Integrated Dell Remote Access Controller 9 ユーザーズガイド

December 2020
Rev. A02

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。

©2020 Dell Inc.またはその関連会社。All rights reserved.（不許複製・禁無断転載）Dell、EMC、およびその他の商標は、Dell Inc. またはその子会社の商標です。その他の商標は、それぞれの所有者の商標である場合があります。

目次

章 1: iDRAC の概要 16
iDRAC を使用する利点 16
主な機能 17
追加された新機能 19
ファームウェア バージョン 4.40.00.00 19
ファームウェア バージョン 4.30.30.30 20
ファームウェア バージョン 4.20.20.20 21
ファームウェア バージョン 4.10.10.10 22
ファームウェア バージョン 4.00.00.00 22
本ガイドの使用方法 23
対応ウェブブラウザ 23
サポートされる OS とハイパーバイザ 23
iDRAC ライセンス 24
ライセンスのタイプ 24
ライセンスの取得方法 25
Dell Digital Locker からライセンス キーを取得する 25
ライセンス操作 25
iDRAC9 のライセンス機能 26
iDRAC にアクセスするためのインタフェースとプロトコル 32
iDRAC ポート情報 34
その他の必要マニュアル 35
デルへのお問い合わせ 36
デルサポートサイトからの文書へのアクセス 36

章 2: iDRAC へのログイン 38
パスワードの強制変更 (FCP) 39
OpenID Connect を使用した iDRAC へのログイン 39
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 39
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 40
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 41
シングルサインオンを使用した iDRAC へのログイン 41
iDRAC ウェブインタフェースを使用した iDRAC SSO へのログイン 41
CMC ウェブインタフェースを使用した iDRAC SSO へのログイン 42
リモート RACADM を使用した iDRAC へのアクセス 42
リモート RACADM を Linux 上で使用するための CA 証明書の検証 42
ローカル RACADM を使用した iDRAC へのアクセス 42
ファームウェア RACADM を使用した iDRAC へのアクセス 43
シンプルな 2 要素認証 (シンプル 2FA) 43
RSA SecurID 2FA 43
システム正常性の表示 44
公開キー認証を使用した iDRAC へのログイン 45
複数の iDRAC セッション 45
セキュアなデフォルトパスワード 46
デフォルトの iDRAC パスワードのローカルでのリセット 46

デフォルトの iDRAC パスワードのリモートでのリセット....47
デフォルト ログイン パスワードの変更....47
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....48
RACADM を使用したデフォルトログインパスワードの変更....48
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....48
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....48
パスワード強度ポリシー....49
IP ブロック....49
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....50
RACADM を使用したアラートの有効化または無効化....51

章 3: 管理下システムのセットアップ....52
iDRAC IP アドレスのセットアップ....52
iDRAC 設定ユーティリティを使用した iDRAC IP のセットアップ....53
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....56
自動検出....56
自動設定を使用したサーバーとサーバコンポーネントの設定....59
セキュリティ向上のためのハッシュパスワードの使用....64
ローカル管理者アカウント設定の変更....66
管理下システムの場所のセットアップ....66
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....66
RACADM を使用した管理下システムの場所のセットアップ....66
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....66
システムパフォーマンスと電力消費の最適化....67
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....67
RACADM を使用した温度設定の変更....68
iDRAC 設定ユーティリティを使用したサーマル設定の変更....72
iDRAC Web インターフェイスを使用した PCIe エアフロー設定の変更....73
管理ステーションのセットアップ....73
iDRAC へのリモートアクセス....73
対応ウェブブラウザの設定....74
Internet Explorer の設定....74
Mozilla Firefox の設定....75
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....75
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....79
デバイスファームウェアのアップデート....79
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....82
自動ファームウェアアップデートのスケジュール設定....83
RACADM を使用したデバイスファームウェアのアップデート....85
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....85
DUP を使用したファームウェアのアップデート....85
リモート RACADM を使用したファームウェアのアップデート....86
Lifecycle Controller Remote Services を使用したファームウェアのアップデート....86
iDRAC からの CMC ファームウェアのアップデート....86
ステージングされたアップデートの表示と管理....87
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....87
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....87
デバイスファームウェアのロールバック....87
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....88
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....89

RACADM を使用したファームウェアのロールバック....89
Lifecycle Controller を使用したファームウェアのロールバック....89
Lifecycle Controller-Remote Services を使用したファームウェアのロールバック....89
iDRAC のリカバリ....89
他のシステム管理ツールを使用した iDRAC の監視....90
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....90
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インポート....91
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....91
BIOS 設定または F2 からのセキュアなブート設定....91
BIOS recovery....93

章 4: iDRAC の設定....94
iDRAC 情報の表示....95
ウェブインタフェースを使用した iDRAC 情報の表示....95
RACADM を使用した iDRAC 情報の表示....96
ネットワーク設定の変更....96
Web インターフェイスを使用したネットワーク設定の変更....96
ローカル RACADM を使用したネットワーク設定の変更....96
IP フィルタの設定....97
暗号スイートの選択....98
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....98
RACADM を使用した暗号スイート選択の設定....98
FIPS モード....99
FIPS モードの有効化....99
FIPS モードの無効化....99
サービスの設定....99
Web インターフェイスを使用したサービスの設定....100
RACADM を使用したサービスの設定....101
HTTPS リダイレクトの有効化または無効化....101
VNC クライアントを使用したリモートサーバーの管理....101
iDRAC ウェブインタフェースを使用した VNC サーバーの設定....102
RACADM を使用した VNC サーバーの設定....102
SSL 暗号化を伴う VNC ビューアの設定....102
SSL 暗号化なしでの VNC ビューアのセットアップ....103
前面パネルディスプレイの設定....103
LCD の設定....103
システム ID LED の設定....104
タイムゾーンおよび NTP の設定....104
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....104
RACADM を使用したタイムゾーンと NTP の設定....105
最初の起動デバイスの設定....105
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....105
RACADM を使用した最初の起動デバイスの設定....106
仮想コンソールを使用した最初の起動デバイスの設定....106
前回のクラッシュ画面の有効化....106
OS から iDRAC へのパススルーの有効化または無効化....106
OS から iDRAC へのパススルー用の対応カード....107
USB NIC 対応のオペレーティングシステム....107
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....108
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....109

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 109
証明書の取得 110
SSL サーバー証明書 110
新しい証明書署名要求の生成 111
自動証明書登録 112
サーバー証明書のアップロード 112
サーバー証明書の表示 113
カスタム署名証明書のアップロード 113
カスタム SSL 証明書署名証明書のダウンロード 113
カスタム SSL 証明書署名証明書の削除 114
RACADM を使用した複数の iDRAC の設定 114
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 115

章 5: OAuth 2.0 を使用した委任認証 116

章 6: iDRAC と管理下システム情報の表示 117
管理下システムの正常性とプロパティの表示 117
アセット追跡の設定 117
システムインベントリの表示 118
センサー情報の表示 119
CPU、メモリー、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 120
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 121
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 121
アイドル サーバーの検出 121
GPU (アクセラレーター) の管理 122
システムの Fresh Air 対応性のチェック 123
温度の履歴データの表示 124
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 124
RACADM を使用した温度の履歴データの表示 124
吸気口温度の警告しきい値の設定 124
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 125
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 125
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 126
FlexAddress メザニンカードのファブリック接続の表示 126
iDRAC セッションの表示または終了 126
ウェブインタフェースを使用した iDRAC セッションの終了 126

章 7: iDRAC 通信のセットアップ 128
DB9 ケーブルを使用したシリアル接続による iDRAC との通信 129
BIOS のシリアル接続用設定 129
RAC シリアル接続の有効化 130
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 130
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 132
シリアルコンソールから RAC シリアルへの切り替え 132
RAC シリアルからシリアルコンソールへの切り替え 132
IPMI SOL を使用した iDRAC との通信 132
BIOS のシリアル接続用設定 133
SOL を使用するための iDRAC の設定 133

対応プロトコルの有効化 134
IPMI over LAN を使用した iDRAC との通信 137
ウェブインタフェースを使用した IPMI over LAN の設定 137
iDRAC 設定ユーティリティを使用した IPMI over LAN の設定 137
RACADM を使用した IPMI over LAN の設定 138
リモート RACADM の有効化または無効化 138
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 138
RACADM を使用したリモート RACADM の有効化または無効化 138
ローカル RACADM の無効化 139
管理下システムでの IPMI の有効化 139
RHEL 6 での起動中の Linux のシリアルコンソールの設定 139
起動後の仮想コンソールへのログインの有効化 140
RHEL 7 でのシリアルターミナルの設定 141
シリアルコンソールからの GRUB の制御 142
サポート対象の SSH 暗号スキーム 142
SSH の公開キー認証の使用 143

章 8: ユーザーアカウントと権限の設定 146
iDRAC ユーザーの役割と特権 146
ユーザー名およびパスワードで推奨される文字 147
ローカルユーザーの設定 148
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 148
RACADM を使用したローカルユーザーの設定 148
Active Directory ユーザーの設定 150
iDRAC の Active Directory 認証を使用するための前提条件 150
サポートされている Active Directory 認証メカニズム 151
標準スキーマ Active Directory の概要 152
標準スキーマ Active Directory の設定 153
拡張スキーマ Active Directory の概要 155
拡張スキーマ Active Directory の設定 157
Active Directory 設定のテスト 164
汎用 LDAP ユーザーの設定 165
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 165
RACADM を使用した汎用 LDAP ディレクトリサービスの設定 166
LDAP ディレクトリサービス設定のテスト 166

章 9: システム設定ロックダウン モード 167

章 10: 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 169
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 169
iDRAC のドメイン名システムへの登録 169
Active Directory オブジェクトの作成と権限の付与 170
Active Directory ユーザーのための iDRAC SSO ログインの設定 170
SSO 用の Active Directory でのユーザーの作成 170
Kerberos Keytab ファイルの生成 171
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 171
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 172
管理ステーションの設定 172
スマートカードログインの有効化または無効化 172

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 172
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 172
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 173
スマート カード ログインの設定 173
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 173
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 173
スマート カードを使用したログイン 174

章 11: アラートを送信するための iDRAC の設定 175
アラートの有効化または無効化 175
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 175
RACADM を使用したアラートの有効化または無効化 176
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 176
アラートのフィルタ 176
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 176
RACADM を使用したアラートのフィルタ 177
イベントアラートの設定 177
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 177
RACADM を使用したイベントアラートの設定 177
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 178
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 178
イベント処置の設定 178
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 178
RACADM を使用したイベントアクションの設定 178
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 179
電子メールアラートの設定 180
WS Eventing の設定 182
Redfish Eventing の設定 183
シャーシイベントの監視 183
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 183
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 184

章 12: iDRAC 9 グループ マネージャー 187
グループマネージャ 187
サマリビュー 188
ネットワーク設定の要件 189
ログインの管理 189
新規ユーザーの追加 189
ユーザーパスワードの変更 190
ユーザーの削除 190
アラートの設定 190
エクスポート 191
検出されたサーバビュー 191
Jobs (ジョブ) ビュー 192
ジョブのエクスポート 193
グループ情報パネル 193

グループ設定 193
選択したサーバでの操作 194
iDRAC グループのファームウェア アップデート 195

章 13: ログの管理 196
システムイベントログの表示 196
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 196
RACADM を使用したシステムイベントログの表示 196
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 197
Lifecycle ログの表示 197
ウェブインタフェースを使用した Lifecycle ログの表示 197
RACADM を使用した Lifecycle ログの表示 198
Lifecycle Controller ログのエクスポート 198
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 198
RACADM を使用した Lifecycle Controller ログのエクスポート 198
作業メモの追加 199
リモートシステムロギングの設定 199
ウェブインタフェースを使用したリモートシステムロギングの設定 199
RACADM を使用したリモートシステムロギングの設定 199

章 14: iDRAC での電源のモニタリングと管理 200
電力の監視 200
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 200
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 201
電力消費量の警告しきい値の設定 201
ウェブインタフェースを使用した電力消費量の警告しきい値の設定 201
電源制御操作の実行 201
ウェブインタフェースを使用した電源制御操作の実行 201
RACADM を使用した電源制御操作の実行 202
電力制限 202
ブレードサーバーの電源上限 202
電力上限ポリシーの表示と設定 202
電源装置オプションの設定 203
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 203
RACADM を使用した電源装置オプションの設定 204
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 204
電源ボタンの有効化または無効化 204
Multi-Vector Cooling 204

章 15: iDRAC ダイレクト アップデート 206

章 16: ネットワークデバイスのインベントリ、監視、および設定 207
ネットワークデバイスのインベントリと監視 207
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 207
RACADM を使用したネットワークデバイスの監視 207
接続ビュー 208
FC HBA デバイスのインベントリと監視 210
ウェブインタフェースを使用した FC HBA デバイスの監視 210

RACADM を使用した FC HBA デバイスの監視....210
SFP トランシーバー デバイスのインベントリーと監視....210
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....211
RACADM を使用した SFP トランシーバーの監視....211
テレメトリー ストリーミング....211
シリアル データ キャプチャ....212
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....213
I/O アイデンティティ最適化対応のカード....214
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....215
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....215
FlexAddress および IO アイデンティティに対するシステム動作....216
IO アイデンティティ最適化の有効化または無効化....217
SSD 摩耗しきい値....218
永続性ポリシーの設定....218

章 17: ストレージデバイスの管理....222
RAID の概念について....224
RAID とは....224
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....225
RAID レベルの選択....225
RAID レベルパフォーマンスの比較....231
対応コントローラ....232
対応エンクロージャ....233
ストレージデバイスの対応機能のサマリ....233
ストレージデバイスのインベントリと監視....238
Web インターフェイスを使用したストレージ デバイスの監視....238
RACADM を使用したストレージデバイスの監視....239
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....239
ストレージデバイスのトポロジの表示....239
物理ディスクの管理....239
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....240
物理ディスクの RAID または非 RAID モードへの変換....241
物理ディスクの消去....242
SED/ISE デバイス データの消去....242
物理ディスクの再構成....244
仮想ディスクの管理....244
仮想ディスクの作成....244
仮想ディスクキャッシュポリシーの編集....246
仮想ディスクの削除....247
仮想ディスク整合性のチェック....247
仮想ディスクの初期化....247
仮想ディスクの暗号化....248
専用ホットスペアの割り当てまたは割り当て解除....248
ウェブインタフェースを使用した仮想ディスクの管理....250
RACADM を使用した仮想ディスクの管理....251
RAID 設定機能....252
コントローラの管理....253
コントローラのプロパティの設定....253
外部設定のインポートまたは自動インポート....256

外部設定のクリア....257
コントローラ設定のリセット....258
コントローラモードの切り替え....258
12 Gbps SAS HBA アダプタの操作....260
ドライブに対する予測障害分析の監視....260
非 RAID モード（HBA モード）でのコントローラの操作....261
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....261
保持キャッシュの管理....261
PCIe SSD の管理....261
PCIe SSD のインベントリと監視....262
PCIe SSD の取り外しの準備....263
PCIe SSD デバイスデータの消去....264
エンクロージャまたはバックプレーンの管理....265
バックプレーンモードの設定....265
ユニバーサルスロットの表示....268
SGPIO モードの設定....269
エンクロージャ資産タグの設定....269
エンクロージャ資産名の設定....269
設定を適用する操作モードの選択....270
ウェブインタフェースを使用した操作モードの選択....270
RACADM を使用した操作モードの選択....270
保留中の操作の表示と適用....270
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....271
RACADM を使用した保留中の操作の表示と適用....271
ストレージデバイス — 操作適用のシナリオ....272
コンポーネント LED の点滅または点滅解除....273
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....273
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....273

章 18: BIOS 設定....274
BIOS ライブスキャン....275
BIOS のリカバリーとハードウェア Root of Trust（RoT）....276

章 19: 仮想コンソールの設定と使用....277
対応画面解像度とリフレッシュレート....278
仮想コンソールの設定....279
Web インターフェイスを使用した仮想コンソールの設定....279
RACADM を使用した仮想コンソールの設定....279
仮想コンソールのプレビュー....279
仮想コンソールの起動....279
Web インターフェイスを使用した仮想コンソールの起動....280
URL を使用した仮想コンソールの起動....280
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....281
仮想コンソールビューアの使用....281
eHTML5 ベースの仮想コンソール....281
HTML5 ベースの仮想コンソール....284
マウスポインタの同期....286
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....287

章 20: iDRAC サービスモジュールの使用 290
iDRAC サービスモジュールのインストール 290
iDRAC Express および Basic からの iDRAC サービスモジュールのインストール 290
iDRAC Enterprise からの iDRAC サービスモジュールのインストール 291
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 291
iDRAC サービスモジュール監視機能 291
iDRAC Web インターフェイスからの iDRAC サービス モジュールの使用 297
RACADM からの iDRAC サービスモジュールの使用 298

章 21: サーバー管理用 USB ポートの使用 299
直接 USB 接続を介した iDRAC インタフェースへのアクセス 299
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 300
USB 管理ポートの設定 300
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 301

章 22: Quick Sync 2 の使用 304
iDRAC Quick Sync 2 の設定 304
ウェブインタフェースを使用した iDRAC Quick Sync 2 の設定 305
RACADM を使用した iDRAC Quick Sync 2 の設定 305
iDRAC 設定ユーティリティを使用した iDRAC Quick Sync 2 の設定 305
モバイルデバイスを使用した iDRAC 情報の表示 305

章 23: 仮想メディアの管理 306
対応ドライブとデバイス 307
仮想メディアの設定 307
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 307
RACADM を使用した仮想メディアの設定 307
iDRAC 設定ユーティリティを使用した仮想メディアの設定 308
連結されたメディアの状態とシステムの応答 308
仮想メディアへのアクセス 308
仮想コンソールを使用した仮想メディアの起動 308
仮想コンソールを使用しない仮想メディアの起動 309
仮想メディアイメージの追加 309
仮想デバイスの詳細情報の表示 310
ドライバーへのアクセス 310
USB のリセット 310
仮想ドライブのマッピング 310
仮想ドライブのマッピング解除 311
BIOS を介した起動順序の設定 312
仮想メディアの一回限りの起動の有効化 312

章 24: vFlash SD カードの管理 313
vFlash SD カードの設定 313
vFlash SD カードプロパティの表示 313
vFlash 機能の有効化または無効化 314
vFlash SD カードの初期化 315
RACADM を使用した最後のステータスの取得 315
vFlash パーティションの管理 316

空のパーティションの作成 316
イメージファイルを使用したパーティションの作成 317
パーティションのフォーマット 318
使用可能なパーティションの表示 318
パーティションの変更 319
パーティションの連結または分離 320
既存のパーティションの削除 321
パーティション内容のダウンロード 321
パーティションからの起動 322

章 25: SMCLP の使用 323
SMCLP を使用したシステム管理機能 323
SMCLP コマンドの実行 323
iDRAC SMCLP 構文 324
MAP アドレス領域のナビゲーション 327
show 動詞の使用 327
-display オプションの使用 327
-level オプションの使用 327
-output オプションの使用 327
使用例 328
サーバー電源管理 328
SEL 管理 328
MAP ターゲットナビゲーション 329

章 26: オペレーティングシステムの導入 331
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 331
リモートファイル共有の管理 331
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 332
RACADM を使用したリモートファイル共有の設定 333
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 334
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 334
SD カードの内蔵オペレーティングシステムの導入 334
BIOS での SD モジュールと冗長性の有効化 334

章 27: 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 336
診断コンソールの使用 336
iDRAC のリセットと iDRAC のデフォルトへのリセット 336
自動リモート診断のスケジュール 337
RACADM を使用した自動リモート診断のスケジュール 337
Post コードの表示 338
起動キャプチャとクラッシュキャプチャビデオの表示 338
ビデオキャプチャの設定 338
ログの表示 339
前回のシステムクラッシュ画面の表示 339
システムステータスの表示 339
システムの前面パネル LCD ステータスの表示 339
システムの前面パネル LED ステータスの表示 340
ハードウェア問題の兆候 340
システム正常性の表示 340

サーバーステータス画面でのエラーメッセージの確認 341
iDRAC の再起動 341
iDRAC ウェブインタフェースを使用した iDRAC のリセット 341
RACADM を使用した iDRAC のリセット 341
システムおよびユーザーデータの消去 341
工場出荷時のデフォルト設定への iDRAC のリセット 342
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 342
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 342

章 28: iDRAC への SupportAssist の統合 343
SupportAssist 登録 343
サービスモジュールのインストール 344
サーバ OS プロキシ情報 344
SupportAssist 344
サービスリクエストポータル 344
収集ログ 344
SupportAssist コレクションの生成 344
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 345
設定 346
収集の設定 346
連絡先情報 346

章 29: よくあるお問い合わせ（FAQ） 347
システムイベントログ 347
iDRAC アラート用のカスタム送信者 E メールの設定 348
ネットワークセキュリティ 348
テレメトリー ストリーミング 348
Active Directory 349
シングルサインオン 350
スマートカードログイン 351
仮想コンソール 351
仮想メディア 354
vFlash SD カード 356
SNMP 認証 356
ストレージデバイス 357
GPU（アクセラレーター） 357
iDRAC サービスモジュール 357
RACADM 359
デフォルトのパスワードを永続的に calvin に設定する 360
その他 360

章 30: 使用事例シナリオ 366
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 366
システム情報の取得とシステム正常性の評価 366
アラートのセットアップと電子メールアラートの設定 367
システムイベントログと Lifecycle ログの表示とエクスポート 367
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 367
正常なシャットダウンの実行 367
新しい管理者ユーザーアカウントの作成 368

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 368
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 368
ラック密度の管理 368
新しい電子ライセンスのインストール 368
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 369

1

iDRAC の概要

Integrated Dell Remote Access Controller（iDRAC）は、サーバー管理者の生産性を向上させ、Dell EMC サーバーの総合的な可用性を高めるように設計されています。iDRAC は、システム問題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 ソリューションの一部であり、ビジネスに不可欠なアプリケーションと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 Dell EMC システムを導入、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 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。

