宛先索引です。有効な値は1～4です。</td>
</tr>
</tbody>
</table>

詳細については、「iDRAC RACADM CLIガイド」は、www.dell.com/idracmanualsにあります。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、Configuration（設定）＞System Settings（システム設定）＞Alert Configuration（アラートの設定）＞SNMP（E-mail Configuration）（SNMP（電子メール設定））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。
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（サブスクリプション）を含むメッセージの受信にサーバー（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 にサブスクリプトして Lifecycle Controller ジョブ関連のイベントを受信することができるです。

Lifecycle Controller ジョブに関する変更についての WS Eventing メッセージを受信する WS Eventing 機能の設定に必要な手順は、iDRAC 1.30.30 向け Web Service Eventing サポートの仕様に記載されています。この仕様の他にも、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（サブスクリプション）を含むメッセージの受信にサーバー（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 にサブスクリプトして 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 のシャーシの管理と監視設定を有効にして、シャーシコンポーネントの監視、アラートの設定、iDRAC RACADM による CMC RACADM コマンドの受け渡し、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 Disabled（無効）に設定します。この設定は、デフォルトでは Enabled（有効）になっています。

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。

Chassis Management and Monitoring（シャーシの管理と監視）オプションが Enabled（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リーに入れ、残りを CMC ログに記録します。これらの 16 個のイベントは、Chassis monitoring（シャーシの監視）が有効に設定された時点で iDRAC で検出されます。

iDRAC が必要な CMC 機能がないことを検出した場合、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

1. PowerEdge FX2/FX2s シャーシに対してのみ表示されます。
2. サーバーモードでのシャーシ管理の設定が一時的に döneminde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、Overview (概要) > iDRAC Settings (iDRAC 設定) > CMC (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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。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 33. アラートメッセージ ID

<table>
<thead>
<tr>
<th>メッセージ ID</th>
<th>説明</th>
<th>説明 (MX プラットフォーム用)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMP</td>
<td>アンペア数</td>
<td>アンペア数</td>
</tr>
<tr>
<td>ASR</td>
<td>自動システムリセット</td>
<td>自動システムリセット</td>
</tr>
<tr>
<td>BAR</td>
<td>バックアップ / 復元</td>
<td>バックアップ / 復元</td>
</tr>
<tr>
<td>BAT</td>
<td>バッテリイベント</td>
<td>バッテリイベント</td>
</tr>
<tr>
<td>BIOS</td>
<td>BIOS 管理</td>
<td>BIOS 管理</td>
</tr>
<tr>
<td>BOOT</td>
<td>起動コントロール</td>
<td>起動コントロール</td>
</tr>
<tr>
<td>CBL</td>
<td>ケーブル</td>
<td>ケーブル</td>
</tr>
<tr>
<td>CPU</td>
<td>プロセッサ</td>
<td>プロセッサ</td>
</tr>
<tr>
<td>CPUA</td>
<td>プロセッサ不在</td>
<td>プロセッサ不在</td>
</tr>
<tr>
<td>CTL</td>
<td>ストレージコントローラ</td>
<td>ストレージコントローラ</td>
</tr>
<tr>
<td>DH</td>
<td>証明書管理</td>
<td>証明書管理</td>
</tr>
<tr>
<td>DIS</td>
<td>自動検出</td>
<td>自動検出</td>
</tr>
<tr>
<td>ENC</td>
<td>ストレージエンクロージャ</td>
<td>ストレージエンクロージャ</td>
</tr>
<tr>
<td>FAN</td>
<td>ファンイベント</td>
<td>ファンイベント</td>
</tr>
<tr>
<td>FSD</td>
<td>デバッグ</td>
<td>デバッグ</td>
</tr>
<tr>
<td>HWC</td>
<td>ハードウェア設定</td>
<td>ハードウェア設定</td>
</tr>
<tr>
<td>IPA</td>
<td>DRAC IP 変更</td>
<td>DRAC IP 変更</td>
</tr>
<tr>
<td>ITR</td>
<td>イントルージョン</td>
<td>イントルージョン</td>
</tr>
<tr>
<td>JCP</td>
<td>ジョブ制御</td>
<td>ジョブ制御</td>
</tr>
</tbody>
</table>

アラートを送信するための iDRAC の設定 183
### 表33. アラートメッセージ ID（続き）

<table>
<thead>
<tr>
<th>メッセージID</th>
<th>説明</th>
<th>説明（MXプラットフォーム用）</th>
</tr>
</thead>
<tbody>
<tr>
<td>LC</td>
<td>Lifecycle Controller</td>
<td>Lifecycle Controller</td>
</tr>
<tr>
<td>LIC</td>
<td>ライセンス</td>
<td>ライセンス</td>
</tr>
<tr>
<td>LNK</td>
<td>リンクステータス</td>
<td>リンクステータス</td>
</tr>
<tr>
<td>LOG</td>
<td>ログイベント</td>
<td>ログイベント</td>
</tr>
<tr>
<td>MEM</td>
<td>メモリ</td>
<td>メモリ</td>
</tr>
<tr>
<td>NDR</td>
<td>NIC OS ドライバ</td>
<td>NIC OS ドライバ</td>
</tr>
<tr>
<td>NIC</td>
<td>NIC設定</td>
<td>NIC設定</td>
</tr>
<tr>
<td>OSD</td>
<td>OS導入</td>
<td>OS導入</td>
</tr>
<tr>
<td>OSE</td>
<td>OSイベント</td>
<td>OSイベント</td>
</tr>
<tr>
<td>PCI</td>
<td>PCIデバイス</td>
<td>PCIデバイス</td>
</tr>
<tr>
<td>PDR</td>
<td>物理ディスク</td>
<td>物理ディスク</td>
</tr>
<tr>
<td>PR</td>
<td>部品交換</td>
<td>部品交換</td>
</tr>
<tr>
<td>PST</td>
<td>BIOS POST</td>
<td>BIOS POST</td>
</tr>
<tr>
<td>PSU</td>
<td>電源装置</td>
<td>電源装置</td>
</tr>
<tr>
<td>PSUA</td>
<td>PSU不在</td>
<td>PSU不在</td>
</tr>
<tr>
<td>PWR</td>
<td>電力消費</td>
<td>電力消費</td>
</tr>
<tr>
<td>RAC</td>
<td>RACイベント</td>
<td>RACイベント</td>
</tr>
<tr>
<td>RDU</td>
<td>冗長性</td>
<td>冗長性</td>
</tr>
<tr>
<td>RED</td>
<td>FWダウンロード</td>
<td>FWダウンロード</td>
</tr>
<tr>
<td>RFL</td>
<td>IDSDMメディア</td>
<td>IDSDMメディア</td>
</tr>
<tr>
<td>RFLA</td>
<td>IDSDM不在</td>
<td>IDSDM不在</td>
</tr>
<tr>
<td>RFM</td>
<td>FlexAddress SD</td>
<td>適用なし</td>
</tr>
<tr>
<td>RRDU</td>
<td>IDSDMの冗長性</td>
<td>IDSDMの冗長性</td>
</tr>
<tr>
<td>RSI</td>
<td>リモートサービス</td>
<td>リモートサービス</td>
</tr>
<tr>
<td>SEC</td>
<td>セキュリティイベント</td>
<td>セキュリティイベント</td>
</tr>
<tr>
<td>SEL</td>
<td>システムイベントログ</td>
<td>システムイベントログ</td>
</tr>
<tr>
<td>SRD</td>
<td>ソフトウェアRAID</td>
<td>ソフトウェアRAID</td>
</tr>
<tr>
<td>SSD</td>
<td>PCIe SSD</td>
<td>PCIe SSD</td>
</tr>
<tr>
<td>STOR</td>
<td>ストレージ</td>
<td>ストレージ</td>
</tr>
<tr>
<td>メッセージ ID</td>
<td>説明</td>
<td>説明（MX プラットフォーム用）</td>
</tr>
<tr>
<td>---------------</td>
<td>------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>SUP</td>
<td>FW アップデートジョブ</td>
<td>FW アップデートジョブ</td>
</tr>
<tr>
<td>SWC</td>
<td>ソフトウェア設定</td>
<td>ソフトウェア設定</td>
</tr>
<tr>
<td>SWU</td>
<td>ソフトウェアの変更</td>
<td>ソフトウェアの変更</td>
</tr>
<tr>
<td>SYS</td>
<td>System Info</td>
<td>System Info</td>
</tr>
<tr>
<td>TMP</td>
<td>温度</td>
<td>温度</td>
</tr>
<tr>
<td>TST</td>
<td>テストアラート</td>
<td>テストアラート</td>
</tr>
<tr>
<td>UEFI</td>
<td>UEFI イベント</td>
<td>UEFI イベント</td>
</tr>
<tr>
<td>USR</td>
<td>ユーザー追跡</td>
<td>ユーザー追跡</td>
</tr>
<tr>
<td>VDR</td>
<td>仮想ディスク</td>
<td>仮想ディスク</td>
</tr>
<tr>
<td>VF</td>
<td>vFlash SD カード</td>
<td>vFlash SD カード</td>
</tr>
<tr>
<td>VFL</td>
<td>vFlash イベント</td>
<td>vFlash イベント</td>
</tr>
<tr>
<td>VFLA</td>
<td>vFlash 不在</td>
<td>vFlash 不在</td>
</tr>
<tr>
<td>VLT</td>
<td>電圧</td>
<td>電圧</td>
</tr>
<tr>
<td>VME</td>
<td>仮想メディア</td>
<td>仮想メディア</td>
</tr>
<tr>
<td>VRM</td>
<td>仮想コンソール</td>
<td>仮想コンソール</td>
</tr>
<tr>
<td>WRK</td>
<td>作業メモ</td>
<td>作業メモ</td>
</tr>
</tbody>
</table>
iDRAC 9 グループマネージャー

グループマネージャーにより、ユーザーは複数のコンソールを使用できるようになり、シンプルで基本的な iDRAC 管理も提供されます。

iDRAC グループマネージャ機能は、デルの第 14 世代サーバーで利用でき、iDRAC GUI を使用してローカルネットワーク上の iDRAC およびその関連サーバーの基本的な管理を簡素化します。グループマネージャにより、別のアプリケーションを使用せずに iXMany コンソールを使用できるようになります。これによりユーザーは一連のサーバーの詳細を開確認することができ、サーバー障害の目視検査などの手動方式よりも強力な管理が可能になります。

グループマネージャはライセンスされた機能であり、Enterpriseライセンスの一部です。グループマネージャ機能にアクセスできるのは、iDRAC マネージャーのみです。

メモ: ユーザー体験を向上できるよう、グループマネージャは最大で 250 のサーバーノードをサポートしています。

トピック:
・ グループマネージャ
・ サマリビュー
・ ネットワーク設定の要件
・ ログインの管理
・ アラートの設定
・ エクスポート
・ 検出されたサーバービュー
・ Jobs（ジョブ）ビュー
・ ジョブのエクスポート
・ グループ情報パネル
・ グループ設定
・ 選択したサーバでの操作

グループマネージャ

グループマネージャ機能を使用するには、iDRAC インデックスページまたはグループマネージャーようす画面で [ グループマネージャー ] を有効にする必要があります。グループマネージャーようす画面には、下の表に示すオプションがあります。

表 34. グループマネージャーのオプション

<table>
<thead>
<tr>
<th>オプション</th>
<th>説明</th>
</tr>
</thead>
</table>
| 既存のグループへの参加 | 既存のグループに参加することができます。特定のグループに参加するには、グループ名とパスコードを知っている必要があります。

メモ: パスワードは iDRAC のユーザー資格情報に関連付けられています。一方、パスコードはグループに関連付けられ、同じグループ内の異なる iDRAC 前で認証されたデバイス通信を確立するために使用されます。 |
| 新しいグループの作成 | 新規グループを作成できます。既存のグループに参加した特定の iDRAC がグループのマスター（プライマリコントローラ）になります。 |
| このシステムについてグループマネージャを無効にする | 特定のシステムから書きのグループに参加しない場合は、このオプションを選択します。ただし、iDRAC からグループマネージャを開く選択すると、いつでもグループマネージャにアクセスできます。グループマネージャを無効にすると、ユーザはその後の Group Manager 操作を実行するために 60 秒待機する必要があります。 |
サマリビュー

グループマネージャー機能が有効になると、そのiDRACでiDRACローカルグループを作成または参加するオプションが有効になります。ローカルネットワークには複数のiDRACグループをセットアップできますが、個々のiDRACは一度に1つのグループのメンバーにしかなりません。iDRACのグループを変更する（新しいグループに参加する）には、前に現在のグループを離脱してから新しいグループに参加する必要があります。グループの作成元のiDRACが、デフォルトでグループのプライマリーコントローラーとして選択されます。ユーザーは、そのグループを制御するための専用グループマネージャープライマリーコントローラーを定義しません。プライマリーコントローラーは、グループマネージャーWebインターフェイスをホストし、GUI ベースのワークフローを提供します。iDRAC メンバーは、現在のプライマリーが長期間オフラインのままになった場合はグループの新しいプライマリーコントローラーを自動的に選択しますが、エンドユーザーに影響しません。通常、すべてのiDRACメンバーから、iDRACインデックスページでグループマネージャーをクリックすることによってグループマネージャーにアクセスできます。

サマリビュー

グループマネージャのページにアクセスするには、管理者権限が必要です。管理者以外のユーザーガiDRACにログオンすると、資格情報の入ったグループマネージャーセッションが表示されない場合があります。グループマネージャーのホームページ（サマリビュー）は大別して6つのセクションで構成されています。1つ目のセクションには、統合されたサマリの詳細が組み込まれたロールアップサマリが表示されます。

- ロールアップグループに含まれるサーバの合計数。
- サーバモデルあたりのサーバ数を示すチャート。
- サーバの正常性を示すドーナツチャート（チャートセクションをクリックすると、サバリストを絞り込み、選択した正常性のサーバのみを確認可能）。
- ローカルネットワーク内で重複するグループが検出された場合の警告ボックス。重複するグループは、通常は同じ名前のグループに別のパスコードが付与されています。重複グループがない場合は、警告ボックスを表示させません。グーツルを制御するiDRAC（プライマリーとサブダリアリコントローラ）が表示されます。

2つ目のセクションには、グループ全体に対してアクションを実行するボタンが組み込まれており、3つ目のセクションでは、グループ内のすべてのiDRACのリストが表示されます。

グループに含まれるすべてのシステムとそのシステムの現在の正常性のステータスが表示されるため、ユーザーガ必要に応じて是正措置を取ることができますサーバに特定のサーバ属性は下表で説明されています。

<table>
<thead>
<tr>
<th>サーバ属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health（正常性）</td>
<td>特定のサーバの正常性ステータスを示します。</td>
</tr>
<tr>
<td>ホスト名</td>
<td>サーバ名を表示します。</td>
</tr>
<tr>
<td>iDRACのIPアドレス</td>
<td>正確なIPv4およびIPv6アドレスを表示します。</td>
</tr>
<tr>
<td>サービスタグ</td>
<td>サービスタグ情報を表示します。</td>
</tr>
<tr>
<td>モデル</td>
<td>デルサーバのモデル番号を表示します。</td>
</tr>
<tr>
<td>iDRAC</td>
<td>iDRACのバージョンを表示します。</td>
</tr>
<tr>
<td>最新ステータスの更新</td>
<td>サーバの最新更新時のタイムスタンプを表示します。</td>
</tr>
</tbody>
</table>

System Information（システム情報）パネルでは、iDRACネットワーク接続性ステータスサーバホストの電源状態、エクスプレッサービスコード、オペレーティングシステム、モデルID、iDRACのDNS名、サーバのBIOSバージョン、サーバのCPU情報、システムメモリおよび位置情報などをサーバに関する詳細情報が表示されます。行01デフォルトクリックすると、iDRACの起動ボタンをクリックして、選択したiDRACインデックスページへのシングルサインオンリダイレクトしたiDRACインデックスページにリダイレクトされるシングルサインオンを実行するボタンをクリックします。選択したサーバで仮想コンソールにアクセスするか、More Actions（追加アクション）ドロップダウンリストでサーバの電源操作を実行できます。

iDRACユーザーログインの管理、およびアラートの設定、グループインベントリのエクスポートは、サポートされたグループアカウントです。

ネットワーク設定の要件

グループマネージャーは、IPv6リンクローカルネットウォーティングを使用してiDRAC間の通信を行います（WebブラウザGUIを除く）。リンクローカル通信はルーティングされないパケットとして定義されています。したがって、ルーターによって分離されたiDRACはローカルグループに参加できません。vLANにiDRAC専用のポートまたは共有LOMが割り当てられている場合、vLANはグループに参加できるiDRACの数を制限します（iDRACは同一vLAN上の必要があり、トラフィックはルーターを通過することとはできません）。
グループ マネージャーが有効な場合、iDRAC の現在のユーザーディスクリプトネットワーク設定に関わらず、iDRAC は IPv6 リンク ローカル アドレスを有効にします。グループ マネージャーは、iDRAC が IPv4 または IPv6 IP アドレス用に設定されている場合に使用できます。

グループ マネージャーは mDNS を使用してネットワーク上の他の iDRAC を検出し、リンク ローカル IP アドレスを使用してグループの通常のインベントリー、監視、管理のための暗号化パケットを送信します。IPv6 リンク ローカル ネットワークを使用する場合、グループ マネージャーのポートおよびパケットはローカル ネットワーク内でのみ使用され、外部ネットワークからアクセスすることはできません。

ポートは次のとおりです（グループ マネージャー固有の機能で使用されるポートのみ、すべての iDRAC ポートが含まれているわけではありません）。
- 5353 (mDNS)
- 443 (Web サーバー) - 構成可能
- 5670 （マルチキャスト グループ通信）
- CO00-FO00 はグループ内で通信するメンバーごとに 1 つずつ空きネットワークを動的に識別

ネットワーキングのベスト プラクティス

- グループは、同じ物理リンクのローカル ネットワーク上にある小規模なグループを想定しています。
- セキュリティを強化するために、専用の iDRAC ネットワーク ポートの使用をお勧めします。共有 LOM もサポートされています。

ネットワークに関するその他の考慮事項

ネットワークドリポジトリ内のルーターによって分離された 2 つの iDRAC は、別々のローカル ネットワーク上にあるとみなされ、同じ iDRAC ローカル グループに参加することはできません。つまり、iDRAC が専用 NIC 設定で構成されている場合、サーバーの背面にある iDRAC 専用ポートに接続されているネットワーク ケーブルは、すべての関連サーバーについてローカル ネットワーク下にある必要があります。

iDRAC が共有 LOM ネットワーク設定で構成されている場合、グループ マネージャーがサーバーハストと iDRAC を検出して共通グループにオーバーディングするには、これらのサーバー両方で使用される共有ネットワーク接続がローカルネットワークに接続されている必要があります。iDRAC が専用 LOM モードと共有 LOM モードの NIC 設定の組み合わせで構成されている場合も、すべてのネットワーク接続がルーターを通過しなければ、共通グループにオーバーディングすることができます。

ログインの管理

このセクションを使用して、グループから新規ユーザーを追加、ユーザーパスワードを変更、ユーザーを削除します。

ログインの管理を含むグループジョブは、1 回限りのサーバ設定です。Group Manager は SCP とジョブを使用して変更を行います。グループ内の各 iDRAC は、各 Group Manager ジョブに対するそれぞれのジョブキューニュル内の個別ジョブを所有します。Group Manager はメンバー iDRAC での変更を検出し、メンバーの設定をロックしたりします。

メモ: グループジョブでは、どの iDRAC に対してもロックダウンモードを設定または上書きしません。

新規ユーザーオプション

このセクションを使用して、グループ内のすべてのサーバ上で新しいユーザーディスクリプトの作成および追加を行います。グループジョブは、そのグループ内のすべてのサーバーにユーザーディスクリプトの作成を含んでいます。グループジョブのステータスは、GroupManager（グループマネージャ） > Jobs（ジョブ） > グループ内の設定にアクセスできます。

メモ: デフォルトでは iDRAC はローカル管理者アカウントで設定されます。ローカル管理者アカウントを使用して、各パラメータの詳細情報にアクセスできます。

詳細については、「ユーザーアカウントと権限の設定」を参照してください。

表 36. 新規ユーザーオプション

<table>
<thead>
<tr>
<th>オプション</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>新規ユーザーオプション</td>
<td>新しいユーザーの詳細情報を入力できます。</td>
</tr>
</tbody>
</table>
表 36. 新規ユーザーオプション（続き）

<table>
<thead>
<tr>
<th>オプション</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>iDRAC 権限</td>
<td>将来使用するために、ユーザーロールの定義できます。</td>
</tr>
<tr>
<td>詳細ユーザー設定</td>
<td>(IPMI) サーバー特権を設定でき、SNMP を有効にできます。</td>
</tr>
</tbody>
</table>

表 37. アラートオプションの設定

<table>
<thead>
<tr>
<th>オプション</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP（電子メール）サーバアドレス設定</td>
<td>サーバーのIPアドレス、SMTPポート番号を設定し、認証を有効にできます。認証を有効にする場合は、ユーザーロールにパスワードを入力する必要があります。</td>
</tr>
<tr>
<td>電子メールアドレス</td>
<td>複数の電子メールアドレスを設定し、システムがアラートを発行する際に送信し、アラートを期待する対象者に電子メールを送信できます。</td>
</tr>
<tr>
<td>アラートカテゴリ</td>
<td>複数のアラートカテゴリを選択して電子メール通知を設定するようにできます。</td>
</tr>
</tbody>
</table>

**メモ: システムロックダウンが有効になった iDRAC のメンバーで、同じグループ内の場合、ユーザーパスワードが最新でないというエラーが返されます。**
エクスポート

このセクションは、グループサマリをローカルシステムにエクスポートするとき、参考にしてください。情報は CSV ファイル形式でエクスポートできます。情報には、グループに含まれる個々のシステムに関連するデータが含まれます。エクスポートには、次の情報が CSV 形式で組み込まれます。サーバの詳細:

- Health (正常性)
- ホスト名
- iDRAC IPv4 アドレス
- iDRAC IPv6 アドレス
- 資産タグ
- モデル
- iDRAC ファームウェアバージョン
- 最新ステータスの更新
- エクスプレスサービスコード
- iDRAC の接続
- 電源状態
- オペレーティングシステム
- サービスタグ
- ノードID
- iDRAC の DNS 名
- BIOS バージョン
- CPU 詳細
- システムメモリ (MB)
- 場所の詳細

メモ: Internet Explorer を使用している場合、CSV ファイルをダウンロードするときは、拡張セキュリティ設定を適宜無効にします。

検出されたサーバビュー

ローカルグループの作成後、iDRAC グループマネージャは、ローカルネットワーク上の他のすべての iDRAC に、新しいグループが作成されたことを通知します。Discovered Servers (検出されたサーバ) に iDRAC を表示するには、各 iDRAC でグループマネージャ機能を有効にしておく必要があります。Discovered Servers View (検出されたサーバビュー) には、いずれかのグループに属する、同じネットワーク上で検出された iDRAC のリストが表示されます。検出されたシステムのリストに iDRAC が表示されない場合は、特定の iDRAC にログオンしてグループに参加する必要があります。グループを作成した iDRAC は、他の iDRAC がそのグループに参加するのを待つ一時的なグループマネージャとして表示されます。

メモ: グループマネージャーコンソールの Discovered Servers View (検出されたサーバビュー) では、ビューに表示された 1 つ、または複数のサーバを該当するグループにオンボードすることができます。動作の進捗状況は GroupManager > Jobs (ジョブ) で追跡できます。また、iDRAC にログインし、オンボードするグループをドロップダウンリストから選択して、該当するグループに参加させることもできます。Group Manager Welcome (グループマネージャへようこそ) 画面には、iDRAC の索引ページからアクセスできます。

### 表 38. グループオンボードオプション

<table>
<thead>
<tr>
<th>オプション</th>
<th>説明</th>
</tr>
</thead>
</table>
| ログイン後にログイン情報変更 | 特定の行を選択し、Onboard and Change Login (ログイン後にログイン情報変更) オプションを選択して、新しく検出されたシステムをグループに参加させます。グループに参加させるには、新しいシステム用の管理者ログイン資格情報を入力する必要があります。システムがデフォルトのパスワードを持ってい る場合、グループへのオンボード時にそのパスワードを変更する必要があります。
グループオンボードにより、同じグループの設定を新しいシステムに適用することができます。 |
<p>| 無視                | システムをどのグループにも追加しない場合は、検出されたサーバリストからシステムを無視することができます。 |</p>
<table>
<thead>
<tr>
<th>オプション</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>無視しない</td>
<td>検出されたサーバリストで復旧するシステムを選択できます。</td>
</tr>
<tr>
<td>再スキャン</td>
<td>検出されたサーバのリストをいつでもスキャンして生成することができます。</td>
</tr>
</tbody>
</table>

**Jobs（ジョブ）ビュー**

ジョブビューでは、グループジョブの進行状況を追跡でき、接続によって引き起こされた障害を修正するためのシンプルな回復に役立ちます。また、監査ログとして実行された最後のグループアクションの履歴も表示します。ユーザーはジョブビューを使用して、グループ全体でのアクションの進行状況を追跡したり、将来の実行がスケジュールされているアクションをキャンセルしたりできます。ジョブビューでは、実行済みの最後の 50 のジョブのステータス、および処理の成功または失敗を表示できます。

<table>
<thead>
<tr>
<th>オプション</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>ステータス</td>
<td>ジョブのステータスと進行中のジョブの状態を示します。</td>
</tr>
<tr>
<td>ジョブ</td>
<td>ジョブの名前を表示します。</td>
</tr>
<tr>
<td>ID</td>
<td>ジョブの ID を表示します。</td>
</tr>
<tr>
<td>開始時刻</td>
<td>開始時刻を表示します。</td>
</tr>
<tr>
<td>終了時刻</td>
<td>終了時刻を表示します。</td>
</tr>
<tr>
<td>処置</td>
<td>キャンセル - スケジュールされたジョブが実行状態に移行する前にキャンセルできます。実行中のジョブは、停止ボタンを使用して停止できます。 再実行 - データは完全に失敗したジョブを再実行できます。 削除 - ユーザーは完了した古いジョブを削除できます。</td>
</tr>
<tr>
<td>エクスポート</td>
<td>グループジョブの情報はローカルシステムにエクスポートして後で参照できます。ジョブリストは csv ファイルフォーマットにエクスポートできます。このジョブリストには、個々のジョブに関連するデータが含まれています。</td>
</tr>
</tbody>
</table>

**メモ:** ジョブエントリごとに、システムのリストには最大 100 台のシステムの詳細が表示されます。それぞれのシステムエントリには、ホスト名、サービスタグ、メンバーのジョブステータス、メッセージ（ジョブが失敗した場合）が含まれます。

ジョブを作成するすべてのグループアクションは、すべてのグループメンバーに対して実行され、即座に有効になります。次のタスクを実行できます。

- ユーザーの追加 / 編集 / 削除
- 電子メールアラートの設定
- グループのパスコードと名前の変更

**メモ:** すべてのメンバーがオンラインかつアクセスできる状態にある場合は、グループジョブは短時間内に完了します。ジョブの開始から完了までに 10 分ほどかかることがあります。アクセスできないシステムがあれば、ジョブが待機状態になり、最大 10 時間アクションを再試行します。

**メモ:** オンボーディングジョブの実行中は、他のジョブをスケジュールできません。次のようなジョブが対象になります。

- 新規ユーザーの追加
- ユーザーパスワードの変更
- ユーザーの削除
- アラートの設定
- 追加のシステムのオンボード
- グループのパスコードの変更
- グループ名の変更

iDRAC 9 グループ マネージャー 191
オンボードイングタスクの実行中に別のジョブを呼び出そうとすると、GMGR0039のエラーコードが表示されます。オンボードイングタスクによってすべての新しいシステムのオンボードが一度でも試行された後は、いつでもジョブを作成できるようになります。

ジョブのエクスポート

ログはローカルシステムにエクスポートして後で参照できます。ジョブリストはcsvファイルフォーマットにエクスポートできます。このジョブリストには、各ジョブに関連するすべてのデータが含まれています。

メモ：エクスポートされたCSVファイルは英語でのみ提供されています。

グループ情報パネル

Group ManagerのサマリビューのGroup Information（グループ情報パネル）には、組み立てられたグループの概要が表示されます。現在のグループ設定はGroup Settings（グループ設定）ボタンをクリックしてアクセスできるGroup Settings（グループ設定）ページで編集できます。ここには、グループに含まれるシステムの数が表示されます。また、グループに含まれるプライマリおよびセカンダリコントローラの情報も提供されます。

グループ設定

グループ設定ページには、選択したグループ属性のリストが表示されます。

表40. グループ設定の属性

<table>
<thead>
<tr>
<th>グループ属性</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>グループ名</td>
<td>グループの名前を表示します。</td>
</tr>
<tr>
<td>システムの数</td>
<td>グループ内のシステムの合計数を表示します。</td>
</tr>
<tr>
<td>作成日</td>
<td>タイムスタンプの詳細を表示します。</td>
</tr>
<tr>
<td>作成者</td>
<td>グループ管理者の詳細を表示します。</td>
</tr>
<tr>
<td>制御システム</td>
<td>制御システムとして機能し、グループ管理タスクを調整するシステムのサービスタグを表示します。</td>
</tr>
<tr>
<td>バックアップシステム</td>
<td>バックアップシステムとして機能するシステムのサービスタグを表示します。制御システムが使用できない場合は、制御システムの役割を果たします。</td>
</tr>
</tbody>
</table>

ユーザーはグループの下の表にリストされている操作を実行できます。これらの操作（グループ名の変更、グループパスコードの変更、メンバーの削除、およびグループの削除）に対してグループ設定ジョブが作成されます。グループジョブのステータスは、GroupManager（グループマネージャ）> Jobs（ジョブ）ページで表示または変更できます。

表41. グループ設定のアクション

<table>
<thead>
<tr>
<th>処置</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>名前の変更</td>
<td>Current Group Name（現在のグループ名）をNew Group Name（新しいグループ名）に変更できます。</td>
</tr>
<tr>
<td>Change Passcode (パスコードの変更)</td>
<td>New Group Passcode（新しいグループパスコード）を入力し、Reenter New Group Passcode（新しいグループパスコードの再入力）でそのパスワードを確認することで、既存のグループパスワードを変更できます。</td>
</tr>
<tr>
<td>システムの削除</td>
<td>グループから複数のシステムを一度に削除できます。</td>
</tr>
<tr>
<td>グループの削除</td>
<td>グループを削除できます。グループマネージャの機能を使用するには、管理者権限が必要です。保留中のジョブは、グループが削除された場合に停止されます。</td>
</tr>
</tbody>
</table>

192 iDRAC 9 グループマネージャ
選択したサーバでの操作

Summary（サマリ）ページで、行をダブルクリックし、シングルサインオンリダイレクトを使用してそのサーバのiDRACを起動できます。ポップアップブロッカーは、ブラウザの設定でオフにしておいてください。More Actions（その他の操作）ドロップダウンリストから該当アイテムをクリックして、選択したサーバ上で次の操作を実行できます。

表42. 選択したサーバ上での操作

<table>
<thead>
<tr>
<th>オプション</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>正常なシャットダウン</td>
<td>オペレーティングシステムをシャットダウンし、システムの電源を切ります。</td>
</tr>
<tr>
<td>コールドリブート</td>
<td>電源を切ってからシステムを再起動します。</td>
</tr>
<tr>
<td>仮想コンソール</td>
<td>新しいブラウザウィンドウで、単一サインオンを使用して仮想コンソールを起動します。</td>
</tr>
<tr>
<td></td>
<td>メモ: この機能を使用するには、ブラウザのポップアップブロッカーを無効にします。</td>
</tr>
</tbody>
</table>

Group Managerのシングルサインオン

グループ内のすべてのiDRACは、共有シーケンスユーティリティのパスコードと共有グループ名に基づいて、相互に信頼します。結果として、グループメンバー内の1つのiDRACの管理者ユーザーは、Group Managerウェブインタフェースのシングルサインオンを介してアクセスする際、グループメンバー内のすべてのiDRACに対する管理者レベルの権限を付与されることになります。iDRACのログには、ユーザーレベルのログオンしたユーザーとして<ユーザー>-<SVCTAG>と記録されます。<SVCTAG>は、ユーザが最初にログインしたiDRACのサブスタンスです。

Group Managerの概念—制御システム

- 自動的に選択—デフォルトでは、Group Managerに設定されている最初のiDRACです。
- Group Manager GUIのワークフローを提供します。
- すべてのメンバーを追跡、記録します。
- タスクを調整します。
- ユーザーがいずれかのメンバーにログインして、Open Group Manager（グループマネージャを開く）をクリックすると、ブラウザはプライマリコントローラにリダイレクトされます。

Group Managerの概念—バックアップシステム

- ブライマリコントローラが一定の時間（10分以上）にわたってオフラインになった場合に、ブライマリコントローラは自動的にセカンダリコントローラを選択して引き続きます。
- ブライマリコントローラとセカンダリコントローラの両方が一定の時間（14分以上）にわたってオフラインになった場合は、新しいブライマリコントローラとセカンダリコントローラが選ばれます。
- すべてのグループメンバーとタスクについて、Group Managerのキャッシュのコピーを保存します。
- 制御システムとバックアップシステムは、Group Managerによって自動的に決定されます。
- ユーザー設定やバックアップシステムは、Group Managerによって自動的に決定されます。

iDRAC 9 グループマネージャー 193
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 wsmann 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、コメントを追加したり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。

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、同じ sel エントリが提供されます。

メモ: idrac を再起動すると、sel と lc のログのタイムスタンプが一致しなくなる場合があります。

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、maintenance（メンテナンス）> system event log（システムイベントログ）の順に移動します。

system event log（システムイベントログ）ページには、システム正常性インジケータ、タイムスタンプ、および記録された各イベントの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 がクリアされると、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、sel をクリアしたユーザー名と 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
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。この操作を行うには、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 ログでは、管理下システムに取り付けられたコンポーネントに関する変更履歴が提供されます。各ログエントリに作業メモを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。

- すべて
- システムの正常性 - System Health (システムの正常性) カテゴリには、システムシャーシ内のハードウェアに関連するアラートがすべて表示されます。
- ストレージ - Storage Health (ストレージの正常性) カテゴリには、ストレージサブシステムに関連するアラートが表示されます。
- アップデート - Update (アップデート) カテゴリには、ファームウェア/ドライバのアップグレード/ダウングレードで発生したアラートが表示されます。
- 監査 - Audit (監査) カテゴリには、監査ログが表示されます。
- 設定 - Configuration (設定) カテゴリには、ハードウェア、ファームウェア、およびソフトウェアの設定変更に関連するアラートが表示されます。
- 作業メモ