- OpenManage Enterprise
- OpenManage Power Center プラグイン
- OpenManage Integration for VMware vCenter
- Dell Repository Manager

iDRAC には次のタイプが用意されています。

- iDRAC Basic — 100～500 シリーズのサーバー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、およびすべてのブ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—すべてのサーバー モジュールで使用可能

トピック：

- iDRAC を使用する利点
- 主な機能
- 追加された新機能
- 本ガイドの使用方法
- 対応ウェブブラウザ
- iDRAC ライセンス
- iDRAC9 のライセンス機能
- iDRAC にアクセスするためのインタフェースとプロトコル
- 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 を使用する利点

次のメリットが挙げられます。

- 可用性の向上 — サーバーの障害発生の防止または障害が発生してからのリカバリー時間の短縮に役立つように、障害発生の可能性または実際に障害が起きたときの早期通知を行います。
- 生産性の向上および総所有コスト（TCO）の削減 — 遠隔地に多数存在するサーバーへの管理者の管理範囲を拡大は、交通費などの運用コストを削減しながら IT スタッフの生産性を向上させることができます。
- セキュアな環境 — リモートサーバーへのセキュアなアクセスを提供することにより、管理者はサーバーおよびネットワークのセキュリティを維持しながら、重要な管理作業を行うことができます。
- Lifecycle Controller を使用した高度な組み込み型管理 — Lifecycle Controller は、ローカル導入の場合は Lifecycle Controller GUI を使用し、リモート導入の場合は 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）インターフェイスを使用して、導入および簡単な保守を行います。

Lifecycle Controller GUI の詳細については『*Lifecycle Controller ユーザーズ ガイド*』を、リモート サービスについては https://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。

主な機能

iDRAC の主要機能は次のとおりです。

メモ: 一部の機能は、iDRAC Enterprise または Datacenter ライセンスでのみ使用可能です。ライセンスで使用できる機能については、「iDRAC ライセンス 、p. 24」を参照してください。

インベントリと監視

- テレメトリー データ ストリーミング。
- 管理下サーバーの正常性の表示。
- オペレーティング システム エージェントなしでのネットワーク アダプターとストレージ サブシステム (PERC および Direct Attach Storage) のインベントリーおよび監視。
- システムインベントリの表示およびエクスポート。
- 温度、電圧、およびイントルージョンなどのセンサー情報の表示。
- CPU 状況、プロセッサ自動スロットル、および予測障害の監視。
- メモリ情報の表示。
- 電力消費の監視および制御。
- SNMPv3 get と alert のサポート。
- ブレード サーバーの場合：管理モジュール Web インターフェイスを起動し、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ソール接続を介して、iDRAC へのアクセスを提供します。詳細については、https://www.dell.com/cmcmanuals から入手可能な『*Chassis Management Controller ユーザーズ ガイド*』を参照してください。
- ホストオペレーティングシステムで使用可能なネットワークインタフェースを表示します。
- 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 アプリが設定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、https://www.dell.com/idracmanuals から入手可能な『*Lifecycle Controller リモート サービス クイック スタート ガイド*』を参照してください。
- 仮想アドレス、イニシエータ、およびストレージターゲットの永続性ポリシーを設定します。
- 実行時にシステムに接続されたストレージデバイスをリモートから設定します。
- ストレージデバイスに対して次の手順を実行します。
  - 物理ディスク：物理ディスクのグローバルホットスペアとしての割り当てまたは割り当て解除。
  - 仮想ディスク：
    - 仮想ディスクの作成。
    - 仮想ディスクキャッシュポリシーの編集。
    - 仮想ディスク整合性のチェック。
    - 仮想ディスクの初期化。
    - 仮想ディスクの暗号化。
    - 専用ホットスペアの割り当てまたは割り当て解除。
    - 仮想ディスクの削除。
  - コントローラ：
    - コントローラプロパティの設定。
    - 外部設定のインポートまたは自動インポート。
    - 外部設定のクリア。
    - コントローラ設定のリセット。
    - セキュリティキーの作成または変更。
  - PCIe SSD デバイス：
    - サーバー内の PCIe SSD デバイスの正常性のインベントリとリモート監視。
    - PCIe SSD の取り外し準備。

    - データのセキュア消去。
  - バックプレーンのモードの設定（統合モードまたは分割モード）。
  - コンポーネント LED の点滅または点滅解除。
  - デバイス設定の、即時、次回のシステム再起動時、もしくはスケジュールされた時間での適用、または単一ジョブの一部としてバッチ適用する保留中操作としての適用。

アップデート

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

メンテナンスとトラブルシューティング

- 電源関連の操作の実行および消費電力の監視。
- 温度設定の変更によるシステムパフォーマンスと電力消費の最適化。
- OpenManage Server Administrator に依存しないアラートの生成。
- イベントデータのログ：Lifecycle ログおよび RAC ログ。
- イベントおよび改善された電子メールアラート通知のための電子メールアラート、IPMI アラート、リモートシステムログ、WS Eventing ログ、Redfish イベント、および SNMP トラップ（v1、v2c、および v3）の設定。
- 前回のシステムクラッシュイメージのキャプチャ。
- 起動キャプチャビデオおよびクラッシュキャプチャビデオの表示。
- CPU、メモリー、I/O モジュールのパフォーマンス インデックスの帯域外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製。
  - システムの自動リカバリー オプション。
  - PSU を除くすべてのシステムコンポーネントのフルパワー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リセットする
  - インバンドでの 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。
- 次の方法による SupportAssist コレクションの生成：
  - 自動 — OS Collector ツールを自動で呼び出す iDRAC サービスモジュールを使用します。

iDRAC に関する Dell のベスト プラクティス

- Dell iDRAC は、個々の管理ネットワーク上に配置することを目的にしています。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は、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がセキュリティおよびその他のリスクにさらされる可能性が生じ、Dell はそのようなリスクに対して一切の責任を負いません。
- Dell EMC では、ラックおよびタワー 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、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 へのアクセスを承認されたサーバー管理者に限定する必要があります。

セキュアな接続

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

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

- スマートカードログイン機能を使用した 2 要素認証。2 要素認証は、物理的なスマートカードとスマートカードの PIN に基づいています。
- シングルサインオンおよび公開キー認証。
- 各ユーザーに特定の権限を設定するためのロール ベースの許可。
- iDRAC にローカルで保存されたユーザーアカウントの SNMPv3 認証。これを使用することが推奨されますが、デフォルトで無効になっています。
- ユーザー ID とパスワード設定。
- デフォルトログインパスワードの変更。
- セキュリティ向上のための単方向ハッシュ形式を使用したユーザーパスワードおよび BIOS パスワードの設定。
- FIPS 140-2 レベル 1 の機能。
- 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、仮想コンソール、仮想メディア向け)。
- 暗号化トランスポート層を使用してセキュリティを強化するセキュアシェル (SSH)。
- IP アドレスごとのログイン失敗回数の制限により、制限を超えた IP アドレスからのログインの阻止。
- iDRAC に接続するクライアントの IP アドレス範囲の限定。
- ラックおよびタワー型サーバーで使用可能の専用ギガビットイーサネットアダプタ (追加のハードウェアが必要となる場合あり)。

追加された新機能

このセクションでは、次に示すリリースで追加された新機能の一覧を示します。

- ファームウェア バージョン 4.30.30.30 、p. 20
- ファームウェア バージョン 4.20.20.20 、p. 21
- ファームウェア バージョン 4.10.10.10 、p. 22
- ファームウェア バージョン 4.00.00.00 、p. 22

メモ: リリース 4.00.00.00 以降では、SMCLP および VMCLI はサポートされていません。

ファームウェア バージョン 4.40.00.00

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。

- 仮想コンソールで enhanced HTML5 (eHTML5) 仮想 KVM 機能のサポートを追加
- eHTML5 仮想メディアのサポートを追加
- ストレージ GUI ページを改善
- PSU および SEP バックプレーンの直接アップデートのサポートを追加
- カスタム デフォルトのアップロードおよびカスタム デフォルトを使用した iDRAC のデフォルト設定へのリセットのサポートを追加
- 対応デバイスでのシステム ロックダウン モード サポートを改善

本リリースで追加されたその他の機能の一覧を次に示します。

- **自動化**
  - Redfish アップデートのサポート
- **監視/アラート/トラブルシューティング**
  - FPGA 監視
  - 履歴記録を含む SMART データ ログの機能拡張
  - 内蔵電圧センサーのレポート作成機能
  - 適用するためにサーバーの再起動を必要とするジョブ キュー エントリー (例 : BIOS アップデート) の実際の開始と完了に関する情報を報告
  - SupportAssist 収集での CPU のシリアル番号の指定
- **テレメトリー** (iDRAC Datacenter ライセンスが必要)
  - マルチクライアント サポート
  - 細分性の高い指標レポート オプション

- 利用可能な 193 個の指標定義のいずれかを使用して新しいカスタム MRD (指標レポート定義) を転記し、必要なレポート間隔 (MRD で繰り返し間隔と呼ばれる) を設定します。
- 1 つの MRD は、最大 68 個の指標定義 (指標 ID) を持つことができます。
- プロビジョニングを行い、最大 24 個の新しいカスタム MRD を作成します。これには、24 個の新しい指標レポートがあります。iDRAC は、最大 48 個の指標レポート (用意された 24 個とカスタムの 24 個) をサポートできます。

- **セキュリティ**
  - 自動証明書登録機能の拡張 (iDRAC Datacenter ライセンスが必要)
  - 2FA 用に iDRAC に RSA SecurID クライアントを統合 (iDRAC Datacenter ライセンスが必要)
  - 「ネットワーク デバイスによる NTP 認証が必須」という STIG 要件に準拠
  - Web サーバーからの Telnet および TLS 1.0 の削除
- **プラットフォーム機能のサポート**
  - BOSS 1.5 アップデート
  - Infiniband サポート

4.40.00.00 リリースでは、次の機能が iDRAC GUI の [ストレージ] ページに追加されています。

- ダッシュボードから、稼働状態の変更を解決するための推奨アクションを確認可能。
- ストレージの監視情報、ストレージ ハードウェアとソフトウェアのインベントリー、保留中および現在のストレージ ジョブのリスト、SEKM のタブが含まれるように [ストレージ] ページを変更。
  - ストレージ インベントリーから、すべてのストレージ関連のハードウェアとソフトウェアを検索可能。
  - 一元化された [保留中および現在のジョブ] タブでジョブをキューに登録して監視することが可能。
  - ストレージ ページを使用して、SEKM を構成可能。
- ストレージ デバイスを監視する場合は、各デバイス テーブルに表示される列をカスタマイズ可能。列のカスタマイズが保存されてユーザー セッション間で保持される。
- 各デバイス ページに表示される新しい基本および詳細フィルターを使用して、表示されるオブジェクトのリストを簡単かつ効率的にカスタマイズ可能。
- ストレージ構成ウィザードで、仮想ディスクを作成するために「基本」と「詳細」の 2 つのオプションを用意。
  - 基本仮想ディスク ウィザードでは、使用可能な RAID 構成のリストから VD を迅速に作成可能。iDRAC は、自動的に仮想ディスクのデフォルト値を設定して、プロセスを合理化。
  - 仮想ディスクの詳細設定ウィザードでは VD のすべての詳細を選択可能で、仮想ディスクに対して新しいボリュームを作成または既存のボリュームを選択可能。
- 各デバイス ページで、関連するデバイスを表示またはグループ操作を実行できる新しいグローバル処置が使用可能。
  - 例えば、物理ディスクを選択して、点滅、点滅解除、および仮想ディスクの作成などのグループ操作を実行することができます。
  - また、画面から移動せずにドライブを選択することによって、物理ディスクのインベントリーを表示し、仮想ディスクを作成することもできます。
- 数値の代わりに、物理ディスクのサイズが可視化されたデータとして表示され、スケールに値が表示されます。
  - これにより、ドライブ上の使用済み領域と使用可能な容量がわかります。
- ディスクはさまざまな物理ディスクのプロパティに基づいてフィルタリングできます。
  - フィルタリング プロパティが表示されるため、ユーザーは現在適用されているフィルタリングを知ることができます。

ファームウェア バージョン 4.30.30.30

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。

- AMD システム向け PERC 11 のサポートを追加
- PERC 11 の背後の NVMe ドライブのサポートを追加
- AMD システム向け HBA11 のサポートを追加
- AMD システム向け CUPS のサポートを追加
- Boot Optimized ストレージ ソリューション 1.5 (BOSS1.5/BOSS-S2) のサポートを追加
- BOSS 1.5 セキュア ファームウェア アップデートのサポートを追加
- 新しい Matrox ビデオ ドライバーのサポートを追加
- NVMe Opal SED のサポートを追加
- 信頼できるセキュア ブートの HW チェーンのサポートを追加
- Mellanox CX6 向け InfiniBand アダプターのサポートを追加
- PowerEdge C6525 向け 24x NVMe バックプレーンのサポートを追加

- 新しい Matrox ビデオ ドライバーのサポートを追加
- iDRAC に Starlord（ConnectX-6 Dx 100GbE）のサポートを追加
- BOSS-S2/PERC 11/HBA 11 に対する FQDD 関連の変更を追加
- バックプレーンなしのストレージ デバイス（M.2、U.2 など）のサポートを追加
- NVMe ドライブ向け Secure Enterprise Key Management（SEKM）のサポートを追加
- 拡張 iDRAC メモリー（512MB～1024MB）
- 認証が無効になっているときに送信が失敗した E メールの RESTUI の変更

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 Dell パーツ ナンバー JTK7F（Broadcom）のサポート
- （4x10/25）MX Mezz、Dell パーツ 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））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のサポート。

その他

- 1 台以上のスレッドを搭載した C6420 シャーシでの電源オン時の温度センサー ボードのケーブル検出のサポート。
- SLED GUI での 6420 のスロット番号表示のサポート。
- AC 喪失またはグローバル リセット時の ADR フロー用に、AEP および BPS メモリーの常時待機をサポート。
- 10 x 2.5 インチ BP/シャーシ パーツ ナンバーの変更のサポート。
- SEL ログでの「Unsupported Config」の有効化のサポート。

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 のリカバリーと 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 : ストレージ ドライブ
- システム シリアル データ バッファー キャプチャ
- 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 マネージャー : 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 に出力を表示
- **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ーツ ナンバーを含む
- **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 バナー
  - 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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』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のオンラインヘルプ*を参照してください。iDRAC 設定 GUI (起動中に <F2> を押し、**システムセットアップメインメニュー** ページで **iDRAC 設定** をクリック) で **ヘルプ** をクリックするとアクセスできます。
- Redfish — 本書では、タスク関連情報のみが記載されています。フィールドやオプションの詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC Redfish API ガイド*』を参照してください。

対応ウェブブラウザ

iDRAC は、以下のブラウザでサポートされています。

- Internet Explorer/Edge
- Mozilla Firefox
- Google Chrome
- Safari

対応バージョンのリストについては、https://www.dell.com/idracmanuals から入手可能な『*iDRAC リリース ノート*』を参照してください。

サポートされる OS とハイパーバイザ

iDRAC は、ハイパーバイザの以下の 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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC リリース ノート*』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 Secure Enterprise Key Management (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、「iDRAC9 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。提供されるアップセル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、次のシステムで使用可能なデフォルト ライセンスのリストです。

iDRAC Basic ライセンス	iDRAC Express ライセンス	iDRAC Enterprise ライセンス	iDRAC Datacenter ライセンス
PowerEdge ラック/タワー型サーバー シリーズ 100 ~ 500	• PowerEdge C41XX • PowerEdge FC6XX • PowerEdge R6XX • PowerEdge R64XX • PowerEdge R7XX • PowerEdge R74XXd • PowerEdge R74XX • PowerEdge R8XX • PowerEdge R9XX • PowerEdge R9XX • PowerEdge T6XX • Dell Precision Rack R7920	全プラットフォーム、アップグレード オプション付き	全プラットフォーム、アップグレード オプション付き

表 1. デフォルトライセンス

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

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 BMC です。BMC 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。

メモ: 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。

メモ: 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、[**製品登録**] タブに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。

メモ: 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。

メモ: 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。

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

一対一のライセンス管理には 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。

  メモ: 工場出荷時にインストールされたライセンスをエクスポートすることはできますが、インポートすることはできません。このライセンスをインポートするには、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。

  メモ: 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 Web インターフェイ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。

メモ: 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済み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、https://www.dell.com/esmmanuals から入手可能な『*Dell License Manager ユーザーズ ガイド*』を参照してください。

以下は、異なるライセンス操作に対するユーザー権限の要件です。

- ライセンスの表示とエクスポート：ログイン権限。
- ライセンスのインポートと削除：ログイン権限、iDRAC 設定権限、およびサーバー制御権限。

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（https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』）。

iDRAC9 のライセンス機能

次の表は、購入したライセンスに応じて有効になる iDRAC9 機能のリストです。

表 2. iDRAC9 のライセンス機能

特長	iDRAC9 Basic	iDRAC9 Express	iDRAC9 Express（ブレード用）	iDRAC9 Enterprise	iDRAC9 Datacenter
インタフェース / 標準					
iDRAC RESTful API および Redfish	はい	はい	はい	はい	はい
IPMI 2.0	はい	はい	はい	はい	はい
DCMI 1.5	はい	はい	はい	はい	はい
Web ベースの GUI	はい	はい	はい	はい	はい
RACADM コマンドライン（ローカル / リモート）	はい	はい	はい	はい	はい
SSH	はい	はい	はい	はい	はい
シリアルリダイレクト	はい	はい	はい	はい	はい
WSMan	はい	はい	はい	はい	はい
ネットワークタイムプロトコル	いいえ	はい	はい	はい	はい
接続性					
共有 NIC（LOM）	はい	はい	該当なし	はい	はい
専用 NIC	はい	はい	はい	はい	はい
VLAN タグ付け	はい	はい	はい	はい	はい
IPv4	はい	はい	はい	はい	はい

表 2. iDRAC9 のライセンス機能（続き）

特長	iDRAC9 Basic	iDRAC9 Express	iDRAC9 Express（ブレード用）	iDRAC9 Enterprise	iDRAC9 Datacenter
IPv6	はい	はい	はい	はい	はい
DHCP	はい	はい	はい	はい	はい
ゼロタッチ対応 DHCP	いいえ	いいえ	いいえ	はい	はい
ダイナミック DNS	はい	はい	はい	はい	はい
OS パススルー	はい	はい	はい	はい	はい
iDRAC ダイレクト - 前面パネル USB	はい	はい	はい	はい	はい
接続ビュー	はい	はい	いいえ	はい	はい
セキュリティ					
ロール ベースの権限	はい	はい	はい	はい	はい
ローカルユーザー	はい	はい	はい	はい	はい
SSL 暗号化	はい	はい	はい	はい	はい
Secure Enterprise Key Manager	いいえ	いいえ	いいえ	はい（SEKM ライセンスあり）	はい(SEKM ライセンスあり）
IP ブロック	いいえ	はい	はい	はい	はい
ディレクトリサービス（AD、LDAP）	いいえ	いいえ	いいえ	はい	はい
2 要素認証（スマートカード）	いいえ	いいえ	いいえ	はい	はい
シングルサインオン	いいえ	いいえ	いいえ	はい	はい
PK 認証（SSH 用）	いいえ	はい	はい	はい	はい
FIPS 140-2	はい	はい	はい	はい	はい
セキュア UEFI Boot - 証明書管理	はい	はい	はい	はい	はい
ロックダウンモード	いいえ	いいえ	いいえ	はい	はい
固有の iDRAC デフォルトパスワード	はい	はい	はい	はい	はい
カスタマイズ可能なセキュリティポリシーバナー - ログインページ	はい	はい	はい	はい	はい
容易な多要素認証	いいえ	いいえ	いいえ	いいえ	はい
証明書の自動登録（SSL 証明書）	いいえ	いいえ	いいえ	いいえ	はい
iDRAC Quick Sync 2 - 読み取り動作用のオプションの認証	はい	はい	はい	はい	はい
iDRAC Quick Sync 2 - モバイルデバイス番号を LCL に追加	はい	はい	はい	はい	はい
内蔵ストレージ デバイスのシステム消去	はい	はい	はい	はい	はい
リモートプレゼンス					

表 2. iDRAC9 のライセンス機能（続き）

特長	iDRAC9 Basic	iDRAC9 Express	iDRAC9 Express（ブレード用）	iDRAC9 Enterprise	iDRAC9 Datacenter
電源ボタン	はい	はい	はい	はい	はい
起動制御	はい	はい	はい	はい	はい
シリアルオーバー LAN	はい	はい	はい	はい	はい
仮想メディア	いいえ	いいえ	はい	はい	はい
仮想フォルダ	いいえ	いいえ	いいえ	はい	はい
リモートファイル共有	いいえ	いいえ	いいえ	はい	はい
仮想コンソールへの HTML5 アクセス	いいえ	いいえ	はい	はい	はい
仮想コンソール	いいえ	いいえ	はい	はい	はい
OS への VNC 接続	いいえ	いいえ	いいえ	はい	はい
品質 / 帯域幅制御	いいえ	いいえ	いいえ	はい	はい
仮想コンソール連携機能（最大 6 人の同時ユーザー）	いいえ	いいえ	いいえ（1 人のユーザーのみ）	はい	はい
仮想コンソールチャット	いいえ	いいえ	いいえ	はい	はい
仮想フラッシュパーティション	いいえ	いいえ	いいえ	はい	はい
メモ: vFlash は、PowerEdge Rx5xx/Cx5xx 用の iDRAC9 では使用できません。					
グループマネージャ	いいえ	いいえ	いいえ	はい	はい
NFS/CIFS と共に HTTP/HTTPS をサポート	はい	はい	はい	はい	はい
電力および温度					
リアルタイム電力メーター	はい	はい	はい	はい	はい
電力しきい値および警告	いいえ	はい	はい	はい	はい
リアルタイムの電源グラフ	いいえ	はい	はい	はい	はい
電力カウンタ履歴	いいえ	はい	はい	はい	はい
電力制限	いいえ	いいえ	いいえ	はい	はい
Power Center 統合	いいえ	いいえ	いいえ	はい	はい
温度監視	はい	はい	はい	はい	はい
温度グラフ	いいえ	はい	はい	はい	はい
PCIe エアフローのカスタマイズ（LFM）	いいえ	いいえ	いいえ	いいえ	はい
排気のカスタム制御	いいえ	いいえ	いいえ	いいえ	はい
Delta-T のカスタム制御	いいえ	いいえ	いいえ	いいえ	はい
システム エアフロー消費量	いいえ	いいえ	いいえ	いいえ	はい
カスタム PCIe 吸気温度	いいえ	いいえ	いいえ	いいえ	はい

表 2. iDRAC9 のライセンス機能（続き）

特長	iDRAC9 Basic	iDRAC9 Express	iDRAC9 Express（ブレード用）	iDRAC9 Enterprise	iDRAC9 Datacenter
正常性監視					
完全なエージェントフリーの監視	はい	はい	はい	はい	はい
障害の予測監視	はい	はい	はい	はい	はい
SNMPv1、v2、および v3（トラップおよび取得）	はい	はい	はい	はい	はい
電子メール警告	いいえ	はい	はい	はい	はい
設定可能なしきい値	はい	はい	はい	はい	はい
ファン監視	はい	はい	はい	はい	はい
電源装置監視	はい	はい	はい	はい	はい
メモリ監視	はい	はい	はい	はい	はい
CPU 監視	はい	はい	はい	はい	はい
RAID 監視	はい	はい	はい	はい	はい
NIC 監視	はい	はい	はい	はい	はい
HD 監視（エンクロージャ）	はい	はい	はい	はい	はい
帯域外パフォーマンス監視	いいえ	いいえ	いいえ	はい	はい
過剰な SSD 摩耗に対する警告	はい	はい	はい	はい	はい
カスタマイズ可能な排気温度設定	はい	はい	はい	はい	はい
シリアル コンソール ログ	いいえ	いいえ	いいえ	いいえ	はい
ストレージ ドライブの SMART ログ	いいえ	いいえ	いいえ	いいえ	はい
アイドル サーバーの検出	いいえ	いいえ	いいえ	いいえ	はい
テレメトリー ストリーミング	いいえ	いいえ	いいえ	いいえ	はい
メモ: OpenManage Enterprise Advanced ライセンスと PowerManage プラグイン サポート テレメトリー データは、iDRAC から取得することができます。					
アップデート					
リモートでのエージェントフリー アップデート	はい	はい	はい	はい	はい
組み込みアップデートツール	はい	はい	はい	はい	はい

表 2. iDRAC9 のライセンス機能（続き）

特長	iDRAC9 Basic	iDRAC9 Express	iDRAC9 Express（ブレード用）	iDRAC9 Enterprise	iDRAC9 Datacenter
リポジトリーからのアップデート（自動アップデート）	いいえ	いいえ	いいえ	はい	はい
リポジトリーからアップデートをスケジュール	いいえ	いいえ	いいえ	はい	はい
PSU ファームウェアアップデートの改良	はい	はい	はい	はい	はい
展開と設定					
F10 を使用したローカル設定	はい	はい	はい	はい	はい
組み込み OS 導入ツール	はい	はい	はい	はい	はい
組み込み設定ツール	はい	はい	はい	はい	はい
自動検出	いいえ	はい	はい	はい	はい
リモートでの OS 導入	いいえ	はい	はい	はい	はい
組み込みドライバパック	はい	はい	はい	はい	はい
完全な設定インベントリ	はい	はい	はい	はい	はい
インベントリエクスポート	はい	はい	はい	はい	はい
リモート設定	はい	はい	はい	はい	はい
ゼロタッチ設定	いいえ	いいえ	いいえ	はい	はい
システムの廃棄 / 転用	はい	はい	はい	はい	はい
GUI でのサーバ設定プロファイル	はい	はい	はい	はい	はい
BIOS 設定を iDRAC GUI に追加	はい	はい	はい	はい	はい
診断、サービス、およびログ					
組み込み診断ツール	はい	はい	はい	はい	はい
部品交換	いいえ	はい	はい	はい	はい
メモ: RAID ハードウェアのパーツ交換を実行した後、ファームウェアと設定の交換プロセスが完了すると、Lifecycle ログにパーツ交換エントリーが二重にレポートされます。これは予期される動作です。					
簡単な復元（システム設定）	はい	はい	はい	はい	はい
簡単な復元の自動タイムアウト	はい	はい	はい	はい	はい
メモ: サーバーのバックアップおよび復元機能は、PowerEdge Rx5xx/Cx5xx 用の iDRAC9 では使用できません。					

表 2. iDRAC9 のライセンス機能（続き）

特長	iDRAC9 Basic	iDRAC9 Express	iDRAC9 Express（ブレード用）	iDRAC9 Enterprise	iDRAC9 Datacenter
LED 正常性状態インジケータ	はい	はい	該当なし	はい	はい
LCD 画面（iDRAC9 でオプションが必要）	はい	はい	該当なし	はい	はい
iDRAC Quick Sync 2（BLE/Wi-Fi ハードウェア）	はい	はい	はい	はい	はい
iDRAC ダイレクト（前面 USB 管理ポート）	はい	はい	はい	はい	はい
iDRAC サービスモジュール（iSM）内蔵	はい	はい	はい	はい	はい
コンソールへインバンドアラートを転送する iSM 機能	はい	はい	はい	はい	はい
SupportAssist コレクション（内蔵）	はい	はい	はい	はい	はい
クラッシュ画面キャプチャ	いいえ	はい	はい	はい	はい
クラッシュビデオキャプチャ [1]	いいえ	いいえ	いいえ	はい	はい
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）	いいえ	いいえ	いいえ	いいえ	はい
起動キャプチャ	いいえ	いいえ	いいえ	はい	はい
iDRAC の手動リセット（LCD ID ボタン）	はい	はい	はい	はい	はい
iDRAC のリモートリセット（iSM が必要）	はい	はい	はい	はい	はい
仮想 NMI	はい	はい	はい	はい	はい
OS ウォッチドッグ	はい	はい	はい	はい	はい
システムイベントログ	はい	はい	はい	はい	はい
Lifecycle ログ	はい	はい	はい	はい	はい
Lifecycle Controller ログの拡張ログ	はい	はい	はい	はい	はい
作業メモ	はい	はい	はい	はい	はい
リモート Syslog	いいえ	いいえ	いいえ	はい	はい
ライセンス管理	はい	はい	はい	はい	はい
カスタマー エクスペリエンスの向上					

表 2. iDRAC9 のライセンス機能（続き）

特長	iDRAC9 Basic	iDRAC9 Express	iDRAC9 Express（ブレード用）	iDRAC9 Enterprise	iDRAC9 Datacenter
iDRAC - 高速プロセッサ、大容量メモリ	該当なし	はい	該当なし	はい	はい
HTML5 でレンダリングされた GUI	該当なし	はい	該当なし	はい	はい
BIOS 設定を iDRAC GUI に追加	該当なし	はい	該当なし	はい	はい

[1] ターゲット サーバーに iSM または OMSA エージェントが必要です。

iDRAC にアクセスするためのインタフェースとプロトコル

次の表は、iDRAC にアクセスするためのインタフェースのリストです。

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

表 3. iDRAC にアクセスするためのインタフェースとプロトコル

インタフェースまたはプロトコル	説明
iDRAC 設定ユーティリティ（F2）	iDRAC 設定ユーティリティを使用して、プレオペレーティングシステム処理を実行します。iDRAC 設定ユーティリティーには、他の機能とともに iDRAC Web インターフェイスで使用可能な機能のサブセットが含まれます。 iDRAC 設定ユーティリティーにアクセスするには、起動中に<F2>を押し、**システム セットアップ メイン メニュー**ページで **iDRAC 設定**をクリックします。
Lifecycle Controller（F10）	iDRAC の設定には Lifecycle Controller を使用します。Lifecycle Controller にアクセスするには、起動中に <F10> を押し、**セットアップユーティリティ** > **ハードウェア詳細設定** > **iDRAC 設定** の順に選択します。詳細に関しては、*dell.com/support/idracmanuals* にある『**Lifecycle Controller ユーザーズ ガイド**』を参照してください。
iDRAC Web インターフェイス	iDRAC Web インターフェイスを使用して、iDRAC を管理し、管理対象のシステムをモニターします。ブラウザーは、HTTPS ポートを介して Web サーバーに接続します。データストリームは 128 ビット SSL を使用して暗号化され、プライバシーと整合性を提供します。HTTP ポートへの接続は、いずれも 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、Web サーバー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ー権限に基づきます。
OpenManage Enterprise（OME）Modular Web インターフェイス	**メモ:** このインターフェイスは、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 インターフェイ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 Web インターフェイスへのログイン ● 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、https://www.dell.com/openmanagemanuals から入手可能な『*PowerEdge MX7000 シャーシ向け OME - Modular ユーザーズ ガイド*』を参照してください。
CMC Web インターフェイス	**メモ:** このインターフェイスは、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 インターフェイスでは次の操作が可能です。

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

インタフェースまたはプロトコル	説明
	• 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 Web インターフェイスへのログイン • 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
サーバー LCD パネル / シャーシ LCD パネル	サーバー前面パネルの LCD を使用して、次の操作を行うことができます。 • アラート、iDRAC IP または MAC アドレス、ユーザーによるプログラムが可能な文字列の表示 • DHCP の設定 • iDRAC 静的 IP 設定の設定 ブレードサーバーでは、LCD はシャーシの前面パネルにあり、すべてのブレード間で共有されています。 サーバーを再起動しないで iDRAC をリセットするには、システム識別ボタンを 16 秒間押し続けます。 **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。ブレードサーバーでは、LCD はシャーシの前面パネルにあり、すべてのブレード間で共有されています。
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、インバンド IPMI ホストインターフェイスを介して 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にインストールされているため、実行するには、ユーザーはオペレーティングシステムにログインする必要があります。このユーティリティを使用するユーザーは、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 インターフェイスを使用し、HTTPs チャネルも使用します。**–r** オプションは、ネットワークで RACADM コマンドを実行します。 • ファームウェア RACADM には、SSH 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せずにファームウェア 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 プロンプトの起動後、racadm プレフィックスを付けずに直接コマンドを実行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ブ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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC Redfish API ガイド*』を参照してください。
WSMan	LC-Remote Service 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。LC-Remote Services 機能を使用するには、WinRM クライアント (Windows) や OpenWSMan クライアント

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

インタフェースまたはプロトコル	説明
	（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。 Web Services for Management（WSMan）は、Simple Object Access Protocol（SOAP）ベースのシステム管理用に使用されるプロトコルです。iDRAC は WSMan を使用して、Distributed Management Task Force（DMTF）の共通情報モデル（CIM）ベースの管理情報を伝達します。CIM の情報は、管理下システムで変更可能なセマンティックや情報の種類を定義します。WSMan で使用できるデータは、DMTF プロファイルおよび拡張プロファイルにマッピングされている、iDRAC 計装インタフェースによって提供されます。 詳細については、次の文書を参照してください。 ● https://www.dell.com/idracmanuals から入手可能な『*Lifecycle Controller リモート サービス クイック スタート ガイド*』 ● Dell EMC ナレッジベースサイトの Lifecycle Controller ページ — www.dell.com/support/article/sln311809/ ● MOF およびプロファイル — http://downloads.dell.com/wsman ● DMTF Web サイト — dmtf.org/standards/profiles/
SSH	SSH を使用して RACADM コマンドを実行します。デフォルトでは、SSH サービスは iDRAC 上で有効になっています。SSH サービスは iDRAC で無効にできます。iDRAC は、RSA ホストキーアルゴリズムを使用する SSH バージョン 2 のみをサポートします。iDRAC を最初に起動する際、一意の 1024 ビット RSA ホストキーが生成されます。
IPMITool	IPMITool を使用して、iDRAC 経由でリモートシステムの基本管理機能にアクセスします。インタフェースには、ローカル IPMI、IPMI over LAN、IPMI オーバーシリアル、シリアルオーバー LAN が含まれます。IPMITool の詳細については、dell.com/idracmanuals にある『*Dell OpenManage ベースボード マネジメント コントローラー ユーティリティー ユーザーズ ガイド*』を参照してください。 **メモ:** IPMI バージョン 1.5 はサポートされていません。
NTLM	iDRAC によって、NTLM がユーザーへの認証、整合性、機密性を提供できるようになります。NT LAN Manager（**NTLM**）は Microsoft セキュリティプロトコルのスイートで、Windows ネットワークで動作します。
SMB	iDRAC9 は、Server Message Block（SMB）プロトコルをサポートします。これはネットワークファイル共有プロトコルで、デフォルトでサポートされる SMB の最小バージョンは 2.0 です。SMBv1 はサポートされなくなりました。
NFS	iDRAC9 は、**ネットワークファイルシステム**（**NFS**）をサポートしています。これは分散ファイルシステムプロトコルで、これによりユーザーは、サーバ上にリモートディレクトリを**マウント**できるようになります。

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. 99 を参照してください。

表 4. iDRAC が接続についてリッスンするポート

ポート番号	タイプ	機能	設定可能なポート	最大暗号化レベル
22	TCP	SSH	はい	256 ビット SSL
80	TCP	HTTP	はい	なし
161	UDP	SNMP エージェント	はい	なし
443	TCP	● HTTPS による Web GUI アクセス	はい	256 ビット SSL

表 4. iDRAC が接続についてリッスンするポート（続き）

ポート番号	タイプ	機能	設定可能なポート	最大暗号化レベル
		• 仮想コンソールおよび仮想メディアの eHTML5 オプション • Web サーバーのリダイレクトが有効になっている場合の、仮想コンソールおよび仮想メディアの HTML5 オプション		
623	UDP	RMCP/RMCP+	いいえ	128 ビット SSL
5000	TCP	iDRAC から iSM	いいえ	256 ビット SSL
メモ: 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。				
5900	TCP	仮想コンソールおよび仮想メディアの HTML5、Java、および ActiveX オプション	はい	128 ビット SSL
5901	TCP	VNC	はい	128 ビット SSL
メモ: 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

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

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* には 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 設定ツールユーザーズガイド*』には、ツールを使用してネットワーク内の iDRAC IP アドレスを検出し、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 システムソフトウェアサポートマトリックス*』は、各種 Dell システム、これらのシステムでサポートされているオペレーティングシステム、これらのシステムにインストールできる Dell OpenManage コンポーネントについて説明しています。
- 『*iDRAC サービスモジュールユーザーズガイド*』では、iDRAC サービスモジュールをインストールするための情報が記載されています。
- 『*Dell OpenManage Server Administrator インストールガイド*』では、Dell OpenManage Server Administrator のインストール手順が説明されています。
- 『*Dell OpenManage Management Station Software インストールガイド*』では、Dell OpenManage Management Station Software(ベースボード管理ユーティリティ、DRAC ツール、Active Directory スナップインを含む) のインストール手順が説明されています。
- 『*Dell OpenManage Baseboard Management Controller Management ユーティリティユーザーズガイド*』には、IPMI インタフェースに関する情報が記載されています。
- 『*リリースノート*』は、システム、マニュアルへの最新アップデート、または専門知識をお持ちのユーザーや技術者向けの高度な技術資料を提供します。

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「安全にお使いただくために」には安全や規制に関する重要な情報が記載されています。規制に関する詳細な情報については、**dell.com/regulatory_compliance** にある法規制の順守ホームページを参照してください。保証に関する情報は、このマニュアルに含まれているか、別の文書として同梱されています。
- ラックソリューションに付属の『*ラック取り付けガイド*』では、システムをラックに取り付ける方法について説明しています。
- *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の方法について説明しています。

デルへのお問い合わせ

メモ: アクティブなインターネット接続がない場合は、 ご購入時の納品書、出荷伝票、請求書、またはデル製品カタログで連絡先をご確認いただけます。

デルでは、オンラインおよび電話によるサポートとサービスオプションをいくつかご用意しています。これらのサービスは国および製品によって異なり、お住まいの地域では一部のサービスがご利用いただけない場合があります。Dell のセールス、テクニカルサポート、カスタマーサービスに問い合わせる場合は、https://www.dell.com/support/contents/ja-jp/article/contact-information/international-support-services/international-contact-center にアクセスしてください。

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。
  - すべてのエンタープライズシステム管理および OpenManage Connections のドキュメント - https://www.dell.com/esmmanuals
  - OpenManage のマニュアル - https://www.dell.com/openmanagemanuals
  - iDRAC および Lifecycle Controller のマニュアル - https://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 - https://www.dell.com/omconnectionsclient

製品の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します...**検索ボックスで、製品名を入力します。たとえば、**PowerEdge** または **iDRAC**。

   一致した製品のリストが表示されます。
3. お使いの製品を選択し、検索アイコンをクリックするか、Enter を押します。
4. **文書**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。

製品の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することによっ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. サーバー、ソフトウェア、ストレージなどの目的の製品カテゴリをクリックします。
4. 対象の製品をクリックし、必要に応じて目的のバージョンをクリックします。

   メモ: 一部の製品では、サブカテゴリを順次確認する必要があります。
5. **文書**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。

2

iDRAC へのログイン

iDRAC には、iDRAC ユーザー、Microsoft Active Directory ユーザー、または 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。この一意のパスワードが、iDRAC とお使いのサーバのセキュリティを強化します。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、「ユーザー名およびパスワードで推奨される文字 、p. 147」を参照してください。

デフォルトのパスワードを変更するには、「デフォルト ログイン パスワードの変更 、p. 47」を参照してください。

カスタマイズ可能なセキュリティバナー

ログインページに表示されるセキュリティ通知をカスタマイズできます。通知のカスタマイズには、SSH、RACADM、Redfish、WSMan を使用できます。使用する言語に応じて、通知は 1024 または 512 UTF-8 文字長になります。

OpenID 接続

メモ: この機能は、MX プラットフォームの場合のみ使用できます。

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、ドライバーとダウンロード、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
- 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
- シングルサインオンを使用した iDRAC へのログイン
- リモート RACADM を使用した iDRAC へのアクセス
- ローカル RACADM を使用した iDRAC へのアクセス
- ファームウェア RACADM を使用した iDRAC へのアクセス
- シンプルな 2 要素認証 (シンプル 2FA)
- RSA SecurID 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
- セキュアなデフォルトパスワード
- デフォルト ログイン パスワードの変更
- デフォルトパスワード警告メッセージの有効化または無効化
- パスワード強度ポリシー
- IP ブロック
- 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
- RACADM を使用したアラートの有効化または無効化

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に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 マネージャーでメンバー 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。
   ログイン 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。
   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。

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

Web インターフェイスを使用して iDRAC にログインする前に、サポートされている Web ブラウザーが設定されており、必要な権限を持つユーザー アカウントが作成されていることを確認してください。

メモ: Active Directory ユーザーのユーザー名では、大文字と小文字は区別されません。すべてのユーザーのパスワードでは、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 を使用した LDAP 認証がサポートされています。DH キーは 768 ビットより大きい必要があります。

メモ: LDAP ユーザーに対して RSA 機能を設定して有効にすることができますが、LDAP が Microsoft Active Directory 上で設定されている場合、RSA はサポートされません。したがって、LDAP ユーザーのログインは失敗します。RSA は OpenLDAP に対してのみサポートされています。

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

1. サポートされている Web ブラウザーを開きます。
2. **アドレス**フィールドに「`https://[iDRAC-IP-address]`」と入力し、Enter を押します。

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

   ログイン ページが表示されます。
3. ローカルユーザーの場合は、次の手順を実行します。
   - **ユーザー名** フィールドと **パスワード** フィールドに、iDRAC ユーザーの名前とパスワードを入力します。
   - **ドメイン** ドロップダウンメニューから、**この iDRAC** を選択します。
4. Active Directory ユーザーの場合は、**ユーザー名**フィールドと**パスワード**フィールドに、Active Directory 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た場合は、ドロップダウン メニューで**この iDRAC** を選択します。ユーザー名の形式は、< ドメイン >\< ユーザー名 >、< ドメイン >/< ユーザー名 >、または < ユーザー > @< ドメイン > のいずれかです。

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

   ユーザー名にドメインが指定されていない場合は、**ドメイン** ドロップダウンメニューから Active Directory ドメインを選択します。
5. LDAP ユーザーの場合は、**ユーザー名**フィールドと**パスワード**フィールドに、LDAP のユーザー名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。ドロップダウン メニューではデフォルトで**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、次を実行する必要があります。

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

iDRAC Web インターフェイスは、スマート カードを使用するように設定されているユーザーのスマート カード ログオン ページを表示します。

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

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

1. `https://[IP address]`リンクを使用して iDRAC Web インターフェイスにアクセスします。

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

   メモ: デフォルトの HTTPS ポート番号 (ポート 443) が変更された場合は、`https://[IP address]:[port number]` と入力します。ここで、`[IP address]`は iDRAC の IP アドレスで、`[port number]`は HTTPS ポート番号です。
2. スマート カードをリーダーに挿入して**ログイン**をクリックします。
   スマート カードの PIN の入力を求める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。

メモ: **スマート カード ログオンの CRL チェックを有効にする**がオンになっているローカル ユーザーの場合、iDRAC は、証明書失効リスト（CRL）をダウンロードして、CRL でユーザーの証明書を確認します。CRL で証明書が失効していると記載されているか、何らかの理由で CRL をダウンロードできない場合、ログインは失敗します。

メモ: RSA が有効になっているときにスマート カードを使用して iDRAC にログインした場合、RSA トークンはバイパスされ、直接ログインできます。

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。

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

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

1. リンク `https://[IP address]` を使用して iDRAC にログインします。
   iDRAC ログイン ページが表示され、スマートカードを挿入するよう求められます。
   メモ: デフォルトの HTTPS ポート番号（ポート 443）が変更されている場合は、`https://[IP address]:[port number]` と入力します。ここで、`[IP address]` は iDRAC IP アドレスであり、`[port number]` は HTTPS ポート番号です。
2. スマートカードを挿入し、**ログイン** をクリックします。
   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。