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
- Redfish
- 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。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: バーナリ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。
メモ: MX プラットフォームでは、Lifecycle Controller は、OME - Modular を使用して作成された設定またはインストールジョブの複数のジョブ ID をログに記録します。実行されたジョブの詳細については、OME - Modular ログを参照してください。
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、Maintenance (メンテナンス) > Lifecycle Log (Lifecycle ログ) の順にクリックします。Lifecycle Log (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

ローグは、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。
   フィルタしたログエントリは ログ結果 に表示されます。

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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。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（アクティブまたはアーカイブされたエントリ）を単一の圧縮 XML ファイルで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できます。圧縮 XML ファイルの拡張子は .xml.gz です。ファイルエントリは、各エントリのシーケンス番号に基づいた順番で、シーケンス番号の最も低いものから最も高いものへ並べられます。

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。
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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。参照してください。

作業メモの追加

iDRAC 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。

memo: 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、Dashboard（ダッシュボード） > Notes（メモ） > add note（メモの追加）と移動します。
   Work Notes（作業メモ）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。
   memo: 特殊文字を多用しないよう推奨します。
3. Save（保存）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。この作業を開始する前に、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グインの設定

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、Configuration（設定） > System Settings（システム設定） > Remote Syslog Settings（リモート Syslog 設定）に移動します。
   リモート Syslog 設定ページが表示されます。
2. リモート syslog を有効にして、サーバアドレスおよびポート番号を指定します。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。
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グインの設定

リモートシステムログインを設定するには、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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。参照してください。
iDRAC での電源のモニタリングと管理

iDRAC を使用することで、管理下システムの電源要件のモニターと管理ができます。これは、システムでの消費電力の分配と調整を適切に行うことで、電源停止に対するシステム保護に役立ちます。

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、ライセンス付きの機能です。
- 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。

トピック:
- 電力の監視
- 電力消費量の警告しきい値の設定
- 電源制御操作の実行
- 電力制限
- 電源装置オプションの設定
- 電源ボタンの有効化または無効化
- Multi-Vector Cooling

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
- ピーク時のヘッドドーム値および瞬間的ヘッドドーム値（ラックおよびタワーパーソーの場合）

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。

メモ: iDRAC ファームウェアのアップデートまたはリセット後、電力消費グラフがワイプ/リセットされます。

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、System（システム）> Performance（パフォーマンス）に移動します。
- 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、および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。Reset Historical Peak（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。

表示されたプロバ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 CPU、メモリ、入出力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、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、SystemPerfStatistics サブコマンドを使用します。詳細については、「iDRAC RACADM CLI ユーザーガイド」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。

プレードシステムの警告電力しきい値は、CMC（非 MX プラットフォーム）または OME Modular（MX プラットフォーム）の電力割り当てに設定されています。

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。

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。

ウェブインター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 ウェブインターフェースで、System（システム）> Overview（概要）> Present Power Reading and Thresholds（現在の電力読み取り値およびしきい値）の順に移動します。

2. Present Power Reading and Thresholds（現在の電力読み取り値およびしきい値）セクションで、Edit Warning Threshold（警告しきい値の編集）をクリックします。

3. Warning Threshold（警告しきい値）列に、Watts（ワット）または BTU/hr（BTU/時）の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。この値は、14 で割り切れる最も近い値に丸められます。Watts（ワット）で入力した場合は、システムが自動的に計算して BTU/hr（BTU/時）を表示します。同様に、BTU/時で入力した場合は、Watts（ワット）の値が表示されます。

4. Save（保存）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、ウェブインターフェースまたは 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 Services または WSMAN を使用して、これらの操作を実行することもできます。詳細については、https://www.dell.com/support で「Dell Lifecycle Controller Remote Services クイックスタートガイド」は、www.dell.com/idracmanuals にあります。および「Dell 電源管理」プロファイルマニュアルを参照してください。

iDRAC によるサーバー電源制御操作は、BIOS で設定された電源ボタンの動作とは独立しています。BIOS で物理的な電源ボタンが無効に設定されていても、PushPowerButton 機能を使用して、システムを正常に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、設定 > 電源管理 > 電源制御 の順に移動します。電源制御 オプションが表示されます。

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、「iDRAC RACADM CLI ガイド」を www.dell.com/idracmanuals にあります。を参照してください。

電力制限

高負荷のシステムがデータセンターに示す AC および DC 電力消費量の範囲を対象とする電力しきい値の限界を表示できます。これは、ライセンス付きの機能です。

ブレードサーバーの電源上限

限定されたハードウェアインベントリに基づいて、ブレードサーバーに電源を入る前に、iDRAC はシャーシマネージャーにブレードサーバーの電源要件を提供します。電力消費量が時間の経過とともに増加し、サーバーが最大割り当て電力を消費する場合、iDRAC は CMC（非 MX プラットフォーム）または OME Modular（MX プラットフォーム）に最大電力を増やすよう要求します。その結果、電力供給が増加しますが、消費量が減少しても電力供給は減少しません。

システムの電源が投入されて初期化された後、iDRAC は、実際のハードウェア構成に基づいて新しい電源要件を計算します。CMC（MX プラットフォームでない場合）または OME Modular（MX プラットフォームでない場合）が新しい電源要求の割り当てに失敗しても、システムの電源はオンのままであります。

CMC または OME Modular は優先順位の低いサーバーの未使用電力を回収し、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。

電力上限ポリシーの表示と設定

電源上限ポリシーが有効になっている場合、システムにユーザー定義の電力制限が適用されます。電力上限が有効になっていない場合は、デフォルトの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とは独立しています。指定されたしきい値付近に電力消費量を制限するため、システムパフォーマンスは動的に調整されます。

実際の電力消費量は、作業負荷によって異なります。パフォーマンス調整が完了するまで、一時的にしきい値を超える場合があります。たとえば、潜在的電力消費量の最小値と最大値がそれぞれ 500 W と 700 W のシステムを考えてみます。電力バジェットのしきい値を指定して、消費を 525 W に抑えることができます。この電力バジェットが設定されている場合、システムのパフォーマンスが動的に調整され、電力消費量が 525 W 以下に維持されます。

電力上限が非常に低く、周辺が通常よりも高い場合、システムの電源投入時またはリセット時に電力消費量は一時的に電力上限を超える場合があります。

電力上限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。

電力上限しきい値を BTU/時に設定すると、ワット数への変換で最も近い整数に丸められます。電力上限のしきい値がシステムから読み取られた場合のワット数から BTU/時の変換も切り捨てられます。切り捨てにより、実際の値はわずかに異なる場合があります。
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

電力ポリシーや表示し、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、設定 > 電源管理 > 電源上限ポリシーの順に移動します。

   現在の電力ポリシーや制限が電力上限制限セクションに表示されます。

2. 電力上限の下にある有効を選択します。

3. 電力上限制限セクションに、推奨範囲内のワット、BTU/時、または推奨システム制限値の最大 % で電力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。


詳細については、『iDRAC RACADM CLI ガイド』は、www.dell.com/idracmanuals にあります。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

現在の電力制限値を表示して設定するには、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。

   ☞ 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、ユーザーディフィニティブ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フできます。

2 台の 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。

ホットスペアが有効になると、負荷に基づいて PSU をアクティブ化、またはスリープモードにすることができます。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 がオフの状態で、残り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、少量の電流を提供します。これは 2 台の PSU より 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ない場合、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。

力率は、見かけの電力に対する実際の消費電力の割合です。力率補正が有効になっている場合、サーバは、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、サーバの工場出荷時に力率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、Configuration（設定）> Power Management（電力の管理）> Power Configuration（電源設定）> に移動します。
2. Power Redundancy Policy（電源冗長性ポリシー）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、get/set コマンドと一緒に次のオプ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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。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。

memo: 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。
- 力率の補正を有効または無効にします。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。
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。

memo: 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のみ使用可能です。

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。

Multi-Vector Cooling
Multi-Vector Cooling は、Dell EMC サーバプラットフォームの温度制御に多方面的アプローチを行います。iDRAC ウェブインタフェースで、Multi-Vector Cooling のオプションを設定するには、設定 > システム設定 > ハードウェアの設定 > ファン設定の順に移動します。これにより以下が含まれています（限定は含まれません）。
- サーバ内のさまざまな場所でリアルタイムに温度状態を把握できるようにする大規模なセンサのセット（温度、電源、インベントリなど）。設定に基づいて、ユーザーの必要性に関連するセンサの小規模なサブセットのみが表示されます。
- インテリジェントで適応型の閉回路制御アルゴリズムは、ファンの応答を最適化し、コンポーネントの温度を維持します。
- また、ファンの電力、エアフローの消費、音響を低減します。
- ファンゾーンマッピングを使用すると、必要に応じてコンポーネントの冷却を開始することができます。したがって、電力使用率の効率を犠牲にすることなく、最大のパフォーマンスを実現します。
LFM メトリック（リニアフィート / 毎分・PCIe カードのエアフローユ要件の指定方法に関する業界基準）を用いた、各 PCIe スロットの正確な表示。さまざまな iDRAC インタフェースにこのメトリックを表示することで、次が可能になります。

1. サーバ内の各スロットの LFM 最大値を把握します。
2. 各スロットの PCIe の冷却が必要な方法で行われているかを把握します（エアフロー制御、温度制御）。
3. カードがサーバーパーティ製のカード（ユーザー定義のカスタムカード）の場合、スロットに提供されている最適の LFM 値を確認します。
4. サーバーパーティ製カードにカスタム最小 LFM 値をダイヤルインすると、カード冷却の必要性をさらに正確に定義することが可能になります。

さまざまな iDRAC インタフェースにリアルタイムでシステムエアフローメトリック（CFM、立方フィート / 分）を表示し、各サーバの CFM 電力消費の集計に基づいてデータセンターでのエアフローバランシングを可能にします。

サーマルプロファイルなどのカスタム温度設定（最大パフォーマンス対ワットあたりの最大パフォーマンス、サウンドキャップ）、ファン速度のオプション（最小ファン速度、ファン速度のオフセット）および排気温度の要素設定が可能になります。

1. これらの設定のほとんどは、ベースラインの冷却またはアルゴリズムによって生成された冷却をさらに追加し、ファンの速度がシステム冷却要件を下回らないようにします。
2. 排気温度の要素設定は、排気温度をお客様の希望する設定に制限します。
3. サウンドキャップ オプションは、第 14 世代 PowerEdge サーバの新しい機能です。CPU 電力消費を抑え、ファインの速度と音を制御します。これは、音が出る状況に特有のもので、システムパフォーマンスを低下させることもあります。

システムのレイアウトと設計により、エアフロー性能が向上し（高電力消費）、システム構成で最適化します。これにより、システムの制限が減少し、機能の密度が向上します。

1. 円滑なエアフローにより、ファンの電力消費率に効率的なエアフローを実現します。
2. サウンドキャップは、効率性の向上、パフォーマンスの向上、寿命の延長、振動の低減を目的として設計されています。また、優れた防音効果を提供します。

1. ファンは、フルスピードで長時間運用しても長寿命です（一般的に 5 年以上）。
2. サウンドキャップは、最小限の（必要な）エアフローでコンポーネントの冷却を最適化するために設計されており、高性能 CPU をサポートしています。
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）
- 綜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（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など）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ル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ることがあります。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のパーソナルリティなど（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。

トピック：
- ネットワークデバイスのインベントリと監視
- FC HBA デバイスのインベントリと監視
- SFP トランシーバー デバイスのインベントリと監視
- ネットワークインタフェースキャップチャ
- 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

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

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、System（システム）> Overview（概要）> Network Devices（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。

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、「IDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。 を参照してください。
RACADM または WSMan を使用すると、iDRAC ウェブインターフェースに表示されるプロパティ以外のプロパティが追加表示される場合があります。

接続ビュー
データセンター環境では、サーバのネットワーク接続を手動でチェックして、トラブルシューティングを行うことはできません。iDRAC9 は、iDRAC 接続ビューを使用してこのような作業を合理化します。この機能を使用すると、サーバの展開、更新、監視、および保守に使用しているのと同じ一元化 GUI から、ネットワーク接続をリモートで確認し、トラブルシューティングを行うことができます。iDRAC9 接続ビューには、スイッチポートからサーバのネットワークポートや iDRAC（Integrated Dell Remote Access Controller）専用ポート接続まで、物理マッピングの詳細が表示されます。ブランドに関係なく、サポートされているすべてのネットワークカードが接続ビューに表示されます。

サーバのネットワーク接続を手動でチェックしてトラブルシューティングする代わりに、ネットワーククエリの接続をリモートで表示および管理することができます。

接続ビューには、サーバポートに接続されたスイッチポートと iDRAC 専用ポートの情報が表示されます。サーバのネットワークポートには、PowerEdge LOM、NDC、メザニンカード、PCIe アドインカードが含まれます。

ネットワークデバイスの接続ビューを確認するには、[システム] > [概要] > [ネットワークデバイス] > [接続ビュー] に移動して、接続ビューを表示させます。
また、[iDRAC 設定] > [接続] > [ネットワーク] > [接続設定] > [接続ビュー] をクリックして、接続ビューを有効または無効にすることもできます。

RACADM の SwitchConnection View コマンドを使用して接続ビューを検出できます。また、コマンドを使用して表示することもできます。

フィールドまたは説明
はオプション
有効
接続ビューを有効にするには、有効を選択します。デフォルトでは、有効オプションが選択されていません。

状態
iDRAC 設定の接続ビューで接続ビューオプションを有効にした場合に、有効と表示されます。

スイッチ接続 ID
デバイスポートの接続に使用されているスイッチの LLDP シャーシ ID が表示されます。

スイッチポート接続 ID
デバイスポートが接続されているスイッチポートの LLDP ポート ID が表示されます。

メモ: 接続ビューが有効化されてリンクが接続されると、スイッチ接続 ID とスイッチポート接続 ID が使用可能になります。
関連付けられたネットワークカードには、接続ビューとの互換性が必要です。iDRAC の設定権限を持つユーザーのみ、接続ビュー設定を変更できます。

iDRAC9 4.00.00.00 以降のバージョンにおいて、iDRAC は標準 LLDP パケットの外部スイッチへの送信をサポートしています。これによりネットワーク上での iDRAC を検出するためのオプションが提供されます。iDRAC からは次の 2 種類の LLDP パケットが、アウトバウンドネットワークに送信されます。

- トポロジー LLDP - この機能での LLDP パケットは、サポートされているすべてのサーバー NIC ポートを通過するため、外部スイッチにより、送信元サーバー、NDC ポート [NIC FQDD]、シャーシ内の IOM 位置、プレードシャーシのサービススタグなどの特定ができます。トポロジー LLDP は、iDRAC9 4.00.00.00 以降のバージョンにおいて、すべての PowerEdge サーバーのオプションとして使用できます。LLDP パケットには、サーバーネットワークデバイスの接続情報が含まれており、I/O モジュールおよび外部スイッチによる、それらの構成のアップデートに利用されます。

メモ:
○ MX シャーシ構成が正常に機能するには、トポロジー LLDP を有効にする必要があります。
○ トポロジー LLDP は、1GBe コントローラーではサポートされておらず、10GBe コントローラー（Intel X520、QLogic 578xx）を選択します。

- ディスカバリ LLDP - この機能での LLDP パケットは、使用中のアクティブな iDRAC NIC ポート（専用 NIC または共有 LOM）のみを通過するため、隣接する特定スイッチをスイッチ内の iDRAC 接続ポートの検出ができます。ディスカバリ LLDP は、アクティブな iDRAC ネットワークポートのみに限定されるため、サーバー内のすべてのネットワークポートで検出されるものではありません。ディスカバリ LLDP では、IP アドレス、MAC アドレス、サービススタグなどの iDRAC に類似した詳細情報を保持するために、スイッチは、接続されている iDRAC デバイスおよび iDRAC データの自動検出ができます。

メモ: ボート/バーチャリゼーションの仮想 MAC アドレスがクリアされた場合、仮想 MAC アドレスが MAC アドレスと同じになります。
トポロジー LLDP を有効化または無効化するには、[iDRAC 設定] > [接続] > [ネットワーク] > [共通設定] > [トポロジー LLDP] の順に移動して、トポロジー LLDP を有効または無効にします。デフォルトでは、MX サーバーに対して是有効になっており、他のすべてのサーバーに対しては無効になっています。

iDRAC ディスカバリー LLDP を有効化または無効化するには、[iDRAC 設定] > [接続] > [ネットワーク] > [共通設定] > [iDRAC ディスカバリー LLDP] の順に移動します。デフォルトでは、有効オプションが選択されています。

iDRAC から送信された LLDP パケットは、コマンド show lldp neighbors を用いてスイッチから確認できます。

接続ビューの更新
接続ビューの更新を用いて、スイッチ接続 ID とスイッチポート接続 ID の最新情報を表示します。

メモ: iDRAC にサーバのネットワークポートまたは iDRAC ネットワークポートに関するスイッチの接続およびスイッチのポート接続情報がある場合、何らかの理由でスイッチの接続およびスイッチのポート接続情報が5分以上更新されていないと、スイッチの接続およびスイッチのポート接続情報はすべてのユーザーインターフェースで古くなった（最後の正常なデータ）として表示されます。UI では、黄色い警告マークが表示されます。これは、一般的な表示で警告を示すものではありません。

接続ビューの可能な値
可能な接続ビュー 説明
機能が無効 接続ビュー機能が無効になっています。接続ビューデータを表示するには、機能を有効にします。
リンクなし ネットワークコントローラポートに関連付けられているリンクがダウンしていることを示します。
使用不可 スイッチで LLDP が有効になっていません。スイッチポートで LLDP が有効になっているかどうかを確認します。
非対応 ネットワークコントローラは、接続ビュー機能をサポートしていません。
古いデータ 最後に正常に動作しているデータ。ネットワークコントローラポートのリンクがダウンしているか、システムの電源がオフになっています。最新のデータを取得するには、更新オプションを使用して、接続ビューの詳細を更新します。
有効なデータ 有効なスイッチの接続 ID と、スイッチポートの接続 ID 情報を表示します。

サポートされているネットワークコントローラの接続ビュー
次のカードまたはコントローラで接続ビュー機能がサポートされています。

製造元 タイプ
Broadcom
- 57414 rNDC 25 GE
- 57416/5720 rNDC 10 GbE
- 57412/5720 rNDC 10GbE
- 57414 PCIe FH/LP 25 GE
- 57412 PCIe FH/LP 10GbE
- 57416 PCIe FH/LP 10GbE

Intel
- X710 bNDC 10 Gb
- X710 DP PCIe 10 Gb
- X710 DP PCIe 10 Gb
- X710 + i550 rNDC 10 Gb+1 Gb
- X710 rNDC 10 Gb
- X710 bNDC 10 Gb
- XL710 PCIe 40Gb
- XL710 OCP Mezz 10 Gb
- X710 PCIe 10Gb

Mellanox
- MT27710 rNDC 40Gb
- MT27710 PCIe 40Gb
- MT27700 PCIe 100Gb

206 ネットワークデバイスのインベントリ、監視、および設定
製造元
QLogic
• QL41162 PCIe 10GE 2P
• QL41112 PCIe 10GE 2P
• QL41262 PCIe 25GE 2P

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 ホストバスアダプタ（FC HBA）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。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、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

MEMO: Emulex FC8 HBA は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 FC HBA デバイスの監視

FC HBA デバイス情報は、ウェブインタフェースを使用してビューに進めます。System (システム) > Overview (概要) > Network Devices (ネットワークデバイス) > Fibre Channel (ファイバチャネル) を押します。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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。を参照してください。

SFP トランシーバー デバイスのインベントリと監視

システムに接続されている SFP トランシーバー 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。サポートされているトランシーバーは次のとおりです。

• SFP
• SFP+
• SFP28
• SFP-DD
• QSFP
• QSFP+
• QSFP28
• QSFP-DD
• Base-T モジュール
• AOC & DAC ケーブル
• Ethernet に接続された RJ-45 Base-T
• ファイバチャネル
• 旧アダプターポート

最も有用なトランシーバー情報は、トランシーバー EPROM のシリアル番号とパーティションです。これにより、接続の問題をトラブルシューティングする際に、リモートにインストールされたトランシーバーを検証できます。SFP トランシーバー デバイスごとに、ポートに関する次の情報が表示されます。

• ベンダー名
• パーツ番号
Web インターフェイスを使用した SFP トランシーバーのモニタリング

Web インターフェイスで SFP トランシーバー情報確認するには、[システム] > [概要] > [ネットワークデバイス] の順に移動して、目的のデバイスをクリックします。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。

ポート統計情報では、トランシーバーが使用可能なスロット番号がページ名にも表示されます。

RACADM を使用した SFP トランシーバーの監視

RACADM を使用して SFP トランシーバーの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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。を参照してください。

テレメトリー・ストリーミング

テレメトリーを使用すると、PowerEdge サーバーからリアルタイムでデバイスメトリックス、イベント、データログを収集して、サブスクリプションしている外部クライアントまたはサーバーアプリケーションにストリーミングできます。テレメトリーを使用する場合には、生成する必要があるレポートのタイプと頻度を設定できます。

メモ: この機能はすべてのプラットフォームでサポートされていますが、iDRAC Datacenter ライセンスが必要です。

テレメトリーは「一対多」型のソリューションで、１台または複数の PowerEdge サーバー（iDRAC）からライブシステムデータを収集して、集中方式の「リモートサーバーモニタリング」に対応できます。テレメトリーを使用する場合には、テレメトリーが無効化されるまで、データストリーミングは自動的に行われ続けます。

次の表は、テレメトリーを使用して生成できるメトリックレポートについてまとめたものです。

<table>
<thead>
<tr>
<th>タイプ</th>
<th>メトリックグループ</th>
<th>インベントリ</th>
<th>センサー</th>
<th>統計情報</th>
<th>設定</th>
<th>メトリックス</th>
</tr>
</thead>
<tbody>
<tr>
<td>I/O デバイス</td>
<td>NIC</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
</tr>
<tr>
<td></td>
<td>FC HBA</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
</tr>
<tr>
<td>サーバー デバイス</td>
<td>CPU</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
</tr>
<tr>
<td></td>
<td>メモリ</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
</tr>
<tr>
<td></td>
<td>ファン</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
</tr>
<tr>
<td></td>
<td>PSU</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
</tr>
<tr>
<td></td>
<td>センサー</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
</tr>
<tr>
<td>環境</td>
<td>サーマル</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
</tr>
<tr>
<td></td>
<td>電源</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
<td>はい</td>
</tr>
</tbody>
</table>
メモ:

- StorageDiskSMARTDATA は、SAS/SATA バス プロトコルを使用し、BOSS コントローラー背後にある SSD ドライプでのみサポートされます。
- StorageSensor データは、Ready/Online/RAID 非対応モードで BOSS コントローラーの背後がないドライプについてのみサポートされます。
- NVMeSMARTData は、SSD (PCieSSD/NVMe Express) ドライプで PCie バス プロトコルを備えたもの (SWRAID の背後ではない) でのみサポートされます。
- GPGPUStatistics データは、ECC メモリ機能をサポートする特定の GPGPU モデルでのみ使用できます。
- PSUMetrics は、モジュラー型プラットフォームでは使用できません。
- CUPS はオーバーサーバーのテレメトリ ログは、AMD プラットフォーム サーバーでは無効にする必要があります。同じレポートを収集した場合、すべてのメトリック値は 0 を示します。
- ファン電力および PCIe 電力のメトリックは、一部のプラットフォームで 0 と表示される場合があります。

テレメトリのワークフロー:

1. 未インストールの場合は、Datacenter ライセンスをインストールします。
2. グローバル テレメトリ設定として、テレメトリーの有効化、Rsyslog サーバー ネットワーク アドレスおよび、RACADM、Redfish、SCP、iDRAC GUI の使用ポートなどを指定します。
3. RACADM または Redfish インタフェイスを使用して、必要なデバイス レポートまたはログについて、次のテレメトリー レポート ストリーミング パラメーターを設定します:
   - EnableTelemetry
   - ReportInterval
   - ReportTriggers

4. クライアントの Redfish によって、iDRAC での Redfish EventService へのサブスクリプションリクエストを作成します。
5. 事前定義されたトリガー条件が満たされると iDRAC は、サブスクリプトされたクライアントについて、メトリック レポートまたはログイベントデータを生成してプッシュします。

機能的制限:

1. セキュリティ上の理由から、iDRAC とクライアントの通信は、HTTPS ペースのみがサポートされています。
2. 安定性の理由から、iDRAC によるテレメトリーのサブスクリプションは最大 4 つまでサポートされています。
3. 管理者による手動削除の場合であっても、サブスクリプションの削除は、Redfish インターフェイスを介した場合にのみサポートされます。

テレメトリー機能の動作:

- 事前定義されたトリガー条件が満たされると iDRAC は、すべてのサブスクリプトされたクライアントについて、サブスクリプションで指定された宛先に対し、メトリック レポートまたはログイベントデータを生成してプッシュ (HTTP POST) します。クライアントが新しいデータを送信するのは、サブスクリプションが正常に作成された場合のみです。
- メトリックデータには、ノードからのデータ収集時のタイムスタンプが YYYY-MM-DD のフォーマットで含まれています。このフォーマットのタイムスタンプは、レポートの生成/送信時のものは異なります。
- クライアントは、Redfish インターフェイスを介して HTTP DELETE メッセージをサブスクリプションリソースの URI に送信することにより、サブスクリプションを終了することができます。
- サブスクリプションが iDRAC または クライアントによって削除された場合、iDRAC によるレポート送信 (HTTP POST) は行われません。配信エラーが事前定義された閾値を超えると、iDRAC によってサブスクリプションが削除される場合があります。
- ユーザーに管理者権限がある場合はサブスクリプションを削除できますが、Redfish インターフェイスを介した場合にのみ行えます。
- iDRAC によるサブスクリプション終了についてのクライアントの通知は、最終メッセージとしての "Subscription terminated" イベントの送信で行われます。
サブスクリプションは永続的で、iDRAC の再起動後も保持されます。ただし、racreset または LCwipe オペレーションのいずれかの実行によって削除することも可能です。

RACADM、Redfish、SCP、iDRAC などのユーザーインターフェイスには、クライアントサブスクリプションの現在のステータスが表示されます。

### シリアル データ キャプチャ

iDRAC では、シリアルデータ キャプチャ機能を使用して、後で取得するためにコンソール リダイレクト シリアルをキャプチャしておくことができます。この機能には iDRAC Datacenter ライセンスが必要です。

シリアルデータ キャプチャ機能の目的は、システムのシリアルデータをキャプチャして保存し、後でデバッグ目的で取得できるようにすることです。

RACADM、Redfish、iDRAC インターフェイスを使用して、シリアルデータ キャプチャを有効または無効することができます。この処理を有効にすると、iDRAC はシリアルMUX モードの設定に関係なく、ホスト シリアルデバイス 2 で受信したシリアルトラフィックをキャプチャします。

以下の BIOS シリアル通信入力オプションにおいて、SDC (シリアルデータ キャプチャ) 有効時に、シリアルデータは収集されません。ただし、SOL (connect com2) セッションも接続した場合は、シリアルデータが収集されます。

- オフ
- コンソール リダイレクトなしでオン
- 自動

シリアル通信設定、シリアルポートアドレス、シリアルデバイス 2、シリアル通信入力オプションでの COM ポートアドレスに関しては、iDRAC でのシリアルデータ キャプチャ用に設定したものと同じにする必要があります。

SDC を動作させるためのシリアルポート構成では、ホストがシリアルデータをシリアルデバイス 2 (Serial2) 以外に送信するようにする必要があります。次表に示した BIOS 設定の詳細において、これらの BIOS シリアル通信設定およびシリアルデータキャプチャの効果が適用されるのは、ラックおよびタワーサーバーのみです。

<table>
<thead>
<tr>
<th>BIOS 設定</th>
<th>シリアルデータ キャプチャ</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExtSerialConnector=Serial1 SerialComm=OnConRedirCom1 SerialPortAddress=Serial1Com2Serial2Com1</td>
<td>はい</td>
</tr>
<tr>
<td>ExtSerialConnector=Serial2 SerialComm=OnConRedirCom1 SerialPortAddress=Serial1Com2Serial2Com1</td>
<td>はい</td>
</tr>
<tr>
<td>ExtSerialConnector=Serial1 SerialComm=OnConRedirCom2 SerialPortAddress=Serial1Com1Serial2Com2</td>
<td>はい</td>
</tr>
<tr>
<td>ExtSerialConnector=Serial2 SerialComm=OnConRedirCom2 SerialPortAddress=Serial1Com1Serial2Com2</td>
<td>はい</td>
</tr>
<tr>
<td>ExtSerialConnector=Serial1 SerialComm=OnConRedirCom1 SerialPortAddress=Serial1Com1Serial2Com2</td>
<td>いいえ</td>
</tr>
<tr>
<td>ExtSerialConnector=Serial2 SerialComm=OnConRedirCom1 SerialPortAddress=Serial1Com1Serial2Com2</td>
<td>いいえ</td>
</tr>
<tr>
<td>ExtSerialConnector=Serial1 SerialComm=OnConRedirCom2 SerialPortAddress=Serial1Com1Serial2Com2</td>
<td>いいえ</td>
</tr>
<tr>
<td>ExtSerialConnector=Serial2 SerialComm=OnConRedirCom2 SerialPortAddress=Serial1Com1Serial2Com2</td>
<td>いいえ</td>
</tr>
<tr>
<td>ExtSerialConnector=Serial1 SerialComm=OnConRedirCom2 SerialPortAddress=Serial1Com1Serial2Com2</td>
<td>いいえ</td>
</tr>
</tbody>
</table>

IDRAC GUI を使用したシリアルデータ キャプチャを有効化/無効化するには、[メインテナンス] > [診断] > [シリアルデータログ] ページに移動し、有効化または無効化のチェックボックスを選択します。

詳細:
- この属性は、iDRAC の再起動後も維持されます。
- ファームウェアをデフォルトにリセットすると、この機能は無効になります。
シリアルデータキャプチャが有効になっている間、バッファーに最新のデータが追加され続けます。ユーザーカシリアルデータキャプチャを無効にし、再び有効にした場合、iDRACは最後のアップデートから追加を開始します。

ユーザーカが任意のインタフェースからシリアルデータキャプチャフラグを有効にすると、システムシリアルデータキャプチャが開始されます。iDRACは継続的にデタキャプチャーを開始し、1024 MBを超えて共有メモリーを保存します。このバッファーは循環バッファーです。

### メモ:
- この機能を使用するには、ログイン権限とシステム制御権限が必要です。
- この機能にはiDRAC Datacenterライセンスが必要です。

### 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できます。これにより、アプリケーションは電源状態の変更（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。これにより、システムの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。

I/O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できます。

- 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。I/O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、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。

### 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。

<table>
<thead>
<tr>
<th>製造元</th>
<th>タイプ</th>
</tr>
</thead>
</table>
| Broadcom | - 5719 Mezz 1 GB  
- 5720 Pcle 1 GB  
- 5720 bNDC 1 GB  
- 5720 rNDC 1 GB  
- 57414 Pcle 25 GbE |
### 表43. I/O アイデンティティ最適化対応のカード（続き）

<table>
<thead>
<tr>
<th>製造元</th>
<th>タイプ</th>
</tr>
</thead>
</table>
| Intel | - i350 DP FH PCIe 1 GB  
- i350 QP PCIe 1 GB  
- i350 QP rNDC 1 GB  
- i350 Mezz 1 GB  
- i350 bNDC 1 GB  
- x520 PCIe 10 GB  
- x520 bNDC 10 GB  
- x520 Mezz 10 GB  
- x520 + i350 rNDC 10 GB+1 GB  
- X710 bNDC 10 GB  
- X710 QP bNDC 10 GB  
- X710 PCIe 10 GB  
- X710 + i350 rNDC 10 GB+1 GB  
- X710 rNDC 10 GB  
- XL710 QSFP DP LP PCIe 40 GE  
- XL710 QSFP DP FH PCIe 40 GE  
- X550 DP BT PCIe 2 x 10 Gb  
- X550 DP BT LP PCIe 2 x 10 Gb  
- XXV710 Fab A/B Mezz 25 Gb (MX プラットフォーム用) |
| Mellanox | - ConnectX-3 Pro 10G Mezz 10 GB  
- ConnectX-4 LX 25GE SFP DP rNDC 25 GB  
- ConnectX-4 LX 25GE DP FH PCIe 25 GB  
- ConnectX-4 LX 25GE DP LP PCIe 25 GB  
- ConnectX-4 LX Fab A/B Mezz 25GB (MX プラットフォーム用) |
| QLogic | - 57810 PCIe 10 GB  
- 57810 bNDC 10 GB  
- 57810 Mezz 10 GB  
- 57800 rNDC 10 GB+1 GB  
- 57840 rNDC 10 GB  
- 57840 bNDC 10 GB  
- QME2662 Mezz FC16  
- QLE 2692 SP FC16 Gen 6 HBA FH PCIe FC16  
- SP FC16 Gen 6 HBA LP PCIe FC16  
- QLE 2690 DP FC16 Gen 6 HBA FH PCIe FC16  
- DP FC16 Gen 6 HBA LP PCIe FC16  
- QLE 2742 DP FC32 Gen 6 HBA FH PCIe FC32  
- DP FC32 Gen 6 HBA LP PCIe FC32  
- QLE2740 PCIe FC32  
- QME2692-DEL Fab C Mezz FC16 (MX プラットフォーム用)  
- QME2742-DEL Fab C Mezz FC32 (MX プラットフォーム用)  
- QL41262+MKR-DE Fab A/B Mezz 25 Gb (MX プラットフォーム用)  
- QL41232+MKR-DE Fab A/B Mezz 25 Gb (MX プラットフォーム用)  
- QLogic 1 x 32Gb QLE2770 FC HBA  
- QLogic 2 x 32Gb QLE2772 FC HBA |
| Emulex | - LPe15002B-M8 (FH) PCIe FC8  
- LPe15002B-M8 (LP) PCIe FC8  
- LPe15000B-M8 (FH) PCIe FC8  
- LPe15000B-M8 (LP) PCIe FC8  
- LPe31000-M6-SP PCIe FC16 |
表 43. I/O アイデンティティ最適化対応のカード（続き）

<table>
<thead>
<tr>
<th>製造元</th>
<th>タイプ</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LPe31002-M6-D DP PCIe FC16</td>
</tr>
<tr>
<td></td>
<td>• LPe32000-M2-D SP PCIe FC32</td>
</tr>
<tr>
<td></td>
<td>• LPe32002-M2-D DP PCIe FC32</td>
</tr>
<tr>
<td></td>
<td>• LPe31002-D Fab C Mezz FC16 (MX プラットフォーム用)</td>
</tr>
<tr>
<td></td>
<td>• LPe32002-D Fab C Mezz FC32 (MX プラットフォーム用)</td>
</tr>
<tr>
<td></td>
<td>• LPe35002-M2 FC32 2-ポート</td>
</tr>
<tr>
<td></td>
<td>• LPe35000-M2 FC32 1-ポート</td>
</tr>
</tbody>
</table>