メモ: RSA が有効化されている間に AD ユーザーが SSO を構成すると、RSA トークンはバイパスされ、ユーザーは直接ログインします。

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

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

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

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

1. Active Directory の有効なアカウントを使って管理ステーションにログインします。
2. 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表示になります。

詳細については、https://www.dell.com/cmcmanuals から入手可能な『*Chassis Management Controller ユーザーズ ガイド*』を参照してください。

リモート RACADM を使用した iDRAC へのアクセス

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

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

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

メモ: iDRAC 証明書は、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 [yourdownloadedderformatcert.crt] -outform pem -out
[outcertfileinpemformat.pem] -text
```

2. 管理ステーションでデフォルトの CA 証明書バンドルの場所を検索します。例えば、RHEL5 64 ビットの場合、これは **/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。
   例えば、`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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

ファームウェア RACADM を使用した iDRAC へのアクセス

SSH インターフェイスを使用して 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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』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。

メモ:

- 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。
- 別の場所から異なる IP アドレスでログインを試みた場合、オリジナルの IP アドレスに対する 2FA でのチェックが保留中の状態であれば、同じトークンが新しい IP アドレスによるログイン試行に対して送信されます。
- この機能は iDRAC Enterprise ライセンスでサポートされています。

2FA が有効になっている場合、次の操作は行えません。

- デフォルトのユーザー資格情報で、コマンドライン インターフェイス (CLI) の UI から 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 マネージャーでメンバー iDRAC を追加する。

メモ: ソース IP からの RACADM、Redfish、WSMAN、IPMI LAN、シリアル、CLI は、iDRAC GUI、SSH 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。

RSA SecurID 2FA

iDRAC は、一度に 1 台の RSA AM サーバーを使用して認証するように設定することができます。RSA AM サーバーのグローバル設定は、すべての iDRAC ローカル ユーザー、AD、および LDAP ユーザーに適用されます。

メモ: RSA SecurID 2FA 機能は、Datacenter ライセンスでのみ使用できます。

iDRAC を RSA SecurID を有効にするように設定するには、前提条件として次を行います。

- Microsoft Active Directory Server を構成します。
- すべての AD ユーザーの RSA SecurID を有効化しようとしている場合は、AD サーバーをアイデンティティ ソースとして RSA AM サーバーに追加します。
- 汎用 LDAP サーバーを使用していることを確認します。
- すべての LDAP ユーザーについて、LDAP サーバーに対するアイデンティティ ソースを RSA AM サーバーに追加する必要があります。

iDRAC で RSA SecurID を有効にするには、RSA AM サーバーの次の属性が必要です。

1. **RSA 認証 API URL** : URL の構文は `https://<rsa-am-server-hostname>:<port>/mfa/v1_1` です。デフォルトでは、ポートは 5555 です。
2. **RSA クライアント ID** : デフォルトでは、RSA クライアント ID は RSA AM サーバー ホスト名と同じです。RSA AM サーバーの認証エージェント設定ページで RSA クライアント ID を検索します。
3. **RSA アクセス キー** - アクセス キーは、RSA AM で**設定** > **システム設定** > **RSA SecurID** > **認証 API** セクションに移動することによって取得できます。これは通常、 `198cv5x195fdi86u43jw0q069byt0x37umlfwxc2gnp4s0xk11ve2lffum4s8302` と表示されます。iDRAC GUI を使用して設定を行うには、次の手順に従います。
   - **iDRAC 設定** > **ユーザー**の順に移動します。
   - [**ローカル ユーザー**] セクションで、既存のローカル ユーザーを選択し、[**編集**] をクリックします。

- [構成] ページの一番下までスクロールします。
- [**RSA SecurID**] セクションで、[**RSA SecurID 構成**] リンクをクリックして、これらの設定を表示または編集します。

次のように設定を行うこともできます。

- **iDRAC 設定** > **ユーザー**の順に移動します。
- [**ディレクトリー サービス**] セクションから [**Microsoft Active Service**] または [**汎用 LDAP ディレクトリー サービス**] のいずれかを選択して、[**編集**] をクリックします。
- [**RSA SecurID**] セクションで、[**RSA SecurID 構成**] リンクをクリックして、これらの設定を表示または編集します。

4. **RSA AM サーバー証明書 (チェーン)**

iDRAC にログインするには、iDRAC GUI と SSH 経由で RSA SecurID トークンを使用します。

RSA SecurID トークン アプリ

RSA SecurID トークン アプリをお使いのシステムまたはスマート フォンにインストールする必要があります。iDRAC にログインしようとすると、アプリに表示されるパスコードを入力するよう求められます。

間違ったパスコードを入力した場合、RSA AM サーバーは、ユーザーに「次のトークン」を入力するようにチャレンジを出します。これは、ユーザーが正しいパスコードを入力した場合でも発生する可能性があります。この入力は、ユーザーが正しいパスコードを生成する適切なトークンを所有していることを証明します。

RSA SecurID トークン アプリから**次のトークン**を取得するには、[**オプション**] をクリックします。[**次のトークン**] をオンにすると、次のパスコードが使用可能になります。この手順では、時間が重要です。時間が過ぎると、iDRAC は、次のトークンの検証に失敗する可能性があります。iDRAC ユーザー ログイン セッションがタイムアウトした場合は、再度ログインを試行する必要があります。

間違ったパスコードを入力した場合、RSA AM サーバーは、ユーザーに「次のトークン」を入力するようにチャレンジを出します。これは、ユーザーが後で正しいパスコードを入力した場合でも発生する可能性があります。この入力は、ユーザーが正しいパスコードを生成する適切なトークンを所有していることを証明します。

RSA SecurID トークン アプリから次のトークンを取得するには、[**オプション**] をクリックして、**次のトークン**をオンにします。新しいトークンが生成されます。この手順では、時間が重要です。時間が過ぎると、iDRAC は、次のトークンの検証に失敗する可能性があります。iDRAC ユーザー ログイン セッションがタイムアウトした場合は、再度ログインを試行する必要があります。

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

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

表 6. システムステータスに可能な値（続き）

ホストシステム	Lifecycle Controller（LC）	リアルタイムステータス	全般のステータス
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。

例えば次のようになります。

ログイン：

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

または

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

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

RACADM コマンドの送信：

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

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

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。

表 7. 複数の iDRAC セッション

インタフェース	セッション数
iDRAC Web インターフェイス	8
リモート RACADM	4
ファームウェア RACADM	SSH - 4 シリアル - 1

iDRAC では、同じユーザーに対して複数のセッションを実行できます。ユーザーが許可されるセッションの最大数を作成した後、他のユーザーはその iDRAC にログインできなくなります。これにより、正当な管理者ユーザーに対して *サービス拒否*が発生する可能性があります。

セッションが使い果たされた場合は、次の救済措置をとります。

- Web サーバーベースのセッションが使い果たされた場合でも、SSH またはローカル RACADM を介してログインできます。
- ログイン後、管理者は `racadm getssninforacadm closessn -i <index>`racadm コマンドを使用して既存のセッションを終了することができます。

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 (セットアップユーティリティ)
- ローカル RACADM
- OpenManage Mobile
- サーバ管理の USB ポート
- USB-NIC

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. 48」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、https://www.dell.com/openmanagemanuals から入手可能な『*PowerEdge MX7000 シャーシ向け OME - Modular ユーザーズガイド*』で OMM のドキュメントを参照してください。

メモ: 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

メモ: これらの手順の前に、USB 管理ポ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、「サーバー管理用 USB ポートの使用 、p. 299」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. 299」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、iDRAC IP 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. 48」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 ユーザー名とパスワードがシステム情報タグで提供されている。

SSH、リモート RACADM、または Web インターフェイスで iDRAC にログインすると、警告メッセージも表示されます。Web インターフェイスと SSH 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. 147」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. 147」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。

   新しいパスワードが設定され、iDRAC にログインされます。

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

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

RACADM を使用したデフォルトログインパスワードの変更

パスワードを変更するには、次の RACADM コマンドを実行します。

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

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

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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

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. 147」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. 147」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。

パスワード強度ポリシー

iDRAC インターフェイスを使用すると、パスワード強度ポリシーを確認し、ポリシーに適合していない場合はエラーを確認することができます。パスワード ポリシーは、以前に保存されたパスワード、他のサーバーからコピーしたサーバー構成プロファイル (SCP)、およびプロファイルに組み込まれたパスワードに適用することはできません。

パスワード設定にアクセスするには、**iDRAC 設定** > **ユーザー** > **パスワード設定**の順に移動します。

このセクションでは、次のフィールドを使用できます。

- **最小スコア**：最小パスワード強度ポリシー スコアを指定します。このフィールドの値は次のとおりです。
  - 0 - 保護なし
  - 1 - 弱い保護
  - 2 - 中程度の保護
  - 3 - 強力な保護
- **簡易ポリシー**：セキュリティで保護されたパスワードに必要な文字を指定します。この画面には次のオプションがあります。
  - 大文字
  - 数字
  - 記号
  - 最小の長さ
- **正規表現**：パスワードの適用には、最小スコアの正規表現が使用されます。値は 1~4 です。

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成されます。

- 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、当該 IP アドレスによるセッション確立を防止させ続ける時間 (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と、一部の SSH クライアントでは、次のような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

プロパティ	定義

`iDRAC.IPBlocking.BlockEnable`	IP ブロック機能を有効にします。連続した失敗が
	`iDRAC.IPBlocking.FailCount`
	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
	`iDRAC.IPBlocking.FailWindow`
	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
	`iDRAC.IPBlocking.PenaltyTime`

`iDRAC.IPBlocking.FailCount`	この値の超過後にログイン試行を拒否させる、IP アドレスからのログイン失敗の回数を設定。

表 8. ログイン再試行の制限プロパティ（続き）

プロパティ	定義
iDRAC.IPBlocking.FailWindow	失敗した試行をカウントさせ続ける時間（秒単位）。この期間の経過後に失敗が発生した場合、カウンターはリセット。
iDRAC.IPBlocking.PenaltyTime	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続けるタイムスパン（秒単位）の指定。

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 バ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 ブート後にホスト 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 を使用したアラートの有効化または無効化

次のコマンドを使用します。

```
racadm set iDRAC.IPMILan.AlertEnable <n>
```

n=0 — 無効

n=1 — 有効

3

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、https://www.dell.com/openmanagemanuals から入手可能な『*OpenManage サーバー管理者ユーザーズガイド*』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
- ステージング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
- 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 - インポートおよびエクスポート
- BIOS 設定または F2 からのセキュアなブート設定
- BIOS recovery

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 設定ユーティリティ
- Lifecycle Controller（*Lifecycle Controller ユーザーズガイド* を参照）
- Dell Deployment Toolkit（*OpenManage Deployment Toolkit ユーザーズガイド* を参照）
- シャーシまたはサーバの LCD パネル（*設置およびサービスマニュアル* を参照）

  メモ: ブレードサーバーの場合、CMC の初期設定中のみ、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 ユーザーズガイド*を参照）

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

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

iDRAC IP アドレスを設定した後で、次の手順を実行します。

- 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 Web インターフェイス
  - セキュアシェル（SSH）— Windows 上では PuTTY などのクライアントが必要です。ほとんどの Linux システムでは SSH をデフォルトで利用できるため、クライアントは必要ありません。
  - IPMITool（IPMI コマンドを使用）またはシェルプロンプト（『*Systems Management Documentation and Tools*』DVD または https://www.dell.com/support から入手できる Windows または Linux の Dell カスタム化インストーラーが必要）

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。

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

1. **NIC の有効化** で、**有効** 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。

   メモ: このオプションは、MX プラットフォームでは使用できません。

   - **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 インターフェイスを使用できるようにします。このインタフェースは、ホストオペレーティングシステムと共有されず、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**

   メモ: ラックサーバとタワーサーバ場合、サーバモデルに応じて 2 つの LOM オプション (LOM1 と LOM2) または 4 つすべての LOM オプションを使用できます。NDC ポート 2 個を備えたブレード サーバーでは 2 つの LOM オプション (LOM1 と LOM2) が使用可能で、NDC ポート 4 個を備えたサーバーでは 4 つのすべての LOM オプションが使用可能です。

   メモ: NDC を 2 個備えたフルハイトサーバではハードウェア仲裁がサポートされないため、*Intel 2P X520–k bNDC 10 G* では共有 LOM がサポートされません。
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 カードまたはクワッド ポートまたはデュアル ポートのメザニン 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、リモートアクセスデバイスはリモートアクセスコントローラ（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。

- **クワッド 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ールオーバー 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。

   詳細については、次のセクションを参照してください：Web インターフェイスを使用したネットワーク設定の変更 、p. 96
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。有効にすると、iDRAC は、そのネットワーク速度に基づいてネットワーク速度を 10、100、または 1000 Mbps に設定します。
6. **ネットワーク速度** で、10 Mbps または 100 Mbps のどちらかを選択します。

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

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: ネットワークチーミング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、ネットワークチーム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チーム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. **NIC MTU** 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 サーバーがある場合は、DNS に iDRAC を登録します。これらは、ディレクトリー 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）などの高度な機能の初期設定要件です。

iDRAC を登録するには、次の手順を実行します。

1. **DNS に DRAC を登録する** を有効にします。
2. **DNS DRAC 名** を入力します。
3. **ドメイン名の自動設定**を選択して、DHCP から自動的にドメイン名を取得します。それ以外の場合は、**DNS ドメイン名**を入力します。

   DNS iDRAC 名フィールドでは、デフォルトの名前の形式は *idrac-Service_Tag* で、Service_Tag はサーバーのサービス タグです。最大長は 63 文字で、次の文字がサポートされています。
   - A～Z
   - a～z
   - 0～9

- ハイフン (-)

IPV4 の設定

IPv4 の設定を行うには、次の手順を実行します。

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します。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）** を有効にして、DHCP サーバが **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します。または、**Static Preferred DNS Server(静的優先 DNS サーバ)** と **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。

メモ: IPv6 が静的に設定されている場合は、必ず IPv6 ゲートウェイを手動で構成してください。これは、動的 IPv6 の場合には必要ありません。固定 IPv6 での手動設定の失敗は、通信喪失の原因となります。

1. **IPv6 の有効化** で、**有効** オプションを選択します。
2. DHCPv6 サーバーが iDRAC に対して自動的に IP アドレス、ゲートウェイ、およびサブネッマスクを割り当てるようにするには、**自動設定の有効** 下で **有効** オプションを選択します。

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

3. [**固定 IP アドレス 1**] 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 が表示されます。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 サーバー アドレスを取得する**] を有効にして、DHCPv6 サーバーからプライマリーおよびセカンダリー DNS サーバー アドレスを取得します。必要に応じて、次の設定を行えます。
   - **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 の設定

IPMI 設定を有効にするには、次の手順を実行します。

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

VLAN 設定

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

メモ: シャーシ（専用）として設定されているブレードサーバでは、VLAN 設定が読み取り専用で、CMC を使用した場合にのみ変更することができます。サーバが共有モードに設定されている場合は、iDRAC の共有モードで VLAN 設定を構成できます。

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

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

CMC ウェブインタフェースを使用した iDRAC IP のセットアップ

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。
   サーバーステータス ページが表示されます。
5. **iDRAC の起動** をクリックし、**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、https://www.dell.com/cmcmanuals から入手可能な『*Chassis Management Controller ユーザーズガイド*』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は、カスタム管理ユーザー資格情報を iDRAC に提供し、それにより、管理コンソールからプロビジョニングされていないサーバを検出し、管理することが可能になります。プロビジョニング サーバーの詳細については、https://www.dell.com/idracmanuals から入手可能な『*Lifecycle Controller リモート サービス クイック スタート ガイド*』を参照してください。

プロビジョニングサーバは固定 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 サーバーの検索に使用されます。

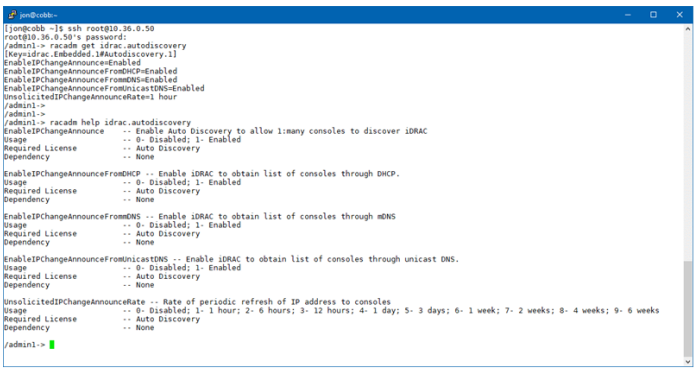
- iDRAC がコンソール アドレスを有している場合は、自身のサービス タグ、IP アドレス、Redfish ポート番号、Web 証明書などを送信します。
- この情報は、定期的にコンソールに対して公開されます。

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 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が指定されている場合、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. iDRAC GUI 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 IP の指定はオプションです。設定しなければ、DHCP または DNS 設定 (手順 7) を使用して検出されます。

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

   メモ: 自動検出では、IPv6 はサポートされません。

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

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

自動設定を使用したサーバーとサーバコンポーネントの設定

自動設定機能により、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パ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 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な、共有の NFS、CIFS、HTTP、または HTTPS のネットワークロケーションにエクスポートされます。SCP ファイル名は、ターゲットサーバのサービスタグまたはモデル番号に基づく名前、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、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。サーバでプロキシ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、さらにプロキシ設定を提供する必要があります。`-s` オプションフラグは次のようにアップデートされます。

表 9. 異なる共有タイプとパスイン値

-s (共有タイプ)	パスイン
NFS	`0` または `nfs`
CIFS	`2` または `cifs`
HTTP	`5` または `http`
HTTPS	`6` または `https`

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パラメーターと、オプションのパ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。

`-i (IPAddress)`：ネットワーク共有の IP アドレス。これは必須フィールドです。

-u (Username)：ネットワーク共有にアクセスできるユーザー名。これは、CIFS の必須フィールドです。

-p (Password)：ネットワーク共有にアクセスできるユーザーパスワード。これは、CIFS の必須フィールドです。

-d (ShutdownType)：正常な場合は 0、強制の場合は 1 (デフォルト設定：0)。これはオプションのフィールドです。

-t (Timetowait)：ホストがシャットダウンするまでの待機時間 (デフォルト設定：300)。これはオプションのフィールドです。

-e (EndHostPowerState)：オフの場合は 0、オン場合は 1 (デフォルト設定：1)。これはオプションのフィールドです。

追加のオプションフラグは iDRAC ファームウェア 3.00.00.00 以降でサポートされ、HTTP プロキシのパラメーターを有効にし、プロファイルファイルにアクセスするための再試行タイムアウトを設定します。

—pd (ProxyDefault)：デフォルトのプロキシ設定を使用。これはオプションのフィールドです。

—pt (ProxyType)：ユーザーは http または socks (デフォルト設定：http) をパスイン可能。これはオプションのフィールドです。

—ph (ProxyHost)：プロキシホストの IP アドレス。これはオプションのフィールドです。

—pu (ProxyUserName)：プロキシサーバにアクセスできるユーザー名。これはプロキシのサポートに必要です。

—pp (ProxyPassword)：プロキシサーバにアクセスできるユーザーパスワード。これはプロキシのサポートに必要です。

—po (ProxyPort)：プロキシサーバのポート (デフォルト設定は 80)。これはオプションのフィールドです。

—to (Timeout)：設定ファイルを取得するための再試行タイムアウトを分単位で指定 (デフォルトは 60 分)。

iDRAC ファームウェア 3.00.00.00 以降では、JSON フォーマットのプロファイルファイルがサポートされています。Filename パラメーターが存在しない場合は、次のファイル名が使用されます。

- <サービスタグ>-config.xml、例：CDVH7R1-config.xml
- <モデル番号>-config.xml、例：R640-config.xml
- config.xml
- <サービスタグ>-config.json、例：CDVH7R1-config.json
- <モデル番号>-config.json、例：R630-config.json
- config.json

メモ: HTTP の詳細については、https://www.dell.com/support にあるホワイトペーパー『*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。

メモ:

- 自動設定を有効にできるのは、**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ます。
- サーバが自動設定動作を実行した後、自動設定機能は無効になります。

DHCP サーバプール内のすべての Dell PowerEdge サーバが同じモデルタイプと番号の場合、単一の SCP ファイル (config.xml) が必要です。config.xml ファイル名は、デフォルトの SCP ファイル名として使用されます。.xml ファイルのほかに、14G システムでは .json ファイルも使用できます。ファイルは config.json になります。

ユーザーは、個々のサーバのサービスタグまたはサーバモデルを使用してマッピングされた、別の設定ファイルを必要とする個々のサーバを設定することができます。特定の要件に対応したサーバを個々に持つ環境では、各サーバやサーバタイプを区別するために、異なる SCP ファイル名を使用することができます。たとえば、設定するサーバモデルに PowerEdge R740s と PowerEdge R540s がある場合は、R740-config.xml および R540-config.xml の 2 つの SCP ファイルを使用します。

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

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

自動設定シーケンス

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

DHCP オプション

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

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

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

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

DHCP Option 60 は DHCP クライアントと特定のベンダーを識別し、関連付けます。クライアントのベンダー ID を元に動作するよう設定されている DHCP サーバには、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 はそれ自身をベンダー ID「*iDRAC*」で識別します。したがって、新しい「ベンダークラス」を追加し、その下に「コード 60」の「範囲のオプション」を作成した後で、DHCP サーバ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

Windows でオプション 43 を設定するには、次の手順を実行します。

1. DHCP サーバで、**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。
   範囲のオプション ダイログボックスが表示されます。
4. 下にスクロールして、**043 ベンダー固有の情報** を選択します。
5. **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 ファイルを含む共有の場所を持つサーバの IP アドレスを入力します。
   値は、**ASCII** 下に入力すると表示されますが、左側にバイナリとしても表示されます。
6. **OK** をクリックして設定を保存します。

Windows でのオプション 60 の設定

Windows でオプション 60 を設定するには、次の手順を実行します。

1. DHCP サーバで、**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、その下の項目を展開します。
3. **IPv4** を右クリックして、**ベンダークラスの定義** を選択します。
4. **追加** をクリックします。
   次のフィールドで構成されるダイアログボックスが表示されます。
   - **表示名**
   - **説明：**
   - **ID： バイナリ： ASCII：**
5. **表示名：** フィールドで、iDRAC と入力します。

6. **説明：** フィールドで、Vendor Class と入力します。
7. **ASCII：** セクションをクリックして、iDRAC を入力します。
8. **OK**、**終了** の順にクリックします。
9. DHCP ウィンドウで **IPv4** を右クリックし、**事前定義されたオプションの設定** を選択します。
10. **オプションクラス** ドロップダウンメニューから **iDRAC**（手順 4 で作成済み）を選択し、**追加** をクリックします。
11. **オプションタイプ** ダイアログボックスで、次の情報を入力します。
    - **名前** - iDRAC
    - **データタイプ** - 文字列
    - **コード** — 060
    - **説明** - デルのベンダークラス識別子
12. **OK** をクリックして、**DHCP** ウィンドウに戻ります。
13. サーバー名下のすべての項目を展開し、**スコープオプション** を右クリックして、**オプションの設定** を選択します。
14. **詳細設定** タブをクリックします。
15. **ベンダークラス** ドロップダウンメニューから **iDRAC** を選択します。060 iDRAC が、**利用可能なオプション** の列に表示されます。
16. **060 iDRAC** オプションを選択します。
17. DHCP 提供の標準 IP アドレスと共に、iDRAC に送信する必要がある文字列の値を入力します。文字列の値は、正しい SCP ファイルをインポートするのに役立ちます。

    オプションの **データ入力、文字列の値** 設定については、次の文字オプションと値のあるテキストパラメータを使用します。
    - Filename (-f) - エクスポートしたサーバ設定プロファイル（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 以降では、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 option 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。

      メモ: Sharename (-n)、ShareType (-s)、および IPAddress (-i) は、渡す必要がある必須の属性です。-n は、HTTP または HTTPS には必要ありません。
    - 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。

      メモ: デフォルト設定は 0 です。
    - Timetowait (-t) - ホストシステムがシャットダウンするまで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。

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

    NFS: -f system_config.xml -i 192.168.1.101 -n /nfs_share -s 0 -d 1
    CIFS: -f system_config.xml -i 192.168.1.101 -n cifs_share -s 2 -u <*USERNAME*> -p <*PASSWORD*> -d 1 -t 400
    HTTP: -f system_config.json -i 192.168.1.101 -s 5
    HTTP: -f http_share/system_config.xml -i 192.168.1.101 -s http
    HTTP: -f system_config.xml -i 192.168.1.101 -s http -n http_share
    HTTPS: -f system_config.json -i 192.168.1.101 -s https

Linux でのオプション 43 およびオプション 60 の設定

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

1. この DHCP サーバーが割り当てることができるアドレスのブロックまたはプールを確保しておきます。

2. オプション 43 を設定し、名前のベンダークラス識別子をオプション 60 に使用します。

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

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

- Filename (–f) - エクスポート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。
  メモ: ファイルの命名規則の詳細については、「自動設定を使用したサーバーとサーバコンポーネントの設定 、p. 59」を参照してください。
- Sharename (-n) — ネットワーク共有の名前を示します。
- ShareType (-s) - 共有タイプを示します。0 は NFS を示し、2 は CIFS を示し、5 は HTTP を示し、6 は HTTPS を示します。
  メモ: Linux NFS、Linux NFS、CIFS、HTTP、および　HTTPS 共有の例：
  - **NFS**：`-f system_config.xml -i 192.168.0.130 -n /nfs -s 0 -d 0 -t 500`

    NFS ネットワーク共有に NFS2 または NFS3 を使用していることを確認してください
  - **CIFS**：`-f system_config.xml -i 192.168.0.130 -n sambashare/config_files -s 2 -u user -p password -d 1 -t 400`
  - **HTTP**：`-f system_config.xml -i 192.168.1.101 -s http -n http_share`
  - **HTTPS**：`-f system_config.json -i 192.168.1.101 -s https`
- IPAddress (-i) - ファイル共有の IP アドレスを示します。
  メモ: Sharename (-n)、共有タイプ (-s) および IP アドレス (-i) は、渡されなければならない必要な属性です。HTTP または HTTPS では -n は、必要ありません。
- Username (-u) - ネットワーク共有へのアクセスにユーザー名が必要なことを示します。この情報は、CIFS にのみ必要です。
- Password (-p) - ネットワーク共有へのアクセスにパスワードが必要なことを示します。この情報は、CIFS にのみ必要です。
- ShutdownType (-d) - シャットダウンのモードを示します。0 は正常なシャットダウン、1 は強制シャットダウンを示します。
  メモ: デフォルト設定は 0 です。
- TimeToWait (-t) - ホスト システムがシャットダウンするまでの待機時間を示します。デフォルト設定は 300 です。
- EndHostPowerState (-e) - ホストの電源状態を示します。0 はオフを、1 はオンを示します。デフォルトでは 1 に設定されています。
  メモ: ShutdownType (-d)、TimeToWait (-t)、および EndHostPowerState (-e) は、オプションの属性です。

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

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

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

自動設定を有効にする前の前提条件

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

- サポートされ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、アクセス可能なこと、およびファイアウォールとユーザー権限が正しく設定されていることを確認します。
- サーバ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、SCP ファイルに必要な変更が完了していることを確認し、自動設定処理が開始されたときに正しい設定を適用できるようにします。
- iDRAC がサーバーを呼び出して自動設定機能を初期化するのに対して必要に応じて DHCP サーバーは設定され、DHCP 構成がアップデートされます。

iDRAC ウェブインタフェースを使用した自動設定の有効化

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

自動設定を有効化するには、次の手順を実行します。

1. iDRAC 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)** と移動します。
   ネットワーク ページが表示されます。
2. **自動設定** セクションで、**DHCP プロビジョニングを有効にする** ドロップダウンメニューから次のいずれかのオプションを選択します。
   - **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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

自動設定機能の詳細に関しては、https://www.dell.com/support にあるホワイトペーパー『*Dell EMC iDRAC を使用した、Lifecycle Controller 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と BIOS パスワードを設定できます。ユーザー認証メカニズムは影響を受けず (SNMPv3 と IPMI を除く)、パスワードをプレーンテキスト形式で指定できます。

新しいパスワードハッシュ機能により次のことが可能になります。

- 独自の SHA256 ハッシュを生成して iDRAC ユーザーパスワードと BIOS パスワードを設定できます。これにより、サーバ構成プロファイル、RACADM、および WSMan で SHA256 の値を指定できます。SHA256 パスワードの値を提供する場合は、SNMPv3 と IPMI を介して認証することはできません。
  メモ: リモート RACADM または WSMan または Redfish は、IDRAC のハッシュパスワードの設定 / 交換には使用できません。リモート RACADM または WSMan または Redfish でのハッシュパスワードの設定 / 交換には SCP を使用できます。
- 現在のプレーンテキストメカニズムを使用して、すべての iDRAC ユーザーアカウントと BIOS パスワードを含むテンプレートサーバをセットアップすることができます。サーバのセットアップ後、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インポートした後、最新の Dell IPMI 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、ハッシュされたパスワード値が設定されているユーザーの IPMI 認証が失敗します。
- iDRAC GUI などののその他のインターフェイスにはユーザーアカウントが有効であると表示されます。

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

ハッシュパスワードを含め、エクスポートするにはサーバー制御権限が必要です。

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

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

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

SNMPv3 および IPMI 認証なしでのハッシュパスワードの生成

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 = ALITTLEBITOFSALT - 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 SOMEPASSWORDALITTLEBITOFSALT|sha256sum  -><HASH>
   ```