### IO アイデンティティ最適化向けにサポートされている NIC ファームウェアバージョン

第14世代 Dell PowerEdgeサーバでは、必要なNICファームウェアがデフォルトで使用可能です。次の表では、I/Oアイデンティティ最適化機能向けのNICファームウェアを示しています。

iDRACがリモート割り当てアドレス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またはリモート割り当てアドレスと永続性ポリシーの動作

次の表では、仮想アドレス管理（VAM）設定と永続性ポリシーの動作、および依存関係が説明されています。

表 44. 仮想ロモート割り当てアドレスと永続性ポリシーの動作

<table>
<thead>
<tr>
<th>OME Modularでのリモート割り当てアドレス機能の状態</th>
<th>iDRACで設定されているモード</th>
<th>iDRACにおけるI/Oアイデンティティ機能状況</th>
<th>SCP</th>
<th>永続性ポリシー</th>
<th>永続性ポリシーのクリア-仮想アドレス</th>
</tr>
</thead>
<tbody>
<tr>
<td>リモート割り当てアドレス有効</td>
<td>リモート割り当てアドレスモード</td>
<td>仮想アドレス管理（VAM）設定済み</td>
<td>仮想アドレス管理（VAM）設定済み</td>
<td>仮想アドレス管理（VAM）設定済み</td>
<td>リモート割り当てアドレスに設定</td>
</tr>
<tr>
<td>リモート割り当てアドレス有効</td>
<td>リモート割り当てアドレスモード</td>
<td>VAM未設定</td>
<td>リモート割り当てアドレスに設定</td>
<td>リモート割り当てアドレスに設定</td>
<td>永続性なし-リモート割り当てアドレスに設定</td>
</tr>
<tr>
<td>リモート割り当てアドレス有効</td>
<td>リモート割り当てアドレスモード</td>
<td>Lifecycle Controllerで指定したパスを使って設定済み</td>
<td>Lifecycle Controllerで指定したパスを使って設定済み</td>
<td>Lifecycle Controllerで指定したパスを使って設定済み</td>
<td>永続性なし-リモート割り当てアドレスに設定</td>
</tr>
<tr>
<td>リモート割り当てアドレス有効</td>
<td>リモート割り当てアドレスモード</td>
<td>VAM未設定</td>
<td>リモート割り当てアドレスに設定</td>
<td>リモート割り当てアドレスに設定</td>
<td>リモート割り当てアドレスに設定</td>
</tr>
<tr>
<td>リモート割り当てアドレス無効</td>
<td>リモート割り当てアドレスモード</td>
<td>VAM設定済み</td>
<td>設定されたVAMが持続</td>
<td>設定されたVAMが持続</td>
<td>仮想アドレスのクリア-仮想アドレス無効</td>
</tr>
<tr>
<td>リモート割り当てアドレス無効</td>
<td>リモート割り当てアドレスモード</td>
<td>VAM未設定</td>
<td>ハードウェアMACアドレスに設定</td>
<td>ハードウェアMACアドレスに設定</td>
<td>永続性のサポートなし-カードの動作に依存</td>
</tr>
<tr>
<td>リモート割り当てアドレス無効</td>
<td>リモート割り当てアドレスモード</td>
<td>Lifecycle Controllerで指定したパスを使って設定済み</td>
<td>Lifecycle Controllerで指定したパスを使って設定済み</td>
<td>Lifecycle Controllerで指定したパスを使って設定済み</td>
<td>永続性のサポートなし-カードの動作に依存</td>
</tr>
<tr>
<td>リモート割り当てアドレス無効</td>
<td>リモート割り当てアドレスモード</td>
<td>VAM未設定</td>
<td>ハードウェアMACアドレスに設定</td>
<td>ハードウェアMACアドレスに設定</td>
<td>ハードウェアMACアドレスに設定</td>
</tr>
</tbody>
</table>
### OME Modular でのリモート割り当てアドレス機能の状態

<table>
<thead>
<tr>
<th></th>
<th>iDRAC で設定されているモード</th>
<th>iDRAC における I/O アイデンティティ機能状況</th>
<th>SCP</th>
<th>永続性ポリシー</th>
<th>永続性ポリシーのクリア・仮想アドレス</th>
</tr>
</thead>
<tbody>
<tr>
<td>リモート割り当てアドレス有効</td>
<td>コンソールモード</td>
<td>有効</td>
<td>VAM 設定済み</td>
<td>設定された VAM が持続</td>
<td>永続性とクリアの両方が機能することが必要</td>
</tr>
<tr>
<td>リモート割り当てアドレス有効</td>
<td>コンソールモード</td>
<td>有効</td>
<td>VAM 未設定</td>
<td>ハードウェア MAC アドレスに設定</td>
<td>ハードウェア MAC アドレスに設定</td>
</tr>
<tr>
<td>リモート割り当てアドレス有効</td>
<td>コンソールモード</td>
<td>無効</td>
<td>Lifecycle Controller で指定したパスを使って設定済み</td>
<td>当該のサイクルに対して Lifecycle Controller 設定が持続</td>
<td>永続性のサポートなし。カードの動作に依存</td>
</tr>
<tr>
<td>リモート割り当てアドレス無効</td>
<td>コンソールモード</td>
<td>有効</td>
<td>VAM 設定済み</td>
<td>設定された VAM が持続</td>
<td>永続性とクリアの両方が機能することが必要</td>
</tr>
<tr>
<td>リモート割り当てアドレス無効</td>
<td>コンソールモード</td>
<td>有効</td>
<td>VAM 未設定</td>
<td>ハードウェア MAC アドレスに設定</td>
<td>ハードウェア MAC アドレスに設定</td>
</tr>
<tr>
<td>リモート割り当てアドレス無効</td>
<td>コンソールモード</td>
<td>無効</td>
<td>Lifecycle Controller で指定したパスを使って設定済み</td>
<td>当該のサイクルに対して Lifecycle Controller 設定が持続</td>
<td>永続性のサポートなし。カードの動作に依存</td>
</tr>
</tbody>
</table>

### FlexAddress および I/O アイデンティティに対するシステム動作

#### 表 44. FlexAddress および I/O アイデンティティに対するシステム動作（続き）

### 表 45. FlexAddress および I/O アイデンティティに対するシステム動作

<table>
<thead>
<tr>
<th>タイプ</th>
<th>CMC における FlexAddress 機能状況</th>
<th>iDRAC における I/O アイデンティティ機能状況</th>
<th>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</th>
<th>VA プログラミングソース</th>
<th>再起動サイクル VA 持続動作</th>
</tr>
</thead>
<tbody>
<tr>
<td>FA と同等の永続性を持つサーバー</td>
<td>有効</td>
<td>無効</td>
<td>CMC からの FlexAddress</td>
<td>FlexAddress 仕様による</td>
<td></td>
</tr>
<tr>
<td>N/A、有効、または無効</td>
<td>有効</td>
<td>無効</td>
<td>なし - 新規または永続的</td>
<td>FlexAddress 仕様による</td>
<td></td>
</tr>
<tr>
<td></td>
<td>有効</td>
<td>なし - 新規または永続的</td>
<td>リモートエージェント仮想アドレス</td>
<td>FlexAddress 仕様による</td>
<td></td>
</tr>
<tr>
<td></td>
<td>無</td>
<td>なし - 新規または永続的</td>
<td>仮想アドレスがクリア済み</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VAM 永続性ポリシー機能を備えたサーバー</td>
<td>有効</td>
<td>無効</td>
<td>CMC からの FlexAddress</td>
<td>FlexAddress 仕様による</td>
<td></td>
</tr>
<tr>
<td></td>
<td>有効</td>
<td>なし - 新規または永続的</td>
<td>リモートエージェント仮想アドレス</td>
<td>FlexAddress 仕様による</td>
<td></td>
</tr>
<tr>
<td></td>
<td>無</td>
<td>なし - 新規または永続的</td>
<td>リモートエージェント仮想アドレス</td>
<td>FlexAddress 仕様による</td>
<td></td>
</tr>
<tr>
<td></td>
<td>有効</td>
<td>なし - 新規または永続的</td>
<td>リモートエージェント仮想アドレス</td>
<td>FlexAddress 仕様による</td>
<td></td>
</tr>
<tr>
<td></td>
<td>無</td>
<td>なし - 新規または永続的</td>
<td>リモートエージェント仮想アドレス</td>
<td>FlexAddress 仕様による</td>
<td></td>
</tr>
</tbody>
</table>

214 ネットワークデバイスのインベントリ、監視、および設定
### IO 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。I/O アイデンティティ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。この機能が有効である場合、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がクリアされ、I/O アイデンティティ最適化の有効化または無効化が実行されます。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。I/O アイデンティティ最適化機能を有効にする前に、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ます。

I/O アイデンティティ最適化機能を有効にした後、iDRAC からサーバ設定プロファイルファイルをエクスポートし、SCP 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。

SCP 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、https://www.dell.com/supportにある『NIC プロファイル』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

1. iDRAC ウェブインタフェースで、Configuration（設定）> System Settings（システム設定）> Hardware Settings（ハードウェア設定）> I/O Identity Optimization（I/O アイデンティティ最適化）に移動します。

2. I/O Identity Optimization（I/O アイデンティティ最適化）タブをクリックし、Enable（有効にする）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、このオプション選択を解除します。

3. 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 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にするには、次のコマンドを使用します。

```bash
racadm set iDRac.ioidopt.IOIDOptEnable Enabled
```

この機能を有効にした後、設定を変更するには、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にするには、次のコマンドを使用します。

```bash
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。

```bash
racadm get iDRac.IOIDOpt
```

### SSD 摩耗しきい値

iDRAC では、すべての SSD の残存量と書き込み耐久性および NVMe PCIe SSD での利用可能なスペアについて、それらのしきい値を設定できます。
SSD の残留定格書き込み耐久性および NVMe PCIe SSD の利用可能なスペアの値が iDRAC のしきい値を下回ると、iDRAC はそうしたイベントを LC ログに記録し、選択されたアラートのタイプに応じて、E メールアラート、SNMP ブラック、IPMI アラート、リモート Syslog への記録、WS イベント、OS に通知を行います。

IDRAC によって利用可能なスペアと警告用のしきい値が提示されるのは、NVMe PCIe SSD だけです。PERC および HBA に接続されている SSD に利用可能なスペアは適用されません。

SSD 摩耗しきい値アラート機能の Web インターフェイスを用いた設定

残留定格書き込み耐久性および利用可能なスペアについてのアラートしきい値を Web インターフェイスで設定するには、次の手順を実行します。

1. iDRAC Web インターフェイスで、設定 > システム設定 > ハードウェア設定 > SSD 摩耗しきい値 と移動します。
   SSD 摩耗しきい値ページが表示されます。

2. [ 残留定格書き込み耐久性 ] — この値は 1~99% の間で設定できます。デフォルト値は 10% です。この機能のアラートタイプは、[ SSD 摩耗の書き込み耐久性 ] であり、しきい値イベントの結果によるセキュリティアラートは [ 警告 ] になります。

3. [ 利用可能なスペアアラートしきい値 ] — この値は 1~99% の間で設定できます。デフォルト値は 10% です。この機能のアラートタイプは、[ SSD 摩耗の利用可能なスペア ] であり、しきい値イベントの結果によるセキュリティアラートは [ 警告 ] になります。

SSD 摩耗しきい値アラート機能の RACADM を用いた設定

残留定格書き込み耐久性を設定するには、次のコマンドを使用します。

```
racadm set System.Storage.RemainingRatedWriteEnduranceAlertThreshold n
```
ここで n は 1~99%。

利用可能なスペアのアラートしきい値を設定するには、次のコマンドを使用します。

```
racadm System.Storage.AvailableSpareAlertThreshold n
```
ここで n は 1~99%。

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、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。これによって仮想アドレス、イニシエータ、およびストレージアーキテクチャ設定の永続性またはクリアランスが決定します。個々の永続性ポリシーは、システム内の通用可能なすべてのデバイスのすべてのポートおよびバ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。

1. メモ：永続性ポリシー機能はデフォルトで設定されている場合は機能しないことがあります。VirtualAddressManagement 属性が iDRAC で FlexAddress（MX ブラケットフォームでない場合）または RemoteAssignedAddress（MX ブラケットフォームの場合）モードに設定されている場合、および、FlexAddress またはリモート割り当てアドレス機能が CMC（MX ブラケットフォームでない場合）または OME Modular（MX ブラケットフォームの場合）で無効になっている場合、VirtualAddressManagement 属性を iDRAC のコンソールモードに設定するか、FlexAddress またはリモート割り当てアドレス機能を CMC または OME Modular で有効にしてください。

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
• ストレージアーキテクチャ

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、ポリシーに応じて設定される場合。ポリシーが適用されると、設定されたデバイスと、これらのデバイス用に設定された値に対して、一つのログエントリが記録されます。

SNMP、電子メール、または WS-eventing 通知用にイベント処置が有効化されます。リモートシスログ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

表 46. 永続性ポリシーのデフォルト値

<table>
<thead>
<tr>
<th>永続性ポリシー</th>
<th>AC 電源喪失</th>
<th>コールドプート</th>
<th>ウォームプート</th>
</tr>
</thead>
<tbody>
<tr>
<td>仮想アドレス: 補助電源駆動デバイス</td>
<td>選択されていません</td>
<td>選択済み</td>
<td>選択済み</td>
</tr>
<tr>
<td>仮想アドレス: 非補助電源駆動デバイス</td>
<td>選択されていません</td>
<td>選択されていません</td>
<td>選択済み</td>
</tr>
<tr>
<td>イニシエータ</td>
<td>選択済み</td>
<td>選択済み</td>
<td>選択済み</td>
</tr>
<tr>
<td>ストレージターゲット</td>
<td>選択済み</td>
<td>選択済み</td>
<td>選択済み</td>
</tr>
</tbody>
</table>

メモ: 永続性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、永続性ポリシーを再度有効にして仮想アドレスは取得されません。永続性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。

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 Web インターフェイスで、[設定] > [システム設定] > [ハードウェア設定] > [I/O アイデンティティ最適化] と移動します。
2. I/O インタフェース設定ページをクリックします。
3. 永続性ポリシー設定セクションで、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。
   - [ウォームリセット] - 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。
   - [コールドリセット] - 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。
   - [AC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。
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 オプジェクトと set サブコマンドを使用します。

- イニシエータには、iDRAC.IOIDOPT.InitiatorPersistencePolicy オプジェクトを使用
- ストレージターゲットには、iDRAC.IOIDOpt.StorageTargetPersistencePolicy オプジェクトを使用

詳細については、『iDRAC RACADM CLI ガイド』は、www.dell.com/idracmanuals にあります。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 47. iSCSI イニシエータ - デフォルト値**

<table>
<thead>
<tr>
<th>iSCSI イニシエータ</th>
<th>IPv4 モードでのデフォルト値</th>
<th>IPv6 モードでのデフォルト値</th>
</tr>
</thead>
<tbody>
<tr>
<td>IscsiiInitiatorIpAddr</td>
<td>0.0.0.0</td>
<td>::</td>
</tr>
<tr>
<td>IscsiiInitiatorIpv4Addr</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>IscsiiInitiatorIpv6Addr</td>
<td>::</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>IscsiiInitiatorSubnet</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>IscsiiInitiatorSubnetPrefix</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IscsiiInitiatorGateway</td>
<td>0.0.0.0</td>
<td>::</td>
</tr>
<tr>
<td>IscsiiInitiatorIpv4Gateway</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>IscsiiInitiatorIpv6Gateway</td>
<td>::</td>
<td>::</td>
</tr>
<tr>
<td>IscsiiInitiatorPrimDns</td>
<td>0.0.0.0</td>
<td>::</td>
</tr>
<tr>
<td>IscsiiInitiatorIpv4PrimDns</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>IscsiiInitiatorIpv6PrimDns</td>
<td>::</td>
<td>::</td>
</tr>
<tr>
<td>IscsiiInitiatorSecDns</td>
<td>0.0.0.0</td>
<td>::</td>
</tr>
<tr>
<td>IscsiiInitiatorIpv4SecDns</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>IscsiiInitiatorIpv6SecDns</td>
<td>::</td>
<td>::</td>
</tr>
<tr>
<td>IscsiiInitiatorName</td>
<td>値がクリア</td>
<td>値がクリア</td>
</tr>
<tr>
<td>IscsiiInitiatorChapId</td>
<td>値がクリア</td>
<td>値がクリア</td>
</tr>
<tr>
<td>IscsiiInitiatorChapPwd</td>
<td>値がクリア</td>
<td>値がクリア</td>
</tr>
<tr>
<td>IPvVer</td>
<td>ipv4</td>
<td>ipv6</td>
</tr>
</tbody>
</table>

**表 48. iSCSI ストレージ ターゲットの属性 — デフォルト値**

<table>
<thead>
<tr>
<th>iSCSI ストレージ ターゲットの属性</th>
<th>IPv4 モードでのデフォルト値</th>
<th>IPv6 モードでのデフォルト値</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectFirstTgt</td>
<td>無効</td>
<td>無効</td>
</tr>
<tr>
<td>FirstTgtIpAddress</td>
<td>0.0.0.0</td>
<td>::</td>
</tr>
<tr>
<td>FirstTgtTcpPort</td>
<td>3260</td>
<td>3260</td>
</tr>
<tr>
<td>FirstTgtBootLun</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FirstTgtIsccsName</td>
<td>値がクリア</td>
<td>値がクリア</td>
</tr>
<tr>
<td>FirstTgtChapId</td>
<td>値がクリア</td>
<td>値がクリア</td>
</tr>
<tr>
<td>FirstTgtChapPwd</td>
<td>値がクリア</td>
<td>値がクリア</td>
</tr>
</tbody>
</table>
### 表 48: iSCSI ストレージ ターゲットの属性 — デフォルト値（続き）

<table>
<thead>
<tr>
<th>iSCSI ストレージターゲットの属性</th>
<th>IPv4 モードでのデフォルト値</th>
<th>IPv6 モードでのデフォルト値</th>
</tr>
</thead>
<tbody>
<tr>
<td>FirstTgtIpVer</td>
<td>ipv4</td>
<td></td>
</tr>
<tr>
<td>ConnectSecondTgt</td>
<td>無効</td>
<td>無効</td>
</tr>
<tr>
<td>SecondTgtIpAddress</td>
<td>0.0.0.0</td>
<td>::</td>
</tr>
<tr>
<td>SecondTgtTcpPort</td>
<td>3260</td>
<td>3260</td>
</tr>
<tr>
<td>SecondTgtBootLun</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SecondTgtiscsiName</td>
<td>値がクリア</td>
<td>値がクリア</td>
</tr>
<tr>
<td>SecondTgtChapId</td>
<td>値がクリア</td>
<td>値がクリア</td>
</tr>
<tr>
<td>SecondTgtChapPwd</td>
<td>値がクリア</td>
<td>値がクリア</td>
</tr>
<tr>
<td>SecondTgtIpVer</td>
<td>ipv4</td>
<td></td>
</tr>
</tbody>
</table>
Managing storage devices

Starting with iDRAC 3.15.15.15 release, iDRAC supports Boot Optimized Storage Solution (BOSS) controller in the 14th generation of PowerEdge servers. BOSS controllers are designed specifically for booting the operating system of the server. These controllers support limited RAID features and the configuration is staged.

Starting with iDRAC 4.30.30.30 release, iDRAC supports PERC 11, HBA 11, and BOOS1.5 for AMD systems.

**NOTE:** BOSS controllers support only RAID level 1.

iDRAC has expanded its agent-free management to include direct configuration of the PERC controllers. It enables you to remotely configure the storage components attached to your system at run-time. These components include RAID and non-RAID controllers and the channels, ports, enclosures, and disks attached to them. For the 14th generation of PowerEdge servers, PERC 9 and PERC 10 controllers are supported.

The complete storage subsystem discovery, topology, health monitoring, and configuration are accomplished in the Comprehensive Embedded Management (CEM) framework by interfacing with the internal and external PERC controllers through the MCTP protocol over I2C interface. For real-time configuration, CEM supports PERC9 controllers and above. The firmware version for PERC9 controllers must be 9.1 or later.

**NOTE:** The Software RAID (SWRAID) is not supported by CEM and thus is not supported in the iDRAC GUI. SWRAID can be managed using the WSMan API and RACADM.

Using iDRAC, you can perform most of the functions that are available in OpenManage Storage Management including real-time (no reboot) configuration commands (for example, create virtual disk). You can completely configure RAID before installing the operating system.

You can configure and manage the controller functions without accessing the BIOS. These functions include configuring virtual disks and applying RAID levels and hot spares for data protection. You can initiate many other controller functions such as rebuilds and troubleshooting. You can protect your data by configuring data-redundancy or assigning hot spares.

The storage devices are:

- Controllers — Most operating systems do not read and write data directly from the disks, but instead send read and write instructions to a controller. The controller is the hardware in your system that interacts directly with the disks to write and retrieve data. A controller has connectors (channels or ports) which are attached to one or more physical disks or an enclosure containing physical disks. RAID controllers can span the boundaries of the disks to create an extended amount of storage space — or a virtual disk — using the capacity of more than one disk. Controllers also perform other tasks, such as initiating rebuilds, initializing disks, and more. To complete their tasks, controllers require special software known as firmware and drivers. In order to function properly, the controller must have the minimum required version of the firmware and the drivers installed. Different controllers have different characteristics in the way they read and write data and execute tasks. It is helpful to understand these features to most efficiently manage the storage.

- Physical disks or physical devices — Reside within an enclosure or are attached to the controller. On a RAID controller, physical disks or devices are used to create virtual disks.

- Virtual disk — It is storage created by a RAID controller from one or more physical disks. Although a virtual disk may be created from several physical disks, it is viewed by the operating system as a single disk. Depending on the RAID level used, the virtual disk may retain redundant data if there is a disk failure or have particular performance attributes. Virtual disks can only be created on a RAID controller.

- Enclosure — It is attached to the system externally while the backplane and its physical disks are internal.

- Backplane — It is similar to an enclosure. In a Backplane, the controller connector and physical disks are attached to the enclosure, but it does not have the management features (temperature probes, alarms, and so on) associated with external enclosures. Physical disks can be contained in an enclosure or attached to the backplane of a system.

**NOTE:** Enclosure properties is not applicable for MX platforms. Hence, in the iDRAC web interface on MX platforms, ignore the Connector value under Enclosure properties.

**NOTE:** In any MX chassis which contains storage sleds and compute sleds, iDRAC pertaining to any of the compute sleds in that chassis will report all storage sleds (both assigned and unassigned). If any one of the assigned or unassigned blades are in Warning or Critical health state, the blade controller also reports the same status.
In addition to managing the physical disks contained in the enclosure, you can monitor the status of the fans, power supply, and temperature probes in an enclosure. You can hot-plug enclosures. Hot-plugging is defined as adding of a component to a system while the operating system is still running.

The physical devices connected to the controller must have the latest firmware. For the latest supported firmware, contact your service provider.

Storage events from PERC are mapped to SNMP traps and WSMan events as applicable. Any changes to the storage configurations are logged in the Lifecycle Log.

### Table 49. PERC capability

<table>
<thead>
<tr>
<th>PERC Capability</th>
<th>CEM configuration Capable Controller (PERC 9.1 or later)</th>
<th>CEM configuration Non-capable Controller (PERC 9.0 and lower)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time</td>
<td><img src="image" alt="NOTE: For PowerEdge Rx5xx/Cx5xx servers, PERC 9, PERC 10, and PERC 11 controllers are supported." /> If there is no existing pending or scheduled jobs for the controller, then configuration is applied. If there are pending or scheduled jobs for that controller, then the jobs have to be cleared or you must wait for the jobs to be completed before applying the configuration at run-time. Run-time or real-time means, a reboot is not required. Configuration is applied. An error message is displayed. Job creation is not successful and you cannot create real-time jobs using Web interface.</td>
<td></td>
</tr>
<tr>
<td>Staged</td>
<td>If all the set operations are staged, the configuration is staged and applied after reboot or it is applied at real-time.</td>
<td>Configuration is applied after reboot</td>
</tr>
</tbody>
</table>

**Topics:**

- RAID の概念について
- 対応コントローラ
- 対応エンクロージャ
- Summary of supported features for storage devices
- ストレージデバイスのインベントリと監視
- ストレージデバイスのトポロジの表示
- 物理ディスクの管理
- 仮想ディスクの管理
- RAID 設定機能
- コントローラの管理
- PCIe SSD の管理
- エンクロージャまたはバックプレーンの管理
- 設定を適用する操作モードの選択
- 保留中の操作の表示と適用
- ストレージデバイス — 操作適用のシナリオ
- コンポーネント LED の点滅または点滅解除

**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のデータの保存を管理するためのテクノロジーです。RAIDの重要な要素は、複数の物理ディスクの容量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、パラ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。

 Memo: RAID (RAID Advisory Board) は、RAIDの実装に使用される仕様を定義しています。RAIDはRAIDレベルで定義しますが、異なるベンダによるRAIDレベルでの商用実装は、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 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。これからの方法を使うと、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。方法には、次のようなものがあります。

- 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。ミラーのデータのうち1つが失敗した場合、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けられます。ミラーリングされたディスクの両方に同じデータが入っています。ミラーリングされたRAIDディスクグループは、読み取り操作ではRAID5ディスクグループと同様で、書き込み速度はより高速です。

- ストライピング：ディスクストライピングでは、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ピングされます。ストライピングされたディスクは、通常の仮想ディスクのアドレスで構成されます。ストライピングされたディスクは、他のディスクと同様に、物理ディスクの両方を重複することなく、データが書き込まれます。ストライピングで消費される容量は、各物理ディスクで同じです。物理ディスクの両方をストライピングしたデータに書き込む必要があります。ストライピングされたディスクは、ストライピングディスクグループを構成するため、ストライピングによってデータの冗長性を実現します。

- ストライピング・パリティディスクを含まない、ストライピングによって消費されるディスク容量は、ストライピングのディスク容量に50％のデータが存在するようなストライピングを考慮します。この場合、ストライピングサイズは64KB、ストライピングパレイメントサイズは16KBとなります。

- ストライピングパレイメント—単一の物理ディスク上のストライピングの一部です。

- ストライピングパレイメントサイズ—ストライピングパレイメントによって消費されるディスク容量。たとえば、64KBのディスク容量、ストライピングの各ディスクには16KBのデータが存在するようなストライピングを考えます。この場合、ストライピングパレイメントサイズは64KB、ストライピングサイズは16KBとなります。

- パリティの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推定される冗長データ、ストライピングを行っているディスクの1つが失敗した場合、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。

- スパコン：物理ディスクグループのストレージ容量をRAID10、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**

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。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。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。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。

RAID レベルを選択する場合の、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。

• 可用性またはフォールトトレランス - 可用性またはフォールトトレランスとは、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 ポリュームでは、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。特定のアプリケーションには、一部の RAID レベルがより適している場合があります。

• コスト効率 - RAID ポ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場合、簡便に複製できる、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言えません。

• 故障までの平均時間（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と、常にディスク障害の可能性も増加します。冗長データが必要な状況ではこのオプションは避けることができません。社内のシステムサポートスタッフの仕事量に影響します。

• ボリューム - ボリュームは、単一ディスクによる非 RAID 仮想ディスクによるものである。O-ROM<Ctrl><r> など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できます。各 RAID レベルまたは連続的には、異なるパフォーマンスとデータ保護の特徴があります。

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むます。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。
- 原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リング（複製）されます。1台の物理ディスクが故障すると、ミラーのもう一方のデータを使用してデータを再構築できます。

RAID 1 の特徴
- \( n+n \) 個のディスクをディスク \( n \) 個分の容量を持つ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リングされるため、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が障害が起きた場合、仮想ディスクの動作は中断されません。データは、故障し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実現します。物理ディスクをパリティ専用に割り当てることなく、パリティ情報はディスク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。ディスク容量の点から RAID 6 はより高価です。

RAID レベル 50 (RAID 5 セット全体にわたるストライピング)

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を必要です。
- 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 セット全体にわたるストライピング)

RAID 60 では RAID 6 に設定された複数の物理ディスクに分けてストライピングが施されます。たとえば、4 つの物理ディスクで実装された RAID 6 ディスクグループがさらに 4 つの物理ディスク実装されたディスクグループに継続されると 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 60 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。ディスク容量の点から RAID 60 はより高価です。

RAID レベル 10（ストライプ化ミラー）

RAID 10 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化されます。ストライプ化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リングされます。RAID 10 はストライプのミラーリング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止されません。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、より一般的な RAID レベルに関連するパフォーマンス特性を比較したものです。この表は、RAID レベルを選択するための一般的なガイドラインを示しています。RAID レベルを選択する前に、お使いの環境要件を評価してください。

表 50. RAID レベルパフォーマンスの比較

<table>
<thead>
<tr>
<th>RAID レベル</th>
<th>データ冗長性</th>
<th>読み取りパフォーマンス</th>
<th>書き込みパフォーマンス</th>
<th>再構築パフォーマンス</th>
<th>必要な最小ディスク数</th>
<th>使用例</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID 0</td>
<td>なし</td>
<td>大変良好</td>
<td>大変良好</td>
<td>該当なし</td>
<td>無</td>
<td>非重要データ。</td>
</tr>
<tr>
<td>RAID 1</td>
<td>優秀</td>
<td>大変良好</td>
<td>正常</td>
<td>正常</td>
<td>$2N (N = 1)$</td>
<td>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。</td>
</tr>
<tr>
<td>RAID 5</td>
<td>正常</td>
<td>連続読み取り： 良。トランザクション読み取り：大変良好</td>
<td>ライトバックキャッシュを使用しない限り普通</td>
<td>普通</td>
<td>$N + 1 (N = ディスクが最低限 2 台)$</td>
<td>データベース、および読み取りを数の多いトランザクションに使用。</td>
</tr>
<tr>
<td>RAID 10</td>
<td>優秀</td>
<td>大変良好</td>
<td>普通</td>
<td>正常</td>
<td>$2N \times X$</td>
<td>データの多い環境（大きいレコードなど）。</td>
</tr>
</tbody>
</table>
表 50. RAID レベルパフォーマンスの比較（続き）

<table>
<thead>
<tr>
<th>RAID レベル</th>
<th>データ冗長性</th>
<th>読み取りパフォーマンス</th>
<th>書き込みパフォーマンス</th>
<th>再構築パフォーマンス</th>
<th>必要な最小ディスク数</th>
<th>使用例</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID 50</td>
<td>正常</td>
<td>大変良好</td>
<td>普通</td>
<td>普通</td>
<td>N + 2 (N = 最低 ( \geq 4 ) 台)</td>
<td>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。</td>
</tr>
<tr>
<td>RAID 6</td>
<td>優秀</td>
<td>連続読み取り: 良。トランザクション読み取り:大変良好</td>
<td>ライトバックキャッシュを使用しない限り普通</td>
<td>不良</td>
<td>N + 2 (N = ディスクが最低 ( \geq 2 ) 台)</td>
<td>重要な情報。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。</td>
</tr>
<tr>
<td>RAID 60</td>
<td>優秀</td>
<td>大変良好</td>
<td>普通</td>
<td>不良</td>
<td>X x (N + 2) (N = 最低 ( \geq 2 ) 台)</td>
<td>重要な情報。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。</td>
</tr>
</tbody>
</table>

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 インターフェースは次の BOSS コントローラをサポートしています。
- BOSS-S1 アダプタ
- BOSS-S1 モジュラー (プレードサーバ用)
- BOSS-S2 アダプター

iDRAC インターフェースは次の PERC11 コントローラーをサポートしています。
- PERC H755 アダプター
- PERC H755 前面
- PERC H755N 前面
- PERC H755 MX

iDRAC インターフェースは次の PERC10 コントローラをサポートしています。
- PERC H740P ミニ
- PERC H740P アダプタ
- PERC H840 アダプタ
- PERC H745P MX

iDRAC インターフェース是次の PERC 9 コントローラをサポートしています。
- PERC H330 ミニ
- PERC H330 アダプタ
- PERC H730P ミニ
- PERC H730P アダプタ
- PERC H730P MX

サポートされる非 RAID コントローラ

iDRAC インターフェースは、12 Gbps SAS HBA 外部コントローラと HBA330 ミニ、またはアダプタコントローラをサポートしています。
iDRAC は、HBA330 MMZ、HBA330 MX アダプタをサポートしています。
Summary of supported features for storage devices

The following tables provide the features supported by the storage devices through iDRAC.

**Table 51. Supported features for storage controllers**

<table>
<thead>
<tr>
<th>Feature</th>
<th>PERC 10</th>
<th>PERC 9</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>H740P Mini</td>
<td>H740P Adapter</td>
</tr>
<tr>
<td></td>
<td>H840 Adapter</td>
<td>H330 Mini</td>
</tr>
<tr>
<td>Assign or unassign physical disk as a global hot spare</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Convert to RAID/Non RAID</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Rebuild</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Cancel Rebuild</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Create virtual disks</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Rename virtual disks</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Edit virtual disks cache policies</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Check virtual disk consistency</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Cancel check consistency</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Initialize virtual disks</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Cancel initialization</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Encrypt virtual disks</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Assign or unassign dedicated hot spare</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Feature</td>
<td>PERC 10</td>
<td>PERC 9</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td></td>
<td>H740P Mini</td>
<td>H740P Adapter</td>
</tr>
<tr>
<td>Delete virtual disks</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Cancel Background Initialization</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Online Capacity Expansion</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>RAID Level Migration</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Discard Preserved Cache</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Set Patrol Read Mode</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Manual Patrol Read Mode</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Patrol Read Unconfigured Areas</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Check Consistency Mode</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Copyback Mode</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Load Balance Mode</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Check Consistency Rate</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Rebuild Rate</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>BGI Rate</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Reconstruct Rate</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Import foreign configuration</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Auto-import foreign configuration</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Clear foreign configuration</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Reset controller configuration</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
</tbody>
</table>
Table 51. Supported features for storage controllers (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>PERC 10</th>
<th>PERC 9</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>H740P Mini</td>
<td>H740P Adapter</td>
</tr>
<tr>
<td>Create or change security keys</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Secure Enterprise Key Manager</td>
<td>Staged</td>
<td>Staged</td>
</tr>
<tr>
<td>Inventory and remotely monitor the health of PCIe SSD devices</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Prepare the PCIe SSD to be removed</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Securely erase the data for PCIe SSD</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Configure Backplane mode (split/ unified)</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Blink or unblink component LEDs</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Switch controller mode</td>
<td>Staged</td>
<td>Staged</td>
</tr>
<tr>
<td>T10P virtual disk support for Virtual Disks</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

**NOTE:** Added support for

- eHBA mode for PERC 10.2 or greater firmware which supports convert to Non-RAID disks
- convert controller to HBA mode
- RAID 10 uneven span

Table 52. Supported features of storage controllers for MX platforms

<table>
<thead>
<tr>
<th>Feature</th>
<th>PERC 10</th>
<th>PERC 9</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>H745P MX</td>
<td>H730P MX</td>
</tr>
<tr>
<td>Assign or unassign physical disk as a global hot spare</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Convert to RAID/Non RAID</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Rebuild</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Cancel Rebuild</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Feature</td>
<td>PERC 10</td>
<td>PERC 9</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td></td>
<td>H745P MX</td>
<td>H730P MX</td>
</tr>
<tr>
<td>Create Virtual disks</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Rename Virtual disks</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Edit Virtual Disks Cache Policies</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Check Virtual Disk Consistency</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Cancel Check Consistency</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Initialize Virtual Disks</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Cancel Initialization</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Encrypt Virtual Disks</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Assign or unassign dedicated hot spare</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Delete Virtual Disks</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Cancel Background Initialization</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Online Capacity Expansion</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>RAID Level Migration</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Discard Preserved Cache</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Set Patrol Read Mode</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Manual Patrol Read Mode</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Patrol Read Unconfigured Areas</td>
<td>Real-time</td>
<td>Real-time (only in web interface)</td>
</tr>
<tr>
<td>Check Consistency Mode</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Copyback Mode</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Load Balance Mode</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Check Consistency Rate</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Rebuild Rate</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>BGI Rate</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Reconstruct Rate</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Import Foreign Configuration</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Auto-import Foreign Configuration</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Clear Foreign Configuration</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Reset Controller Configuration</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Create or change security keys</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Inventory and remotely monitor the health of PCIe SSD devices</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Prepare the PCIe SSD to be removed</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Securely erase the data for PCIe SSD</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Configure Backplane mode (split/unified)</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Blink or unblink component LEDs</td>
<td>Real-time</td>
<td>Real-time</td>
</tr>
<tr>
<td>Switch Controller Mode</td>
<td>Not applicable</td>
<td>Staged</td>
</tr>
</tbody>
</table>
Table 52. Supported features of storage controllers for MX platforms (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>PERC 10</th>
<th>PERC 9</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>H745P MX</td>
<td>H730P MX</td>
</tr>
<tr>
<td>T10P! Support for Virtual Disks</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

NOTE: H745P MX supports eHBA mode with PERC 10.2 and higher.

Table 53. Supported features for storage devices

<table>
<thead>
<tr>
<th>Feature</th>
<th>PCIe SSD</th>
<th>BOSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Virtual Disks</td>
<td>Not applicable</td>
<td>Staged</td>
</tr>
<tr>
<td>Reset Controller Configuration</td>
<td>Not applicable</td>
<td>Staged</td>
</tr>
<tr>
<td>Fast Initialization</td>
<td>Not applicable</td>
<td>Staged</td>
</tr>
<tr>
<td>Delete Virtual Disks</td>
<td>Not applicable</td>
<td>Staged</td>
</tr>
<tr>
<td>Full Initialization</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Inventory and remotely monitor the health of PCIe SSD devices</td>
<td>Real-time</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Prepare the PCIe SSD to be removed</td>
<td>Real-time</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Securely erase the data for PCIe SSD</td>
<td>Staged</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Blink or unblink component LEDs</td>
<td>Real-time</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

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、BOSS コントローラ、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

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。

アラートと SNMP トッパは、ストレージイベント用に生成されます。イベントが Lifecycle ログに記録されます。

メモ: BOSS コントローラの正確なインベントリのために、再起動時システムインベントリ収集操作 (CSIOR) が完了していることを確認してください。CSIOR はデフォルトで有効になっています。

メモ: PSU ケーブルを取り外す際にシステムにエラーキャッシュの WSMan コマンドを列挙すると、エンクロージャのブライマリ・ステータスは、警告ではなく正常として表示されます。

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。

- [ストレージ] > [概要] > [サマリー] と移動して、ストレージ コンポーネントと最近ログに記録されたイベントのサマリーページを表示します。このページは、30 秒ごとに自動更新されます。
ストレージデバイスの表示

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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。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、System Summary（システムサマリ）に移動します。iDRAC Settings.System Summary（iDRAC Settings.System の概要）ページが表示されます。Backplane Inventory（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。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。

ストレージデバイスのトポロジーの表示
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ーを表示するには、Storage（ストレージ）> Overview（概要）の順に移動します。Overview（概要）ページには、システム内のストレージコンポーネントが階層的に表示されます。使用可能なオプションは次のとおりです。

- コントローラー
- 物理ディスク
- 仮想ディスク
- エンクロージャ

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、次のことを行いできます。

- 物理ディスクのプロパティの表示
- 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
- 物理ディスクの再構成
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られた仮想ディスクを再構築します。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が再構築されます。

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ができます。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を追加することはできます。ホットスペアがすべて自动生成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。

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。

1. Lifecycle Controller が有効になっていることを確認します。
2. 処理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、そのドライブが処理完了状態であることを確認してください。
3. 物理ディスクがRAIDモードでない場合は、iDRACウェブインタフェース、RACADM、Redfish、WSManなどのiDRACインタフェース、または<Ctrl+R>を使用してRAIDモードに変換します。

保留操作への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た場合は、保留操作が作成されます。ジョブは作成されません。その後、同じディスクのグローバルホットスペアの割り当てを解除すると、グローバルホットスペアの割り当て保留操作はクリアされます。

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、設定>ストレージ設定の順に移動します。
   - ストレージ設定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. 物理ディスクの構成をクリックします。
   - コントローラに関連付けられているすべての物理ディスクが表示されます。
4. 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の割り当てを選択します。
ホットスペアの割り当てを解除するには、アクション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。

Apply Now（今すぐ適用）をクリックします。

必要なディスクを削除するか、またはスケジュールされた時刻を適用することもできます。選択した操作モードに基づいて、設定が適用されます。

5. ホットスペアの割り当てを解除するには、アクション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。

6. Apply Now（今すぐ適用）をクリックします。

必要に応じて、次の再起動時またはスケジュールされた時刻を選択します。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、「iDRAC RACADM CLIガイド」は、www.dell.com/idracmanualsにあります。を参照してください。

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モードに変換すれば、そのディスクはすべてのRAID操作に対応します。ディスクが非RAIDモードであると、そのディスクはオペレーティングシステムに公開され（この点が未設定の良好なディスクと異なります）、ダイレクトパススルーモードが使用されます。

PERC 10では、ドライブを非RAIDに変換できません。ただし、PERC 10.2以降のバージョンではサポートされています。

物理ディスクのRAIDまたは非RAIDモードへの変換は、次の手順を実行することによって行うことができます。

1. iDRACウェブインタフェースで、Storage（ストレージ）> Overview（概要）> Physical Disks（物理ディスク）とクリックします。

2. Advanced Filter（詳細検索）をクリックします。さまざまなパラメータを設定できる詳細なリストが表示されます。

3. Group By（グループ化基準）ドロップダウンメニューでエンクロージャまたは仮想ディスクを選択します。エンクロージャまたは仮想ディスクが選択されなかった場合、エラーメッセージが表示されます。

4. 必要なパラメータを全部選択したら、Apply（適用）をクリックします。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。

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

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、Storage（ストレージ）> Overview（概要）> Physical Disks（物理ディスク）とクリックします。

2. Advanced Filter（詳細検索）をクリックします。さまざまなパラメータを設定できる詳細なリストが表示されます。

3. Group By（グループ化基準）ドロップダウンメニューでエンクロージャまたは仮想ディスクをどれか選択します。エンクロージャまたは仮想ディスクが選択されなかった場合、エラーメッセージが表示されます。

4. 必要なパラメータをすべて選択したら、Apply（適用）をクリックします。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。

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。

RAIDモードに変換するか、または非RAIDモードに変換するかに応じて、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。

メモ: S140コントローラでは、RACADMインターフェースのみを使用して、eenthymまたはRAIDモードからRAIDモードに変換できます。サポートされるソフトウェアRAIDモードは、WindowsまたはLinuxモードです。

コマンドの詳細については、「iDRAC RACADM CLIガイド」は、www.dell.com/idracmanualsにあります。を参照してください。
物理ディスクの消去

システム消去機能を使用すると、物理ドライブの内容を消去できます。この機能には、RACADM または LC GUIを使用してアクセスできます。サーバの物理ドライブは、2つのカテゴリに分類されます。

- セキュア消去ドライブ - ISE、SED SAS、SATA ドライブ、PCIe SSDなど暗号消去機能を備えたドライブです。
- 上書き消去ドライブ - 暗号消去をサポートしていないすべてのドライブです。

RACADM SystemEraseサブコマンドには、次のカテゴリのオプションがあります。

- SecureErasePDオプションは、すべてのセキュア消去ドライブを暗号的に消去します。
- OverwritePDオプションは、すべてのドライブのデータを上書きします。

メモ：BOSS物理ディスクの暗号消去は、SystemEraseメソッドによる実行が可能です。これにはLC-UI、Wsman、およびRacadmでサポートされています。

SystemEraseを実行する前に、次のコマンドで、サーバのすべての物理ディスクの消去機能を確認してください。