   ```
   Generate Hex Representation of Salt -> echo -n ALITTLEBITOFSALT | 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。

```
set iDRAC.Users.4.SHA256Password
ca74e5fe75654735d3b8d04a7bdf5dcdd06f1c6c2a215171a24e5a9dcb28e7a2
```

```
set iDRAC.Users.4.SHA256PasswordSalt
```

4. パスワードの設定後に、通常のプレーンテキストパスワード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 SNMP v3 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 2) 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. iDRAC 設定ユーティリティで、**ユーザー設定** に移動します。
   iDRAC 設定のユーザー設定 ページが表示されます。
2. **ユーザー名**、**LAN ユーザー権限**、**シリアルポートユーザー権限**、および **パスワードの変更** の詳細情報を指定します。
   オプションについては、『iDRAC 設定ユーティリティオンラインヘルプ』を参照してください。
3. **戻る**、**終了** の順にクリックし、**はい** をクリックします。
   ローカル管理者アカウント設定が設定されます。

管理下システムの場所のセットアップ

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

ウェブインタフェースを使用した管理下システムの場所のセットアップ

システムの場所の詳細を指定するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**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、データセンター内の管理下システムの場所について詳細情報を入力します。
   オプションの詳細については、『iDRAC オンラインヘルプ』を参照してください。
3. **適用** をクリックします。システムの場所の詳細情報が iDRAC に保存されます。

RACADM を使用した管理下システムの場所のセットアップ

システムの場所の詳細を指定するには、`System.Location` グループオブジェクトを使用します。

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

iDRAC 設定ユーティリティを使用した管理下システムの場所のセットアップ

システムの場所の詳細を指定するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**システムの場所** に移動します。
   iDRAC 設定のシステムの場所 ページが表示されます。
2. データセンター内の管理下システムの場所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。
   詳細が保存されます。

システムパフォーマンスと電力消費の最適化

サーバ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、エアフロー、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 エアフロー消費量**：リアルタイムのシステム エアフロー消費量 (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空気温度上昇を制限し、インフラストラクチャ レベルの冷却を最適化します。
- **排気温度制御**：データセンターのニーズに合わせて、サーバーから排出される空気の温度制限を指定します。
- **カスタム PCIe 吸気温度**：サード パーティー デバイスの要件に適合する適切な入力吸気温度を選択します。
- **PCIe エアフロー設定**：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、サード 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 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]** > **[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]** > **[システム BIOS 設定]** > **[システム プロファイル設定]** ページで定義されたものと同じシステム プロファイル設定を使用することを示します。

     このオプションはデフォルトで [**デフォルトの温度プロファイル設定**] に設定されています。BIOS プロファイルに依存しないカスタムアルゴリズムを選択することもできます。使用可能なオプションには以下があります：
     - **最大パフォーマンス (パフォーマンス最適化)**:
       - メモリまたは CPU スロットルの確率を削減。
       - ターボモードのアクティブ化の確率を増加。
       - 一般に、アイドル負荷および応力負荷ではファン速度が上昇。
     - **最小電力 (1 ワットあたりのパフォーマンス最適化)**:
       - 最適なファン電力状態に基づいて、最小のシステム消費電力のために最適化。
       - 一般に、アイドル負荷および応力負荷ではファン速度が減少。
     - **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、占有されている領域でサーバの一時的な導入または評価が含まれることがありますが、ベンチマークまたはパフォーマンス重視のアプリケーションには使用しないでください。

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

     デフォルト値は **デフォルト、70°C (158°F)** です。

     このオプションを使用すると、排気温度が選択した排気温度制限を超過しないように、システムのファン速度を変更させることが可能になります。この機能はシステム負荷およびシステム冷却能力に依存するため、すべてのシステム稼動条件下で常に保証されるとは限りません。
   - **ファン速度オフセット** — このオプションを選択すると、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、冷却が追加で必要になることがあります。ファン速度オフセットにより、ファン速度が温度制御アルゴリズムによって計算されたベースラインファン速度を超過する速度に、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なファン速度まで上昇させます。

- **中ファン速度** - ファン速度を中程度近くまで上昇させます。
- **高ファン速度** - ファンの速度を最大速度近くまで上昇させます。
- **ファン最大速** - ファンの速度を最大速度まで上昇させます。
- [**オフ**] — ファン速度オフセット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は、すべてのファンの速度を同じ割合で上昇させます。ファン速度は、個々のコンポーネントの冷却の必要性に応じてオフセット速度を超える速度を増加する場合があります。全体的なシステム電力消費量の上昇が予測されます。

ファン速度オフセットでは、システムファン速度を 4 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ド パーティ製 PCIe カードの場合、45ºC 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、他のカスタム 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、設定最大速度です (システムの設定によっては、最大速度は 100%までとなることがあります)。

    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

オブジェクト	説明	使用状況	例

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

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

表 10. 温度設定（続き）

オブジェクト	説明	使用状況	例
	ト値（%PWM）が読み取られます。 • この値は、システムによって異なります。 • FanSpeedOffset オブジェクトを使用してインデックス値 1 でこの値を設定します。		FanSpeedHighOffsetVal たとえば「66」などの数値が返されます。この値は、次のコマンドを使用したときに、ベースラインファン速度上に高速ファン速度オフセット（66% PWM）が適用されることを意味します。 racadm set system.thermalsettings FanSpeedOffset 1
FanSpeedLowOffsetVal	• この変数を取得すると、低速ファン速度オフセット設定用のファン速度オフセット値（%PWM）が読み取られます。 • この値は、システムによって異なります。 • FanSpeedOffset オブジェクトを使用してインデックス値 0 でこの値を設定します。	0 ~ 100 の値	racadm get system.thermalsettings FanSpeedLowOffsetVal これにより、「23」などの値が返されます。これは、次のコマンドを使用したときに、ベースラインファン速度上に低速ファン速度オフセット（23 % PWM）が適用されることを意味します。 racadm set system.thermalsettings FanSpeedOffset 0
FanSpeedMaxOffsetVal	• この変数を取得すると、最速ファン速度オフセット設定用のファン速度オフセット値（%PWM）が読み取られます。 • この値は、システムによって異なります。 • FanSpeedOffset を使用してインデックス値 3 でこの値を設定します。	0 ~ 100 の値	racadm get system.thermalsettings FanSpeedMaxOffsetVal これにより、「100」などの値が返されます。これは、次のコマンドを使用したときに、最速ファン速度オフセット（フルスピードのこと、100% PWM）が適用されることを意味します。通常、このオフセットはファン速度がフルスピードまで上昇する原因となります。 racadm set system.thermalsettings FanSpeedOffset 3
FanSpeedMediumOffsetVal	• この変数を取得すると、中速ファン速度オフセット設定用のファン速度オフセット値（%PWM）が読み取られます。 • この値は、システムによって異なります。	0 ~ 100 の値	racadm get system.thermalsettings FanSpeedMediumOffsetVal これにより、「47」などの値が返されます。これは、次のコマン

表 10. 温度設定（続き）

オブジェクト	説明	使用状況	例
	• FanSpeedOffset オブジェクトを使用してインデックス値 2 でこの値を設定します。		ドを使用したときに、ベースラインファン速度上に中速ファン速度オフセット（47 % PWM）が適用されることを意味します。 racadm set system.thermalsettings FanSpeedOffset 2
FanSpeedOffset	• get コマンドでこのオブジェクトを使用すると、既存のファン速度オフセット値が表示されます。 • set コマンドでこのオブジェクトを使用すると、必要なファン速度オフセット値を設定することができます。 • このインデックス値により、適用されるオフセットが決定され、FanSpeedLowOffsetVal、FanSpeedMaxOffsetVal、FanSpeedHighOffsetVal および FanSpeedMediumOffsetVal オブジェクト（以前に定義済み）が、オフセットが適用される値になります。	値： • 0 - 低速ファン速度 • 1 - 高速ファン速度 • 2 - 中速ファン速度 • 3 - 最大ファン速度 • 255 - なし	既存の設定を表示するには、次のコマンドを実行します。 racadm get system.thermalsettings.FanSpeedOffset ファン速度オフセットを高い値（FanSpeedHighOffsetVal で定義済み）に設定するには、次のコマンドを実行します。 racadm set system.thermalsettings.FanSpeedOffset 1
MFSMaximumLimit	MFS の最大制限の読み取り	1～100 の値	MinimumFanSpeed オプションを使用して設定できる最大値を表示するには、次のコマンドを実行します。 racadm get system.thermalsettings.MFSMaximumLimit
MFSMinimumLimit	MFS の最低制限の読み取り	0 ～ MFSMaximumLimit の値 デフォルト値は 255 です(なしを意味します)。	MinimumFanSpeed オプションを使用して設定できる最小値を表示するには、次のコマンドを実行します。 racadm get system.thermalsettings.MFSMinimumLimit
MinimumFanSpeed	• システムが稼働するために必要な最小ファン速度を設定できます。 • ファン速度のベースライン（フロアー）が定義され、定義されたこのファン速度値よりも低い速度でファンが	MFSMinimumLimit ～ MFSMaximumLimit の値 get コマンドが 255 を報告した場合は、ユーザーが設定したオフセットが適用されていないことを意味します。	システムの最小速度が 45% PWM（45 は MFSMinimumLimit ～ MFSMaximumLimit の値である必要があります）よりも低く

表 10. 温度設定（続き）

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

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

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

iDRAC 設定ユーティリティを使用したサーマル設定の変更

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

   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、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 インターフェイスを使用した 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。

メモ: 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 インターフェイスで、**[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下に [**PCIe エアフロー設定**] ページが表示されます。
2. 以下を指定します。
   - [**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。

   次のメッセージが表示されます。

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

   後で再起動 または **今すぐ再起動** をクリックします。

   メモ: 設定を反映にするには、システムを再起動する必要があります。

管理ステーションのセットアップ

管理ステーションは、iDRAC インタフェースにアクセスしてリモートで PowerEdge サーバーを監視および管理するために使用されるコンピュータです。

管理ステーションをセットアップするには、次の手順を実行します。

1. サポートされているオペレーティングシステムをインストールします。詳細については、リリースノートを参照してください。
2. サポートされている Web ブラウザー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 (Web ブラウザーを使用した 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)。

   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、Java 8 以降が必要です。

4. 『*Dell Systems Management Tools and Documentation*』DVD から、SYSMGMT フォルダーにあるリモート RACADM 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、https://www.dell.com/idracmanuals から入手可能な『*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。
   - SSH クライアント
   - TFTP
   - Dell OpenManage Essentials

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。

- ブレードサーバー - 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、https://www.dell.com/cmcmanuals から入手可能な『*Chassis Management Controller ユーザーズ ガイド*』を参照してください。
- ラックおよびタワーサーバー — iDRAC NIC を専用または LOM1 に設定し、管理ステーションが iDRAC と同じネットワークに存在することを確認します。

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

対応ウェブブラウザの設定

メモ: 対応ブラウザーとバージョンの詳細については、https://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 ブラウザーを設定します。

メモ: Internet Explorer または Firefox を使用して iDRAC ウェブインタフェースにアクセスする場合は、このセクションで説明されている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。

メモ: 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. **ツール インターネットオプション セキュリティ ローカルネットワーク** または **ローカルイントラネット** をクリックします。
3. **カスタムレベル** をクリックして **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)** をクリックするか、またはウェブブラウザを再度立ち上げて iDRAC ウェブインタフェースへの接続を確立します。IP を追加するように求められない場合は、IP を信頼済みサイトのリストへ手動で追加することを推奨します。

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

信頼済みサイトリストに iDRAC IP アドレスを追加するには、次の手順を実行します。

1. **ツール** > **インターネットオプション** > **セキュリティ** > **信頼済みサイト** > **サイト** の順にクリックします。
2. **この Web サイトをゾーンに追加する** に、iDRAC IP アドレスを入力します。
3. **追加** をクリックし、**OK** をクリックして、次に **閉じる** をクリックします。
4. **OK** をクリックし、ブラウザを更新します。

Active Directory SSO を有効にするための Internet Explorer の設定

Internet Explorer のブラウザ設定を行うには、次の手順を実行します。

1. Internet Explorer で、**ローカルイントラネット** に移動して **サイト** をクリックします。
2. 次のオプションのみを選択します。
   - 他のゾーンにリストされていないすべてのローカル (イントラネット) サイトを含める。

- プロキシサーバーをバイパスするすべてのサイトを含める。

3. **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. **閉じる** 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 インターフェイスにアクセスして、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」セキュリティ機能があります。このホワイトリスト機能を有効にする場合は、ビューア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ア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、不必要なプラグインインストールを避けるには、次の手順を実行してください。

1. Firefox ウェブブラウザのウィンドウを開きます。
2. アドレスフィールドに `about:config` と入力し、<Enter> を押します。
3. **プリファレンス名** 列で、**xpinstall.whitelist.required** を見つけてダブルクリックします。
   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、**xpinstall.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、**xpinstall.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）** で `network.negotiate` と入力します。
3. network.negotiate-auth.trusted-uris にドメイン名を追加します（コンマ区切りのリストを使用）。
4. network.negotiate-auth.delegation-uris にドメイン名を追加します（コンマ区切りのリストを使用）。

仮想コンソールを使用するためのウェブブラウザの設定

管理ステーションで仮想コンソールを使用するには、次の手順を実行します。

1. 対応バージョンのブラウザ（Internet Explorer（Windows）、Mozilla Firefox（Windows または Linux）、Google Chrome、Safari）がインストールされていることを確認します。
   対応ブラウザバージョンの詳細に関しては、https://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 ビューアは、Internet Explorer でのみサポートされます。HTML5 または Java ビューアは、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、Java 8 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、**ユニバーサルアクセス** ウィンドウ内の **補助装置にアクセスできるようにする** オプションを選択します。

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

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

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

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

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

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

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

3. IE でタイトルバーの情報を表示するには、**コントロールパネル** > **デスクトップのカスタマイズ** > **個人設定** > **Windows クラシック** 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 Microsoft Edge 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。
2. 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
   ```