```bash
# racadm storage get pdisks -o -p SystemEraseCapability
```

ISEおよびSEDドライブを消去するには、次のコマンドを使用します。

```bash
# racadm systemerase -secureerasepd
```

上書き消去ドライブを消去するには、次のコマンドを使用します。

```bash
# racadm systemerase -overwritepd
```

メモ：RACADM SystemEraseは、上記のコマンドで消去された物理ディスクから、すべての仮想ディスクを削除します。

メモ：RACADM SystemEraseは、消去操作を実行するためにサーバを再起動させます。

メモ：個々のPCIe SSDまたはSEDデバイスは、iDRAC GUIまたはRACADMを使用して消去できます。詳細については、「PCIe SSD デバイスデータの消去」および「SED デバイスデータの消去」の項を参照してください。

Lifecycle Controller GUI内のシステム消去機能の詳細については、「Lifecycle Controllerユーザーズガイド」は、www.dell.com/idracmanualsにあります。を参照してください。

SEDデバイスデータの消去

メモ：この操作は、SEDデバイスが仮想ディスクの一部の場合にはサポートされていません。デバイス消去を実行する前に、ターゲットのSEDデバイスを仮想ディスクから取り外しておく必要があります。

暗号消去では、ディスク上のすべてのデータが完全に消去されます。SEDの暗号消去を実行すると、すべてのブロックが上書きされ、SED上の全データが完全に失われます。暗号消去中、ホストはSEDにアクセスできません。SEDデバイス消去は、リアルタイムに実行するか、システム再起動後に適用できます。

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、動作はキャンセルされます。システムを再起動して操作を再開する必要があります。

SEDデバイスデータを消去する前に、次を確認します。

- 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。
- 選択したSEDドライブが仮想ディスクの一部ではない。

メモ：

- SEDの消去は、リアルタイムまたはステージング操作として実行できます。
- SEDドライブが消去された後も、データのキャッシングにより、OS内では引き続きアクティブとして表示される可能性があります。この場合、OSを再起動すると、消去されたSEDドライブは表示されなくなり、データは報告されなくなります。
- 暗号的消去機能は、第14世代PowerEdgeサーバのSEDでサポートされます。
ウェブインタフェースを使用した SED デバイスデータの消去

SED 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、Storage (ストレージ) > Overview (概要) > Physical Disks (物理ディスク) に移動します。
   Physical Disk (物理ディスク) ページが表示されます。
2. Controller (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 SED 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 SED に対する Cryptographic Erase (暗号消去) を選択します。
   Cryptographic Erase (暗号消去) 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、Action (アクション) 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 (Controller) 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。
   - Apply Now (今すぐ適用) - このオプションを選択して、アクションをただちに適用します。システムの再起動は不要です。
   - At Next Reboot (次の再起動時) - このオプションを選択すると、次回システム再起動時にアクションを適用します。
   - 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。アクションは、開始時刻と終了時刻の間に適用されます。
   - 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)
5. 適用をクリックします。
   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。
   ジョブが正常に作成された場合、選択したコントローラにそのジョブ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。
   保留中の操作が作成されないと、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 SED デバイスデータの消去

SED デバイスを安全に消去するには、次の手順を実行します。

```bash
racadm storage cryptographicerase:<SED_FQDD>
cryptographicerase 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。
```

```bash
racadm jobqueue create <SED_FQDD> -s TIME_NOW -realtime

cryptographicerase コマンドを実行した後にターゲットステージングジョブを作成するには、次の手順を実行します。
```

```bash
racadm jobqueue create <SED_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。
```

```bash
racadm jobqueue view -i <job ID>

詳細については、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。参照してください。
```

物理ディスクの再構築

物理ディスクの再構築は、故障したディスクの内容を再構築する機能です。これは、自動再構築オプションがfalse (偽) に設定されている場合にのみ当てはまります。冗長仮想ディスクがある場合、故障した物理ディスクの内容を再構築操作で再構築できます。構築は通常の動作中に実行できますが、実行するとパフォーマンスが劣化します。
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
- 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
- バックグラウンドの初期化のキャンセル
- RAID レベルのマイグレーション

メモ: iDRAC インタフェースを使用して 240 の仮想ディスクを管理および監視することができます。VD を作成するには、デバイスセットアップ (F2)、PERCLI コマンドラインツール、または Dell OpenManage Server Administrator (OMSA) のいずれかを使用します。

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 コントローラが 1 つまたは複数の物)

therapyディスクから作成する、ストレージのことを指します。仮想ディスクは複数の物理ディスクから作成できますが、オペレーティングシステムからは単一のディスクとして認識されます。

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」の情報をよくお読みください。

PERC 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できます。仮想ディスクを作成するには、サーバーコントロールユーザーの権限が必要です。最大 64 の仮想ドライブを作成することができ、同じドライブグループでは最大 16 の仮想ドライブを作成することができます。

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場合。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場合。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。
- 1 つのドライブグループでサポートされる仮想ディスクの最大数に達している場合。選択したグループから 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。
- ジョブが現在実行されている場合、または選択したコントローラ上にスケジュール設定されている場合。ジョブが完了するまで待つ、ジョブを削除してから、新しい操作を試行する必要があります。ジョブキューページで、スケジュール設定されたジョブのステータスを表示し管理することができます。
- 物理ディスクが非 RAID モードである場合。IDRAC ウェブインタフェース、RACADM、Redfish、WSMan などの IDRAC インタフェースを使用するか、<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: iDRAC インタフェースを使用して 240 の仮想ディスクを管理および監視することができます。VD を作成するには、デバイスセットアップ (F2)、PERCLI コマンドラインツール、または Dell OpenManage Server Administrator (OMSA) のいずれかを使用します。

仮想ディスクに対する保存中の操作に追加モードで仮想ディスクを削除し、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存中の作成操作がクリアされます。

メモ: PERC H330 では RAID 6 および RAID 60 はサポートされません。
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、次のことを考慮してください。

- コントローラ上に保存されない仮想ディスク名 - 仮想ディスク作成時に指定期間より前に保存されている仮想ディスク名は、コントローラ上には保存されません。異なるオペレーティングシステムを使用して再起動した場合、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ている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、その一部を仮想ディスクに使用します。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バインドされます。したがって、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ことができる物理ディスクの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。
- 仮想ディスクを作成する際、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は、物理ディスクの数が制限されるため、使用できる物理ディスクの数も限られます。ストライプとスパンの制限は、RAIDレベルに次のように影響します。
  - 最大スパン数は、RAID10、RAID50、およびRAID60に影響します。
  - 最大ストライプ数は、RAID0、RAID5、RAID50、RAID6およびRAID60に影響します。
  - 1つのミラーレベルの物理ディスク数は常に2です。これはRAID1およびRAID10に影響します。
- PCIe SSD上で仮想ディスクを作成できません。

Web インターフェイ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 Web インターフェイスで、【ストレージ】＞【概要】＞【仮想ディスク】＞【詳細フィルター】の順に移動します。
2. 【仮想ディスク】セクションで次の操作を実行します。
   a. 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。
   b. 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。
   c. 【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】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。
   d. 容量フィールドで、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。
   e. 【スパン数】フィールドは、選択した物理ディスクに基づいて表示されます（手順3）。この値を設定することはありません。これは、複数RAIDレベルの選択後、自動的に計算されます。
      - スパン数フィールドは、RAID10、RAID50、およびRAID60に適用されます。RAID10選択時にコンテナが不均等RAID10をサポートしている場合、スパン数は表示されません。コントローラによって、適切な値が自動的に設定されます。RAID50およびRAID60において、RAID作成に最小数のディスクが使用されている場合、このフィールドは表示されません。より多くのディスクが使用された場合、この値は変更できます。
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の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。
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やを変更することができます。

**メモ:** 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。また、ディスクキャッシュポリシーやは、ディスクキャッシュポリシーやを設定するかを指定します。

- **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のポリシーより続きます。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どうかを必ずしも評価し、必要なときに先読みを開始します。
- **先読み** — コントローラはデータシーケンシ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、先読みポリシーより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より選択すると、コントローラは先読みポリシーより使用しません。

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。ライトスルーは、ディスクドライブにデータが無事に書き込まれた場合にのみ書き込みポリシーよりシステム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に時間がかかる場合、ライトバックキャッシュよりも優れたディスク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ディスクキャッシュに保存された後でのみ書き込み要求完了信号を送信します。ライトバックキャッシュは、ディスクドライブにデータが無事に書き込まれた場合にのみ書き込みポリシーよりシステム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が遅い場合、ライトバックキャッシュよりもディスクへの書き込みが遅くなる可能性があります。また、ディスクキャッシュポリシーやは、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より影響しません。

**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やまたは書き込みポリシーより影響します。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きは限りません。
- 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、ポリシーや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い、ポリシーや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ない場合、ベースの電源がオフになるたびにデータが失われることはありません。そのため、一部の PERC ではこのポリシーやは設定できません。

したがって、PERC に応じてポリシーやの値が設定されます。

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。
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）情報の正確性を検証します。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によって冗長データが再構成されます。仮想ドライブに劣化ステータスがある場合、整合性チェックによって仮想ディスクを準備完了ステータスに戻せる場合があります。整合性チェックはWebインタフェースまたはRACADMを使用して実行できます。

整合性チェック操作は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、リアルタイムの操作です。

仮想ディスクの初期化

仮想ディスクの初期化で、ディスク上のデータはすべて消去されますが、仮想ディスク設定は変更されません。使用前に設定された仮想ディスクは初期化する必要があります。

高速初期化

高速初期化では、仮想ディスク内のすべての物理ディスクが初期化されます。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。この初期化タスクは、物理ディスク上の既存の情報が消去されないため、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。

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ることはありません（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ません。

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8MBが上書きされ、ブートマーカーがすべてまたはパーティション情報がクリアされます。操作完了にかかる時間は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完了の5分後に開始されます。

完全または低速初期化

完全初期化では、仮想ディスク内のすべての物理ディスクが初期化されます。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。完全初期化が完了後には、仮想ディスクの作成時に実行することができません。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、バックグラウンド初期化は必要ありません。完全初期化中に、ホストは仮想ディスクにアクセスできません。仮想ディスクの完全初期化は、システムを再起動すると、操作は中止され、仮想ディスクでバックグラウンドの初期化プロセスが開始されます。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は自動的に設定されます。

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ごく一部です。

---

### 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）、作成された仮想ディスクの暗号化はSEDドライプを使って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。

### メモ
暗号化はコントローラで有効ですが、VDをiDRACから作成する場合は、VDの暗号化を手動で有効にする必要がありま...
仮想ディスクの容量は、互換物理ディスクを既存の仮想ディスクグーに追加することでも拡張できます。このオプションでは、新たに増加した仮想ディスクのサイズを入力できません。特定の仮想ディスク上の既存の物理ディスクグループで使用されているディスク容量、仮想ディスクの既存のRAIDレベル、および仮想ディスクに追加された新規ドライブの数に基づいて、新たに増加した仮想ディスクサイズが計算され、表示されます。

容量の拡張では、ユーザーが最終的なVDのサイズを指定できます。内部では、最終的なVDのサイズはPERCにバーサンテージで伝達されます（このバーサンテージは、ローカルディスクが拡張できるアレイの空き容量のうち、ユーザーが使用する容量）。このバーサンテージロジックのため、再設定を完了後の最終VDサイズは、ユーザーが可能な限り最大のVDサイズを最終VDサイズとして入力していない場合、ユーザーが入力したサイズとは異なる可能性があります（バーサンテージ80%を下回ることになります）。ユーザーが可能な限り最大のVDサイズを入力した場合は、入力したサイズと再設定後の最終VDサイズに違いはありません。

RAIDレベルの移行

RAIDレベルの移行（RLM）とは、仮想ディスクのRAIDレベルを変更することです。iDRAC9には、RLMを使用してVDサイズを拡張するオプションがあります。RLMでは、1つの方法として、仮想ディスクのRAIDレベルを移行することで、仮想ディスクのサイズを拡張できます。

RAIDレベルの移行とは、特定のRAIDレベルのVDを別のRAIDレベルに変換するプロセスです。VDを別のRAIDレベルに移行した場合、そのVD上のユーザーデータは、新しい構成のフォーマットに再配置されます。

この構成は、ステージングとリアルタイムの両方でサポートされます。

次の表に、ディスクを追加する場合とディスクを追加しない場合の双方で、VDの再設定（RLM）時に有効とされるVDレイアウトを示します。

表54. 有効なVDレイアウト

<table>
<thead>
<tr>
<th>ソースVDレイアウト</th>
<th>ディスクを追加する場合の有効なターゲットVDレイアウト</th>
<th>ディスクを追加しない場合の有効なターゲットVDレイアウト</th>
</tr>
</thead>
<tbody>
<tr>
<td>R0（単一ディスク）</td>
<td>R1</td>
<td>非対応</td>
</tr>
<tr>
<td>R0</td>
<td>R5/R6</td>
<td>R5/R6</td>
</tr>
<tr>
<td>R1</td>
<td>R0/R5/R6</td>
<td>R0</td>
</tr>
<tr>
<td>R5</td>
<td>R0/R6</td>
<td>R5</td>
</tr>
<tr>
<td>R6</td>
<td>R0/R5</td>
<td>R0/R6</td>
</tr>
</tbody>
</table>

OCEまたはRLMが実行中の場合に許可される操作

OCE/RLMを実行中の場合、次の操作が可能になります。

表55. 許可される操作

<table>
<thead>
<tr>
<th>コントローラー側から（バックグラウンドではOCE/RLM経由でVDが機能）</th>
<th>VD側から（OCE/RLM経由で機能）</th>
<th>同じコントローラー上にある他の準備完了状態の物理ディスクから</th>
<th>同じコントローラー上にある他のVD（OCE/RLM経由で機能していない）から</th>
</tr>
</thead>
<tbody>
<tr>
<td>設定のリセット</td>
<td>削除</td>
<td>点滅</td>
<td>削除</td>
</tr>
<tr>
<td>ログのエクスポート</td>
<td>点滅</td>
<td>点滅解除</td>
<td>点滅</td>
</tr>
<tr>
<td>巡回読み取りモードの設定</td>
<td>点滅解除</td>
<td>グローバルネットワークスベースの割り当て</td>
<td>点滅解除</td>
</tr>
<tr>
<td>巡回読み取りの開始</td>
<td>非RAIDディスクへの変換</td>
<td>名前の変更</td>
<td></td>
</tr>
<tr>
<td>コントローラーブロバティの変更</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>物理ディスク電源の管理</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAID対応ディスクへの変換</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>非RAIDディスクへの変換</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
許可される操作（続き）

<table>
<thead>
<tr>
<th>コントローラー側から（バックグラウンドでは OCE/RLM 経由で BD が機能）</th>
<th>BD 側から（OCE/RLM 経由で機能）</th>
<th>同じコントローラー上にある他の準備完了状態の物理ディスクから</th>
<th>同じコントローラー上にある他の BD（OCE/RLM 経由で機能していない）から</th>
</tr>
</thead>
<tbody>
<tr>
<td>コントローラー モードの変更</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

OCE と RLM の制限

OCE と RLM には次の一般的な制限があります。

- OCE/RLM は、ディスクグループの含む仮想ディスクが１つのみのシリコンに限定されています。
- OCE はRAID50およびRAID60ではサポートされません。RAID10、およびRAID50、RAID60では、RLM がサポートされていません。
- コントローラー上に最大数の仮想ディスクがすでに存在する場合は、どの仮想ディスクにおいてもRAIDレベルの移行または容量の拡張を行うことはできません。
- RLM/OCE が完了するまで、RLM/OCE を実行中のすべての仮想ディスクの書き込みキャッシュポリシーが、コントローラ下によってライトスルーに変更されます。
- Virtual Disks（仮想ディスク）の再設定では通常、再設定操作が完了するまで、ディスクのパフォーマンスに影響があります。
- ディスクグループ内の物理ディスクの合計数は、32 以下にする必要があります。
- 対象とする仮想ディスク内物理ディスクでバックグラウンド操作（BGI/再構築/コピーバック/巡回読み取り）が何かすでに実行中の場合、その時点では再設定（OCE/RLM）が許容されません。
- 仮想ディスクに関連付けられたドライブでの再設定（OCE/RLM）の進行中に何らかのディスク移行を実行すると、再設定が失敗します。
- RLM/OCE 用に追加した新規ドライブは、再構築が完了した後で仮想ディスクの一部に組み込まれます。ただし、これらの新規ドライブの State（状態）は再構築の開始直後に Online（オンライン）に変わります。

初期化のキャンセル

この機能では、仮想ディスク上でバックグラウンドの初期化をキャンセルできます。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は、仮想ディスクの作成後に自動的に起動します。冗長仮想ディスクのバックグラウンド初期化によって、仮想ディスクでパリティ情報が準備され、書き込みパフォーマンスが向上します。ただし、バックグラウンド初期化の進行中には、仮想ディスクの作成など一部のプロセスは実行できません。初期化のキャンセルによって、バックグラウンド初期化がキャンセルされると、0 〜 5 分以内に自動的に再開します。

Memo: バックグラウンド初期化は、RAID 0 の仮想ディスクには適用されません。

ウェブインタフェースを使用した仮想ディスクの管理

1. iDRAC ウェブインタフェースで、[ 設定 ] > [ ストレージ設定 ] > [ 仮想ディスク設定 ] の順に移動します。
2. [ 仮想ディスク ] から、仮想ディスクを管理するコントローラーを選択します。
3. [ アクション ] ドロップダウンメニューから、アクションを選択します。

アクションを選択すると、追加の [ アクション ] ワインドウが表示されます。目的の値を選択または入力します。

- 名前の変更
- 削除
- [ キャッシュポリシーの編集 ] - 次のオプションのキャッシュポリシーを変更できます。
  - [ 読み取りポリシー ] - 次の値を選択できます。
    - 適応先読み - 所定のポリシーについて、直近の２回のディスクアクセスが連続したセクタで行われた場合、コントローラーが先読みキャッシュポリシーを使用することを示します。読み取り要求がランダムの場合、コントローラーは先読みなしモードに戻ります。
    - 先読みなし - 所定のポリシーについて、先読みポリシーが使用されないことを示します。
    - 先読みあり - 所定のポリシーについて、データが要求されることを見越して、コントローラーが要求データを順次先読みし、追加データをキャッシュメモリに保存することを示します。これにより、連続したデータの読み取り速度が向上します。ただし、ランダムデータへのアクセスにはあまり効果があります。
  - 書き込みポリシー - 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 - 所定のポリシーについて、ディスクサブシステムでトランスカショ内のすべてのデータの受信が完了したとき、コントローラがホストシステムにデータ転送完了信号を送信することを示します。
ライトバック — 所定のボリュームについて、コントローラキャッシュでトランザクション内のすべてのデータの受信が完了したとき、コントローラがホストシステムにデータ転送完了信号を送信することを示します。その後、コントローラは、キャッシュされたデータをストレージデバイスにバックグラウンドで書き込みます。

強制ライトバック — 強制ライトバックキャッシュを使用した場合、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ュが使用されると、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：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 — デスクでデフォルトの書き込みキャッシュモードが使用されていることを示します。SATAディスクの場合、これは有効になっています。SASディスクの場合、これは無効になっています。

○ 有効 — デスクの書き込みキャッシュが有効になっていることを示します。これにより、パフォーマンスが向上しますが、電源喪失時のデータ損失の可能性も高まります。

○ 無効 — デスクの書き込みキャッシュが無効になっていることを示します。これにより、パフォーマンスは低下しますが、データ損失の可能性が低下します。

強制ライトバック — 強制ライトバックキャッシュを使用した場合、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ュが使用されると、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：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 — デスクでデフォルトの書き込みキャッシュモードが使用されていることを示します。SATAディスクの場合、これは有効になっています。SASディスクの場合、これは無効になっています。

○ 有効 — デスクの書き込みキャッシュが有効になっていることを示します。これにより、パフォーマンスが向上しますが、電源喪失時のデータ損失の可能性も高まります。

○ 無効 — デスクの書き込みキャッシュが無効になっていることを示します。これにより、パフォーマンスは低下しますが、データ損失の可能性が低下します。

RAIDレベルの移行
- デスク名、現在のRAIDレベル、および仮想ディスクのサイズを表示します。新しいRAIDレベルを選択できます。新しいRAIDレベルに移行するには、ユーザーは既存の仮想ディスクにドライブを追加する必要がある場合があります。この機能は、RAID 10、50および60では適用されません。

初期化：高速 — 物理ディスク上のメタデータが更新され、それでも、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。

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。

RAIDADM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 initvd:<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>
```

RACADMを使用した仮想ディスクの管理
ホットスペアの割り当て

ホットスペアの割り当て解除

RAID 設定機能

次の表に、RACADM および WSMAN で使用できる RAID 設定機能の一部を示します。

⚠️ 注意: 物理ディスクを制的にオンラインまたはオフラインにすると、データが失われることがあります。

表 56. RAID 設定機能

<table>
<thead>
<tr>
<th>機能</th>
<th>RACADM コマンド</th>
<th>説明</th>
</tr>
</thead>
</table>
| オンライン強制            | racadm storage forceonline:<PD FQDD>             | 電源障害、データの破損、またはその他の理由により、物理ディスクがオフラインになることがあります。この機能を使用すると、他のすべてのオプションが使用されなくなったときに、物理ディスクを強制的にオンライン状態に戻すことができます。コマンドを実行すると、コンテーラーはドライプをオンライン状態に戻し、仮想ディスク内のメンバーを復元します。これは、コンテーラーがデータから読み取り、そのメータデータに書き込むことができる場合にのみ発生します。

オフライン強制

| 機能                     | racadm storage forceoffline:<PD FQDD>           | この機能は、仮想ディスク設定からドライプを削除してオフラインにするため、VD設定が劣化します。ドライプが近い将来故障する可能性がある場合、またはSMART障害が報告されている場合にのみオンラインである場合に役立ちます。既存のRAID構成の一部であるドライプを使う場合にも使用できます。

物理ディスクの交換

| 機能                     | racadm storage replacephysicaldisk:<Source PD FQDD> -dstpd <Destination PD FQDD> | VD のメンバーである物理ディスクから別の物理ディスクにデータをコピーできます。ソースディスクはオンライン状態である必要がありますが、宛先ディスクは準備完了状態であり、ソースを交換するために同じサイズとタイプである必要があります。

起動デバイスとしての仮想ディスク

| 機能                     | racadm storage setbootvd:<controller FQDD> -vd <VirtualDisk FQDD> | 仮想ディスクは、この機能を使用して起動デバイスとして設定できます。これにより、冗長性のあるVDが起動デバイスとして選択され、オペレーティングシステムがインストールされている場合に、フォールトトレランスが有効になります。

外部設定のロック解除

| 機能                     | racadm storage unlock:<Controller FQDD> -key <Key id> -passwd <passphrase> | この機能は、宛先とは異なるソース コントローラー暗号化を持つロックされたドライプを認証するために使用されます。ロック解除されると、ドライプを1つのコントローラーから別のコントローラーに正常に移行できます。
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
- 保持キャッシュの破棄

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
- 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
- 暗号化モード（ローカルキー管理およびSecure Enterprise key Manager）

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。SASおよびSATA HDDで1週間に1回、自動的に実行されます。

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。

- 物理ディスクはSSDです。
- 物理ディスクが仮想ディスクに含まれていない、またはネットスペアとして割り当てられている。
- 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動作中に一時停止され、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。

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コントローラのみ使用可能です。

250 Managing storage devices
整合性チェック

整合性チェックは、冗長(パリティ)情報の正確性を検証します。このタスクは冗長仮想ディスクの作成に必要となります。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。このタスクの完了後、パリティ情報が初期化されます。

バックグラウンド初期化プロセスは、冗長仮想ディスクの作成に伴う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は最下位となります。バックグラウンド初期化が完了するまで実行する必要があります。バックグラウンド初期化の完了後に、システムパフォーマンスに与える影響は最小となります。バックグラウンド初期化が完了した場合、整合性チェックタスクの最優先となります。整合性チェックの優先順は最下位となり、完了までに最も長い時間がかかります。バックグラウンド初期化完成後、パリティ情報が初期化されます。

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セスを変更するときは、セキュリティキーを生成したり、変更したりします。コントローラは暗号化キーを使用して、SEDへのアクセスをロックまたはアンロックします。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、次の機能を使用して管理します。

1. ローカルキー管理 (LKM) システム：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は、セキュリティキー識別子とパスフレーズを入力して暗号化キーを生成する必要があります。
2. Secure Enterprise Key Manager (SEKM)：この機能では、キー管理サーバー (KMS) を使用してキーを生成します。SEKMを使用する場合、KMS の情報で iDRAC を設定し、さらに SSL/TLS 関連の設定も行う必要があります。

**memo:**
- このタスクは、eHBA モードで実行されている PERC ハードウェアコントローラーではサポートされていません。
- 「保留中の操作に追加」モードでセキュリティキーを作成しながらジョブが作成しないで、その後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という保留中の操作はクリアされます。

**memo:**
- SEKM を有効にするには、サポートされている PERC ファームウェアがインストールされていることを確認してください。
- SEKM では、TLS 1.2 のみがサポートされます。
- SEKM が有効になっている場合、PERC ファームウェアを以前のバージョンにダウングレードすることはできません。SEKM モードになっている同一システムで、他の PERC コントローラー・ファームウェアをダウングレードした場合でも、操作が失敗する可能性があります。SEKM モードになっている PERC コントローラーのファームウェアをダウングレードするには、OS DUP アップデートの手順で実行するか、またはコントローラで SEKM を無効にした上で iDRACからダウングレードを再試行します。

**memo:** ホットプラグ接続されたロック済みのポリュームを特定のサーバーから別のサーバーにインポートした場合、LC ログを確認すると、コントローラー属性の CTL エントリが適用されていることがわかります。
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、Storage (ストレージ) > Overview (概要) > Controllers (コントローラ) の順に移動します。
2. Controller (コントローラ) セクションで、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。
   - Current Value (現在の値) 列に、各プロパティの既存の値が表示されます。各プロパティの Action (処置) ドロップダウンメニューからオプションを選択して、この値を変更できます。

   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. Apply Operation Mode (操作モードの適用) 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: コントローラ内部に利用可能な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 レベルの変更後に入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

外部設定とは、1つのコントローラから別のコントローラに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格納されてい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駆動状態の仮想ディスク、あるいはインポート可能ですでに存在している仮想ディスク専用のホットスパースが含まれている場合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 RAID1 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であるため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 RAID5 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、RAID5 仮想ディスクは失敗状態にあり、インポートできません。

仮想ディスクの他に、外部設定には、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ているが、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内に存在しなくなっているという場合、その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ー (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のロックを解除し、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。物理ディスクの状況が外部の場合、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、ホットスペアの割り当てがあります。

MEMO: 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、ユーザーの操作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ています。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、手動による操作なしに、検出し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。

MEMO: システムでオペレーティングシステムを実行している場合、外部エンクロージャー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、2 台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

MEMO: システムに未完了の外部ディスク構成がある場合は、1 つ以上の既存のオンライン仮想ディスクの状態も外部として表示されます。

MEMO: BOSS コントローラの外部設定のインポートはサポートされていません。

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、設定 → ストレージ設定 の順に移動します。
2. コントローラドロップダウンメニューから、インポートする外部設定のコントローラを選択します。
3. 外部設定の下にある インポート をクリックして、適用 をクリックします。

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、物理ディスクには仮想ディスク（外部設定）のすべて、または一部が含まれている場合があります。物理ディスクが外部の場合、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、物理ディスクに接続されるディスク上のすべてのデータが永続的に消去されます。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があります。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、設定 > ストレージ設定 > コントローラ設定 の順に移動します。

2. コントローラードロップダウンメニューから、クリアする外部設定のコントローラを選択します。

メモ: BOSSコントローラーの外部設定をクリアするには、設定をリセットをクリックします。

3. 設定のクリア をクリックします。

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、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、コントローラ上のネットワークがすべて削除されます。設定からディスクが削除される以外に、データは削除されません。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、データは削除されません。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。サーバ制御の権限が必要です。

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、Storage (ストレージ) > Overview (概要) > Controllers (コントローラ) の順に移動します。

2. Actions (処置)から、1つまたは複数のコントローラのReset Configuration (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

```
racadm storage resetconfig:<Controller FQDD>
```
コントローラモードの切り替え

PERC 9.1 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。コントローラーは、ドライバーがオペレーティングシステムを経由する際のHBAコントロラーと同様に動作します。コントローラー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。

PERC 10 以降のコントローラーは、拡張HBAモードをサポートしており、現在のコントローラーモードオプションからHBAを置き換えます。ただし、PERC 9 は引き続きHBAモードをサポートしています。

1. コントローラーがRAIDモードで設定されている場合は、HBAモードに設定する前に、仮想ディスク、ホットスペア、外部設定のすべてが削除され、システムの起動時にその他の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モードに設定すると、CONRAKの保留値を設定してからモードを切り替えても、保留値は変更されません。

RAIDモードを切り替え前に、モードを切り替えるためのサーバー制御権限があることが必要です。

1. コントローラーをRAIDからHBAに変更する前に、次の機能があります。

- RAIDレベル0、1、または10で仮想ディスクを作成します。
- RAIDディスクをホストに提示します。
- 仮想ディスクのデフォルトキャッシュポリシーを、先読みを伴うライトバックとして設定します。
- 仮想ディスクと非RAIDディスクを有効な起動デバイスとして設定します。
- 次の場合、すべての未設定ディスクは自動的に非RAIDに変換されます。
  - システムの起動時
  - コントローラーのリセット時
  - 仮想ディスクリストがホットプール插入されている場合

1. コントローラーモードを切り替え前に、次の機能があります。

- RAIDコントローラがコントローラーモードの変更をサポートしている。コントローラーモードを変更するオプションは、RAIDフォーマットリセットが必要とするコントローラでは使用できません。
- ストレージ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。
- 障害の発生した物理ディスクが削除または固定キャッシュがクリアされている。
- SEDに関連付けられているローカルセキュリティキーが削除する必要があります。
- コントローラーが保存キャッシュが存在していない（必須）。
- コントローラーモードを切り替えるためのサーバー制御権限がある。

1. コントローラーモードを切り替え前に、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（MXプラットフォームには非該当）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/cmcmanualsに『PowerEdge FX2/FX2s対応Dell Chassis Management Controller運用ガイド1.2 コーディザインガイド』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WSMan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モードで設定されている場合は、HBAモードに設定する前に、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。
- コントローラーモード設定中にその他の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、保留値が開始されます。
- 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す。また、RAIDEnhancedAutoImportForeignConfig属性は自動的にEnabled（有効）に設定されます。

次のリストに、WSManまたはRACADMインタフェースでサーバ設定プロファイア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、ドライプを準備完了で変換して仮想ディスクを作成するようにエクスポートサーバ設定プロファイル (SCP) を編集できます。

RAID から HBA にモードを変更するときに、RAIDaction getiuc がデフォルト動作に設定されます。属性が存在するとき、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、SCP 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 SCP 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 ステップ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には、次の手順を実行します。

1. iDRAC Web インターフェースで、ストレージ > 概要 > コントローラーの順にクリックします。

2. コントローラーの現在の設定が表示されます。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には、以下のコマンドを実行します。

```bash
$ racadm get Storage.Controller.1.RequestedControllerMode[key=<Controller_FQDD>]
```

次に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：

```bash
$ racadm set Storage.Controller.1.RequestedControllerMode HBA [Key=<Controller_FQDD>]
```

- ジョブを作成して変更を適用するには、次の手順を実行します。

```bash
$ racadm jobqueue create <Controller Instance ID> -s TIME_NOW -r pwrcycle
```

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

Dell PowerEdge サーバーには、オペレーティング システムがインストールされ、Dell HBA を動作させるための適切なデバイス ドライバがロードされている必要があります。POST 後、HBA ボートは無効になり、HBA デバイスドライバは、HBA をリセットし、ストレージデバイスに接続されているポートを有効にします。オペレーティング システムがないと、ドライバはロードされず、iDRAC が Dell HBA に接続されたストレージデバイスを表示できる保証はありません。

非 RAID コントローラーとは、RAID 機能がない HBA です。これらのコントローラーは、仮想ディスクをサポートしません。

14 世代 iDRAC インターフェースは、12 Gbps SAS HBA コントローラーと HBA330（内蔵またはアダプター）コントローラーをサポートしています。

非 RAID コントローラーについて、次のことを実行できます。

- 非 RAID コントローラーに該当するコントローラー、物理ディスク、エンクロージャのプロパティを表示します。また、エンクロージャに関連付けられている EMM、ファン、電源ユニット、温度プローブのプロパティを表示します。プロパティは、コンポーネント管理ツール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ベント情報の表示。
- 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消。
メモ:
• 非 RAID コントローラをイベントリーまたはモニタリングする前に、再起動時のシステム イベントリーの収集（CSIOR）操作を有効化します。
• 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。

メモ: SAS HBA コントローラーの背後にある障害ドライブの検出はサポートされていません。

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 では各ディスクの予測障害分析が実行され、ディスク障害が予測された場合はアラートが通知されますこのコントローラで障害予測のために物理ディスクがチェックされ、存在する場合は、この情報が iDRAC に渡されます。iDRAC によりすぐにアラートが記録されます。

非 RAID モード (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、複数のジョブを順に実行するようにスケジュールする。
保持キャッシュの管理

保存キャッシュ管理機能は、コントローラのキャッシュデータを破棄するオプションをユーザーに提供するコントローラオプションです。ライトバックポリシーでは、データはキャッシュに書き込まれてから物理ディスクに書き込まれます。仮想ディスクがオンラインになったり、何かの理由で削除された場合、キャッシュ内のデータが削除されます。

PREC コントローラは、電源障害が発生したりケーブルが抜かれたりした場合に、仮想ディスクが復旧するかキャッシュがクリアされるまで、保持キャッシュまたはデータキャッシュに書き込まれたデータを保持します。

コントローラのステータスは保持キャッシュの影響を受けます。コントローラに保存されたキャッシュがある場合、コントローラ状態は劣化と表示されます。保持キャッシュは、次の条件を満たした場合にのみ破棄できます。

- コントローラに外部設定がないこと。
- コントローラにオフラインディスクまたは欠落仮想ディスクがないこと。
- どこの仮想ディスクへのケーブルも切断されていない。

PCIe SSD の管理

Peripheral Component Interconnect Express (PCIe) ソリッドステートデバイス (SSD) は、低遅延で、1秒あたりの入出力速度 (IOPS) が高く、エンタープライズクラスストレージの信頼性と保守性が必要なソリューションのために設計された、高性能ストレージデバイスです。PCIe SSD では、高速 PCIe 2.0 または PCIe 3.0 準拠のインタフェースを備えた Single Level Cell (SLC) および Multi-Level Cell (MLC) NAND フラッシュチップに沿って用意されています。第 14 世代の PowerEdge サーバには、SSD を接続する方法が 3 種類あります。エクステンダを使用し、バックプレーンを介して SSD に接続する方法、バックプレーンからマザーボードまでスリムケーブルを使用して直接接続し、エクステンダは使用しない方法、マザーボード上の HHHL (アドイン) カードを使用する方法を選択できます。

メモ: 第 14 世代 PowerEdge サーバでは、業界標準の NVMe-MI 仕様に基づく NVMe SSD がサポートされています。ただし、Dell 専用の仕様をサポートするために使用されている第 13 世代 PowerEdge サーバは SSD に基づいています。前世代までのサーバからの SSD の追加は、iDRAC 9 ではサポートされていません。

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 では、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

第 14 世代 PowerEdge サーバの一部でのみ、最大 32 の NVMe SSD がサポートされています。

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
- LED の点滅または点滅解除（デバイスを識別）

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 のインベントリおよびリアルタイム監視
- 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

SSD に対しては次の操作を実行できます。

- 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

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。

メモ: NVMe デバイスが S140 で制御されている場合、取り外し準備および暗号消去の操作はサポートされません。点滅および点滅解除はサポートされます。

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は、2つの FQDN が表示されます。1つの FQDN は標準ドライブライト用で、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。SSD がコントローラに直接接続されている場合、コントローラ FQDD は SSD が CPU に直接接続されていることを示し、CPU.1 として報告します。

ソフトウェアイベントリには、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 のイベントリと監視
PClE SSD デバイスをイ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、「Storage (ストレージ)」を選択し、「Overview (概要)」> 「Physical Disks (物理ディスク)」の順に移動します。プロパティページが表示されます。PCIe SSD の場合、「Name (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 のイベントリと監視を行います。

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

メモ：この操作は、PCIe SSD が S140 コントローラを使用して構成されている場合はサポートされません。

PCIe SSD は秩序だったホットスワップをサポートしており、デバイスがインストールされているシステムを停止または再起動することなく、デバイスを追加または取り外すことができます。データの損失を避けるため、デバイスを物理的に取り外す前に「Prepare to Remove (取り外しの準備)」操作を行うことが必要です。

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する対応システムに PCIe SSD が取り付けられている場合のみサポートされます。PCIe SSD に対して正しいハードウェア設定が行われていることを確認するには、システム固有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。

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。

Prepare to Remove (取り外しの準備) 操作によって、バックグラウンド処理および進行中の I/O 処理が停止されるため、デバイスを安全に取り外すことができます。これにより、デバイス上のステータス LED が点滅します。Prepare to Remove (取り外しの準備) 操作を開始後、次の条件を満たすと、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（点滅する黄色）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。
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、Storage（ストレージ） > Overview（概要） > Physical Disks（物理ディスク）の順に移動します。
   - 物理ディスクのセットアップページが表示されます。
2. コントローラー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いただけに処置を使用します。
   - 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。

5. 機能を使用します。

   - 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処処置が表示されます。
   - ジョブが正常に作成された場合、選択したコントローラ上にそのジョブ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。

   メモ: PCIe SSD デバイスの場合、Apply Now (今すぐ適用) オプションのみ使用できます。ステージングされたモードでは、この操作はサポートされていません。

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。

```bash
racadm storage preparetoremove:<PCIeSSD FQDD>
```  
```bash
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。

```bash
racadm jobqueue view -i <job ID>
```

詳細については、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。を参照してください。

PCIe SSD デバイスデータの消去

メモ: この操作は、PCIe SSD が S140 コントローラを使用して構成されている場合はサポートされません。

暗号消去では、ディスク上のすべてのデータが完全に消去されます。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、動作はキャンセルされます。システムを再起動して操作を再開する必要があります。

PCIe SSD デバイスデータの消去する前に、次のこと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。
- ドライブが消去された後、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のネ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。
- 暗号的消去機能は、第14世代PowerEdgeサーバのネットプラグ対応PCIe SSDでサポートされます。

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、Storage（ストレージ）> Overview（概要）> Physical Disks（物理ディスク）に移動します。

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. Cryptographic Erase（暗号消去）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、Action（アクション）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、次のいずれかのオプションを選択します。
   - At Next Reboot（次の再起動時）-このオプションを選択すると、次回システム再起動時にアクションを適用します。
   - 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。アクションは、開始時刻と終了時刻の間に適用されます。
     - 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（コールドリブート）

5. 適用をクリックします。
   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。
   ジョブが正常に作成された場合、選択したコントローラにそのジョブ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。
   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
バックプレーンモードの設定

デルの第14世代PowerEdgeサーバーは、新しく内部ストレージトポロジーをサポートします。このトポロジーでは、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組の内部ドライバに接続することができます。この構成では、フェーラーバーや高可用性（HA）機能のないハイフォーマンスマードに使用されます。エキスパンダーは、2台のストレージコントローラ間で内部ドライバペアを分割します。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プ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。

一 統合モード - これがデフォルトモードです。2台目のPERCコントローラを取り付けられている場合でも、プライマリPERCコントローラに、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があります。
二 分割モード -1台のコントローラは最初の12ドライプにアクセスでき、2台目のコントローラは残りの12ドライプ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。
三 分割モード -4:20 -1台のコントローラは最初の4ドライプにアクセスでき、2台目のコントローラは残りの20ドライプ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。
四 分割モード -8:16 -1台のコントローラは最初の8ドライプにアクセスでき、2台目のコントローラは残りの16ドライプ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。
五 分割モード -16:8 -1台のコントローラは最初の16ドライプにアクセスでき、2台目のコントローラは残りの8ドライプ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。
六 分割モード -20:4 -1台のコントローラは最初の20ドライプにアクセスでき、2台目のコントローラは残りの4ドライプ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。エキスパンダー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ーの機能をチェックするか、2台目のPERCコントローラが存在するかどうかをチェックしません。

**メモ**：1つのPERCのみが接続された状態でバックプレーンを分割モードにするか、2つのPERCが接続された状態でバックプレーンを統合モードにするとき、ケーブルエラー（またはその他のエラー）が発生する可能性があります。

設定を変更するときは、サービス制御権限を持っている必要があります。他にRAID操作が保留中であるか、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、この設定が保存されている場合、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、データの一部があることを示す警告メッセージが表示されます。
- LCワイヤまたはiDRACリセット操作では、このモードに対するエキスパンダー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、ステージできません。
- 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、ドライブの間接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は、ドライブの間接付けに伴って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プ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、「設定」 > 「ストレージ設定」 > 「エンクロージャ設定」の順に移動します。
2. コントローラメニューでコントローラを選択して、そのコントローラに関連するエンクロージャを設定します。
3. アクションドロップダウンメニューで、エンクロージャモードの編集を選択します。
    エンクロージャモードの編集ページが表示されます。
4. 現在値列で、バックプレーンまたはエンクロージャに対して必要なエンクロージャモードを選択します。このオプションは次のとおりです。
    - 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

Memo: C6420 の場合、使用できるモードは分割モードと分割モード-6:6:6:6 です。一部の値は、特定プラットフォームでのみサポートされている場合があります。

R740xd および R940 の場合、新しいバックプレーンゾーンを適用するにはサーバのパワーサイクルが必要です。C6420 の場合、新しいバックプレーンゾーンを適用するには（ブレードシャーシの）A/C サイクルが必要です。

5. 保留中の操作に追加をクリックします。
   ジョブ ID が作成されます。
6. 今すぐ適用をクリックします。
7. 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。
8. 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。
   ```bash
   racadm get storage.enclosure.1.backplanecurrentmode
   ```
   出力は次のとおりです。
   ```plaintext
   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。
   ```bash
   racadm get storage.enclosure.1.backplanerequestedmode
   ```
   出力は次のとおりです。
   ```plaintext
   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。
   ```bash
   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。
   ```bash
   racadm get storage.enclosure.1.backplanerequestedmode
   ```
   出力は次のとおりです。
   ```plaintext
   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。

```bash
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。

```bash
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. backplanerquestedmode 属性値を表示するには、次のコマンドを実行します。

```bash
racadm get storage.enclosure.1.backplanerquestedmode
```

出力は次のとおりです。

```bash
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。

```bash
racadm serveraction powercycle
```

10. システムが POST と CSIOR を完了した後、次のコマンドを入力して backplanerquestedmode を確認します。

```bash
racadm get storage.enclosure.1.backplanerquestedmode
```

出力は次のとおりです。

```bash
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。

```bash
racadm get storage.enclosure.1.backplanecurrentmode
```

出力は次のとおりです。

```bash
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。

```bash
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 サーバー、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、スロット番号の高いものから 4つ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。Topology (トポロジ) ページ上のエクレ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けられたバックプレーンのみが System Inventory (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 コントローラーは、I2C モード (Dell バックプレーンのデフォルト設定) またはシリアル汎用入力/出力 (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 コントローラー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。特定のチャンネルアダプターをサポートするには、バックプレーンのモードを SGPIO モードに変更する必要があります。

SGPIOモードの設定

ストレージコントローラーは、I2Cモード（Dellバックプレーンのデフォルト設定）またはシリアル汎用入力/出力（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 コントローラー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。特定のチャンネルアダプターをサポートするには、バックプレーンのモードを SGPIO モードに変更する必要があります。

SGPIOモードは、パッケージバックプレーンのみでサポートされます。このモードは、エキスパンダーベースのバックプレーンまたはダウンストリームモードのパッケージ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、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には、SGPIOモードは無効な状態にリセットされます。これによって、iDRACの設定とバックプレーンの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の設定と一致するように変更されます。

装置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 Web インターフェイスを使用して、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。

これが無効に設定されていると、I2Cモードとなります。有効に設定されていると、SGPIOモードに設定されます。

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。

エンクロージャ資産タグの設定

エンクロージャ資産タグの設定によって、ストレージエンクロージャの資産タグを設定できます。

ユーザーは、エンクロージャを識別するために、エンクロージャの資産タグのプロパティを変更できます。これらのフィールドは無効な値がないチェックされ、無効な値が入力されている場合、エラーが表示されます。これらのフィールドは、エンクロージャファームウェアの一部であり、最初に示されるデータは、ファームウェアに保存されている値になります。

メモ:資産タグは、ヌル文字を含め、最大10文字に制限されています。

メモ:これらの操作は、内蔵のエンクロージャではサポートされません。

エンクロージャ資産名の設定

エンクロージャ資産名の設定によって、ストレージエンクロージャの資産名を設定できます。

ユーザーは、エンクロージャを簡単に特定できるように、エンクロージャの資産名プロパティを変更できます。これらのフィールドは無効な値がないチェックされ、無効な値が入力されている場合、エラーが表示されます。これらのフィールドは、エンクロージャファームウェアの一部であり、最初に示されるデータは、ファームウェアに保存されている値になります。
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。
   - Storage（ストレージ） > Physical Disks（物理ディスク）
   - Storage（ストレージ） > Virtual Disks（仮想ディスク）
   - Storage（ストレージ） > Controllers（コントローラ）
   - Storage（ストレージ） > Enclosures（エンクロージャ）

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。
   - Apply Now（今すぐ適用）- ただし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 コントローラでのみ使用できます。完了予定のジョブがある場合、このオプションはブ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。
   - At Next Reboot（次回の再起動時）- 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。
     - 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。
       - 開始時刻と終了時刻 - 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。
   - Add to Pending Operations（保留中の操作に追加）- 設定を適用するための保留中の操作を作成するには、このオプションを選択します。コントローラのすべての保留中の操作は、Storage（ストレージ） > Overview（概要） > Pending Operations（保留中の操作）ページで表示できます。

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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。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ー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はできませんが、個々の保留中の操作を削除することはできます。

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、Storage (ストレージ) > Overview (概要) > Pending Operations (保留中の操作) の順に移動します。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する、確定する、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 Pending Operations (保留中の操作) ページおよび Pending Operations (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。
　　• At Next Reboot (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。
　　• At Scheduled Time (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。
　　○ 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。アクションは、開始時刻と終了時刻の間に適用されます。
　　○ 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 (コールドプート)

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が表示されます。

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。Job Queue (ジョブキュー) をクリックして Job Queue (ジョブキュー) 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、または、保留中の操作が他に存在しない場合、Pending Operations (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。

Pending Operations (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。
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い場合、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。
- 保留中の操作が作成されず、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、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。
- 保留中の操作が作成されず、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。

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、続いてストレージ設定操作を行うため、このページに進みます。
  - 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。選択したコントローラ上でジョブが作成されるまで、こうした保留中の操作は適用されません。
- 保留中の操作が作成されず、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、続いてストレージ設定操作を行うため、このページに進みます。
  - 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、続いてストレージ設定操作を行うため、このページに進みます。
  - 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。
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。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。
   - Storage (ストレージ) > Overview (概要) > Physical Disks (物理ディスク) > Status (ステータス) - 識別したPhysical Disks (物理ディスク)ページが表示されるため、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。
   - Storage (ストレージ) > Overview (概要) > Virtual Disks (仮想ディスク) > Status (ステータス) - 識別したVirtual Disks (仮想ディスク)ページが表示されるため、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. 物理ディスクを選択する場合
   - すべてのコンポーネント LEDを選択または選択解除 - Select/Deselect All (すべて選択 / 選択解除)オプションを選択してBlink (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、Unblink (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Blink (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、Unblink (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. 仮想ディスクを選択する場合
   - 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 - Select/Deselect All (すべて選択 / 選択解除)オプションを選択してBlink (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、Unblink (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、Blink (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、Unblink (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選択または選択解除 - Select/Deselect All (すべて選択 / 選択解除)オプションを選択し、Blink (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、Unblink (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、Blink (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、Unblink (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の LED の点滅または点滅解除

コンポーネント LED の点滅と点滅解除を切り替えるには、次のコマンドを使用します。

```bash
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。
BIOS設定では、特定のサーバに使用されている複数の属性を表示できます。このBIOS構成設定では、各属性のさまざまなパラメータを変更できます。1つ以上の属性を選択すると、その属性に関連するさまざまなパラメータが表示されます。別の属性を変更する前に、属性の複数のパラメータを変更して変更を適用できます。ユーザーが構成グループを拡張すると、属性がアルファベット順に表示されます。

 Memo: 属性レベルのヘルプコンテンツは動的に生成されます。

適用

適用ボタンは、属性のいずれかが変更されるまで、グレー表示のままになります。属性を変更して 適用 をクリックすると、必要とされる変更値により、実際に属性を変更できます。リクエストがBIOS属性の設定に失敗した場合、エラーが返され、SMIL APIエラーまたはジョブ作成エラーに対応するHTTP応答ステータスコードが通知されます。この時点で、メッセージが生成され、表示されます。詳細については、「第14世代Dell EMC PowerEdgeサーバーのイベントおよびエラーメッセージリファレンスガイド」を参照してください。

変更の破棄

変更の破棄ボタンは、属性のいずれかが変更されるまで、グレー表示のままになります。変更の破棄ボタンをクリックすると、直前の変更がすべて破棄され、以前の値または初期値が復元されます。

適用して再起動

適用して再起動ボタンは、属性または Boot Sequence の値が変更されると、構成の適用に関して2つの選択肢が表示されます。適用して再起動と次回の再起動時に適用です。どちらの選択肢を選択しても、そのジョブの進行状況を監視できるように、ジョブキューページが表示されます。

ユーザーは、LCログでBIOS設定関連の監査情報を確認できます。

次回の再起動時に適用

次回の再起動時に適用をクリックすると、サーバの次回の再起動時に、必要な変更がすべて設定されます。次回の再起動時に適用します。どちらの選択肢を選択しても、そのジョブの進行状況を監視できるように、ジョブキューページが表示されます。

ユーザーは、LCログでBIOS設定関連の監査情報を確認できます。

保留中の値をすべて削除

保留中の値をすべて削除ボタンは、直前の設定変更で保留中になっている値がある場合にのみ使用できます。設定の変更を適用しないと決めた場合は、保留中の値をすべて削除ボタンをクリックして、すべての変更を削除します。リクエストがBIOS属性の削除に失敗した場合、エラーが返され、SMIL APIエラーまたはジョブ作成エラーに対応するHTTP応答ステータスコードが通知されます。この時点で、EEMIメッセージが生成され、表示されます。
保留中の値

iDRACを介したBIOS属性の設定は、すぐにBIOSに適用されるわけではありません。変更を適用するには、サーバーを再起動する必要があります。BIOS属性を変更すると、保留値がアップデートされます。属性にすでに保留中の値がある場合（設定されている場合）、その属性がGUIに表示されます。

BIOS設定の変更

BIOS設定を変更すると、監査ログエントリが生成され、LCログに保存されます。

BIOSライブスキャン

BIOSライブスキャンでは、ホストに電源が投入されてPOSTが実行されていないときに、BIOSプライマリROM内のBIOSイメージの整合性と信頼性が検証されます。

メモ:

- この機能にはiDRACDatacenterライセンスが必要です。
- この機能を操作するにはデバッグ権限が必要です。

次の状況において、iDRACはBIOSイメージの変更不可のセクションを自動的に検証します。

- ACサイクル/コールドプート時
- ユーザーが指定したスケジュールに従って
- オンデマンドで（ユーザーによる開始）

ライブスキャンが正常に完了した場合、LCログに結果が記録されます。失敗した場合は、LCLとSELに結果が記録されます。

トピック:

- BIOSライブスキャン
- BIOSのリカバリとハードウェアRoot of Trust（RoT）

BIOSライブスキャン

BIOSライブスキャンでは、ホストに電源が投入されてPOSTが実行されていないときに、BIOSプライマリROM内のBIOSイメージの整合性と信頼性が検証されます。

メモ:

- この機能にはiDRACDatacenterライセンスが必要です。
- この機能を操作するにはデバッグ権限が必要です。

次の状況において、iDRACはBIOSイメージの変更不可のセクションを自動的に検証します。

- ACサイクル/コールドプート時
- ユーザーが指定したスケジュールに従って
- オンデマンドで（ユーザーによる開始）

ライブスキャンが正常に完了した場合、LCログに結果が記録されます。失敗した場合は、LCLとSELに結果が記録されます。

BIOSのリカバリとハードウェアRoot of Trust（RoT）

PowerEdgeサーバーでは、悪意のある攻撃、電力サージ、またはその他の予期しない事象によって破壊したBIOSイメージを回復することが必要になります。起動できないモードから機能するモードにPowerEdgeサーバーを戻すには、BIOSを回復するための予備の代替BIOSイメージが必要になります。この代替/リカバリBIOSは、（プライマリBIOSSPIとともに多重化された）2番目のSPIに保存されています。

リカバリーシーケンスは、次のいずれかの方法を使用して開始できます。いずれの方法でも、iDRACがBIOSリカバリーテスクの主要なオーケストレーターになります。

272 BIOS設定
1. **BIOS プライマリーイメージ/リカバリーメージの自動リカバリ**: Intel Boot Guard または BIOS 自体によって BIOS の破損が検出されると、ホストの起動プロセス中に BIOS イメージが自動的にリカバリされます。

2. **BIOS プライマリー/リカバリーメージの強制リカバリ**: アップデートされた新しい BIOS を入手した場合、または起動に失敗して BIOS がクラッシュした場合に、BIOS をアップデートするため、ユーザーガ OOB リクエストを開始します。

3. **プライマリー BIOS ROM アップデート**: 単一のプライマリー ROM は、データ ROM とコード ROM に分かれています。IDRAC には、コード ROM に対するフル アクセス/フル コントロール権があります。必要に応じてコード ROM にアクセスするため、MUX を切り替えます。

4. **BIOS ハードウェア Root of Trust (RoT)**: この機能は、モデル番号が RX5X、CX5XX、TX5X のサーバーで使用できます。IDRAC はホストの起動時に毎回、RoT が実行されていることを確認します（ただし、コールド ブート時と A/C サイクル時のみで、ウォームリブート時は行われません）。RoT は自動的に実行されます。ユーザーがインタフェースを使用して RoT を開始することはできません。この IDRAC ブートの最初のポリシーによって、AC サイクル時およびホストの DC サイクル時に、ホスト BIOS ROM の内容が毎回検証されます。このプロセスによって、BIOS のセキュリティが駆動され、ホスト ブート プロセスのセキュリティが強化されます。
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用のライセンスが必要な機能です。ブレードサーバでは、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で、同じ管理下サーバコンソールが同時に表示されます。
- Java、ActiveX、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。

**メモ**: デフォルトでは、仮想コンソールのタイプはHTML5に設定されています。

**メモ**: Web サーバー構成の変更は、どのようなものでも既存の仮想コンソールセッションを終了させます。

- 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与えられます。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ことが通知されます。最初のユーザーは30秒以内に応答する必要があり、応答しない場合は、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与えられます。2つのセッションが同時にアクティブな場合は、最初のユーザーに2人目のユーザー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。最初のユーザーと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は、最初のユーザーのセッションが終了すると、2人目のユーザーのセッションも自動的に終了します。
- キーボードマクロは、すべてのプラグインでサポートされています。以下は、ActiveXおよびJavaプラグインでサポートされているマクロのリストです。

### 表 57. ActiveXおよびJavaプラグインでサポートされているキーボードマクロ

<table>
<thead>
<tr>
<th>Mac クライアント</th>
<th>Win クライアント</th>
<th>Linux クライアント</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-Alt-Del</td>
<td>Ctrl-Alt-Del</td>
<td>Ctrl-Alt-Del</td>
</tr>
<tr>
<td>Alt-SysRq-B</td>
<td>Alt-SysRq-B</td>
<td>Alt-SysRq-B</td>
</tr>
<tr>
<td>-</td>
<td>Win-P</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td>Ctrl-Alt-F&lt;1-12&gt;</td>
</tr>
<tr>
<td>Alt-SysRq</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>SysRq</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>PrtScrn</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Alt-PrtScrn</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>一時停止</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

**メモ**: HTML プラグインでサポートされているキーボードマクロについては、「HTML5ベースの仮想コンソール」セクションを参照してください。

**メモ**: ウェブインタフェースに表示されるアクティブな仮想コンソールセッションの数は、アクティブなウェブインタフェースセッションのみです。この数には、Telnet、SSH、RACADMなどの他のインタフェースからのセッションは含まれません。

**メモ**: お使いのブラウザで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.71」を参照してください。
仮想クリップボード

仮想クリップボードを用いると、テキストをコピー/貼り付けることができます。仮想コンソールからiDRACのホストサーバーに対して行えます。この操作は、クライアントコンピュータからiDRACのホストサーバーへの一方向のみのアクションです。

仮想クリップボードの使用は、次の手順で行えます。

1. ホストサーバーのデスクトップで貼り付け先とするウィンドウに、マウスのカーソルまたはキーボードのフォーカスを移動します。
2. vConsoleで[コンソール制御]を選択します。
3. OSクリップボードバッファからのコピーを、キーボードのホットキー、マウス、タッチパッドコントロールなど、クライアントOSに応じた操作で行います。あるいは、テキストボックスに対して手動でテキストを入力することもできます。
4. [クリップボードをホストに送信]をクリックします。
5. こうしたテキストは、ホストサーバーのアクティブウィンドウに表示されます。

メモ:

- この機能はASCIIテキストのみをサポートしています。
- 制御文字はサポートされていません。
- 改行やタブなどの文字は使用可能です。
- テキストボッファーのサイズは4000文字までです。
- 最大長を超えるバッファが貼り付けられた場合、iDRAC GUIの編集ボックスでは、最大バッファサイズへの切り捨てが行われます。

トピック:

- 対応画面解像度とリフレッシュレート
- 仮想コンソールの設定
- 仮想コンソールのプレビュー
- 仮想コンソールの起動
- 仮想コンソールビューアの使用

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 58. 対応画面解像度とリフレッシュレート

<table>
<thead>
<tr>
<th>画面解像度</th>
<th>リフレッシュレート (Hz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>720x400</td>
<td>70</td>
</tr>
<tr>
<td>640x480</td>
<td>60, 72, 75, 85</td>
</tr>
<tr>
<td>800x600</td>
<td>60, 70, 72, 75, 85</td>
</tr>
<tr>
<td>1024x768</td>
<td>60, 70, 72, 75, 85</td>
</tr>
<tr>
<td>1280x1024</td>
<td>60</td>
</tr>
<tr>
<td>1920x1200</td>
<td>60</td>
</tr>
</tbody>
</table>

モニターの画面解像度は1920x1200ピクセルに設定することをお勧めします。

仮想コンソールは、60 Hzのリフレッシュレートで最大1920x1200のビデオ解像度をサポートします。この解像度を実現するには、次の条件を満たす必要があります。
1920 x 1200 の解像度をサポートする VGA に接続された KVM/モニター。

- 最新の Matrox ビデオドライバー（Windows 用）

最大解像度が 1920 x 1200 未満のローカル KVM/モニターをいずれかの VGA コネクターに接続すると、仮想コンソールでサポートされる最大解像度は低下します。

iDRAC 仮想コンソールは、物理的なディスプレイが存在する場合に、オンボード Matrox G200 グラフィックスコントローラを活用して接続されているモニターの最大解像度を決定します。モニターが 1920 x 1200 以上の解像度をサポートしている場合、仮想コンソールは 1920 x 1200 の解像度をサポートします。接続されているモニターがサポートする最大解像度がそれよりも低い場合（多くの KVM が該当します）、仮想コンソールの最大解像度が制限されます。