Java プラグインを使用するためのウェブブラウザの設定

Firefox または IE を使用しており、Java ビューアを使用する場合は、Java Runtime Environment (JRE) をインストールします。

メモ: 64 ビットのオペレーティングシステムでは 32 ビットまたは 64 ビットの JRE バージョン、32 ビットのオペレーティングシステムでは 32 ビットの JRE バージョンをインストールします。

Java プラグインを使用するために IE を設定するには、次の手順を実行します。

- Internet Explorer でファイルダウンロード時の自動プロンプトを無効化します。
- Internet Explorer で *セキュリティ強化モード* を無効化します。

ActiveX プラグインを使用するための IE の設定

ActiveX 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、IE ブラウザを設定する必要があります。ActiveX アプリケーションは、iDRAC サーバからの署名付き CAB ファイルとして提供されます。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、仮想コンソールを起動すると、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 ベースの仮想コンソールが起動します。Internet Explorer で ActiveX ベースアプリケーションのダウンロード、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ーを開く場合、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、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. ブラウザのキャッシュをクリアします。
2. iDRAC IP またはホスト名を **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 **中低** にリセットするか、設定を変更して署名済みの ActiveX プラグインのインストールを許可します。
4. ブラウザの暗号化されたコンテンツのダウンロードを有効にし、サードパーティ製のブラウザ拡張を有効にします。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ブラウザ拡張を有効にする）** オプションを選択します。

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

5. **ツール** > **インターネットオプション** > **セキュリティ** と進み、アプリケーションを実行するゾーンを選択します。
6. **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。
   - **署名済み ActiveX コントロールのダウンロード** に対して **プロンプト** を選択します。
   - **ActiveX コントロールとプラグインの実行** に対して **有効** または **プロンプト** を選択します。
   - **スクリプトを実行しても安全だとマークされた ActiveX コントロールのスクリプトの実行** に対して **有効** または **プロンプト** を選択します。
7. **OK** をクリックして、**セキュリティ設定** ウィンドウを閉じます。
8. **OK** をクリックして、**インターネットオプション** ウィンドウを閉じます。

   メモ: Internet Explorer 11 を搭載したシステムでは、**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。

   メモ:
   - Internet Explorer のさまざまなバージョンが、**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、サーバーをあるブラウザの信頼済みサイトのリストに追加した後で、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**のエラーがでる場合、コードサイニング証明書のパ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. **ツール** > **インターネットオプション** > **セキュリティ** > **信頼済みサイト** の順に選択します。
3. 信頼済みサイトゾーンに対して **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。または、イントラネットゾーンのサイトに iDRAC アドレスを追加することもできます。イントラネットゾーンと信頼済みサイトゾーンのサイトについては、保護モードはデフォルトでオフになっています。
4. **サイト** をクリックします。
5. **このウェブサイトをゾーンに追加する** フィールドに iDRAC のアドレスを追加し、**追加** をクリックします。
6. **閉じる** をクリックして、**OK** をクリックします。
7. 設定を有効にするために、ブラウザを閉じてから再起動します。

ブラウザキャッシュのクリア

仮想コンソールの操作中に問題（範囲外エラーや同期問題など）が発生した場合は、ブラウザのキャッシュをクリアして、システムに格納されている可能性のある古いバージョンのビューアを削除してから再試行してください。

メモ: ブラウザのキャッシュをクリアするには、管理者権限が必要です。

古い Java バージョンのクリア

Windows または Linux で古いバージョンの Java ビューアをクリアするには、次の手順に従います。

1. コマンドプロンプトで、`javaws-viewer` または `javaws-uninstall` を実行します。
   Java キャッシュ ビューアが表示されます。
2. iDRAC 仮想コンソールクライアント という項目を削除します。

管理ステーションへの CA 証明書のインポート

仮想コンソールまたは仮想メディアを起動すると、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. 112

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 の信頼済み証明書ストアへの CA 証明書のインポート

Secure Hash Algorithm（SHA）を使用し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 ツール 1.0.X 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 の信頼済み証明書ストアへインポートするには、次の手順を実行します。

1. OpenSSL コマンドプロンプトを開きます。
2. コマンド `openssl x509 -in (name of CA cert) -noout -hash` を使用して、管理ステーションで現在使用中の CA 証明書で 8 バイトのハッシュを実行します。

   出力ファイルが生成されます。たとえば、CA 証明書ファイルの名前が **cacert.pem** である場合は、コマンドは次のようになります。

   ```
   openssl x509 -in cacert.pem -noout -hash
   ```

   「431db322」に類似した出力が生成されます。
3. CA ファイルの名前を出力ファイルの名前に変更し、「.0」という拡張子を付けます。たとえば、431db322.0 とします。
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。他のキーボードはサポートされず、これらを使用すると、予期しない問題が発生することがあります。

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

デバイスファームウェアのアップデート

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

- Fibre Channel（FC）カード
- 診断
- オペレーティングシステムドライバパック
- ネットワークインタフェースカード（NIC）
- RAID コントローラ
- 電源供給ユニット（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 コレクタ

注意: PSU ファームウェアのアップデートは、システム構成と 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場合、エラーメッセージが表示されます。再起動を必要としないアップデートは即時に適用されます。システム再起動を必要とするアップデートはステージングされ、次のシステム再起動時に実行されるようにコミットされます。すべてのアップデートを実行するために必要なシステム再起動は 1 度のみです。

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 に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。

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、次の方法で実行できます。

- ローカルシステムまたはネットワーク共有からサポートするイメージタイプを 1 つずつアップロード。
- FTP、TFTP、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。

  メモ: HTTP/HTTPS は、ダイジェスト認証または認証なしのいずれかでのみサポートします。
- カタログファイルおよびカスタムリポジトリを使用した定期的な自動ファームウェアアップデートをスケジューリング。

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

表 11. イメージファイルのタイプと依存関係

	.D9 イメージ		iDRAC DUP	
インタフェース	**対応**	**LC の有効化が必要**	**対応**	**LC の有効化が必要**
BMCFW64.exe ユーティリティ	はい	いいえ	いいえ	該当なし
Racadm FWUpdate (古い)	はい	いいえ	いいえ	該当なし
Racadm Update (新しい)	はい	はい	はい	はい
iDRAC UI	はい	はい	はい	はい
WSMan	はい	はい	はい	はい

表 11. イメージファイルのタイプと依存関係（続き）

	.D9 イメージ		iDRAC DUP	
インタフェース	対応	LC の有効化が必要	対応	LC の有効化が必要
インバンド OS DUP	いいえ	該当なし	はい	いいえ
Redfish	はい	該当なし	はい	該当なし

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

メモ: 複数のファームウェアのアップデートを帯域外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

コンポーネント名	ファームウェアのロールバックのサポート（有または無）	帯域外 — システム再起動の必要性	インバンド — システム再起動の必要性	Lifecycle Controller GUI — 再起動の必要性
診断	いいえ	いいえ	いいえ	いいえ
オペレーティングシステムのドライバパック	いいえ	いいえ	いいえ	いいえ
iDRAC	はい	いいえ	なし*	はい
BIOS	はい	はい	はい	はい
RAID コントローラ	はい	はい	はい	はい
BOSS	はい	はい	はい	はい
NVDIMM	いいえ	はい	はい	はい
バックプレーン	はい	はい	はい	はい
メモ: アクティブ バックプレーンの場合は、システムの再起動が必要です。パッシブ バックプレーンの場合、ダイレクト アップデートは 4.00.00.00 リリース以降からのみサポートされています。以前のバージョンのサーバーでは、再起動が必要です。				
エンクロージャ	はい	はい	いいえ	はい
NIC	はい	はい	はい	はい
電源供給ユニット	はい	はい	はい	はい
CPLD	いいえ	はい	はい	はい
メモ: CPLD ファームウェアのアップグレードが完了すると、iDRAC は自動的に再起動します。				
FC カード	はい	はい	はい	はい
NVMe PCIe SSD ドライブ	はい	はい	はい	はい
SAS/SATA ハードドライブ	いいえ	はい	はい	いいえ
OS コレクタ	いいえ	いいえ	いいえ	いいえ
CMC（PowerEdge FX2 サーバー）	いいえ	はい	はい	はい

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

コンポーネント名	ファームウェアのロールバックのサポート (有または無)	帯域外 — システム再起動の必要性	インバンド — システム再起動の必要性	Lifecycle Controller GUI — 再起動の必要性
診断	いいえ	いいえ	いいえ	いいえ
オペレーティングシステムのドライバパック	いいえ	いいえ	いいえ	いいえ
iDRAC	はい	いいえ	なし*	はい
BIOS	はい	はい	はい	はい
RAID コントローラ	はい	はい	はい	はい
BOSS	はい	はい	はい	はい
NVDIMM	いいえ	はい	はい	はい
バックプレーン	はい	はい	はい	はい
エンクロージャ	はい	はい	いいえ	はい
NIC	はい	はい	はい	はい
電源供給ユニット	いいえ	いいえ	いいえ	いいえ
CPLD	いいえ	はい	はい	はい
FC カード	はい	はい	はい	はい
NVMe PCIe SSD ドライブ	はい	いいえ	いいえ	いいえ
SAS/SATA ハードドライブ	いいえ	はい	はい	いいえ
OS コレクタ	いいえ	いいえ	いいえ	いいえ

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

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

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、ネットワーク共有上 (CIFS、NFS、HTTP、または HTTPS) のリポジトリーから、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

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

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

iDRAC ウェブインタフェースを使用して単一デバイスのファームウェアをアップデートするには、次の手順を実行します。

1. **[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。

2. [**アップデート**] タブで、[**場所のタイプ**] として [**ローカル**] を選択します。

   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** セクションに iDRAC にアップロードされた各ファームウェアファイルとそのステータスが表示されます。

   ファームウェア イメージ ファイルが有効で、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**] 情報を確認します。

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。
   - ファームウェアアップデートをキャンセルするには、**キャンセル** をクリックします。

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

6. [**ジョブ キュー**] ページを表示するには、[**ジョブ キュー**] をクリックします。このページを使用してステージングされたファームウェア アップデートを表示し管理するか、または [**OK**] をクリックして現在のページを更新しファームウェア アップデートのステータスを表示します。

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

メモ: ファームウェア ファイルのアップロード後にセッションが期限切れになると、続行できなくなります。この問題は、RACADM をリセットすることによってのみ解決できます。

自動ファームウェアアップデートのスケジュール設定

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

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

メモ: DRM の詳細については、www.dell.com/openmanagemanuals > Repository Manager を参照してください。

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

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

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

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

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

メモ: ジョブがすでに スケジュール済み である場合は、自動アップデートの次回スケジュールを作成しないでください。現在のスケジュール済みジョブが上書きされます。

1. iDRAC ウェブインタフェースで、**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。
   ファームウェアのアップデート ページが表示されます。
2. **自動アップデート** タブをクリックします。
3. **自動アップデートの有効化** オプションを選択します。
4. 次のオプションのいずれかを選択して、アップデートのステージ後にシステム再起動が必要かどうかを指定します。
   - **アップデートをスケジュール** — ファームウェアアップデートをステージしても、サーバーは再起動しません。

- **アップデートをスケジュールしてサーバーを再起動** — ファームウェアアップデートのステージ後のサーバー再起動を有効にします。

5. 次のいずれかを選択して、ファームウェアイメージの場所を指定します。
   - **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。ネットワーク共有ロケーションの詳細を入力してください。

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

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

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

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

RACADM を使用した自動ファームウェア アップデートのスケジュール

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

- ファームウェアの自動アップデートを有効にする：

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

- ファームウェアの自動アップデートのステータスを表示する：

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

- ファームウェアのアップデートの開始時刻および頻度をスケジュールする：

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

  例：
  - CIFS 共有を使用してファームウェアを自動アップデートする：

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

  - FTP を使用してファームウェアを自動アップデートする：

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

- 現在のファームウェアのアップデートのスケジュールを表示する：

```
racadm AutoUpdateScheduler view
```

- ファームウェアの自動アップデートを無効にする：

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

- スケジュールの詳細をクリアする：

```
racadm AutoUpdateScheduler clear
```

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のファームウェアをアップデートするには、update 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* にある *https://www.dell.com/idracmanuals* を参照してください。

例：

- リモート HTTP 共有からアップデート ファイルをアップロードします。

```
racadm update -f <updatefile> -u admin -p mypass -l http://1.2.3.4/share
```

- リモート HTTPS 共有からアップデート ファイルをアップロードします。

```
racadm update -f <updatefile> -u admin -p mypass -l https://1.2.3.4/share
```

- アップデートのリポジトリを使用して比較レポートを生成する場合：

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

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

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

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

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

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。
   iDRAC の導入 ページが表示されます。
3. **iDRAC の起動** ウェブインタフェースをクリックし、**iDRAC ファームウェアアップデート** を実行します。

DUP を使用したファームウェアのアップデート

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

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

  メモ: Linux で DUP ユーティリティーを使用して 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 usbarbitrator stop コマンドを使用して「usbarbitrator」サービスが停止されていることを確認します。

DUP 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作成されることで生じていきます。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_21.60.5.EXE および 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、3 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、NDT09 でのみサポートされています。
- グループ B は、NDT09 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。NDT09 を単独で使用していれば、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、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。その場

合「このデバイスのジョブはすでに存在します」というエラーで失敗す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、アップデート ソフトウェアでは解決できません。また、グループ A とグループ C のデバイスをサポートするには、両方の DUP が必要です。この競合は、デバイスでのロールバック実行時にも生じます。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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

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

Lifecycle Controller – Remote Services を使用してファームウェアをアップデートする方法の詳細については、https://www.dell.com/idracmanuals から入手可能な『*Lifecycle Controller リモート サービス クイック スタート ガイド*』を参照してください。

iDRAC からの CMC ファームウェアのアップデート

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

アップデートを適用する前に、次の事項を確認してください。

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

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

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

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

1. CMC ウェブインタフェースを起動します。
2. **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。
   Chassis Management Controller ファームウェアアップデート設定 ページが表示されます。
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。
4. **Current CMC Setting (現在の CMC 設定)** で、**Chassis Management at Server Mode (サーバモードでのシャーシ管理)** オプションに **Manage and Monitor (管理と監視)** が表示されていることを確認します。これは、CMC で設定できます。

ステージングされたアップデートの表示と管理

設定ジョブおよびアップデートジョブなどのスケジューリングされたジョブを表示および管理できます。これは、ライセンス付きの機能です。次回の起動時に実行するためにキュ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ジングされたアップデートの表示と管理

iDRAC ウェブインタフェースを使用してスケジュールされたジョブのリストを表示するには、**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ューに入れられていたすべてのジョブを削除できます。アクティブなジョブ、(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 を使用したステージングされたアップデートの表示と管理

RACADM を使用してステージング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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

デバイスファームウェアのロールバック

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
- バックプレーン

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

ファームウェアをロールバックする前に、次を確認してください。

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

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

- iDRAC ウェブインタフェース
- CMC Web インターフェイス (MX プラットフォームでは未サポート)
- OME-Modular Web インターフェイス (MX プラットフォームでサポート)
- CMC RACADM CLI (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 1 つ、または複数の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、「ジョブキューをアップデートしています」のメッセージが表示されます。
4. **ジョブキュー** をクリックします。
   ステージ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用にステージされているか、またはすでに実行状況である。

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

CMC ウェブインタフェースを使用したファームウェアのロールバック

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

1. CMC ウェブインタフェースにログインします。
2. **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. 88」の項で説明されているとおりにデバイスファームウェアのロールバックを実行します。

RACADM を使用したファームウェアのロールバック

1. 次の `swinventory` コマンドで、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 swinventory
   ```

   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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

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

詳細については、https://www.dell.com/idracmanuals から入手可能な『*Lifecycle Controller ユーザーズガイド*』を参照してください。

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

詳細については、https://www.dell.com/idracmanuals から入手可能な『*Lifecycle Controller リモートサービスクイックスタートガイド*』を参照してください。

iDRAC のリカバリ

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

- iDRAC ブートローダーは、起動可能なイメージがないことを検出します。
- システムの正常性と識別 LED が 1/2 秒以下の間隔で点滅します (LED はラックおよびタワーサーバの背面と、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 EXT3 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。

他のシステム管理ツールを使用した iDRAC の監視

iDRAC は、Dell Management Console または Dell OpenManage Essentials を使用して検出および監視できます。また、Dell Remote Access Configuration Tool (DRACT) を使用して、iDRAC の検出、ファームウェアのアップデート、および Active Directory のセットアップを行うこともできます。詳細については、それぞれのユーザーズガイドを参照してください。

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、それらすべてを 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プ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てはいません。

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、ジョブキューページで見ることができます。

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。

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しく選択する必要があります。たとえば、import.xml です。

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。

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、複数のシステムに 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。

   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。
7. 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ーを接続することで 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。
8. LCL に、ジョブの進行状況が表示されます。
9. 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。
10. 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ルのインポート

サーバ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. **設定** > **サーバ設定プロファイル** に移動します。
   サーバ設定プロファイル 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。

   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。
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、次の手順を実行します。

1. **設定** > **サーバ設定プロファイル** に移動します。
   サーバ設定プロファイル ページが表示されます。
2. **エクスポート** をクリックします。
3. 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。
4. 設定のバックアップを必要とするコンポーネントを選択します。
5. **エクスポートタイプ** を選択し、次のオプションのいずれかを選択します。
   - **基本**
   - **交換エクスポート**
   - **クローンエクスポート**
6. **エクスポートファイルフォーマット** を選択します。
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てから、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する業界標準を表しています。

有効にすると、UEFI セキュアブートにより、署名されていない UEFI デバイスのドライバのロードが阻止されてエラーメッセージが表示され、そのデバイスの動作は拒否されます。署名されていないデバイスのドライバをロードするときは、セキュアブートを無効にする必要があります。

Dell 第 14 世代以降の PowerEdge サーバでは、異なるインタフェース (RACADM、WSMAN、REDFISH、LC-UI) を使用して、セキュアブート機能を有効または無効にすることができます。

使用可能なファイルフォーマット

セキュアブートポリシーには 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。プラットフォームの製造元またはプラットフォームの所有者のどちらかが、パブリック 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、プラッ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ーは、db と dbx を使用して、プレ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を関連付ける必要があり、dbx ではキーまたはハッシュ値を関連付けません。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

ポリシーコンポーネント	使用可能なファイルフォーマット	使用可能なファイル拡張子	最大レコード数
PK	X.509 証明書(バイナリ DER 形式のみ)	1. .cer 2. .der 3. .crt	1 回
KEK	X.509 証明書(バイナリ DER 形式のみ) 公開キーストア	1. .cer 2. .der 3. .crt 4. .pbk	1 回以上
DB および DBX	X.509 証明書(バイナリ DER 形式のみ) 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)	1. .cer 2. .der 3. .crt 4. .efi	1 回以上

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継承しています。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、リセット、すべてリセット 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、リセット、すべてリセット など、PK、KEK、DB、DBX 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) を選択し、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、およびリセット 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 すべてリセット 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、すべてリセット 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、https://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。

4

iDRAC の設定

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

iDRAC を設定する前に、iDRAC ネットワーク設定と対応ブラウザー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な機能の詳細については、iDRAC ライセンス 、p. 24 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 Web インターフェイス
- RACADM
- Remote Services (『Lifecycle Controller Remote Services ユーザーズガイド』を参照)
- IPMITool (『*ベースボード マネジメント コントローラー管理ユーティリティー 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
8. 必要な証明書を取得します。
9. iDRAC ユーザーを追加し、権限を設定します。
10. 電子メールアラート、SNMP トラップ、または IPMI アラートを設定し、有効にします。
11. 必要に応じて電力上限ポリシーを設定します。
12. 前回のクラッシュ画面を有効にします。
13. 必要に応じて仮想コンソールと仮想メディアを設定します。
14. 必要に応じて vFlash SD カードを設定します。
15. 必要に応じて最初の起動デバイスを設定します。
16. 必要に応じて OS を iDRAC パススルーに設定します。

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
- 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 が有効
- 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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』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。

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

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

Web インターフェイ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 Web インターフェイスで、**iDRAC 設定** > **接続性** > **ネットワーク** > **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。
   ネットワーク設定で**自動専用 NIC** を選択した場合、NIC 選択が共有 LOM (1、2、3、4) で、iDRAC 専用 NIC でリンクが検知されると、iDRAC は NIC 選択を変更し、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。切り替えまでの時間は、共有から専用の場合は 5 秒、専用から共有までの場合は 30 秒です。この値は、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。

   メモ: iDRAC が DHCP を使用しており、その IP アドレスのリースを取得している場合、NIC または Ipv4 または DHCP が無効化されていると、DHCP サーバーのアドレス プールに戻されて解放されます。

ローカル RACADM を使用したネットワーク設定の変更

使用可能なネットワークプロパティのリストを生成するには、コマンドを使用します。

```
racadm get iDRAC.Nic
```

DHCP を使用して IP アドレスを取得するには、次のコマンドを使って `DHCPEnable` オブジェクトを書き込み、この機能を有効にします。