物理モニターがサーバーのいずれの VGA ポートにも接続されていない場合、仮想コンソールで使用可能な解像度は、インストールされている OS によって決まります。

物理モニターがないホスト OS に基づく仮想コンソールの最大解像度:

- Windows の場合：1600 x 1200（1600 x 1200、1280 x 1024、1152 x 864、1024 x 768、800 x 600）
- Linux の場合：1024 x 768（1024 x 768、800 x 600、848 x 480、640 x 480）

メモ: ナノオペレーティングシステムを使用している場合は、仮想コンソールの状態を停止します。

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 ワンプ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。

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. Configuration（設定）＞Virtual Console（仮想コンソール）の順に移動します。仮想コンソールページが表示されます。
2. 仮想コンソールを選択して、必要な値を指定します。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。
   1. 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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。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、System（システム）＞Properties（プロパティ）＞System Summary（システムサマリー）ペー
ージで仮想コンソールの状態をプレビューできます。Virtual Console Preview（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、ライセンス付きの機能です。

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。

memo: 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（1MB/秒）が利用可能。

memo: 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 を使用するか、または該当するブラウザで利用可能な必須プラグイン（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です。
Java プラグインを使用して仮想コンソールを起動するときに、Java コンパイルエラーが表示されることがあります。これを解決するには、[Java コントロールパネル] > [一般] > [ネットワーク設定] の順に移動し、[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に設定されている場合、最初は仮想コンソールが起動しないことがあります。これは、ネットワーク接続が遅速で、一時的な認証情報（仮想コンソールが接続に使用）のタイムアウトが 2 分であるためです。ActiveX クライアントブラウザのダウンタイムオフセットと、この時間を許容する場合があります。プラグインが正常にダウンロードされると、仮想コンソールを通常どおり起動できます。
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。

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。
• Configuration（設定）> Virtual Console（仮想コンソール）の順に移動します。仮想コンソールページが表示されます。
 Launch Virtual Console（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。
Virtual Console Viewer（仮想コンソールビューア）に、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、管理ステーションからリモートシステムのマウスやキーボードを制御できます。
アプリケーションを起動した後に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 つは管理下サーバ用で、もう 1 つは管理ステーション用です。カーネルを同期するには、「マウスポインタの同期、p. 281」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 Login（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る場合、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、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。

memo: Internet Explorer は、ローカル、Active Directory、LDAP、スマートカード（SC）、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、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、LDAP ログインをサポートします。
仮想コンソールへのアクセス権限が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初、発行元を確認するプロンプトが表示されます。
   Yes（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や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. Continue（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. 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。

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下することがあります。これは、ネットワーク接続が遅速になっていることや、結果として、仮想コンソールセッションの開始時にビデオフレームが1つ欠落します。すべてのビデオフレームを送信し、その後のビデオ品質を改善するには、次のいずれかの操作を行います。

- システムサマリ ページの仮想コンソールビューアセクションで、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、スライダー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

HTML5 の拡張 OS サポートについてはリリースノートをチェックします。

HTML5 を使用して仮想コンソールにアクセスする場合、クライアントとターゲットのキーボードレイアウト、OS、およびブラウザで表示する言語を使用する必要があります。たとえば、すべてが英語（米国）またはサポートされているいずれかの言語である必要があります。
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。

 Memo: デフォルトでは、仮想コンソールのタイプは HTML5 に設定されています。

 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、コンソールプレゼンテー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 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ています。

HTML5 の仮想コンソールでは、次のメニューにオプションを使用できます。

 - Add Power Control（電源制御の追加）
 - 起動順序
 - チャット
 - キーボード
 - 画面キャプチャ
 - 更新
 - フルスクリーン
 - 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ックをサーバーに渡す）オプションは、HTML5 仮想コンソールではサポートされていません。すべての機能キーには、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
   - 縦横比
   - タッチモード
   - マウスアクセラレーション

 Keyboard（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とき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。

 Keyboard Macros（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）をクリックしてサーバーに選択されたキーの組み合わせを適用します。

 - Ctrl+Alt+Del
 - Ctrl+Alt+F1
 - Ctrl+Alt+F2
 - Ctrl+Alt+F3
 - Ctrl+Alt+F4
 - Ctrl+Alt+F5
 - Ctrl+Alt+F6
 - Ctrl+Alt+F7
 - Ctrl+Alt+F8
 - Ctrl+Alt+F9
 - Ctrl+Alt+F10
 - Ctrl+Alt+F11
 - Ctrl+Alt+F12
 - Alt+Tab
 - Alt+ESC
 - Ctrl+ESC
 - Alt+Space
 - Alt+Enter
 - Alt+Hyphen
 - Alt+F1
 - Alt+F2
 - Alt+F3
 - Alt+F4

仮想コンソールの設定と使用 279
** Aspect Ratio（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。
  ○ 保存
  ○ 維持しない
  適用をクリックしてサーバーで選択された設定を適用します。

** Touch Mode（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で選択された設定を適用します。

** Mouse Acceleration（マウスの加速） - オペレーティングシステムに基づいてマウスの加速を選択します。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。
  ○ 相対座標（Windows、Linux の最新バージョン、Mac OS-X）
  ○ 相対座標、アクセルレーションなし
  ○ 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で選択された設定を適用します。

** Virtual Media（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 ファイルおよび 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。

** 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

** Mac OS バージョン 10.10.2（またはそれ以降）をシステムにインストールすることをお勧めします。

サポート対象ブラウザとバージョンの詳細については、「iDRAC ソースノート」は、www.dell.com/idracmanuals にあります。を参照してください。
マウスポイントの同期

仮想コンソールを介して管理下システムに接続すると、管理下システムのマウスのスムーズな動きを管理ステーションのマウスポイントと同期させ、ビューワのウィンドウに2つのマウスポイントが表示されることがあります。

Red Hat Enterprise Linux または Novell SUSE Linux を使用する場合、仮想コンソールビューワを起動する前に、Linux のマウスマスを設定します。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ワにおけるマウス応答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ワに2つのマウスカーネルが表示される場合、サーバのオペレーティングシステムで相対位置がサポートされていることから示します。これは、Linux オペレーティングシステムまたは Lifecycle Controller でよく起こる現象で、サーバのマウス加速設定が仮想コンソールクライアントのマウス加速度設定と異なる場合に2つのマウスカーネルが表示されます。この問題を解決するには、シングルカーネルに切り替えたり、管理下システムと管理ステーション上でマウスの加速を一致させます。

- シングルカーネルに切り替えるには、ツールメニューから シングルカーネル を選択します。
- マウス設定を変更するには、Tools (ツール) > Session Options (セッションオプション) > Mouse (マウス) の順に移動します。Mouse Acceleration (マウスアクセラレーション) タブで、オペレーティングシステムに応じて Windows (Windows) または Linux (Linux) を選択します。

シングルカーネ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。

memo: 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 分散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 Predictable Pointer Acceleration (予測可能ポインタアクセラレーション) 機能が原因である可能性があります。DRAC 仮想コンソールでマウスを正しく同期するには、この機能を無効にする必要があります。Predictable Pointer Acceleration (予測可能ポインタアクセラレーション) 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/periodicals/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度をオフにした場合、仮想コンソールビューワで、Tools (ツール) > Session Options (セッションオプション) > Mouse (マウス) の順に移動します。Mouse Acceleration (マウスアクセラレーション) タブで None (なし) を選択します。

管理下サーバコンソールへの権限のアクセスについては、ローカルコンソールを無効化し、Virtual Console page (仮想コンソールページ) で Max Sessions (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 のブラウジン用の仮想コンソール経由で渡す

Pass all keystrokes to server (すべてのキーストロークをサーバに渡す) オプションを有効化して、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ワを介して管理ステーションから管理下システムに送信できます。これが無効の場合、すべてのキーの組み合わせは、仮想コンソールセッションを実行している管理ステーションに送られます。すべてのキーストロークをサーバに送るには、仮想コンソールビューワで、Tools (ツール) > Session Options (セッションオプション) > General (一般) タブと移動し、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ブラウジンタイプ (Java または ActiveX)。

Java クライアントの場合、Pass all keystrokes to server (すべてのキーストロークをサーバに渡す) 機能と Single Cursor (単一カーネル) モードを動作させるには、ネイティブブラウジンをロードする必要があります。ネイティブブラウジンがロードされていない場合、Pass all keystrokes to server (すべてのキーストロークをサーバに渡す) と Single Cursor (シングルカーネル) オプションは選択解除されます。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、Pass all keystrokes to server (すべてのキーストロークをサーバに渡す) 機能を動作させるためにはネイティブブラウジンをロードする必要があります。ネイティブブラウジンがロードされていない場合、Pass all keystrokes to server (すべてのキーストロークをサーバに渡す) オプションは選択被解除されています。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。

仮想コンソールの設定と使用 281
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よ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。

全面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。

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
  - 音量をミュートするキー
  - 音量を上げるキー
  - 音量を下げるキー
  - 次のトラックキー
  - 前のトラックキー
  - メディアの再生/一時停止キー
  - メディアの選択キー
  - ブラウザの開始およびホームキー
  - メタリの起動キー
  - 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。これらのキーの一部は、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が有効になると、<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て、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 にエントリーを追加する
  - echo "1" > /proc/sys/kernel/sysrq

仮想コンソールの設定と使用
すべてのキーストローやサバ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で再起動）するキーサイクルの動作は、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 ソール
- SSH/Telnet または外部シリアルコネクタ

オープンソース IPMI ソールの使用
B IOS/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。

```
Ipmtool -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. サーバがオペレーティングシステムで起動すると、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/kern sysrqを使用して有効にします。

4. ブレーキシーケンス -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の直接接続)

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 com2 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、ブレーキ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やサバ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非効的な場合、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。
iDRAC サービスモジュールの使用

iDRAC サービスモジュールは、サーバーへのインストールが推奨され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）。これは、オペレーティングシステムから得られるモニタリング情報によってiDRACを補完します。これは、Web インターフェース、Redfish、RACADM、WSMan など、iDRAC インターフェースで使用可能な追加データを提供することができるiDRACを補完します。ユーザーはiDRAC サービスモジュールでモニタリングする機能を設定することで、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。

この機能はDell Precision PR7910 システムには適用されません。

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でサポートされるオペレーティングシステム
- iDRAC サービスモジュール監視機能
- 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
- RACADM からのiDRAC サービスモジュールの使用

dell.com/supportからiDRAC サービスモジュールをダウンロードし、インストールできます。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管理者権限が必要です。インストールについては、www.dell.com/idracservicemoduleにある「iDRAC Service Module User’s Guide」（iDRAC サービスモジュールユーザーズガイド）を参照してください。

この機能はDell Precision PR7910 システムには適用されません。

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でサポートされるオペレーティングシステム
- iDRAC サービスモジュール監視機能
- 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
- RACADM からのiDRAC サービスモジュールの使用

dell.com/supportからiDRAC サービスモジュールをダウンロードし、インストールできます。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管理者権限が必要です。インストールについては、www.dell.com/idracservicemoduleにある「iDRAC Service Module User’s Guide」（iDRAC サービスモジュールユーザーズガイド）を参照してください。
Microsoft Windows オペレーティングシステムまたは Linux オペレーティングシステムの場合、リモートまたはローカルでサーバにログインします。

2. デバイスリストから「SMINST」という名前でマウントされたボリュームを見つけて、適切なスクリプトを実行します。
   - Windows の場合、コマンドプロンプトを開き、ISM-Win.bat バッチファイルを実行します。
   - Linux の場合、シェルプロンプトを開き、ISM-Lx.sh スクリプトファイルを実行します。

3. インストールが完了したら、iDRAC でサービスモジュールが Installed（インストール済み）となり、インストールの日付が表示されます。

   メモ：インストールがホストオペレーティングシステムで利用できるのは 30 分間です。インストールが 30 分以内に開始しない場合は、サービスモジュールのインストールを始めからやり直す必要があります。

iDRAC Enterprise からの iDRAC サービスモジュールのインストール

1. SupportAssist 登録ウィザードで、Next（次へ）をクリックします。
2. iDRAC Service Module Setup（iDRAC サービスモジュールのセットアップ）ページから、Install Service Module（サービスモジュールのインストール）をクリックします。
3. Launch Virtual Console（仮想コンソールの起動）をクリックしてから、セキュリティ警告ダイアログボックスの Continue（続行）をクリックします。
4. ISM インストールファイルの場所を確認するには、リモートまたはローカルでサーバにログインします。

   メモ：インストールがホストオペレーティングシステムで利用できるのは 30 分間です。インストールが 30 分以内に開始しない場合は、インストールを始めからやり直す必要があります。

5. デバイスリストから「SMINST」という名前でマウントされたボリュームを見つけて、適切なスクリプトを実行します。
   - Windows の場合、コマンドプロンプトを開き、ISM-Win.bat バッチファイルを実行します。
   - Linux の場合、シェルプロンプトを開き、ISM-Lx.sh スクリプトファイルを実行します。

6. 画面に表示される指示に従ってインストールを完了します。
   インストールを完了してから、iDRAC Service Module Setup（iDRAC サービスモジュールのセットアップ）ページで、Install Service Module（サービスモジュールのインストール）ボタンを無効にすると、サービスモジュールのステータスが Running（実行中）として表示されます。

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

iDRAC 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、www.dell.com/idracservice 또는「IDRAC サービスモジュールユーザーのガイド」（IDRAC サービスモジュールユーザーズガイド）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 Collection との統合、この機能は 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利用可能です。
- NVMe PCIe SSD の取り外し準備。詳細については、www.dell.com/support/article/sln310557 を参照してください。

286 iDRAC サービスモジュールの使用
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 v2.3 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 と共有着しています。iDRAC サービスモジュールは、同様の情報（OS 名、OS バージョン、完全修飾ドメイン名 (FQDN) など）を iDRAC に提供します。デフォルトでは、このモニタリング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。

iSM バージョン 2.0 以降では、オペレーティングシステムの情報機能が OS ネットワークインタフェースの監視によって強化されています。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 を使用して表示できます。

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 ログに複製できます。これは、OpenManage Server Administrator によって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、同様の RACADM 内、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様です。

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に記録します。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 からは、iDRAC サービスモジュールインストールをローカルに実行して、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ル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の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、通知されないことがあります。システムはアクティブ化されるようにサーバがリセットされます。ASR は、通常のカウントダウンする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。

再起動、電源の入れ直し、指定時間経過後のサーバの電源オフといった、システムの自動リカバリ操作を実行できます。この機能を有効にするためには、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と、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、無効になります。

Windows Management Instrumentation プロバイダ

WMI は Windows ドライバモデルに対する拡張機能のセットであり、オペレーティングシステムインタフェースを提供し、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、サーバーウェア、オペレーティングシステム、アプリケーションを管理するための Distributed Management Task Force (DMTF) 基づく Microsoft が実装した Web-Based Enterprise Management (WBEM) 規格および Common Information Model (CIM) 規格です。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することができます。iDRAC は、iDRAC サービスモジュールを通じて WMI クラスを公開し、サーバの正常性情報を提供します。デフォルトでは、WMI 情報機能は有効になっています。iDRAC サービスモジュールは、WMI を通じて WSMAN 監視クラスを iDRAC に開示します。これらのクラスは、root/cimv2/dcim 名前空間に開示されます。

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、WMI 情報機能によって iDRAC サービスモジュールに提供される機能を DCIM_account クラスを使用して説明します。サポート対象のクラスおよびプロファイルの詳細については、https://www.dell.com/support にある、WSMan プロファイルに関するドキュメントを参照してください。

### 表 59. DCIM_account クラスの例

<table>
<thead>
<tr>
<th>CIM インタフェース</th>
<th>WinRM</th>
<th>WMIC</th>
<th>PowerShell</th>
</tr>
</thead>
<tbody>
<tr>
<td>クラスのインスタンスを列挙します。</td>
<td>winrme wmi/root/cimv2/dcim/ dcim_account</td>
<td>wmic /namespace:\root\cimv2\dcim PATH dcim_account</td>
<td>Get-WmiObject - dcim_account - namespace root/ cimv2/dcim</td>
</tr>
<tr>
<td>特定のクラスのインスタンスを取得します。</td>
<td>winrm q wmi/root/cimv2/dcim/ DCIM_Account? CreationClassName=DCIM_Account+Name=IDRAC.Embedded.1#Users.2+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc</td>
<td>wmic /namespace:\root\cimv2\dcim PATH dcim_account where Name=&quot;IDRAC.Embedded.1#Users.16&quot;</td>
<td>Get-WmiObject - Namespase root\cimv2\dcim -Class dcim_account -filter &quot;Name='IDRAC.Embedded.1#Users.16'&quot;</td>
</tr>
<tr>
<td>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。</td>
<td>winrme wmi/root/cimv2/dcim/* - dialect:association -filter: {object=DCIM_Account ? CreationClassName=DCIM_Account+Name=IDRAC.Embedded.1#Users.2+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc }</td>
<td>wmic /namespace:\root\cimv2\dcim PATH dcim_account where Name='IDRAC.Embedded.1#Users.2' ASSOC</td>
<td>Get-Wmiobject - Query &quot;ASSOCIATORS OF {DCIM_Account.CreationClassName='DCIM_Account',Name='IDRAC.Embedded.1#Users.2',SystemCreationClassName='DCIM_SPComputerSystem',SystemName='systemmc'}&quot; - namespace root/ cimv2/dcim</td>
</tr>
<tr>
<td>インスタンスの参照を取得します。</td>
<td>winrme wmi/root/cimv2/dcim/* - dialect:association -associations -filter: {object=DCIM_Account ? CreationClassName=DCIM_Account+Name=IDRAC.Embedded.1#Users.2+SystemCreationClassName=DCIM_SPComputerSystem+SystemName=systemmc }</td>
<td>wmic /namespace:\root\cimv2\dcim PATH dcim_account where Name='IDRAC.Embedded.1#Users.2' ASSOC</td>
<td>適用なし</td>
</tr>
</tbody>
</table>
iDRAC のリモートハードリセット

iDRAC を使用すると、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、サポート対象サーバを監視できます。iDRAC は、さまざまな理由で応答しなくなることがあります。そのような場合には、サーバの電源を切って 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、サーバの電源を切ってから再投入するか、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と、iDRAC が応答不能になったときはいつでも、AC パワーサイクルを行わずに iDRAC をリセットすることができる。iDRAC CPU をリセットするには、サーバの電源を切ってから再投入するか、AC パワーサイクルを実行する必要があります。

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:
    ```bash
to 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:
    ```bash
```
  - 強制的および非強制的に Windows PowerShell スクリプトを使用する:
    ```bash
Invoke-iDRACHardReset
Invoke-iDRACHardReset -force
```
  - プログラムメニューのショートカットを使用する:
    簡素化のために、iSM は Windows 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。

- 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。
    ```bash
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。
    ```bash
```
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 オペレーティングシステムの制限により、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。

<table>
<thead>
<tr>
<th>結果</th>
<th>説明</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>成功</td>
</tr>
<tr>
<td>1</td>
<td>iDRAC リセット対応ではない BIOS バージョン</td>
</tr>
<tr>
<td>2</td>
<td>非対応プラットフォーム</td>
</tr>
<tr>
<td>3</td>
<td>アクセス拒否</td>
</tr>
<tr>
<td>4</td>
<td>iDRAC リセット失敗</td>
</tr>
</tbody>
</table>

表 60. エラー処理

### 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から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、この機能によって、OS ログに複製されたすべての Lifecycle ログが SNMP トラップに変換されます。

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。

デフォルトでこの機能は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できますが、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。両方を使用する代わりに、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ています。

### 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使用します。このコマンドは、SSH または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せん。

```
./Enable-iDRACSNMPTrap.sh 1/agentx -force
```

-force を指定しない場合は、net-SNMP が設定されていることを確認して、snmpd サービスを再起動します。
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、トラップの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。

```
```

**メモ:** トラブルに対する 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、https://www.dell.com/support にあるテクニカルホワイトペーが「帯域内 SNMP アラート」を参照してください。

**ホスト OS を介した iDRAC アクセス**

この機能を使用することで、iDRAC の 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、WSMan、RedFish インタフェースを介して、ハードウェアパラメーターを設定およびモニタできます。iDRAC サーバが設定されていない場合はデフォルトの iDRAC 資格情報を使用でき、iDRAC サーバが以前に設定済みである場合は同じ iDRAC 資格情報を引き続き使用できます。

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 をを使ったインストール**

この機能は、ウェブパックを使用してインストールできます。この機能は、標準的な ISM インストール済み環境で無効に設定されています。有効な場合、デフォルトのリスニングポート番号は 1266 です。このポート番号を 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 はインパ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。この機能が有効な場合は、ファイアウォールルールが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ンス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。この機能が有効の場合は、リスニングポート番号が表示されます。

**メモ:** この機能を有効にするには、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いることを確認してください。
iDRAC Web インターフェイ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 を使用します。入力値の詳細を次に示します。

- <host-name>：iSM がインストールされ、OS 機能を介して iDRAC がアクセスできるように設定されたサーバーの完全ホスト名。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。これは接続ポート番号と呼ばれ、リスニング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。iDRAC ウェブインターフェース、WSMan、RACADM インタフェースから、ポート番号を変更できます。

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できます。利用できるオプションは次のとおりです。

- 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。ポート番号を指定しない場合は、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、残りのパラメータは無視できます。この機能には、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。新しいポート番号設定によって既存の OS2iDRAC インバウンドファイアウォールルールが上書きされ、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 アドレスの範囲を指定します。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) 形式です。たとえば、10.94.111.21/24 です。この範囲外の IP アドレスは、iDRAC へのアクセスが制限されます。

iDRAC サービスマジュールの使用

iDRAC サービスマジュールのインストール中に監視機能を有効にした場合、インストールが完了した後に iDRAC サービスマジュールが OpenManage Server Administrator の存在を検出すると、iDRAC サービスマ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、iDRAC サービスマジュールは、OS および iDRAC へのログイン後に、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 インター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の 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. [iDRAC 設定] > [概要] > [iDRAC サービスモジュール] > [サービス ジュールの設定] 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

   **メモ:** サーバーに複数のオペレーティングシステムがあり、iDRAC サービスモジュールがすべてのオペレーティングシステムにインストールされている場合、iDRAC が接続するのは、すべてのオペレーティングシステムのうちで最新インスタンスの ISM だけです。他のオペレーティングシステムにあるより古い ISM インスタンスについては、すべて「TLS エラー」と表示されます。ISM と接続する iDRAC が、すでに ISM がインストール済みである別のオペレーティングシステムにある場合は、そのオペレーティングシステムにある ISM をアンインストールしてから再インストールするようにします。

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。
   - [OS ログでの Lifecycle ログの複製] - Lifecycle Controller のログをオペレーティングシステムのログに変換ようにします。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。
   - [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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。参照してください。
サーバー管理用 USB ポートの使用

14 世代のサーバでは、専用のマイクロ USB ポートを使用して iDRAC を設定できます。マイクロ USB ポートを使用して、次の機能を実行することができます。

- USB ネットワークインタフェースを使用してシステムに接続し、iDRAC ウェブインタフェースや RACADM などのシステム管理ツールにアクセスします。
- USB ドライバに保存されている SCP ファイルを使用して、サーバを設定します。

メモ: USB ポートの管理、または USB ドライバ上のサーバ設定ファイル (SCP) のインポートによるサーバ設定を行うには、システム制御権限が必要です。USB ポートの管理に関する詳細については、ホワイトペーパー『13 世代以降のサーバでの USB ポートの割り当てと USB ドライブの管理』をお読みください。

メモ: USB デバイスが挿入されると、アラート/レポートが生成されます。この機能は、Intel ベースのサーバーでのみ使用できます。

管理 USB 設定を構成するには、iDRAC 設定 > 設定 > 管理 USB の設定と移動します。次のオプションを使用できます。

- USB 管理ポート—USB ドライバが接続されている場合に SCP ファイルをインポートする、またはマイクロ USB ポートを使用して iDRAC にアクセスする場合に、ポートを有効にするには、有効を選択します。
- iDRAC 管理対象: USB SCP—USB ドライバに保存されている SCP をインポートして、システムを設定するには、次のオプションから選択します。
  - 無効: SCP インポートを無効化
  - サーバにデフォルト資格情報があるときにのみ有効—このオプションが選択されている場合は、次のデフォルトのパスワードが変更されていない場合にのみ、SCP をインポートできます。
    - BIOS
    - iDRAC ウェブインタフェース
  - 壓縮された設定ファイルにのみ有効—このオプションを選択すると、ファイルが圧縮形式である場合にのみ、SCP ファイルをインポートできます。
    - このオプションを選択すると、圧縮されたファイルをパスワードで保護することができます。Zip ファイルのパスワードオプションを使用して、ファイルを保護するパスワードを入力できます。

メモ: このオプションを選択すると、圧縮されたファイルをパスワードで保護することができます。Zip ファイルのパスワードオプションを使用して、ファイルを保護するパスワードを入力できます。

メモ: 有効—実行時にチェックを実行せずに SCP ファイルをインポートするには、このオプションを選択します。

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
- USB デバイスのサーバ設定プロファイルを使用した iDRAC の設定

直接 USB 接続を介した iDRAC インタフェースへのアクセス

IDRAC ダイレクト機能を使用すると、ノートパソコンを IDRAC USB ポートに直接接続することができます。この機能を使用すると、ウェブインタフェース、RACADM、WSMan などの IDRAC インタフェースと直接やりとりして、高度なサーバ管理やサービスを実現できます。

サポート対象プラウザおよびオペレーティングシステムのリストについては、『IDRAC ソリューション ノート』は、www.dell.com/idracmanuals にあります。を参照してください。

メモ: Windows オペレーティングシステムを使用している場合は、この機能を使用するために RNDIS ドライバをインストールする必要があります。

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」、p. 295を参照してください。
3. ノートパソコンがIPアドレス169.254.0.4を取得するのを待ちます。IPアドレスを取得するまでは数秒かかります。iDRACがIPアドレス169.254.0.3を取得します。
4. ベブリンクタフェース、RACADM、Redfish、WSMan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。
5. iDRACがUSBポートを使用している場合、LEDが点滅してアクティビティを示します。点滅の頻度は1秒あたり4回です。
6. 目的のアクションを完了したら、システムからUSBケーブルを外します。

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 USB管理ポートを使用すると、iDRACをサーバーレベルで設定できます。iDRACでUSB管理ポートを設定し、サーバ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にサーバ設定をインポートします。

USB管理ポートの設定
システムBIOSを使用して、iDRACダイレクトUSBポートを有効または無効することができます。システムBIOS>内蔵デバイスの順に移動します。iDRACダイレクトUSBポートを有効にするにはオフを、無効にするにはオフを選択します。
iDRACでUSB管理ポートを設定するには、サーバ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、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た。
- デバイスはiDRACまたはOSから除外されました。

USB管理ポートを設定するには、次の手順を実行します。
1. iDRACウェブインターフェースで、iDRAC設定>設定>管理USBの設定と移動します。
2. USB管理ポートは有効に設定されています。
3. iDRAC管理対象：USB SCP設定 ドロップダウンメニューでオプションを選択し、USBドライバに保存されているサーバ設定プロファイルファイルをインポートしてサーバを設定します。
- 無効
- サーバにデフォルト資格情報があるときにのみ有効
- 压縮された設定ファイルにのみ有効
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 と control 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（SCP）は、USB デバイスのルートディレクトリの下の System_Configuration_XML サブディレクトリにあるものです。このファイルには、サーバーのすべての属性と値のペアが含まれています。これには、iDRAC、PERC、RAID、および BIOS の属性が含まれます。このファイルを編集して、サーバー上的任意の属性を構成できます。ファイル名は、<servicetag>-config.xml、<servicetag>-config.json、<modelnumber>-config.xml、または config.json です。

コントロールファイルには、インポート操作を制御するためのパラメーターが含まれ、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。コントロールファイルには、次の 3 つのパラメーターが含まれています。