```
racadm set iDRAC.IPv4.DHCPEnable 1
```

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

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

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

IP フィルタの設定

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

- IP フィルタは、iDRAC にアクセス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 にログインできなくなります。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。

メモ: 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。

メモ: クライアント IP アドレスからのログイン試行が拒否されると、「`ssh 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。

メモ: Dell Deployment Toolkit (DTK) を使用する場合は、権限について https://www.dell.com/openmanagemanuals から入手可能な『*OpenManage 導入ツールキット ユーザーズガイド*』を参照してください。

iDRAC ウェブインタフェースを使用した IP フィルタの設定

これらの手順を実行するには、設定権限が必要です。

IP フィルタを設定するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**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。
   メモ: **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。

メモ: 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

^

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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』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 インターフェイスで、**[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** オプションの下のにある **暗号文字列の設定** 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.customCipherString ALL:!DHE-RSA-AES256-GCM-SHA384:!DHE-RSA-AES256-GCM-SHA384`
- `racadm set idraC.webServer.customCipherString ALL:-DHE-RSA-CAMELLIA256-SHA`
- `racadm set idraC.webServer.customCipherString ALL:!DHE-RSA-AES256-GCM-SHA384:!DHE-RSA-AES256-SHA256:+AES256-GCM-SHA384:-DHE-RSA-CAMELLIA256-SHA`

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

FIPS モード

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

IDRAC は今後 FIPS モードのサポートを正式に認証します。

FIPS モードのサポートと検証済み FIPS との違い

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

FIPS モードの有効化

注意: FIPS モードを有効にすると、iDRAC を工場出荷時の設定にリセットします。設定を復元する場合は、FIPS モードを有効にする前にサーバ構成プロファイル（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。

3. 変更の確認を求めるメッセージが表示されます。**OK** をクリックします。
   iDRAC が FIPS モードで再起動します。iDRAC に再接続するまでに少なくとも 60 秒間待機します。
4. iDRAC の信頼できる証明書をインストールします。

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

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

RACADM を使用した FIPS モードの有効化

RACADM CLI を使用して、次のコマンドを実行します。

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

FIPS モードの無効化

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

サービスの設定

iDRAC では、次のサービスを設定し、有効にできます。

ローカル設定	ローカル RACADM および iDRAC 設定ユーティリティを使用して iDRAC 設定へのアクセス（ホストシステムから）を無効にします。
Web サーバ	iDRAC Web インターフェイスへのアクセスを有効にします。Web インターフェイスを無効にすると、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 アーキテクチャを使用して、iDRAC でセキュアなエンタープライズ 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。
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	Redfish RESTful API のサポートを有効にします。
VNC サーバ	SSL 暗号化あり、または無しで VNC サーバを有効にします。

Web インターフェイスを使用したサービスの設定

iDRAC Web インターフェイ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 インターフェイスで、**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ります。

   [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。

   メモ: セキュリティ（暗号化）モードが**なし**から **SEKM** に変更された場合、リアルタイム ジョブは実行できません。ただし、このジョブは [ステージング] ジョブ リストに追加されます。また、このモードが **SEKM** から**なし**に変更されれば、リアルタイム ジョブは正常に実行されます。

   KeySecure サーバーで [クライアント証明書] セクションの**ユーザー名**フィールドの値を変更した場合（**共通名（CN）**を**ユーザー ID（UID）**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 の既存ユーザー名が一致していることを確認します。一致していない場合、[ユーザー名] フィールドの設定、SSL 証明書の再生成、KMS へのサインオン、iDRAC への再アップロードを順に実行する必要があります。

   b. 新しいユーザー アカウントを使用している場合：
      - **ユーザー名**の文字列と iDRAC SSL 証明書の [ユーザー名] フィールドが一致していることを確認します。
      - 一致していない場合、iDRAC KMS 属性のユーザー名とパスワードを再設定する必要があります。
      - 証明書にユーザー名が含まれていることを確認したら、後は単に、キーの所有権を以前のユーザーから新しいユーザーに移行し、新たに作成した KMS ユーザー名と一致させるだけです。

   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ポート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。
   - SEKM は、クライアント証明書の [**ユーザー名**] フィ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。

- サード パーティー CA を iDRAC CSR への署名に使用している場合、サード パーティー CA がクライアント証明書の**ユーザー名**フィ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**フィールドの値として**共通名**を使用してください。
- [ユーザー名] フィールドと [パスワード] フィ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。

メモ: KeySecure キー管理サーバーの場合、

- SSL 証明書リクエスト作成時に、**件名の代替名**フィールドにキー管理サーバーの IP アドレスを含める必要があります。
- IP アドレスの形式は「IP:xxx.xxx.xxx.xxx」にする必要があります。

RACADM を使用したサービスの設定

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

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

これらのオブジェクトの詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

HTTPS リダイレクトの有効化または無効化

デフォルトの iDRAC 証明書における証明書警告問題、またはデバッグ目的の一時的な設定を理由に、HTTP から HTTPs への自動リダイレクトを行いたくない場合は、http ポート (デフォルトは 80) から https ポート (デフォルトは 443) へのリダイレクトが無効化されるように iDRAC を設定することができます。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
```

VNC クライアントを使用したリモートサーバーの管理

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

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

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

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 つめのセッション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。

ビデオ暗号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) 中に、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、仮想メディアのみを許可します。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) を待ってから、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。
   仮想コンソール ページが表示されます。
2. **VNC サーバー** セクションで VNC サーバーを有効にし、パスワードとポート番号を指定して、SSL 暗号化を有効または無効にします。
   フィールドについては、『iDRAC オンラインヘルプ』を参照してください。
3. **適用** をクリックします。
   VNC サーバーが設定されました。

RACADM を使用した VNC サーバーの設定

VNC サーバを設定するには、`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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

SSL 暗号化を伴う VNC ビューアの設定

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

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

SSL トンネルアプリケーションを設定するには、次の手順を実行します。

1. SSL トンネルが、`<localhost>:<localport number>` での接続を受け入れるように設定します。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 サーバに接続します。iDRAC で VNC サーバを設定するときに SSL 暗号化オプションが無効になっている場合、VNC ビューアに接続するには、以下を実行します。

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

形式は `<iDRAC IP address:VNC port number>` 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 ID LED 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)。有効にすると、アクティブな仮想コンソールセッションがある場合に、サーバの 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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

iDRAC 設定ユーティリティを使用した LCD の設定

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

1. iDRAC 設定ユーティリティで、**前面パネルセキュリティ** に移動します。
   iDRAC 設定。前面パネルセキュリティ ページが表示されます。
2. 電源ボタンを有効化または無効化します。
3. 以下を指定します。
   - 前面パネルへのアクセス
   - LCD メッセージ文字列
   - システム電源装置、周囲温度装置、およびエラーディスプレイ
4. 仮想コンソール表示を有効化または無効化します。
   オプションについては、『iDRAC 設定ユーティリティオンラインヘルプ』を参照してください。
5. **戻る**、**終了** の順にクリックし、**はい** をクリックします。

システム ID LED の設定

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

ウェブインタフェースを使用したシステム ID LED の設定

システム ID LED ディスプレイを設定するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

タイムゾーンおよび NTP の設定

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

タイムゾーンまたは NTP の設定には、設定権限が必要です。

iDRAC ウェブインタフェースを使用したタイムゾーンと NTP の設定

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

1. **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、`set` コマンドを、 `iDRAC.Time` のオブジェクトおよび `iDRAC.NTPConfigGroup` グループとともに使用します。

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

メモ: iDRAC は、ホスト (ローカル時刻) と時刻を同期します。したがって、時刻の同期が適切であるように、iDRAC とホストの両方に同じタイムゾーンを設定することをお勧めします。タイムゾーンを変更する場合は、ホストと iDRAC の両方で変更し、その後、ホストを再起動する必要があります。

最初の起動デバイスの設定

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

最初の起動デバイスは次のいずれかに設定できます。

- 通常起動
- PXE
- BIOS セットアップ
- ローカルフロッピー / プライマリリムーバブルメディア
- ローカル CD/DVD
- ハードドライブ
- 仮想フロッピー
- 仮想 CD/DVD/ISO
- ローカル SD カード
- Lifecycle Controller
- BIOS 起動マネージャ
- UEFI デバイスパス
- 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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

仮想コンソールを使用した最初の起動デバイスの設定

サーバ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アで表示される際に、起動するデバイスを選択できます。Boot Once (一回のみ起動) は、「最初の起動デバイスの設定 、p. 105」に記載されているすべてのデバイスでサポートされます。

仮想コンソールを使用して最初の起動デバイスを設定するには、次の手順を実行します。

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

前回のクラッシュ画面の有効化

管理下システムのクラッシュの原因をトラブルシューティングするため、iDRAC を使用してシステムのクラッシュイメージを取得できます。

メモ: Server Administrator の詳細については、https://www.dell.com/openmanagemanuals から入手可能な『*OpenManage インストール ガイド*』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 へのパススルーの有効化または無効化

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

メモ: iDRAC サービスモジュール (ISM) は、オペレーティングシステムから iDRAC を管理するための多くの機能を提供します。詳細については、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。

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、Chassis Management Controller 経由です。

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

このチャネルは以下を使用して有効化できます。

- iDRAC ウェブインタフェース
- RACADM または 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 へのパススルー機能を有効化する、または OS ホスト IP アドレスを設定するためには、15 秒間待つ必要があります。

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

- iDRAC は、専用 NIC または共有モードを使用するように設定されている。(NIC の選択が、LOM の 1 つに割り当てられていることを意味する。)
- ホストオペレーティングシステムと iDRAC が同一サブネットおよび同一 VLAN 内にある。
- ホストオペレーティングシステム IP アドレスが設定されている。
- OS から iDRAC へのパススルー機能をサポートするカードが装備されている。
- 設定権限がある。

この機能を有効にする場合は、以下に留意してください。

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

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

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

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

メモ: USB NIC が無効状態のときに iDRAC サービス モジュールを起動すると、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 チーミングが有効になっている場合、LOM パススルーを使用してホストサーバから 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

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

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

カテゴリ	製造元	タイプ
NDC	Broadcom	• 5720 QP rNDC 1G BASE-T
	Intel	• x520/i350 QP rNDC 1G BASE-T

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

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、以下を実行します。

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

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

出力は次のとおりです。

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

3. サーバーを再起動します。
4. ESXi プロンプトで、`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 バ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 ブート後にホスト 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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC 属性レジストリー*』を参照してください。

iDRAC 設定ユーティリティを使用した OS から iDRAC へのパススルーの有効化または無効化

iDRAC 設定ユーティリティを使用して OS から iDRAC へのパススルーを有効または無効にするには、次の手順を実行します。

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

   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。

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

4. 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。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。

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

ログインタイプ	証明書タイプ	取得方法
Active Directory を使用したシングルサインオン	信頼済み CA 証明書	CSR を生成し、認証局の署名を取得します。 SHA-2 証明書もサポートされています。
ローカルユーザーまたは Active Directory ユーザーとしてのスマートカードログイン	• ユーザー証明書 • 信頼済み CA 証明書	• ユーザー証明書 — スマートカードベンダーが提供するカード管理ソフトウェアを使用して、スマートカードユーザー証明書を Base64 でエンコードされたファイルとしてエクスポートします。 • 信頼済み CA 証明書 — この証明書は、CA によって発行されます。 SHA-2 証明書もサポートされています。
Active Directory ユーザーログイン	信頼済み CA 証明書	この証明書は、CA によって発行されます。 SHA-2 証明書もサポートされています。
ローカルユーザーログイン	SSL 証明書	CSR を生成し、認証局の署名を取得します。 メモ: iDRAC にはデフォルトの自己署名型 SSL サーバ証明書が付属しています。iDRAC ウェブサーバ、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。

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 ポリシーファイルのインストールが必要になる場合があります。ポリシーファイルのインストールの詳細については、Java のマニュアルを参照してください。

iDRAC ウェブサーバには、デルの自己署名固有の 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。認証局とは、情報テクノロジ業界において、信頼のおける審査、識別、およびその他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 などがあります。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 VerSign や Thawte などの CA に送信します。CA は、ルート CA または中間 CA になります。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 が信頼されます。カスタム SSL 証明書がすでに使用されているときにカスタム署名証明書をアップロードすると、そのカスタム SSL 証明書は無効になり、カスタム署名証明書で署名された 1 回限りの自動生成 SSL 証明書が使用されます。カスタム署名証明書はプライベートキーなしでダウンロードできます。既存のカスタム署名証明書を削除することもできます。カスタム署名証明書を削除すると、iDRAC はリセットされ、新しい自己署名 SSL 証明書が自動生成されます。自己署名証明書が再生成されると、iDRAC と管理ステーション間で信頼関係を再確立する必要があります。自動生成された SSL 証明書は自己署名され、有効期限は 7 年と 1 日、開始日は 1 日前になります (管理ステーションと iDRAC でタイムゾーン設定が異なるため)。

iDRAC ウェブサーバの SSL 証明書は、証明書署名要求 (CSR) の生成時に共通名 (CN) の左端部分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と呼ばれます。iDRAC 以外でワイルドカード CSR が生成された場合は、1 つの署名済みワイルドカード SSL 証明書で複数の iDRAC にアップロードすることができ、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に接続する間、iDRAC はブラウザによって信頼されます。ビューアを起動すると、iDRAC はビューアのクライアントによって信頼されます。

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、サーバのクライアントがサーバの ID を信頼し、サーバとの暗号化セッションのネゴシエーションをできるようになります。

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

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

Web インターフェイスを使用した CSR の生成

新規の CSR を生成するには、次の手順を実行します。

メモ: 新しい CSR を生成すると、ファームウェアに保存されている以前の CSR データがそれぞれ上書きされます。CSR 内の情報は、SSL サーバー証明書内の情報と一致する必要があります。そうでない場合、iDRAC はその証明書を受け入れません。

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 が生成されます。管理ステーションにそれを保存します。

RACADM を使用した CSR の生成

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

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

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。この機能を有効にすると、既存の Web サーバー証明書は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 ライセンスが必須です。
- 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

メモ: これらのパラメーターの詳細については、*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、有効期限が切れると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 - NDES サーバーで問題が発生しました。
- なし - デフォルト。

メモ: 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。**証明書アップロード** ページが表示されます。
2. **ファイル パス** で **参照** をクリックして、管理ステーションの証明書を選択します。
3. **適用** をクリックします。
   SSL サーバー証明書が iDRAC にアップロードされます。
4. iDRAC をすぐに、または後でリセットするかどうかを尋ねるポップアップメッセージが表示されます。必要に応じて、**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 はリセットされ、新しい証明書が適用されます。リセット中は、iDRAC を数分間使用できなくなります。
   メモ: 新しい証明書を適用するには iDRAC をリセットする必要があります。iDRAC がリセットされるまで、既存の証明書がアクティブになります。

RACADM を使用したサーバー証明書のアップロード

SSL サーバ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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

iDRAC の外でプライベートキーを使用して CSR が生成された場合に、iDRAC に証明書をアップロードするには、次の手順を実行します。

1. CSR を既知のルート CA に送信します。CA 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。
   iDRAC がリセットされると、新しい証明書が適用されます。リセット中、iDRAC は数分間使用できません。

   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は、既存の証明書が有効です。

サーバー証明書の表示

現在 iDRAC で使用されている SSL サーバー証明書を表示できます。

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 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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

カスタム署名証明書のアップロード

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

ウェブインタフェースを使用したカスタム署名証明書のアップロード

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

1. **iDRAC Settings (iDRAC 設定)** > **Connectivity (接続)** > **SSL** の順に移動します。
   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 SSL 証明書署名証明書をアップロードするには、`sslcertupload` コマンドを使用し、次に `racreset` コマンドを使用して iDRAC をリセットします。

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

カスタム SSL 証明書署名証明書のダウンロード

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

カスタム署名証明書のダウンロード

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

1. **iDRAC Settings (iDRAC 設定)** > **Connectivity (接続)** > **SSL** の順に移動します。
   SSL ページが表示されます。
2. **カスタム SSL 証明書署名証明書** で、**カスタム SSL 証明書署名証明書のダウンロード** を選択して **次へ** をクリックします。
   選択した場所にカスタム署名証明書を保存できるポップアップメッセージが表示されます。

RACADM を使用したカスタム SSL 証明書署名証明書のダウンロード

カスタム SSL 証明書署名証明書をダウンロードするには、`sslcertdownload` サブコマンドを使用します。詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

カスタム SSL 証明書署名証明書の削除

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

iDRAC ウェブインタフェースを使用したカスタム署名証明書の削除

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

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

RACADM を使用したカスタム SSL 証明書署名証明書の削除

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

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

RACADM を使用した複数の iDRAC の設定

RACADM を使用して、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整理されています。
- 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、https://www.dell.com/support/home/ja-jp//products?app=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。

```
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、グループ内のすべての設定プロパティ（グループ名とインデックスで指定）と、ユーザーのすべての設定プロパティを表示します。

2. 必要に応じて、テキストエディタを使用して設定ファイルに変更を加えます。

   メモ: このファイルは、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 ユーティリティは、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、ユーザーと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。

5

OAuth 2.0 を使用した委任認証

委任認証機能を使用すると、ユーザーまたはコンソールは、最初に認証サーバーから取得した OAuth 2.0 JSON Web Token (JWT) を使用して iDRAC API にアクセスできます。OAuth JWT が取得されると、ユーザーまたはコンソールはそれを使用して iDRAC API を呼び出すことができます。これにより、ユーザー名とパスワードを指定して API にアクセスする必要がなくなります。

メモ: この機能は、DataCenter ライセンスでのみ使用できます。この機能を使用するには iDRAC 設定権限またはユーザー設定権限が必要です。

iDRAC では、最大 2 つの認証サーバーの構成がサポートされています。この構成では、ユーザーは次の認証サーバーの詳細を指定する必要があります。

- **名前** - iDRAC 上の認証サーバーを識別する文字列。
- **メタデータ URL** - サーバーによってアドバタイズされる OpenID Connect 準拠 URL。
- **HTTPS 証明書** - サーバーとの通信に iDRAC が使用するサーバー公開キー。
- **オフライン キー** - 認証サーバーの JWK セット ドキュメント。
- **オフライン発行者** - 認証サーバーによって発行されるトークンで使用される発行者文字列。

オンライン設定の場合：

- 認証サーバーを構成する場合、iDRAC 管理者は、iDRAC が認証サーバーにオンライン ネットワーク アクセスできるようにする必要があります。
- iDRAC が認証サーバーにアクセスできない場合、構成は失敗し、有効なトークンが提示されていても、その後の iDRAC API へのアクセス試行は失敗します。

オフライン構成の場合：

- iDRAC は認証サーバーと通信する必要はありませんが、その代わりに、オフラインでダウンロードしたメタデータの詳細を使用して構成されます。オフラインで構成した場合、iDRAC には署名キーの公開部分があり、認証サーバーへのネットワーク接続がなくてもトークンを検証することができます。

6

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。ブ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、メモリー、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 (アクセラレーター) 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 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 ウェブインタフェースにログインすると、**システムサマリ** で管理下システムの正常性や基本的な iDRAC 情報の表示、仮想コンソールのプレビュー、作業メモの追加と表示を行ったり、電源オン / オフ、パワーサイクル、ログの表示、ファームウェアのアップデートとロールバック、前面パネル LED のスイッチオン / オフ、および iDRAC のリセットなどのタスクをを迅速に開始することが可能になります。

[**システム サマリー**] ページにアクセスするには、**[システム]** > **[概要]** > **[サマリー]** の順に移動します。**システムサマリ** ページが表示されます。詳細については、*iDRAC オンラインヘルプ*を参照してください。

iDRAC 設定ユーティリティーを使用して、基本的なシステム サマリー情報を表示することもできます。これを行うには、iDRAC 設定ユーティリティーで、[**システム サマリー**] に移動します。[**iDRAC 設定システム サマリー**] ページが表示されます。詳細については、『*iDRAC Settings Utility Online Help*』(iDRAC 設定ユーティリティー オンライン ヘルプ) を参照してください。

アセット追跡の設定

iDRAC 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。これには、取得、保証、サービスなどの情報が含まれます。

メモ: iDRAC でのアセット追跡は、OpenManage Server Administrator のアセット タグ機能に似ています。ただし、関連するアセット データをレポートするには、これらの両方のツールで属性情報を個別に入力する必要があります。

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指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、**[システム]** > **[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]** > **[インベントリー]** 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 インベントリーには、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ーを収集する場合、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。

ハードウェアコンポーネントのどれかを交換する場合、もしくはファームウェアバージョンをアップデートする場合は、**再起動時にシステムインベントリを収集する** (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。

センサー情報の表示

次のセンサーは、管理下システムの正常性を監視するために役に立ちます。

- **バッテリー** — システム 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サーバの場合のみ利用可能）— システムファンに関する情報を提供します（ファン冗長性、およびファン速度としきい値を表示するファンのリスト）。
- **CPU** - 管理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、プロセッサー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。
- **イントルージョン** — シャーシについての情報を提供します。
- **電源装置**（ラックおよびタワーサーバの場合のみ利用可能）— 電源装置と電源装置の冗長性状態に関する情報を提供します。

  メモ: システムに電源装置が 1 つしかない場合、電源装置の冗長性は **無効** に設定されます。
- **リムーバブルフラッシュメディア** — 内部 SD モジュール（vFlash および内部デュアル SD モジュール（IDSDM））に関する情報を提供します。
  - IDSDM の冗長性が有効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 センサー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 のみが表示されます。
  - システムの電源がオンになったとき、または iDRAC のリセット後は、当初 IDSDM の冗長性が無効化されています。カードの挿入後にのみ IDSDM SD1 センサーのステータスが表示されます。
  - IDSDM の冗長性が有効になっていて、IDSDM に 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 内の 2 枚の SD カード間で冗長性を復元するには、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 つの SD カード間で冗長性を復元する再構築中は、IDSDM センサーの電源がオフであるため、IDSDM ステータスが表示されません。

    メモ: IDSDM 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。
  - IDSDM モジュール内の書き込み保護された、または破損した SD カードに対するシステムイベントログ（SEL）は、SD カードを書き込み可能または破損なしの SD カードと取り換えることによってクリアされるまで繰り返されません。

  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。
- **温度** - システム ボードの吸気温度と排気温度に関する情報です（ラック サーバーにのみ適用されます）。温度プローブは、プローブのステータスが、予め設定された警告/重要閾値の範囲内にあるかどうかを示します。
- **電圧** — さまざまなシステムコンポーネントの電圧センサーの状態と読み取り値を示します。

次の表に、iDRAC Web インターフェイスと RACADM によるセンサー情報の表示についての情報を示します。Web インターフェイスに表示されるプロパティの詳細については、*iDRAC のオンライン ヘルプ*を参照してください。

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 インターフェイスと RACADM を使用したセンサー情報

情報を表示するセンサー	Web インターフェイス使用	RACADM 使用
バッテリー	**ダッシュボード** > **システム正常性** > **バッテリー**	`getsensorinfo` コマンドを使用します。 電源装置については、`get` サブコマンドとともに `System.Power.Supply` コマンドを使用することもできます。 詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。
ファン	**ダッシュボード** > > **システム正常性** > **ファン**	
CPU	**ダッシュボード** > **システム正常性** > **CPU**	

表 17. Web インターフェイスと RACADM を使用したセンサー情報（続き）

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

CPU、メモリー、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

Dell の第 14 世代 Dell PowerEdge サーバーでは、Intel ME が Compute Usage Per Second（CUPS）機能をサポートしています。CUPS 機能は、システムの CPU、メモリー、I/O 使用率、およびシステムレベルの使用率インデックスをリアルタイムで監視します。Intel ME は帯域外（OOB）パフォーマンス監視が可能であり、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、計算、メモリー、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、メモリー、および I/O の使用率インデックスの瞬時値も監視します。

メモ: CUPS 機能は、次のサーバーではサポートされていません。

- PowerEdge R240
- PowerEdge R240xd
- PowerEdge R340
- PowerEdge R6415
- PowerEdge R7415
- PowerEdge R7425
- PowerEdge T140

CPU とチップセットには、専用のリソース監視カウンター（RMC）があります。これらの RMC からデータを照会することで、システムリソースの使用率に関する情報が取得されます。RMC からのデータは、各システム リソースの累積使用率を測定するためにノード マネージャーによって集約されます。これは、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、帯域外管理インターフェイス経由で提供されます。

パフォーマンス パラメーターとインデックス値の Intel センサーの表示は、物理システム全体を対象としています。したがって、インターフェイス上のパフォーマンス データの表示は、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、物理システム全体に対するものになります。

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

4 つのシステム使用率のパラメータは次のとおりです。

- **CPU 使用率** — 各 CPU コアの RMC からのデータは、システム内のすべてのコアの累積使用率を提供するために集約されます。この使用率は、アクティブ状態であった時間と、非アクティブ状態であった時間に基づいています。RMC のサンプルは 6 秒ごとに取得されます。
- **メモリー使用率** — RMC は、各メモリー チャネルまたはメモリー コントローラー インスタンスで発生しているメモリー トラフィックを測定します。これらの RMC からのデータは、システム上のすべてのメモリー チャネルの累積メモリー トラフィックを測定するために集約されます。これは、メモリー帯域幅消費の測定であり、メモリー使用率の測定ではありません。iDRAC ではこのデータを 1 分間集約するため、Linux の **top** など、他の OS ツールのメモリー使用率の表示と一致しない場合があります。iDRAC に表示されるメモリー帯域幅の使用率は、メモリーを多く消費するワークロードであるかどうかを示しています。
- **I/O 使用率** — PCI Express Root Complex のルート ポートごとに 1 つの RMC があり、そのルート ポートや下位セグメントとの間で送受信される PCI Express トラフィックを測定します。これらの RMC からのデータは、パッケージから送信されるすべての PCI Express セグメントの 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です。

- **システムレベルの CUPS インデックス** — CUPS インデックスは、各システム リソースに対して事前に定義された負荷要因を考慮した CPU、メモリー、および I/O インデックスを集約することによって計算します。負荷要因は、システム上のワークロードの性質に依存します。CUPS インデックスは、サーバーで使用可能な計算ヘッドルームの測定値を表します。システムの CUPS インデックスが大きい場合、そのシステムにはさらにワークロードを割り当てるための制限付きヘッドルームが存在します。リソース消費量が減少するにつれて、システムの CUPS インデックスも減少します。CUPS インデックスが低い場合は、大きな計算ヘッドルームが存在し、サーバーが新たなワークロードを受け入れられること、およびサーバーが電力消費量を抑えるために低電力状態になっていることを示します。データ センター全体にワークロードの監視を適用することで、データ センターのワークロードのハイレベルかつ総合的なビューを提供することができるため、ダイナミック データ センター ソリューションが実現します。

メモ: CPU、メモリー、および I/O 使用率インデックスは、1 分で集約されます。そのため、これらのインデックスが瞬間的に急上昇した場合には抑制することが可能です。これらはリソース使用率ではなく、ワークロード パターンを示しています。

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 イベントが有効になっていると、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、デフォルトでは無効になっています。これは、標準の IPMI インターフェイ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、https://www.dell.com/idracmanuals から入手可能な『*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。

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、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。時間ごとのサンプルの 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