- 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
ファイルの例を次に示します。

```xml
<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: SCP のインポート中に SCP ファイルの USB 管理設定を変更すると、ジョブが失敗するか、ジョブがエラーで終了します。エラーを避けるため、SCP の属性をコメントアウトできます。

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。
   メモ: XML ファイルのファイル名とファイルタイプでは、大文字と小文字が区別されます。両方が小文字になっていることを確認します。

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。これは、次の順序で検出されます。
   - <servicetag>-config.xml / <servicetag>-config.json
   - <modelnum>-config.xml / <modelnum>-config.json
   - config.xml / config.json

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. ステージングが必要な設定があり、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、設定を構成するには、サーバーを再起動する必要があります。そうでない場合は、サーバーが再起動され、設定が適用されます。サーバーの電源がすでにオフにになっている場合のみ、[再起動なし] オプション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 はジョブが完了したことを示します。再起動が必要な場合、LCD にジョブステータスが [再起動の待機中] と表示されます。

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 は、USB ポートを使用して実行されているサーバ構成プロファイルの動作の状態を示します。LED は、一部のシステムで利用できない場合があります。
- 緑色の点灯 – USB デバイスからサーバ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。
- オレンジの点滅 – ジョブが失敗したか完了したがエラーが発生した。
- 緑色の点灯 – ジョブが正常に完了した。

メモ: PowerEdge R840 および R940XA では、LCD がある場合、USB ポートを使用してインポート操作が進行中の場合、USB LED が点滅しません。LCD を使用して操作のステータスを確認します。

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。
Quick Sync 2 の使用

Android または iOS モバイル デバイスで動作している Dell OpenManage Mobile を使用すると、直接または OpenManage Essentials や OpenManage Enterprise（OME）コンソールを介してサーバーに簡単にアクセスできます。これにより、サーバーの詳細とインベントリの確認、LC およびシステムイベントログの表示、OME コンソールからのモバイル デバイスへの自動通知の送信、IP アドレスの割り当て、iDRAC パスワードの変更、主要な BIOS 属性の設定、修正アクションの実行を必要に応じて行えます。また、サーバーの電源を入れ直したり、システムコンソールにアクセスしたり、iDRAC GUI にアクセスしたりすることもできます。

Apple App Store または Google Play ストアから OMM を無料でダウンロードできます。iDRAC Quick Sync 2 インターフェイ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（Android 5.0 以降と iOS 9.0 以降のモバイル デバイスに対応）。

メモ: このセクションは、左側のラック イヤーに Quick Sync 2 モジュールが搭載されたサーバーにのみ表示されます。

メモ: この機能は現在、Android オペレーティング システムおよび Apple iOS 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 PowerEdge サーバーのすべての第 14 世代で使用可能です。Quick Sync 2 の左コントロール パネル（左側のラック イヤーに組み込まれている）と Bluetooth Low Energy (およびオプションの Wi-Fi) 対応のモバイル デバイスが必要です。つまり、これらはハードウェア アップセールであり、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 2 の設定手順:

1. メモ: MX プラットフォームには適用されません。

Quick Sync を設定したら、左のコントロール パネルにある Quick Sync 2 ボタンをアクティブにします。Quick Sync 2 のライトがオンになっていることを確認します。モバイル デバイス（Android 5.0 以降または iOS 9.0 以降、OMM 2.0 以降）を使用して、Quick Sync 2 の情報にアクセスします。

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 EMC OpenManage Mobile ユーザーズ ガイド」は、www.dell.com/openmanagemanuals にあります。を参照してください。

トピック:
- iDRAC Quick Sync 2 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 2 の設定

iDRAC Web インターフェイス、RACADM、WSMan、および iDRAC HII を使用して、iDRAC Quick Sync 2 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] — 読み取り/書き込み、読み取り専用、および無効に設定します。読み取り/書き込みは、デフォルトのオプションです。
- [タイムアウト] — 有効または無効に設定します。有効がデフォルト オプションです。
- [タイムアウト制限] — Quick Sync 2 モードを無効にするまでの時間を示します。デフォルトでは秒が選択されています。デフォルト値は 120 秒で、範囲は 120 ～ 3600 秒です。

1. 有効にすると、Quick Sync 2 モードをオフにするまでの経過時間を指定できます。オフにするには、アクティブ化ボタンを使用して再度押します。
2. 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値を許可しません。
ウェブインタフェースを使用した iDRAC Quick Sync 2 の設定

iDRAC Quick Sync 2 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、Configuration > System Settings > Hardware Settings > iDRAC Quick Sync の順に移動します。

2. iDRAC Quick Sync セクションで、次のいずれかを選択し、Android または iOS 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. タイムアウト制限を指定します。
   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 2 の設定

iDRAC Quick Sync 2 機能を設定するには、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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。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 2 の設定

iDRAC Quick Sync 2 を設定するには、次の手順を実行します。

1. iDRAC GUI で Configuration > System Settings > Hardware Settings > iDRAC Quick Sync の順に移動します。

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 (120 ~ 3,600 秒の範囲)。
   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 情報を表示する場合の手順については、「Dell EMC OpenManage Mobile ユーザーズガイド」は、www.dell.com/openmanagemanuals にあります。を参照してください。
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
- ドライバのアップデート
- 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用のライセンスが必要な機能です。ブレードサーバ用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。
- フロッピー、USB フラッシュドライブ、イメージ、キーのいずれか1つと光学ドライブ1台を管理システムの管理ステーションに接続できます。サポート対象フロッピードライブとは、フロッピーイメージまたは使用可能な状態のフロッピードライブ1台です。サポート対象光学ドライブとは、使用可能な状態の光学式ドライブまたは ISO イメージファイル1つです。

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。
- 仮想メディアは、仮想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 ベースの管理システムでは、仮想メディアドライブを接続してドライプレターを設定した場合、自動マウントされます。
- ブロードメッシュシステムでは、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。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。
- 仮想メディアは、管理システムで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れ付けられません）。2つの管理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 128Kbps 以上のネットワーク帯域幅を必要とします。
- LOM または NIC フィルターハードウェアが発生した場合は、仮想メディアセッションを切断できません。

仮想メディアのインストール後、ドライバが Windows ホスト OS に表示されないことがあります。Windows のデバイスマネージャーにある、不明な大容量記憶装置をすべてチェックします。不明なデバイスを右クリックし、ドライバをアップデートするかまたはドライバのアンインストールを選択します。vMedia が切断されて再接続された後、Windows によってデバイスが認識されます。

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
- 仮想メディアの設定
- 仮想メディアへのアクセス
- BIOS を介した起動順序の設定
- 仮想メディアの一回限りの起動の有効化
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。

<table>
<thead>
<tr>
<th>ドライブ</th>
<th>対応メディア</th>
</tr>
</thead>
<tbody>
<tr>
<td>仮想光学ドライブ</td>
<td>• レガシー1.44 フロッピードライブ(1.44フロッピーディスク)</td>
</tr>
<tr>
<td></td>
<td>• CD-ROM</td>
</tr>
<tr>
<td></td>
<td>• DVD</td>
</tr>
<tr>
<td></td>
<td>• CD-RW</td>
</tr>
<tr>
<td></td>
<td>• コンピューションドライブ(CD-ROM メディア)</td>
</tr>
<tr>
<td>仮想フロッピードライブ</td>
<td>• ISO9660 フォーマットの CD-ROM/DVD イメージファイル</td>
</tr>
<tr>
<td></td>
<td>• ISO9660 フォーマットのフロッピーアイメージファイル</td>
</tr>
<tr>
<td>USB フラッシュドライブ</td>
<td>• CD-ROM メディアのある USB CD-ROM ドライブ</td>
</tr>
<tr>
<td></td>
<td>• ISO9660 フォーマットの USB キーイメージ</td>
</tr>
</tbody>
</table>

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。

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iDRACをリセットしないでください。リセットすると、データ損失など、望ましくない結果となる場合があります。

1. iDRAC ウェブインタフェースで、Configuration (設定) > Virtual Media (仮想メディア) > Attached Media (連結されたメディア) と移動します。
2. 必要なオプションを指定します。詳細については、「iDRAC 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。
詳細については、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。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。この操作を行うには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、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. Virtual Media (仮想メディア) セクションで、要件に応じて Detach (連結解除), Attach (連結), または Auto attach (自動連結) 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。
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 62. 連結されたメディアの状態とシステムの応答**

<table>
<thead>
<tr>
<th>連結されたメディアの状態</th>
<th>システム応答</th>
</tr>
</thead>
<tbody>
<tr>
<td>分離</td>
<td>イメージをシステムにマップできません。</td>
</tr>
<tr>
<td>連結</td>
<td>メディアは、クライアントビューが開じられている場合であってもマップされます。</td>
</tr>
<tr>
<td>自動連結</td>
<td>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。</td>
</tr>
</tbody>
</table>

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 Explorerで、Organize（整理）メニューからFolder and search options（フォルダと検索のオプション）をクリックします。View（表示）タブでHide empty drives in the Computer folder（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、しないに関わらず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、次のようなエラーメッセージが表示されます。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。

RFS接続が非アクティブである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。

仮想コンソールを使用した仮想メディアの起動

仮想コンソールで仮想メディアを起動する前に、次のこと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、Configuration（設定）> Virtual Console（仮想コンソール）の順に移動します。
   仮想コンソール ページが表示されます。

2. Launch Virtual Console（仮想コンソールの起動）をクリックします。
   **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. Virtual Media（仮想メディア）> Connect Virtual Media（仮想メディアの接続）の順にクリックします。
   仮想メディアリソースが確認され、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。

仮想メディアを使用しない仮想メディアの起動

仮想メディアが無効になっている場合は、仮想メディアを起動する前に、次のことを確認してください。

- 仮想メディアが連絡状態である。これを行うには、[連結モード]フィールドのドロップダウンの[連結]を選択します。
空のドライブを表示するようにシステムが設定されている。これを行うには、Windows エクスプローラーで「フォルダー 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ーに表示しない」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にアクセスするには、次の手順を実行します。

1. iDRAC Web インターフェイスで、「設定」 > 「仮想メディア」の順に移動します。
2. 「仮想メディアの接続」をクリックします。

仮想メディア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。

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た Windows オペレーティングシステムを実行しているシステムでは、仮想メディアが正しく機能しない場合があります。この問題を解決するには、Microsoft オペレーティングシステムのマニュアルを参照するか、システム管理者にお問い合わせください。

仮想メディアイメージの追加

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. Virtual Media（仮想メディア）> Create Image...（イメージの作成...）をクリックします。
2. Source Folder（ソースフォルダ）フィールドで Browse（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ァイルまたはディレクトリを指定します。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、Browse（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、Virtual Media（仮想メディア）メニューにあるこのフォルダに対するエントリは作動しません。このため、.img ファイルを使用して削除されると、削除されると削除されると削除されると削除されると削除されると削除されると削除されると削除されると削除されます。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 Remove Image（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 Tools（ツール）> Stats（統計）をクリックします。Stats（統計）ウィンドウの Virtual Media（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、「Virtual Media is not connected（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、Virtual Media（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表示されます。
ドライバへのアクセス

Dell EMC PowerEdge サーバーには、システムフラッシュメモリーに内蔵された対応オペレーティングシステムドライバがすべて搭載されています。iDRACを使用すると、ドライバをマウントまたはマウント解除して、お使いのサーバーにオペレーティングシステムを簡単に導入できます。

ドライバをマウントするには、次の手順を実行します。
1. iDRAC Web インターフェイスで、[設定] > [仮想メディア]の順に移動します。
2. [ドライバーのマウント]をクリックします。
3. ポップアップウィンドウから OS を選択し、[ドライバーのマウント]をクリックします。

メモ: デフォルトでは、公開時間は18時間です。

マウントの完了後にドライバをマウント解除するには、次の手順を実行します。
1. [設定] > [仮想メディア]の順に移動します。
2. [ドライバーのマウント解除]をクリックします。
3. ポップアップウィンドウの[OK]をクリックします。

メモ: ドライバーパックがシステムで使用できない場合は、[ドライバーのマウント]オプションが表示されないことがあります。
https://www.dell.com/supportから最新のドライバーパックをダウンロードしてインストールしてください。

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. 假想コンソールビューアで、ツール > 統計をクリックします。
2. 統計ウィンドウが表示されます。
3. 假想メディア下で、USBのリセットをクリックします。
4. 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。
5. Yes (是)をクリックします。
6. 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。
1. 假想メディアウォンドウで、仮想メディアを選択し、CD/DVDのマッピングをクリックします。
2. ドライブのマッピングウィンドウが表示されます。
3. 各デバイスをマッピングします。

メモ: ActiveXまたはJavaベースの仮想メディアを使用している場合は、オペレーティングシステムのDVDまたはUSBフラッシュドライブ(管理ステーションに接続されている)をマッピングするには、管理者権限が必要です。ドライバをマップするには、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. 假想メディアセッションの接続には、仮想メディアメニューから仮想メディアの接続をクリックします。
2. 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にメディア項目が表示されます。
3. メディアアイテムは、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のマップ

メモ: 連結されたメディアページでフロッピーディスクの仮想メディアオプションが有効になっていますと、リストにフロッピーディスクを選択し、メディア項目が表示されます。
4. 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にメディア項目が表示されます。
5. メディアアイテムは、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のマップ
   - ISOファイルを仮想メディアにマップするオプション

メモ: HTML5ベースの仮想コンソールを使用してUSBベースのドライバ、CDまたはDVDなどの物理メディアをマップすることができません。
メモ: RDP セッションを介した仮想コンソール/仮想メディアを使用したマップの USB キーを仮想メディアディスクとして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（マッピングされている）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、Map Removable Disk（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ドロップダウンメニューから選択できません。Browse（参照）をクリックして、イメージを指定してください。

4. 書き込み可能デバイスを読み取り専用としてマップするには、読み取り専用 を選択します。
CD/DVD デバイスにはこのオプションがデフォルトで有効化されており、無効化できません。
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/イメージのマップ後、デバイス名を示すためにその Virtual Media（仮想メディア）メニュー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 foo.iso が CD/DVD にマップされたと命名されます。そのメニューイテムのチェックマークが、それがマップされていることを示します。

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 Client（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場合があります。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。この操作を行うには、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> を押して、System Setup（セットアップユーティリティ）起動します。
2. SATA settings（SATA の設定）に移動します。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 Client（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。

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. Yes（はい）をクリックします。
そのメニューイテムにチェックマークが表示されなくなり、それがホストサーバーにマップされていないことを示します。
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 に連携されている 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。

メモ: Linux OS で仮想 DVD ドライブをマッピング解除するには、ドライブをマウント解除して取り出します。
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. System BIOS Settings (システム BIOS 設定) > Boot Settings (起動設定) > BIOS Boot Settings (BIOS 起動設定) > Boot Sequence (起動順序) と移動します。
   ポップアップウィンドウに、仮想光学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、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、次の準備をしてください。

・ 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 フラッシュメディア）をブートプー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。
vFlash SD カードの管理

vFlash SD カードは、工場出荷時に注文して取り付けることが可能な Secure Digital (SD) カードです。最大容量 16 GB のカードを利用できます。カードの挿入後は、パーティションの作成と管理をするために vFlash 機能を有効にする必要があります。vFlash はライセンスが必要な機能です。

メモ：vFlash は、AMD プラットフォーム サーバーでサポートされています。

vFlash SD カードの設定

vFlash を設定する前に、vFlash SD カードがシステムに挿入されていることを確認してください。システムにカードを取り付けたり取り外したりする方法の詳細については、「設置およびサービス マニュアル」は、www.dell.com/poweredgemanuals にあります。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。

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 Configuration (設定) > System Settings (システム設定) > Hardware Settings (ハードウェア設定) > vFlash の順に移動します。Card Properties (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、次のオプジェクトで `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、「IDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。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 Settings Utility (IDRAC 設定ユーティリティ) で、Media and USB Port Settings (メディアおよび USB ポートの設定) に移動します。Media and USB Port Settings (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、Configuration (設定) > System Settings (システム設定) > Hardware Settings (ハードウェア設定) > vFlash の順に移動します。
   SD カードプロパティ ページが表示されます。
2. vFLASH Enabled (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 Settings . Media and USB Port Settings (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カードが書き込み禁止の場合は、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、Configuration (設定) > System Settings (システム設定) > Hardware Settings (ハードウェア設定) > vFlashの順に移動します。
   SD Card Properties (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、「iDRAC RACADM CLIガイド」は、www.dell.com/idracmanualsにあります。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vFlashSD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 Settings . Media and USB Port Settings (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. Yes (はい) をクリックします。初期化が開始されます。
4. Back (戻る) をクリックして、同じiDRAC Settings . Media and USB Port Settings (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`が入力されます。
   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、racadm vflashpartition status -a コマンドを使用します。
4. 特定のパーティションの最新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: 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、または内容のコピーには Access Virtual Media (仮想メディアへのアクセス) 機能が必要です。

- 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: WSMAN、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 (vFlash は現在別のプロセスで使用中です。しばらくしてから再試行してください。)"

フォーマットや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ます。フロッピーや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、Configuration (設定) > Systems Settings (システム設定) > Hardware Settings (ハードウェア設定) > vFlash > Create Empty Partition (空のパーティションの作成) の順に移動します。
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、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。
パーソナル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。

共有がユーザー名/パスワードを使用して設定されていない場合は、次のようにパラメータを指定する必要があります。

```
-u anonymous -p anonymous
```

**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、フロッピーや、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。作成されるパーティションのサイズは、イメージファイルのサイズと等しくなります。

イメージファイルからパーティションを作成する前に、次のこと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: アップロードされるイメージとエミュレーションタイプが適合する。iDRAC で不適切なイメージタイプでデバイスがエミュレートされる可能性があります。たとえば、パーティションが ISO イメージを使用して作成され、エミュレーションタイプがハードディスクと指定された場合、このイメージからは BIOS を起動できません。
- 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。
- サポートされるパーティションの最大サイズが4 GB の場合、イメージサイズは4 GB 以下となります。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、イメージファイルサイズは、2 GB 未満となります。

メモ: vFlash パーティションは FAT 32 ファイルシステム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。

メモ: OS のフルインストールは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、Configuration (設定) > System Settings (システム設定) > Hardware Settings (ハードウェア設定) > vFlash > Create From Image (イメージからの作成) の順に移動します。
   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、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。フロッピーや、またはハードディスクエミュレーションタイプには、読み取り/書き込みパーティションが作成されます。次の場合には、エラーメッセージが表示されます。
- カードが書き込み禁止になっている。
ラベル名が既存のパーティションのラベルに一致する。
• イメージファイルのサイズが4GBを超えるか、カード上の空き容量を超えている。
• イメージファイルが存在しないか、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。

```bash
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、作成された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の拡張子の大文字と小文字は区別されます。ファイル名の拡張子が大文字の場合（例えば、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。

共有がユーザー名/パスワードを使用して設定されていない場合は、次のようにパラメーターを指定する必要があります。

```bash
-u anonymous -p anonymous
```

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パーティションは、ハードディスクまたはフロッピーのタイプに限られ、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は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、Configuration（設定）> System Settings（システム設定）> Hardware Settings（ハードウェア設定）> vFlash > Format（フォーマット）の順に移動します。
   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Configuration（設定）> System Settings（システム設定）> Hardware Settings（ハードウェア設定）> vFlash > Manage（管理）の場合に移動します。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、ステータス処理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. iDRACウェブインタフェースで、Configuration（設定）> System Settings（システム設定）> Hardware Settings（ハードウェア設定）> vFlash > Manage（管理）の順に移動します。
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、次のとおりパーティションの読み取り/書き込み状態を変更します。

  o 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
パーセッションの連結または分離
1つ、または複数のパーセッションを連結すると、これらのパーセッ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。複数のパーセッ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。

パーセッ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。

パーセッ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。

パーセッションを連結または分離する前に、次の操作を行うこと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セッションの連結または分離
パーセッ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. iDRACウェブインタフェースで、Configuration（設定）＞System Settings（システム設定）＞Hardware Settings（ハードウェア設定）＞vFlash＞Manage（管理）の順に進動します。
   パーセッ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。
   - パーセッ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セッションを連結します。
   - パーセッ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セッションを分離します。

RACADMを使用したパーセッションの連結または分離
パーセッ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。
   - パーセッションを連結：
     racadm set iDRAC.vflashpartition.<index>.AttachState 1
   - パーセッションを分離：
     racadm set iDRAC.vflashpartition.<index>.AttachState 0

連接されたパーセッ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接されたパーセッションを制御し、ドライブ文字を割り当てます。
- 読み取り専用パーセッションは、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接されたパーセッ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。サポートしていない場合は、オペレーティングシステムからパーセッ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固有のパーセッションタイプEXT2を読み取ることはできません。また、Linux環境では、Windows固有のパーセッションタイプ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る。
- 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. iDRAC ウェブインタフェースで、Configuration（設定）＞System Settings（システム設定）＞Hardware Settings（ハードウェア設定）＞vFlash＞Manage（管理）の順に移動します。
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、パーティションが永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、Configuration（設定）＞System Settings（システム設定）＞Hardware Settings（ハードウェア設定）＞vFlash＞Download（ダウンロード）の順に移動します。
2. パーティションのダウンロード ページが表示されます。
3. 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を除く）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。
4. 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。
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、フロッピーやおよびハードディスクタイプのパーティションには .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、「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 p. 317」を参照してください。

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、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。を参照してください。

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 回限りの起動では、1 度だけパーティションからデバイスを起動します。デバイスの起動順序が永続的に一番目になるわけではないです。
Server Management Command Line Protocol (SMCLP) 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、管理下の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ジョン 1.0 基づいています。

メモ: プロファイル、拡張、MOF に関する情報は https://www.dell.com/support から、DMTF に関する全体情報は dmtf.org/standards/profiles/ から入手できます。

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
- SMCLP コマンドの実行
- iDRAC SMCLP 構文
- MAP アドレス領域のナビゲーション
- show 動詞の使用
- 使用例

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表示
- 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 ブレードサーバは -s を使用します。
- yx1x ラックおよびタワーサーバは、admin-> を使用します。
- yx2x ブレード、ラック、およびタワーサーバは、admin-> を使用します。

y は、M（ブレードサーバの場合）、R（ラックサーバの場合）、および T（タワーサーバの場合）など英数字であり、x は数字です。これは、Dell PowerEdge サーバの世代を示します。
メモ：-sを使用したスクリプトでは、これらを wy1x システムに使用できますが、wy2x システム以降は、ブレード、ラック、およびタワーハードウェアに admin->を使用した1つのスクリプトを使用できます。

### iDRAC SMCLP 構文

iDRAC SMCLP には、動詞とターゲットの概念を使用して、CLI 経由でシステムを管理する機能が備わっています。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 63. SMCLP 動詞

<table>
<thead>
<tr>
<th>動詞</th>
<th>定義</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd</td>
<td>シェルを使用して MAP を移動します</td>
</tr>
<tr>
<td>set</td>
<td>プロパティを特定の値に設定します</td>
</tr>
<tr>
<td>ヘルプ</td>
<td>特定のターゲットのヘルプを表示します</td>
</tr>
<tr>
<td>reset</td>
<td>ターゲットをリセットします</td>
</tr>
<tr>
<td>show</td>
<td>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</td>
</tr>
<tr>
<td>start</td>
<td>ターゲットをオンにします</td>
</tr>
<tr>
<td>stop</td>
<td>ターゲットをシャットダウンします</td>
</tr>
<tr>
<td>exit</td>
<td>SMCLP シェルセッションを終了します</td>
</tr>
<tr>
<td>バージョン</td>
<td>ターゲットのバージョン属性を表示します</td>
</tr>
<tr>
<td>load</td>
<td>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</td>
</tr>
</tbody>
</table>

次の表は、ターゲットのリストが示されています。

#### 表 64. SMCLP ターゲット

<table>
<thead>
<tr>
<th>ターゲット</th>
<th>定義</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin1</td>
<td>管理ドメイン</td>
</tr>
<tr>
<td>admin1/profiles1</td>
<td>iDRAC 内の登録済みプロファイル</td>
</tr>
<tr>
<td>admin1/hdwr1</td>
<td>ハードウェア</td>
</tr>
<tr>
<td>admin1/system1</td>
<td>管理下システムターゲット</td>
</tr>
<tr>
<td>admin1/system1/capabilities1</td>
<td>管理下システム SMASH 収集機能</td>
</tr>
<tr>
<td>admin1/system1/capabilities1/elecap1</td>
<td>管理下システムターゲット機能</td>
</tr>
</tbody>
</table>

SMCLP の使用 319
表 64. SMCLP ターゲット（続き）

<table>
<thead>
<tr>
<th>ターゲット</th>
<th>定義</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin1/system1/logs1</td>
<td>レコードログ収集ターゲット</td>
</tr>
<tr>
<td>admin1/system1/logs1/log1</td>
<td>システムイベントログ（SEL）のレコードエントリ</td>
</tr>
<tr>
<td>admin1/system1/logs1/log1/record*</td>
<td>管理下システムの SEL レコードの個々のインスタンス</td>
</tr>
<tr>
<td>admin1/system1/settings1</td>
<td>管理下システム SMASH 収集機能</td>
</tr>
<tr>
<td>admin1/system1/capacities1</td>
<td>管理下システム機能 SMASH 収集</td>
</tr>
<tr>
<td>admin1/system1/consoles1</td>
<td>管理下システムコンソール SMASH 収集</td>
</tr>
<tr>
<td>admin1/system1/sp1</td>
<td>サービスプロセッサ</td>
</tr>
<tr>
<td>admin1/system1/sp1/timesvc1</td>
<td>サービスプロセッサ時間サービス</td>
</tr>
<tr>
<td>admin1/system1/sp1/capabilities1</td>
<td>サービスプロセッサ機能 SMASH 収集</td>
</tr>
<tr>
<td>admin1/system1/sp1/capabilities1/clpcap1</td>
<td>CLP サービス機能</td>
</tr>
<tr>
<td>admin1/system1/sp1/capabilities1/pwrmgtcap1</td>
<td>システムの電源状態管理サービス機能</td>
</tr>
<tr>
<td>admin1/system1/sp1/capabilities1/acctmgtcap*</td>
<td>アカウント管理サービス機能</td>
</tr>
<tr>
<td>admin1/system1/sp1/capabilities1/rolemgtcap*</td>
<td>ローカル役割ベースの管理機能</td>
</tr>
<tr>
<td>admin1/system1/sp1/capabilities1/elecap1</td>
<td>認証機能</td>
</tr>
<tr>
<td>admin1/system1/sp1/settings1</td>
<td>サービスプロセッサ設定収集</td>
</tr>
<tr>
<td>admin1/system1/sp1/settings1/clpsetting1</td>
<td>CLP サービス設定データ</td>
</tr>
<tr>
<td>admin1/system1/sp1/clpsvc1</td>
<td>CLP サービスプロトコルサービス</td>
</tr>
<tr>
<td>admin1/system1/sp1/clpsvc1/clpendpt*</td>
<td>CLP サービスプロトコルエンドポイント</td>
</tr>
<tr>
<td>admin1/system1/sp1/clpsvc1/tcpendpt*</td>
<td>CLP サービスプロトコル TCP エンドポイント</td>
</tr>
</tbody>
</table>

320  SMCLP の使用
<table>
<thead>
<tr>
<th>ターゲット</th>
<th>定義</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin1/system1/sp1/jobq1</td>
<td>CLP サービスプロトコルジョブキューリング</td>
</tr>
<tr>
<td>admin1/system1/sp1/jobq1/job*</td>
<td>CLP サービスプロトコルジョブ</td>
</tr>
<tr>
<td>admin1/system1/sp1/pwrmgtsvcl</td>
<td>電源状態管理サービス</td>
</tr>
<tr>
<td>admin1/system1/sp1/account1-16</td>
<td>ローカルユーザーーアカウント</td>
</tr>
<tr>
<td>admin1/sysetml/sp1/account1-16/identity1</td>
<td>ローカルユーザー識別アカウント</td>
</tr>
<tr>
<td>admin1/sysetml/sp1/account1-16/identity2</td>
<td>IPMI 識別（LAN）アカウント</td>
</tr>
<tr>
<td>admin1/sysetml/sp1/account1-16/identity3</td>
<td>IPMI 識別（シリアル）アカウント</td>
</tr>
<tr>
<td>admin1/sysetml/sp1/account1-16/identity4</td>
<td>CLP 識別アカウント</td>
</tr>
<tr>
<td>admin1/system1/sp1/acctsvc2</td>
<td>IPMI アカウント管理サービス</td>
</tr>
<tr>
<td>admin1/system1/sp1/acctsvc3</td>
<td>CLP アカウント管理サービス</td>
</tr>
<tr>
<td>admin1/system1/sp1/rolesvc1</td>
<td>ローカル役割ベース認証（RBA）サービス</td>
</tr>
<tr>
<td>admin1/system1/sp1/rolesvc1/Role1-16</td>
<td>ローカル役割</td>
</tr>
<tr>
<td>admin1/system1/sp1/rolesvc1/Role1-16/privilege1</td>
<td>ローカル役割権限</td>
</tr>
<tr>
<td>admin1/system1/sp1/rolesvc2</td>
<td>IPMI RBA サービス</td>
</tr>
<tr>
<td>admin1/system1/sp1/rolesvc2/Role1-3</td>
<td>IPMI 役割</td>
</tr>
<tr>
<td>admin1/system1/sp1/rolesvc2/Role4</td>
<td>IPMI シリアルオーバーLAN（SOL）役割</td>
</tr>
<tr>
<td>admin1/system1/sp1/rolesvc3</td>
<td>CLP RBA サービス</td>
</tr>
<tr>
<td>admin1/system1/sp1/rolesvc3/Role1-3</td>
<td>CLP 役割</td>
</tr>
<tr>
<td>admin1/system1/sp1/rolesvc3/Role1-3/privilege1</td>
<td>CLP 役割権限</td>
</tr>
</tbody>
</table>
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。

ルートのターゲットは、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 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表示します。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、アンシエーション、パーセージに制限できます。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 1 行につき 1 つのキー=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 ベブサイト（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、p. 323
- SEL 管理、p. 323
- MAP ターゲットナビゲーション、p. 324

322  SMCLP の使用
サーバー電源管理
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
  次のような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
  次のような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
  次のようなメッセージが表示されます:
  system1 has been reset successfully

SEL管理
次の例は、SMCLP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
  Commands:
  cd
  show
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
Commands:
cd
show
help
exit
version

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:
cd . を入力
- 1つ上のレベルに移動:
cd .. を入力
- 終了:
exit
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リテイを使用できます。

- リモートファイル共有
- コンソール

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
- 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
- SDカードの内蔵オペレーティングシステムの導入

リモートファイル共有を使用したオペレーティングシステムの導入

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、次の手順を実行してください。

1. iDRAC ウェブインタフェースおよび iDRAC RACADM コマンドラインインタフェースでサポートされています。
2. 設定 > システム設定 > ハードウェア設定 > 最初の起動デバイスの順に移動します。
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 機能を選択して、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。

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、CIFS、HTTP、または HTTPS 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。

メモ: HTTP または HTTPS 機能を使用している RFS は、iDRAC ウェブインタフェースおよび iDRAC RACADM コマンドラインインタフェースでサポートされています。

メモ: HTTP または HTTPS 経由でサポートされています。
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。
仮想メディアが取り外されているか、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。接続すると、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 OME Modular 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:
- 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。
- iDRAC に IPv4 と IPv6 の両方が設定されている場合、DNS サーバには、iDRAC ホスト名を両方のアドレスに関連付けたレコードを含めることができます。iDRAC で IPv4 オプションが無効になっている場合、iDRAC は外部 IPv6 共有にアクセスできない可能性があります。DNS サーバに引き続き IPv4 レコードが含まれている可能性があるため、DNS の名前解決で IPv4 アドレスを返すことがあります。このような場合には、iDRAC で IPv4 オプションを無効にするときに DNS サーバから IPv4 DNS レコードを削除することをお勧めします。
- CIFS は Active Directory ドメインの一部である場合は、イメージファイルパスに IP アドレスとともにドメイン名を入力します。
- NFS は IPv4 アドレスのみをサポートします。
- 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。
- CIFS を使用していて、Active Directory ドメインの一部である場合は、イメージファイルパスに IP アドレスとともにドメイン名を入力します。
- NFS 共有からファイルにアクセスする場合は、次の共有許可を設定します。
  - Linux：共有許可が少なくとも Others (その他) アカウントの Read (読み取り) に設定されていることを確認します。
  - Windows：共有プロパティのセキュリティタブに移動し、全員をグループ名またはユーザー名フィールドと読み取り権利に追加します。
- iDRAC VFlash 機能と RFS には、関連性がありません。
- ネットワーク共有ファイルパスでは、英語の ASCII 文字のみがサポートされています。
- iDRAC と RFS の接続されていない場合、OS ドライブの取り出し機能はサポートされていません。
- CMC のウェブインタフェースでは、HTTP または HTTPs 経由の RFS 機能は使用できません。

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 の設定 > 仮想メディア > 連結されたメディア の順に移動します。
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. Remote File Share（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。
4. 次にイメージファイルパスの例を挙げます。
  - CIFS — //<IP to connect for CIFS file system>/<file path>/<image name>
  - NFS — //<IP to connect for NFS file system>/<file path>/<image name>
  - HTTP — http://<URL>/<file path>/<image name>
  - HTTPs — https://<URL>/<file path>/<image name>

1 メモ: Windows 7 システムでホストされる CIFS 共有を使用する際に出入力エラーを回避するには、次のレジストリキーを変更します。
- HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache を 1 に設定
- HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\Size を 3 に設定

1 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。

オペレーティングシステムの導入
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. 145 を参照してください。

NFS 共有は IPv4 アドレスのみをサポートします。

メモ：ネットワーク共有のユーザー名とパスワードは許可される文字は、ネットワーク共有のタイプによって決定されます。IPv4 では、共有のタイプによって定義されるネットワーク共有資格情報の有効な文字をサポートします。ただし、<、>、(コンマ)を除きます。

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：画像パスにユーザー資格情報が含まれるのは、HTTPS を使用して、GUI と RACADM に資格情報が表示されないことを示しています。URL に資格情報を入力する場合は、「@」記号の使用を避けてください。区切り文字であるためです。

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/sdc0 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 /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する必要があります。

```
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 Linux ディストリビューションを使用する場合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>：ネットワーク共有上のイメージの場所（場所を二重引用符で囲む）「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」の項でイメージファイルパスの例を参照
-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、（一つ重引用符）、（二重引用符）、＜（小なり記号）、＞（大なり記号）は使用できません。

メモ：Windows 7 システムでホストされる CIFS 共有を使用する際に入出力エラーを回避するには、次のレジストリキーを変更します。
仮想メディアを使用したオペレーティングシステムの導入

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、仮想メディアが接続状態になっている。
- 仮想メディアが自動接続モードの場合、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、ドライバー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. 次のうちのいずれか1つを実行してください。
   - 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接続します。

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展開を完了します。

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に 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、ドライプの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。

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. Internal USB Port（内蔵 USB ポート）を On（オン）に設定します。これを Off（オフ）に設定した場合、IDSDM は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カードのどちらからもマスターすることができる。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、取り外された場合は常に、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。
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
- System Health (システム正常性)

トピック:

- 診断コンソールの使用
- Post コードの表示
- 起動キャプチャとクラッシュキャプチャビデオの表示
- ログの表示
- 前回のシステムクラッシュ画面の表示
- システムステータスの表示
- ハードウェア問題の兆候
- システム正常性の表示
- サーバーテスト画面でのエラーメッセージの確認
- iDRAC の再起動
- システムおよびユーザーデータの消去
- 工場出荷時のデフォルト設定への iDRAC のリセット

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、Maintenance (メンテナンス) > Diagnostics (診断) の順に移動します。
   Diagnostics Console Command (診断コンソールコマンド) ページが表示されます。
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。

iDRAC のリセットと iDRAC のデフォルトへのリセット

1. iDRAC ウェブインタフェースで、Maintenance (メンテナンス) > Diagnostics (診断) の順に移動します。
   次のオプションがあります。
   - iDRAC をリセットするには、Reset iDRAC（iDRAC のリセット）をクリックします。iDRAC で正常な再起動操作が実行されます。再起動後に、ブラウザを更新して iDRAC に再接続し、ログインします。
   - Reset iDRAC to Default Settings（iDRAC をデフォルト設定にリセット）をクリックして、iDRAC をデフォルト設定にリセットします。Reset iDRAC to Default Settings（iDRAC をデフォルト設定にリセット）をクリックすると、Reset
iDRACを工場出荷時のデフォルト設定にリセット 
ウィンドウが表示されます。この処置は、iDRACを工場出荷時のデフォルトにリセットします。次のオプションのいずれかを選択します。

a. すべての設定を破棄しても、ユーザーとネットワーク設定は維持する。
b. すべての設定を破棄し、デフォルトのユーザー名をrootに、パスワードを出荷時の値（root/shipping値）にリセットする。
c. すべての設定を破棄し、デフォルトのユーザー名をrootに、パスワードをcalvin（root/calvin）にリセットする。

2. Continue（続行）をクリックします。

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、すぐに対応動作するか、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。その後 diagnostics export racadm コマンドを実行して、結果を NFS、CIFS、HTTP、または HTTPS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。詳細については、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開始しない場合、有効期限切れで失敗としてマーカされます。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。

- Power cycle system
- 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の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）

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、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、NFS、HTTP、HTTPS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、ジョブをキャンセルすること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

RACADMを使用した管理下システムのトラブルシューティング

- 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。

  ```bash
  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。

  ```bash
  racadm diagnostics export -f <file name> -l <NFS / CIFS / HTTP / HTTPs share> -u <username> -p <password>
  ```

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 331
オプションの詳細については、『iDRAC RACADM CLI ガイド』は、www.dell.com/idracmanuals にあります。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 Codes (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前の Post コードが表示されます。

Post コードを表示するには、Maintenance (メンテナンス) > Troubleshooting (トラブルシューティング) > Post Code (Post コード) の順に移動します。

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、最新のものから最も古いものへと並びます。
- 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、ライセンス付きの機能です。

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/秒の速度で行われます。起動キャプチャビデオは RAM に保存されているため、iDRAC をリセットすると削除され、利用できなくなります。

MEMO:

- 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 ビデオプレイヤーに表示されるビデオキャプチャ時間は、他のビデオプレイヤーに表示されるビデオキャプチャ時間とは異なります。iDRAC GUI ビデオプレイヤーでは iDRAC タイムゾーンの時刻が表示され、その他はビデオプレイヤーには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が表示されます。

MEMO:

DVC ブートキャプチャファイルはビデオではありません。これから、サーバー起動中に取得される(特定の解像度の)一連の画面上、DVC プレイヤーは、これらの画面を変換して起動ビデオを作成します。ビデオを DVC (少しずつ異なる連続したスナップショット)から .mov(実際のビデオ)形式にエクスポートする際、ビデオが最初にエンコードされたときと同一または同程度の解像度を使用することが想定されます。ビデオは、起動ビデオに同程度の解像度でエクスポートする必要があります。

MEMO:

- プートキャプチャファイルが利用できるようになるまで時間がかかる理由は、ホストの起動後にプートキャプチャパッファーがいっぱいになっていないためです。

[ 起動キャプチャ ] 画面を表示するには、[ メンテナンス ] > [ 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。

MEMO:

- 内蔵ビデオコントローラーが無効になっているサーバーにアドオンビデオコントローラーがある場合、起動キャプチャに関して一定のレイテンシーが想定されます。そのため、ビデオの POST の終了メッセージは次のキャプチャで記録されます。

### 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、Maintenance (メンテナンス) > Troubleshooting (トラブルシューティング) > Video Capture (ビデオキャプチャ) に移動します。
   - 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、ライセンス付きの機能です。

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、Overview（概要）＞Server（サーバ）＞Troubleshooting（トラブルシューティング）＞Last Crash Screen（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。

○メモ: iDRAC がリセットされるか、AC 電源サイクルイベントが発生すると、クラッシュのキャプチャデータがクリアされます。

システムステータスの表示
システムステータスには、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。
- 概要
- バッテリー
- 冷却
- CPU
- 前面パネル
- イントルージョン
- メモリー
- ネットワークデバイス
- 電源装置
- 電圧
- リムーバブルフラッシュメディア
- シャーシコントローラ

次の管理下システムのステータスを表示できます。
- ラックおよびタワーサーバーの場合：LCD 前面パネルおよびシステム ID LED ステータス、または LED 前面パネルおよびシステム ID LED ステータス
- ブレードサーバーの場合：システム ID LED のみ

システムの前面パネル LCD ステータスの表示
該当するラックサーバーおよびタワーサーバーの LCD 前面パネルステータスを表示するには、iDRAC ウェブインタフェースで、システム＞概要＞前面パネルの順に選択します。前面パネルページが表示されます。

前面パネルセクションには、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き（LCD 前面パネルの青色で示されます）、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: ラックサーバー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。
選択に基づき、テキストボックスに現在の値が表示されます。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。文字数は62に制限されています。なしを選択する場合、LCDにはホームメッセージが表示されません。

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グループ内のオブジェクトを使用します。詳細については、「IDRAC RACADM CLIガイド」は、www.dell.com/idracmanualsにあります。を参照してください。

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の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「システム > 概要 > 前面パネル」の順に選択します。前面パネルセクションには、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ァイア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。

システムが正常に動作していると（LED前面パネルの青色の正常性アイコンで表示されます）、エラーを非表示するおよびエラーを再表示するの両方がグレーパッチされます。ラックサーバおよびタワーパ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、「IDRAC RACADM CLIガイド」は、www.dell.com/idracmanualsにあります。を参照してください。

ハードウェア問題の兆候
ハードウェア関連の問題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着脱し直して、システムを再起動
- プ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、「設置およびサービスマニュアル」は、www.dell.com/poweredgemanualsにあります。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:お客様は、製品ドキュメントで認められた、あるいはオンラインや電話によるサービス、サポートチームから指示を受けた内容のトラブルシューティング、および簡単な修理作業のみを行ってください。Dellの許可を受けていない保守による損傷は、保証の対象となりません。製品に付属しているマニュアルの「安全にお使いいただくために」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、CMC、およびOME-Modular Webインタフェースの次のコンポーネントのステータスを表示することができます。
- バッテリー
- CPU
- 冷却
- イントルージョン
- メモリ
- 電源装置
- リムーバブルフラッシュメディア
- 電圧
- その他

コンポーネントの詳細を表示するには、サーバー正常性セクションで任意のコンポーネント名をクリックします。
サーバーステータス画面でのエラーメッセージの確認

橙色 LED が点滅し、特定のサーバにエラーが発生した場合、LCD のメイン Server Status（サーバーステータス）画面に、エラーがあるサーバ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。
- Maintenance (メンテナンス) > Diagnostics (診断) に移動します。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、「Chassis Management Controller RACADM CLI ガイド」は、www.dell.com/cmcmanuals にあります。を参照してください。詳細については、「PowerEdge MX7000 シャーシ向け OME - Modular RACADM CLI ガイド」は、www.dell.com/openmanagemanuals にあります。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

 Memo: システムおよびユーザーデータの消去は、iDRAC GUI ではサポートされていません。

システムコンポーネントと次のコンポーネントのユーザーデータは削除できます。
- 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 BIOS リセット
- デフォルト 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。

 Memo: 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。それまで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 — BIOS をデフォルトにリセット
- diag — 組み込み診断機能
- drvpack — 組み込み OS ドライバパック
- lcdata — Lifecycle Controller データの消去
- idrac — iDRAC をデフォルトにリセット
- overwritepd — インスタントセキュア消去（ISE）をサポートしないハードドライブの上書き
- percnvcache — コントローラキャッシュのリセット
vflash — vFLASH のリセット
secureerasepd — ISE をサポートするハードドライブ、SSD、NVMe の消去
allapps — すべての OS アプリケーションのクリア

詳細については、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。を参照してください。

メモ: Dell テックセンターのリンクは、Dell ブランドのシステムの iDRAC GUI に表示されます。WSMan コマンドを使用してシステムデータを消去し、リンクを再び表示する場合は、ホストを手動で再起動し、CSIOR が実行されるのを待ちます。

メモ: システムを消去しても VD が再び表示されることがあります。システムの消去が完了して iDRAC が再起動されたら、CSIOR を実行してください。

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

1. Maintenance (メンテナンス) > Diagnostics (診断) と移動します。

2. IDRA 本体設定ページが表示されます。

3. Yes (はい) をクリックします。

iDRAC のリセットが開始されます。

4. 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。

工場出荷時のデフォルト設定への iDRAC のリセット

iDRAC ウェブインタフェースを使用して iDRAC の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. Maintenance (メンテナンス) > Diagnostics (診断) と移動します。

2. IDRA 本体設定ページが表示されます。

3. Yes (はい) をクリックします。

iDRAC のリセットが開始されます。

4. 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。

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. Maintenance (メンテナンス) > Diagnostics (診断) と移動します。

2. 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。

3. Yes (はい) をクリックします。

iDRAC のリセットが開始されます。

4. 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。

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. Maintenance (メンテナンス) > Diagnostics (診断) と移動します。

2. 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。

3. Yes (はい) をクリックします。

iDRAC のリセットが開始されます。

4. 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。

メモ: Dell テックセンターのリンクは、Dell ブランドのシステムの iDRAC GUI に表示されます。WSMan コマンドを使用してシステムデータを消去し、リンクを再び表示する場合は、ホストを手動で再起動し、CSIOR が実行されるのを待ちます。

メモ: システムを消去しても VD が再び表示されることがあります。システムの消去が完了して iDRAC が再起動されたら、CSIOR を実行してください。
SupportAssist では、SupportAssist コレクションを作成し、その他の SupportAssist 機能を使用してシステムとデータセンターを監視することができます。iDRAC は、プラットフォーム情報の収集用のアプリケーションインタフェースを提供します。この情報により、プラットフォームとシステムの問題を解決するためのサポートサービスを有効にできます。iDRAC では、サーバーの SupportAssist コレクションを生成し、そのコレクションを管理ステーション（ローカル）の場所、または FTP、Trivial File Transfer Protocol (TFTP)、HTTP、HTTPS、共通インターネットファイルシステム (CIFS)、ネットワークファイル共有 (NFS) などの共有ネットワークの場所にエクスポートできます。コレクションは、標準の ZIP 形式で生成されます。このコレクションは、トラブルシューティングまたはイベントリコレクションのためにテクニカルサポートに送信することができます。

トピック:
- SupportAssist 登録
- サービスモジュールのインストール
- サーバ OS プロキシ情報
- SupportAssist
- サービスリクエストポータル
- 収集ログ
- SupportAssist コレクションの生成
- 設定
- 収集の設定
- 連絡先情報

SupportAssist 登録
SupportAssist の自動化、プロアクティブ、および予測機能を利用するには、システムを SupportAssist に登録する必要があります。コレクションを生成してローカルまたはネットワークに保存でき、登録せずに Dell EMC に送信することもできます。

連絡先および配送先情報
登録を完了するには、連絡先と配送先情報を入力する必要があります。

主要連絡先情報
会社名、国名、氏名*、電話番号*、代替番号、および E-mail アドレス*を入力します。詳細が正しく表示されていることを確認し、フィールドを編集する場合は変更を行います。

*フィールドが必須であることを示しています。

セカンダリー連絡先情報
名、氏、電話番号、代替番号、E-mail アドレスを入力し、詳細が正しく表示されていることを確認し、フィールドを編集する場合は変更を行います。

メモ: セカンダリー連絡先情報はいつでも削除できます。

自動ディスパッチ
SupportAssist に登録されている iDRAC を介して Dell-EMC に重要イベントが報告されると、自動ディスパッチワークフローが開始されることがあります。このワークフローは、転送されているイベントと、登録済みのデバイスの SupportAssist 保証レベルに基づいています。自動ディスパッチワークフローが有効にあるには、SupportAssist 登録プロセス中にディスパッチ情報を入力する

メモ: セカンダリー連絡先情報はいつでも削除できます。
必要があります。ディスバッチ パートと一緒にオンサイト サポートが必要な場合は、[ オンサイト サポート付きパーソナル ディスバッチ]を選択します。

①メモ: 自動ディスバッチは、Windows 用 iDRAC サービス モジュール (iSM) v3.4.0 を搭載したシステムで有効です。今後の iSM リリースでは、追加のオペレーティングシステムの自動ディスバッチがサポートされます。

発送先住所
住所と希望連絡時間帯を入力します。

エンドユーザーライセンス契約
必要なすべての情報を入力した後に、エンドユーザーライセンス契約（EULA）に同意して登録プロセスを完了する必要があります。詳細について確認する場合は、EULA を印刷できます。いつでも登録プロセスをキャンセルして終了することができます。

サービスモジュールのインストール
SupportAssist を登録して使用するには、iDRAC Service Module (iSM) がシステムにインストールされている必要があります。サービスモジュールのインストールが開始されると、インストール手順を参照することができます。iSM が正常にインストールされるまで、次へボタンは無効のままです。

サーバ OS プロキシ情報
接続に問題がある場合、OS プロキシ情報の入力が求められます。サーバ、ポート、ユーザー名、およびパスワードを入力して、プロキシ設定を行います。

SupportAssist
SupportAssist を設定したら、SupportAssist ダッシュボードを確認し、サービスリクエストサマリ、保証ステータス、SupportAssist の概要、サービスリクエスト、および収集ログを確認できます。収集ログを表示または送信するために登録の必要はありません。

サービスリクエストポータル
サービスリクエスト は、各イベントについて、状態（開始/終了）、説明、ソース（イベント/電話）、サービスリクエスト ID、開始日、および終了日 の詳細を表示します。イベントを選択して各イベントのさらに詳細を表示できます。サービスリクエストポータルを確認して、個別のケースについての追加情報を表示することもできます。

収集ログ
収集ログには、収集の時刻、収集タイプ（手動、スケジュール済み、イベントベース）、収集されたデータ（カスタム選択、すべてのデータ）、収集ステータス（エラーで終了、正常に終了）、ジョブ ID、通信ステータス、および、および通信の日付と時刻の詳細が表示されます。iDRAC 内で最後に保持されたコレクションはデルに送信できます。

①メモ: 生成された収集ログの詳細をフィルタリングして、ユーザーの選択に基づいて特定個人情報（PII）を削除することができま

SupportAssist コレクションの生成
OS およびアプリケーションログの生成
- 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にインストールして実行する必要があります。
- OS Collector は出荷時に iDRAC にインストールされています。削除した場合は、iDRAC にインストールする必要があります。

サーバ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場合、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。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したり、またはサーバーサポートシステムやiDRACからインターネットへアクセスしたりする必要はありません。

サーバーの正常性レポートを生成してから、収集ログをエクスポートできます。

- 管理ステーション（ローカル）。
- 共通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）などの共有ネットワーク。CIFSまたはNFSなどの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。
- Dell EMCへ。

SupportAssist Collection は、標準の ZIP フォーマットで生成されます。コレクションには次の情報が含まれています。

- すべてのコンポーネントのハードウェアインベントリ（システムコンポーネントの設定とファームウェアの詳細、マザーボードシステムイベントログ、iDRAC状態情報、および Lifecycle Controller のログを含む）
- 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。
- ストレージコントローラログ。
- iDRAC デバッグログ。
- HTML5 ビューアが含まれており、コレクションが完了するとアクセスできるようになります。

データが生成された後、複数の XML ファイルとログファイルを含むデータを表示できます。

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、Maintenance（メンテナンス）＞SupportAssist に移動します。
2. サーバが SupportAssist に登録されていない場合は、SupportAssist 登録ウィザードが表示されます。キャンセル＞登録のキャンセルの順にクリックします。
3. Start a Collection（収集の開始）をクリックします。
4. コレクションに含まれるデータセットを選択します。
5. PII のコレクションは、フィルタすることもできます。
6. 収集を保存する必要のある宛先を選択します。
   a. サーバがインターネットに接続されていて、今すぐ送信オプションが有効になっている場合は、このオプションを選択すると、収集ログが Dell EMC SupportAssist に送信されます。
   b. Save locally（ローカルに保存）オプションでは、生成された収集をローカルシステムに保存できます。
   c. Save to Network（ネットワークに保存）オプションでは、生成された収集がユーザ定義の CIFS または NFS 共有場所に保存されます。

memo: Save to Network（ネットワークに保存）が選択され、デフォルトの場所が使用できない場合は、指定されたネットワークの詳細は今後のコレクションのためのデフォルトの場所として保存されます。デフォルトの場所が既に存在している場合、コレクションでは、指定された詳細が 1 度だけ使用されます。

Save to Network（ネットワークに保存）オプションが選択され、ネットワークの詳細を提供したユーザーが今後の収集のデフォルトとして保存されます（前のネットワーク共有場所が保存されていない場合）。

7. Collect（収集）をクリックして収集の生成を続行します。
8. 要求された場合は、End User Level Agreement (EULA)（エンドユーザーレベル契約 (EULA)）に同意して続行します。
以下の場合は、OS and Application Data（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、選択できません。
- iSM がインストールされていない、またはホスト OS 上で実行されている
- OS Collector が iDRAC から削除されている
- OS-BMC パススルーが iDRAC で無効になっている
- 前のコレクションからのキャッシュされた OS アプリケーションデータが iDRAC で使用できない

設定
このページでは、収集ログの設定を設定できます。ログされている場合は、連絡先の詳細を更新したり、Eメール通知を有効または無効にしたり、言語設定を変更したりすることができます。

収集の設定
収集は、任意のネットワークの場所に保存できます。Set Archive Directory（アーカイブディレクトリの設定）を使用して、ネットワークの場所を設定します。コレクションは、任意のネットワークの場所に保存できます。Set Archive Directory（アーカイブディレクトリの設定）を使用して、ネットワークの場所を設定します。ネットワーク接続をテストする前に、目的のプロトコルのタイプ（CIFS/NFS）、対応する IP アドレス、共有名、ドメイン名、ユーザ名とパスワードを入力します。Test Network Connection（ネットワーク接続のテスト）ボタンは、目的の共有への接続を確認します。

連絡先情報
このページでは、SupportAssist の登録中に追加された連絡先情報の詳細が表示されます。この情報は更新できます。
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
- 仮想メモリ
- 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
- iDRAC アラート用のカスタム送信者 E メールの設定
- ネットワークセキュリティ
- テレメトリーストリーミング
- 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
- 仮想メモリ
- vFlash SD カード
- SNMP 認証
- ストレージデバイス
- GPU（アクセラレータ）
- iDRAC サービスモジュール
- RACADM
- デフォルトのパスワードを永続的に calvin に設定する
- その他

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、次の手順を行います。

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タラネット上にある場合は、ローカルインタラネットを選択し、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。
iDRAC アラート用のカスタム送信者 E メールの設定

アラートにより生成された E メールが、クラウドベースの E メールサービスに設定されたカスタム送信者 E メール以外のアドレスから送られてきました。

Support.google.com のプロセスに従って、クラウド E メールを登録する必要があります。

ネットワークセキュリティ

iDRAC Web インターフェイ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。これにより生成された E メールが、クラウドベースの E メールサービスに設定されたカスタム送信者 E メール以外のアドレスから送られてきました。

アラートにより生成された E メールが、クラウドベースの E メールサービスに設定されたカスタム送信者 E メール以外のアドレスから送られてきました。

Support.google.com のプロセスに従って、クラウドベースの E メールを登録する必要があります。

ネットワークセキュリティ

iDRAC Web インターフェイ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。これにより生成された E メールが、クラウドベースの E メールサービスに設定されたカスタム送信者 E メール以外のアドレスから送られてきました。

アラートにより生成された E メールが、クラウドベースの E メールサービスに設定されたカスタム送信者 E メール以外のアドレスから送られてきました。

Support.google.com のプロセスに従って、クラウドベースの E メールを登録する必要があります。
Active Directory

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 Configuration and Management (Active Directory の設定と管理) ページで Test Settings（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、適切なユーザーダ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、User Domain from Login (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、Specify a Domain (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。テスト結果については、次のエラーメッセージが表示されます。この原因は何ですか？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の場合、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証明書のサブジェクト名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、ドメインコントローラのホスト名が証明書のサブジェクト名と一致しない。SSL ハンドシェイク中に証明書の検証なしでドメインコントローラでログインする場合は、証明書の検証を無効にします。

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名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名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選択します。

- 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 ハンドシェイク中に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？

拡張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、すべてのユーザーや役割グループが同一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はありません。

よくあるお問い合わせ (FAQ)
iDRAC は、最初に、設定されたドメインコントローラアドレスに接続します。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で 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です。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、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 サーヴおよび代替 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、このグループのメンバーです。子ドメインに属するユーザーを使用して iDRAC をログインしようとするとき、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？

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スイートは、Computer Configuration (コンピュータ設定) > Security Settings (セキュリティ設定) > Local Policies (ローカルポリシー) > Security Options (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、古いクライアントを klist purge コマンドで削除します。
5. GPO を更新したら、新しいクライアントを作成します。
6. キャッシュを 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. Start (スタート) から gppedit.msc を実行します。Local Group Policy Editor (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。
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、Network（ネットワーク）ペインで優先 DNS サーバおよび代替 DNS サーバを指定しており、優先 DNS サーバに障害が発生すると、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 では、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

仮想コンソールを起動するにはどの Java バージョンが必要ですか？

この機能を使用して IPv6 ネットワーク上で iDRAC 仮想コンソールを起動するには、Java 8 以降が必要です。

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？

仮想コンソールエラーウィンドウを開いて、対応するセッションからのログアウトしてください。

仮想コンソールを起動するにはどの Java バージョンが必要ですか？

この機能を使用して IPv6 ネットワーク上で iDRAC 仮想コンソールを起動するには、Java 8 以降が必要です。

仮想コンソールを起動するにはどの Java バージョンが必要ですか？

この機能を使用して IPv6 ネットワーク上で iDRAC 仮想コンソールを起動するには、Java 8 以降が必要です。

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？

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？

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？
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、サーバ名の横に緑色のステータスが表示されます。無効の場合は、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。お使いのロケーションを確認し、必要に応じて文字セットを再設定します。
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では、次のいずれかの手順を実行します。
- タブセッションオプションメニューで「Mouse Acceleration（マウスアクセラレーション）」で Linuxを選択します。
- タブメニューで「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の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 Tools（ツール）にある Single Cursor（シングルカーソル）オプションが選択されているようにします。デフォルトは、2 カーソールモードです。
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は、キーボードまたはマウスを使用できますか？
いいえ、BIOS で仮想コンソールが有効になっているシステムに、サポートされている Microsoft オペレーティングシステムをリモートインストールするときは、リモートから OK を選択するよう求めめる 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、リモート管理されているサーバを再起動し、再インストールしてから、BIOS で仮想コンソールをオフにする必要があります。
このメッセージは、仮想コンソールが有効に設定されていることをユーザー警告するために、Microsoft によって生成されます。このメッセージが表示されないようにするには、オペレーティングシステムをリモートインストールする前に、iDRAC 設定ユーティリティで仮想コンソールをオフにしてください。
管理ステーションの Num Lock インジケーター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？
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。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？

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？

良好なパフォーマンスを得るために、5MBPS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、1MBPS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は最低限必要なシステム要件は何ですか？

仮想コンソールビューアウィンドウに信頼無しメッセージが表示されるのはなぜですか？

このメッセージが表示される理由としては、仮想コンソールブ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。場合には、仮想コンソールのデスクトップビデオ受信の映像動画が原因でこのメッセージが表示されることもあります。
仮想コンソールアクションオプションにブックマークリストに追加されないのはなぜですか？

このメッセージが表示される理由として、十分な追跡が可能です。通常は、ピクセルの値が高すぎると、ブックマークが表示されません。通常は、パスワード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。
仮想コンソールアクションの設定に依存します。仮想コンソールの設定に依存します。
ローカルシステムから仮想コンソールセッションを確立しています。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？

仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、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？

仮想コンソールアクションが信頼関係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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェブインタフェースから仮想コンソールセッションを確立すると、仮想コンソールセッションを確立するための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ウェビ
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際には、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 サーバでマジックキー機能を有効にします。次のコマンドを使用して、Linux 端末での機能を有効にできます。
   
   ```bash
   echo 1 > /proc/sys/kernel/sysrq
   ```

2. ActiveX ピエーレ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。

仮想コンソールの下部に「リンクが切断されました」というメッセージが表示されるのはなぜですか？

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？

サーバの再起動中には共有ネットワークボートを使用すると、BIOS のネットワークカードをリセットしている間に 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と、この時間が非常に長くなります。この場合、サーバに接続されているスイッチポートの「portfast」を有効にすることが推奨されています。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？

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？

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、仮想フロッピディスクまたは vFlash の位置を確認し、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。

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？

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？

仮想メディアを起動可能設定するデバイスのタイプは？

仮想メディアを起動可能設定するデバイスのタイプは？

仮想メディアを起動可能設定するデバイスのタイプは？

- CDROM/DVD データメディア
- ISO 9660 イメージ
- 1.44 フロッピディスクまたはフロッピーアイテム
USBキーや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キーニ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。

仮想メディアが連続済みであり、リモートフロッピーに接続されています。しかし、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バージョンでは、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、仮想フロッピードライプ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
```

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 CD" /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
```

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ことから、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。これを行うには、スタート＞管理ツール＞サービスに移動します。Windows Event Collector（Windowsイベントコレクタ）を右クリックし、Stop（停止）をクリックします。

フラ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どちらか1つです。両方を使用することはできません。
ブラウザでTLS 1.0のみを使用するよう設定すると、HTML5による仮想メディアの起動が失敗します。
ブラウザの設定で、TLS 1.1以降を使用するようにしてください。
iDRACに仮想メディアの接続ステータスがConnected（接続済み）と表示されているのに、仮想メディアにアクセスできません。
iDRACでAttach Mode（接続モード）がDetach（分離）に設定されているときにActiveXまたはJavaプラグインを使用して仮想メディアにアクセスしようすると、接続ステータスがConnected（接続済み）と表示されることがあります。Attach Mode（接続モード）をAuto-attach（自動連結）またはAttach（接続）に変更して仮想メディアにアクセスしてください。

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、操作の進行中にロックされます。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コミュニティ名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、iDRACエージェントがpublicモデルの要求の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、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。iDRAC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検出セットアップと同じ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

OpenManage Storage Management は、iDRAC よりも多くのストレージデバイスを表示しますが、システムに接続されているすべてのストレージデバイスの情報は表示されません。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。

HBA 330MM2 と 2 つの IOM を持つ MX プラットフォームでは、IOM の取り外しの EEMI メッセージが id ENC42 で生成されますが、IOM 復元用の EEMI メッセージ (ENC41) は生成されません。

iDRAC ウェブインタフェースで IOM の復元を確認するには、次の手順を実行します。

1. ストレージ概要エンクロージャの順に移動します。
2. エンクロージャを選択します。

GPU (アクセラレーター)

iDRAC GUI の CPU/アクセラレーターの下にある [アクセラレーター] セクションがグレーブラック表示されます。

それぞれの属性が Redfish で無効になっている場合、GUI の一部のページで予期される応答が表示されないことがあります。

iDRAC サービスモジュール

一部の PowerEdge サーバーの iDRAC GUI ページで、ISM の詳細が表示されない、または正しく更新されない

ユーザーがサブ NIC をチーニングに追加すると、その構成は無効になります。それ以外、ISM は iDRAC と正しく通信できなくなったります。

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がインストールされているかどうかを確認するために必要な最低限の権限レベルは何ですか？

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番号を確認する方法を教えてください。

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 Service Module のバージョンが[バージョン]タブに一覧表示されます。

・ ESXi を実行しているシステムの場合は、コマンド esxcli software vib list|grep -i open を実行します。iDRAC サービスモジュールが表示されます。

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。

よくあるお問い合わせ (FAQ)
iDRAC Service Module をインストールする前に、サーバが第 12 世代以降の PowerEdge サーバ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ると、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 パススルーを使用して、iDRAC と通信できません

iDRAC Service Module は、OS to iDRAC パススルー機能を使用して、USB NIC 経由で通信を確立します。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、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。

表 65. ルーティング順序の例

<table>
<thead>
<tr>
<th>送信先</th>
<th>ゲートウェイ</th>
<th>Genmask</th>
<th>フラグ</th>
<th>メトリック</th>
<th>参照</th>
<th>使用インタフェース</th>
</tr>
</thead>
<tbody>
<tr>
<td>デフォルト</td>
<td>10.94.148.1</td>
<td>0.0.0.0</td>
<td>UG</td>
<td>1024</td>
<td>0</td>
<td>0 em1</td>
</tr>
<tr>
<td>10.94.148.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0 em1</td>
</tr>
<tr>
<td>link-local</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0 em1</td>
</tr>
<tr>
<td>link-local</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0 enp0s20u12u3</td>
</tr>
</tbody>
</table>

この例では、enp0s20u12u3 が USB NIC インタフェースであり、リンクルート宛先マスクが繰り返され、USB NIC が順序の最初になっていません。このため、OS to iDRAC パススルー経由の iDRAC サービスモジュールと iDRAC 間における接続問題が発生する結果となります。接続問題のトラブルシューティングを行う場合、iDRAC USBNIC の IPv4 アドレス (デフォルトでは 169.254.1.1) にホストのオペレーティングシステムから到達可能かどうか確認してください。

到達可能でない場合は、次の手順を実行します。

1. 一意の宛先マスクで iDRAC USBNIC アドレスを変更します。
2. 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。

VMware ESXi サーバに iDRAC Service Module VIB をインストールすると、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。Service Module 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: `esxcli vmknic -d -p "iDRAC Network"`
  - vSwitch を削除する場合: `esxcli 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。

表 66. Lifecycle ログの場所

<table>
<thead>
<tr>
<th>オペレーティングシステム</th>
<th>場所</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows</td>
<td>イベントビューや Windows ログシステムの Lifecycle ログは、iDRAC Service Module というソース名の下で複製されます。</td>
</tr>
<tr>
<td></td>
<td>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 Service Module のソース名の下に複製されます。</td>
</tr>
<tr>
<td></td>
<td>Lifecycle ログの場所は、iDRAC Service Module インストールを使用して設定できます。iDRAC Service</td>
</tr>
</tbody>
</table>
表66. Lifecycle ログの場所（続き）

<table>
<thead>
<tr>
<th>オペレーティングシステム</th>
<th>場所</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux、SUSE Linux、CentOS、および Citrix XenServer</td>
<td>/var/log/messages</td>
</tr>
<tr>
<td>VMware ESXi</td>
<td>/var/log/syslog.log</td>
</tr>
</tbody>
</table>

Linuxのインストール中に、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 コーディーズ ガイド」は、www.dell.com/idracmanuals にあります。で「Linux 仮想化」の項を参照してください。

特定の構成で GPU パフォーマンスを向上させる方法を教えてください。

BIOS システムパフォーマンスプロファイルでパフォーマンスを設定

[プロセッサの設定]で、NPSを4に、CCXを[自動]に設定

チャネルごとに少なくとも1枚のDIMMを用意

Linux OSでIOMMU=passthrough

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、明確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。

例えば次のようにになります。

```
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プロパティが変更された。
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。ただし、しばらくすると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。

デフォルトのパスワードを永続的に calvin に設定する

固有のデフォルト iDRAC パスワードが設定されてシステムが出荷されており、デフォルトパスワードを calvin に変更する場合は、システム基板のジャンパを使用する必要があります。

注意：ジャンパの設定を変更すると、デフォルトのパスワードは永続的に calvin に変更されます。iDRAC を出荷時の設定にリセットしても、固有のパスワードに戻ることはできません。
ジャンパの場所と手順の詳細については、https://www.dell.com/support でサーバのドキュメントを参照してください。

その他

最新バージョンにアップグレードするとアップグレードに失敗します。

メモ：4.00.00.00/4.10.10.10 以降のビルドにアップグレードするために必要な iDRAC の最小バージョンは、3.30.30.30 です。

OS をインストールすると、ホスト名が自動的に表示され変更される場合も、されない場合もあります。

次の 2 つのシナリオが考えられます。

- シナリオ 1: OS をインストールした後、iDRAC に最新のホスト名が表示されない。OMSA または ISM を iDRAC とともにインストールして、ホスト名を反映させる必要があります。
- シナリオ 2: iDRAC には特定の OS に対するホスト名があり、異なる別の OS がインストールされても、このホスト名が上書きされずに古いホスト名として表示される。これは、ホスト名が OS から送信される情報であり、iDRAC はこの情報を保存するだけであることが原因です。新しい OS がインストールされても、iDRAC はホスト名の値をリセットしません。ただし、OS の新しいバージョンでは、最初の OS の起動時に iDRAC でホスト名を更新できます。

プレードサーバの iDRAC IP アドレスを検索するには、どうすればよいですか？

メモ：Chassis Management Controller (CMC) オプションは、プレードサーバにしか適用できません。
CMC Web インターフェイスを使用する場合:
[シャーシ] > [サーバー] > [セットアップ] > [導入] の順に移動します。表示された表にサーバのIPアドレスが表示されます。
仮想コンソールを使用する場合：サーバーを再起動してPOST中にiDRAC IPアドレスを表示します。OSCAR インターフェイスで「Dell CMC」コンソールを選択し、ローカル シリアル接続を介して 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、「Chassis Management Controller RACADM CLI ガイド」は、www.dell.com/cmcmanuals にあります。を参照してください。

仮想コンソールを使用する場合：サーバーを再起動してPOST中にiDRAC IPアドレスを表示します。

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。

ブレードサーバーのiDRAC IP アドレスを検索するには、どうすればよいですか？

メモ: OME-Modular Web インターフェイス オプションは、MX プラットフォームにのみ該当します。

OME-Modular Web インターフェイスを使用する:
[デバイス] > [コンピューティング] の順に移動します。コンピュータレベルを選択すると、iDRAC IP が管理 IP として表示されます。
OMM アプリケーションを使用する:「Dell EMC OpenManage Mobile ユーザーズ ガイド」は、www.dell.com/openmanagemanuals にあります。を参照してください。

LCD を使用する: 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？

メモ: MX プラットフォームには該当しません。

iDRAC Web インターフェイスから次の操作を行います。
[iDRAC 設定] > [CMC] の順に移動します。[CMC サマリー] 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 インターフェイスで「Dell CMC」コンソールを選択し、ローカル シリアル接続を介して 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。

よくあるお問い合わせ(FAQ) 355
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、「Chassis Management Controller RACADM CLI ガイド」は、www.dell.com/ cmcmanuals にあります。を参照してください。
iDRAC RACADM コマンドの詳細については、「iDRAC RACADM CLI ガイド」は、www.dell.com/idracmanuals にあります。を参照してください。

OME Modular IP アドレスを検索する方法を教えてください。

メモ: MX プラットフォームにのみ該当します。

- iDRAC ウェブインタフェースから次の操作を行います。
  - [iDRAC 設定] > [管理モジュール] の順に移動します。管理モジュールページに OME Modular IP アドレスが表示されます。

ラックおよびタワーサーバーの iDRAC IP アドレスはどのように検索すればよいですか？

- 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。
  - 物理サーバーで、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] の順に移動します。
- 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、モジュールの鍵 > 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 の順に選択します。

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。（MX プラットフォームには該当しません）
  - 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。

共有 LOM で iDRAC にアクセスできない

Windows での BSOD エラーなど、ホスト OS に致命的なエラーがある場合、iDRAC にアクセスできないことがあります。iDRAC にアクセスするには、ホストを再起動して接続を回復します。
Link Aggregation Control Protocol（LACP）を無効にした後、共有 LOM が機能しない。

LACP を無効にする前に、ネットワークアダプタのホスト OS ドライバをロードする必要があります。ただし、パッシブ LACP 設定が使用されている場合は、ホスト OS のドライバがロードされる前に、共有 LOM が機能する可能性があります。LACP 設定については、スイッチのマニュアルを参照してください。

メモ: スイッチが LACP を使用して設定されている場合、ブリブート状態では iDRAC の共有 LOM IP にアクセスできません。

プ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 および OME Modular（MX プラットフォームのみ）の電力バジェットを確認します。シャーシの電源バジェットを超え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、次のことを参照してください: 工場出荷時のデフォルト設定への iDRAC のリセット、p. 336

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?

メモ: MX プラットフォームには該当しません。
1. CMC Web インターフェースにログインし、[シャーシ] > [サーバー] > [セットアップ] の順に移動します。
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。

プ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。

CMC（MX プラットフォーム非該当）および OME Modular（MX プラットフォーム該当）Web インターフェースを確認して、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るかどうかを確認します。表示される場合は、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、p. 80 ファームウェアのアップデートの手順に従います。

メモ: アップデート機能は MX プラットフォームには適用されません。
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。
Linux または Ubuntu で Firefox ブラウザを使用して iDRAC Web インターフェイスにログインできない。パスワードを入力できない。

この問題を解決するには、Firefox ブラウザを再インストールまたはアップグレードします。

SLES および Ubuntu で USB NIC を介して iDRAC にアクセスできない

memo: SLES では、iDRAC インターフェイスを DHCP に設定します。

Ubuntu では、Netplan ユーティリティを使用して iDRAC インターフェイスを DHCP モードに設定します。DHCP を設定するには、次の手順を実行します。
1. /etc/netplan/01-netcfg.yaml を使用します。
2. iDRAC DHCP に [ はい ] を指定します。
3. 設定を適用します。
Redfish での組み込みネットワークアダプターについてのリストで、モデル、製造元、その他のプロパティが表示されない

組み込みデバイスについての FRU 詳細は表示されません。マザーボードの組み込みデバイスについての FRU オブジェクトはありません。そのため、こうした依存プロパティの表示はされません。
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
• システム情報の取得とシステム正常性の評価
• アラートのセットアップと電子メールアラートの設定
• システムイベントログとLifecycleログの表示とエクスポート
• 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
• 正常にシャットダウンの実行
• 新しい管理者ユーザーアカウントの作成
• サーバのリモートコンソールの起動とUSBドライブのマウント
• 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
• システムイベントログとLifecycleログの表示とエクスポート
• 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
• 正常にシャットダウンの実行
• 新しい管理者ユーザーアカウントの作成
• サーバのリモートコンソールの起動とUSBドライブのマウント
• 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

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ブルコレクタからアラートを受取った後、データセンターや5台のサーバがオペレーティングシステムまたはサーバ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っています。原因を識別し、トラブルシューティングを行い、iDRACを使用してサーバを再稼働します。

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アラートを確認し、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（ウォームプート）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——問題のないシステム部品の赤いアイコン。
• ストレージアレイステータス——オン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。
• タ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

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。
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。

システムイベントログと Lifecycle ログの表示とエクスポート
Lifecycle 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 ユーザタフェースで、Maintenance (メンテナンス) > System Event Logs (システムイベントログ) に移動して SEL を表示し、Lifecycle Log (Lifecycle ログ) の順に移動して Lifecycle ログを表示します。
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。また、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 Service Module 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。

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
- Redfish API
- RACADM CLI (iDRAC 別) および CMC (MX プラットフォームには該当しません)
- Dell Update Package (DUP)
- CMC (MX プラットフォームには非該当) OME Modular (MX プラットフォームのみ該当) Web インターフェイス
- 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。
- Dashboard (ダッシュボード) で Graceful Shutdown (正常なシャットダウン) を選択し、Apply (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。

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ユーザーカーの設定
・ 汎用LDAPユーザーカーの設定

サーバ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。
   • Dashboard（ダッシュボード）>Virtual Console（仮想コンソール）と移動し、Launch Virtual Console（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が表示されます。
3. File（ファイル）メニューで、Virtual Media（仮想メディア）>Launch Virtual Media（仮想メディアの起動）の順にクリックします。
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

「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」のセクションを参照してください。

ラック密度の管理

ラックに追加のサーバを取り付ける前に、ラック内の残りの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における複数ネットワークカードへのIOアイデンティティ構成設定の適用

サーバ内にストレージエリアネットワーク（SAN）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、イニシエーター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。この操作を行うには、次の手順を実行します。
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. iDRACからサーバ設定プロファイル（SCP）ファイルをエクスポートします。
4. SCP ファイルの I/O アイデンティティ最適化設定を編集します。
5. SCP ファイルを iDRAC にインポートします。