```
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

```
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

```
winrm e http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/root/dcim/DCIM_SystemAttribute -
u:root -p:calvin -r:https://<iDRAC IP>/wsman -SkipCNcheck -SkipCAcheck -encoding:utf-8 -
a:basic
```

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。以下のプロパティには Datacenter ライセンスが必要です。その他のプロパティは、Datacenter ライセンスなしでも表示されます。

- **温度指標 :**
  - GPU ターゲット温度
  - GPU ハードウェアの最小減速温度
  - GPU シャットダウン温度
  - メモリーの最大動作温度
  - GPU の最大動作温度
  - 温度アラートの状態
  - 電力ブレーキの状態
- **電力指標 :**
  - 電源装置の状態
  - 基板電源装置状態
- **テレメトリー** - すべての GPU テレメトリー レポート データ

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。インベントリーの [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 コントローラーの SMBPB インター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。この情報は、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 ターゲット温度、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ー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 ターゲット温度、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 ツールのコマンド `nvidia-smi -pm 1` を使用します。

テレメトリーを使用して GPU レポートを生成できます。テレメトリー機能の詳細については、次を参照： テレメトリー ストリーミング 、p. 211

メモ: RACADM では、値が空白のダミー GPU エントリー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 `racrest` 操作を実行します。

FPGA 監視

Field-programmable Gate Array (FPGA) デバイスでは、使用中に大量の熱を生成するため、リアルタイム温度センサーでの監視が必要です。FPGA インベントリー情報を取得するには、次の手順を実行します。

- サーバーの電源をオフにします。
- ライザー カードに FPGA デバイスを取り付けます。
- サーバーの電源をオンにします。
- POST が完了するまで待機します。
- iDRAC GUI にログインします。
- **システム** > **概要** > **アクセラレーター**の順に移動します。[GPU] と [FPGA] の両方のセクションを表示できます。
- 特定の FPGA コンポーネントを展開して、次のセンサー情報を表示できます。
  - 電力消費量
  - 温度詳細

メモ: FPGA の情報にアクセスするには、iDRAC ログイン権限が必要です。

メモ: 電力消費センサーはサポートされている FPGA カードでのみ使用可能で、Datacenter ライセンスがある場合にのみ使用可能です。

システムの Fresh Air 対応性のチェック

Fresh Air による冷却は、外気を直接使用してデータセンター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、**System (システム)** > **Overview (概要)** > **Cooling (冷却)** > **Temperature overview (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. サーバーが Fresh Air 対応かどうかについては、**Fresh Air** の項を参照してください。

温度の履歴データの表示

システムが通常サポートされる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。温度を監視するため、システム基板の温度センサーの読み取り値が一定期間にわたって収集されます。データ収集は、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開始されます。データは、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、フレッシュエアがサポートする制限値に基づきます。制限値は、42ºC で警告、47ºC で重大です。これらの値は、2ºC の精度マージンを持った 40ºC と 45ºC の フレッシュエア制限値に対応します。

フレッシュエア制限に関連付られた次の 2 つの固定温度領域が追跡されます。

- 警告領域 - システムが温度センサーの警告しきい値 (42ºC) 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できるのは 12 か月間で 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 (47ºC) 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できるのは 12 か月間で 1% で、これは警告領域の時間にも加算されます。

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

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

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

追加のイベントを生成するよう、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」セクション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 インターフェイスで、**[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 年の温度の保存データ (平均およびピーク値) のグラフを表示するには、「**システム基板温度の歴史的データ**」の項を参照してください。
   詳細については、『iDRAC オンラインヘルプ』を参照してください。

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

   メモ: WX3200 AMD GPU カードは現在、温度センサー用の I2C インターフェイスをサポートしていません。そのため、iDRAC インターフェイスからこのカードの温度を読み取ることができません。

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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

吸気口温度の警告しきい値の設定

システム基板の吸気口温度センサーの最小および最大警告しきい値を変更できます。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、次の手順を実行します。

1. iDRAC Web インターフェイスで、**[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. [**温度プローブ**] 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摂氏または華氏単位で入力します。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 IPv6 DHCP サーバーのアドレスが表示されない場合があります。

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

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

1. **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 FQDD** ドロップダウンメニューからネットワークデバイスを選択し、**適用** をクリックします。
   ホスト OS ネットワークインタフェース セクションに、OS IP の詳細が表示されます。
3. **デバイス FQDD** 列から、ネットワークデバイスリンクをクリックします。
   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ージが表示されます。このページでは、デバイス詳細の表示が可能です。プロパティの詳細については、*『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** 列が次のフォーマットで表示されます。

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

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

RACADM を使用してホストオペレーティングシステムで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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

FlexAddress メザニンカードのファブリック接続の表示

ブレードサーバーでは、FlexAddress により、管理下サーバーの各ポート接続に、永続的なシャーシ割り当てのワールドワイド名と MAC アドレス (WWN/MAC) を使用できます。

取り付け済みの内蔵 Ethernet ポートやオプションのメザニンカードポートごとに、次の情報を表示できます。

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

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

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

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

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

- **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が、iDRAC ウェブインタフェースを使用して iDRAC セッションを終了するには、iDRAC の設定権限が必要です。

iDRAC セッションを表示および終了するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**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、システム管理者権限が必要です。

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

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

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

7

iDRAC 通信のセットアップ

次のいずれかのモードを使用して iDRAC と通信できます。

- iDRAC Web インターフェイス
- DB9 ケーブルを使用したシリアル接続 (RAC シリアルまたは IPMI シリアル) - ラックサーバまたはタワーサーバの場合のみ
- IPMI シリアルオーバー LAN
- IPMI Over LAN
- リモート RACADM
- ローカル RACADM
- リモートサービス

メモ: ローカル RACADM のインポート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にしてください。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

通信のモード	対応プロトコル	対応コマンド	前提条件
iDRAC Web インターフェイス	インターネットプロトコル (https)	該当なし	Web サーバ
ヌルモデム DB9 ケーブルを使用したシリアル	シリアルプロトコル	RACADM IPMI	iDRAC ファームウェアの一部 RAC シリアルまたは IPMI シリアルが有効
IPMI シリアルオーバー LAN	インテリジェントプラットフォーム管理バスプロトコル SSH	IPMI	IPMITool がインストール済みで、IPMI シリアルオーバー LAN が有効
IPMI over LAN	インテリジェントプラットフォーム管理バスプロトコル	IPMI	IPMITool がインストール済みで、IPMI の設定が有効
リモート RACADM	https	リモート RACADM	リモート RACADM がインストール済みで、有効
ファームウェア RACADM	SSH	ファームウェア RACADM	ファームウェア RACADM がインストール済みで、有効
ローカル RACADM	IPMI	ローカル RACADM	ローカル RACADM がインストール済み
リモートサービス [1]	WSMan	WinRM (Windows) OpenWSMan (Linux)	WinRM (Windows) または OpenWSMan (Linux) がインストール済み
	Redfish	各種ブラウザのプラグイン、CURL (Windows と Linux)、Python リクエスト、JSON モジュール	プラグイン、CURL、Python モジュールがインストール済み

[1] 詳細については、https://www.dell.com/idracmanuals から入手可能な『*Lifecycle Controller ユーザーズガイド*』を参照してください。

トピック：

- DB9 ケーブルを使用したシリアル接続による iDRAC との通信

- DB9 ケーブル使用中の RAC シリアルとシリアルコンソール間の切り替え
- IPMI SOL を使用した iDRAC との通信
- IPMI over LAN を使用した iDRAC との通信
- リモート RACADM の有効化または無効化
- ローカル RACADM の無効化
- 管理下システムでの IPMI の有効化
- RHEL 6 での起動中の Linux のシリアルコンソールの設定
- RHEL 7 でのシリアルターミナルの設定
- サポート対象の SSH 暗号スキーム

DB9 ケーブルを使用したシリアル接続による iDRAC との通信

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

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

メモ: ブレードサーバの場合、シリアル接続はシャーシを介して確立されます。詳細については、https://www.dell.com/cmcmanuals から入手可能な『*Chassis Management Controller ユーザーズガイド*』(MX プラットフォームには該当しない) https://www.dell.com/openmanagemanuals から入手可能な『*PowerEdge MX7000 シャーシ向け OME - Modular ユーザーズガイド*』(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: ボーレートを変更した場合、vConsole または GUI からサーバ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、ボ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 テキスト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** > **シリアル通信** と移動します。
4. **リモートアクセスデバイス** に **外部シリアルコネクタ** を選択します。
5. **戻る**、**終了** の順にクリックし、**はい** をクリックします。
6. <Esc> を押して **セットアップユーティリティ** を終了します。

RAC シリアル接続の有効化

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

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

ウェブインタフェースを使用した RAC シリアル接続の有効化

RAC シリアル接続を有効にするには、次のコマンドを実行します。

1. iDRAC ウェブインタフェースで、**iDRAC Settings (iDRAC 設定)** > **Network (ネットワーク)** > **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. **RAC シリアル** で、**有効** を選択し、各属性の値を指定します。
3. **適用** をクリックします。
   RAC シリアル設定が設定されます。

RACADM を使用した RAC シリアル接続の有効化

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

IPMI シリアル接続のベーシックモードおよびターミナルモードの有効化

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

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

- IPMI 基本モード - ベースボード管理ユーティリティー (BMU) に含まれている IPMI シェル (ipmish) など、プログラム アクセス用のバイナリ インターフェイスをサポートします。例えば、IPMI 基本モード経由で 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 バッジで提供されます。
- 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。このモードは限られた数のコマンド (電源制御を含む) と、16 進数の ASCII 文字として入力される raw IPMI コマンドをサポートします。これにより、SSH を介して iDRAC にログインしている際に、オペレーティング システムのブート シーケンスを BIOS に表示できます。`[sys pwd -x]` を使用して IPMI ターミナルからログアウトする必要があります。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。

RACADM を使用したシリアル接続 IPMI モードの有効化

IPMI モードを設定するには、RAC シリアルインタフェースを無効にしてから、IPMI モードを有効にします。

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

n=0 — ターミナルモード

n=1 — 基本モード

RACADM を使用したシリアル接続 IPMI のシリアル設定の有効化

1. コマンドを使用して、IPMI シリアル接続モードを適切な設定に変更します。

   ```
   racadm set iDRAC.Serial.Enable 0
   ```

2. コマンドを使用して、IPMI シリアルボーレートを設定します。

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

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

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

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

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

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

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

5. BIOS でシリアル接続を設定するためには、BIOS セットアッププログラムでシリアル MUX (外部シリアルコネクタ) がリモートアクセスデバイスに対して適切に設定されているようにしてください。

これらのプロパティの詳細については、IPMI 2.0 仕様を参照してください。

IPMI シリアルターミナルモード用の追加設定

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

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

ターミナルモードを設定するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**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
- エコー制御
- ハンドシェイク制御
- 新しい行シーケンス
- 新しい行シーケンスの入力

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

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

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

ターミナルモードを設定するには、`idrac.ipmiserial` グループのオブジェクトで `set` コマンドを使用します。

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

DB9 ケーブル使用中の RAC シリアルとシリアルコンソール間の切り替え

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

シリアルコンソールから RAC シリアルへの切り替え

シリアルコンソールモードの時に、RAC シリアルインタフェース通信モードに切り替えるには、Esc+Shift、9 を押します。

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

RAC シリアルからシリアルコンソールへの切り替え

RAC シリアルインタフェース通信モードの場合にシリアルコンソールモードに切り替えるには、Esc+Shift、Q キーを押します。

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

シリアルコンソールモードで接続されているときにターミナルモードに戻るには、Esc+Shift、9 キーを押します。

IPMI SOL を使用した iDRAC との通信

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

- 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 Emergency Management Services (EMS) または Special Administrator Console (SAC)、Linux シェルでホストシステムを診断する。
- POST 中サーバーの進捗状況を表示し、BIOS セットアッププログラムを再設定する。

SOL 通信モードを設定するには、次の手順を実行します。

1. シリアル接続のための BIOS を設定します。
2. SOL を使用するように iDRAC を設定します。
3. サポートされるプロトコル (SSH、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
   - フェイルセーフボーレート — 115200
   - リモートターミナルの種類 — VT100/VT220
   - 起動後のリダイレクト — 有効
5. **次へ** をクリックしてから、**終了** をクリックします。
6. **はい** をクリックして変更を保存します。
7. <Esc> を押して **セットアップユーティリティ** を終了します。

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

   メモ: ブートローダまたはオペレーティングシステムが GRUB または Linux などのシリアルリダイレクトを提供する場合、BIOS の **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。
   IPMI SOL 設定が設定されます。
3. 文字の蓄積間隔と文字の送信しきい値を設定するには、**詳細設定** を選択します。
   シリアルオーバー LAN 詳細設定 ページが表示されます。
4. 各属性の値を指定し、**適用** をクリックします。

   IPMI SOL の詳細設定が設定されます。これらの値は、パフォーマンスの改善に役立ちます。

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

RACADM を使用した SOL を使用するための iDRAC の設定

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

1. コマンドを使用して IPMI シリアルオーバー LAN を有効にします。

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

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

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

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

メモ: IPMI 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 IPMI SOL のボーレートをアップデートします。

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

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

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

4. コマンドを使用して SOL を有効にします。

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

パラメータ	説明
<id>	ユーザー固有の ID

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

対応プロトコルの有効化

サポートされるプロトコルは、IPMI および SSH です。

Web インターフェイスを使用した対応プロトコルの有効化

SSH を有効にするには、**iDRAC 設定** > **サービス**に移動し、SSH に対して**有効**を選択します。

IPMI を有効にするには、**iDRAC 設定** > **接続性**に移動し、**IPMI 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 セキュリティを有効にするには、次のコマンドを使用します。

SSH

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

SSH ポートを変更するには

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

次のようなツールを使用できます。

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

IPMI プロトコルを使用した SOL

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

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

iDRAC 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 (キージェネレータキー)。iDRAC Web インターフェイスまたは iDRAC 設定ユーティリティーを使用して、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。

メモ: 必要に応じて、**iDRAC 設定** > **サービス** でデフォルトの SOL タイムアウトを変更できます。

1. 『Dell Systems Management Tools and Documentation』DVD から IPMITool をインストールします。
   インストール手順については、『ソフトウェアクイックインストールガイド』を参照してください。
2. コマンドプロンプト (Windows または Linux) で、次のコマンドを実行し、iDRAC から SOL を開始します。

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

   このコマンドで、管理ステーションが管理下システムのシリアルポートに接続されます。
3. IPMItool から SOL セッションを終了するには、「~」を押してから「.」(ピリオド) を押します。

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

メモ: Windows OS を実行しているクライアントから Linux OS を実行しているホストに長い入力テキストをコピーしている間に、IPMI SOL セッションが終了することがあります。セッションが突然終了しないようにするには、長いテキストを UNIX ベースの改行に変換します。

メモ: RACADM ツールを使用して作成された SOL セッションが存在する場合は、IPMI ツールを使用して別の SOL セッションを開始すると、既存のセッションに関する通知とエラーは表示されません。

メモ: Windows OS の設定により、ssh および IPMI ツールを介して接続されている SOL セッションでは、起動後に空白の画面が表示される場合があります。もう一度 SOL セッションを切断して再接続し、SAC プロンプトを表示します。

SSH を使用した SOL

Secure Shell (SSH) 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。リモート RACADM コマンドは、このインターフェイスを使用して解析することができます。

SSH では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 では、一度に最大 2 つから 4 つの SSH セッションをサポートします。

メモ: iDRAC バージョン 4.40.00.00 以降、telnet 機能は iDRAC から削除されているため、関連する属性レジストリ プロパティは廃止されています。これらのプロパティの一部は、既存のコンソール アプリケーションやスクリプトとの後方互換性を維持するために iDRAC で使用できますが、対応する設定は iDRAC ファームウェアによって無視されます。

メモ: SSH 接続の確立中には、2FA が無効化されている場合でも、「その他の認証が必要です」というセキュリティ メッセージが表示されます。

メモ: MX プラットフォームでは、1 つの SSH を iDRAC 通信に使用します。すべてのセッションを使用している場合は、1 つのセッションが解放されるまで、iDRAC は起動しません。

管理ステーションで PuTTY または OpenSSH などの SSH をサポートするオープン ソース プログラムを使用して、iDRAC に接続します。

メモ: Windows では、VT100 または ANSI ターミナル エミュレーターから OpenSSH を実行します。Windows コマンド プロンプトで OpenSSH を実行しても、機能のすべてを使用できません (一部のキーが応答せず、グラフィックが表示されません)。

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

1. シリアルコンソールを有効化するよう BIOS を設定。
2. iDRAC に SOL を設定。
3. iDRAC Web インターフェイスまたは RACADM を使用して、SSH を有効化。

   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 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ーは必要ありません。使用する SSH 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、SSH に自動的にリダイレクトされます。

Windows での PuTTY からの SOL の使用

メモ: 必要に応じて、**iDRAC 設定** > **サービス** でデフォルトの SSH タイムアウトを変更できます。

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

1. iDRAC に接続するには、次のコマンドを実行します。

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

   メモ: ポート番号はオプションです。ポート番号が再割り当てされた場合にのみ必要です。

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

   SSH プロトコルを使用して管理ステーションから管理下システムへの SOL セッションが開始されます。iDRAC コマンドライン コンソールにアクセスするには、ESC キー シーケンスに従ってください。Putty および SOL の接続動作 :

   - POST 時における PuTTY を介した管理下システムへのアクセス中、PuTTY のファンクションキーおよびキーパッドのオプションが次のように設定されます。
     - VT100+ — F2 はパスしますが、F12 はパスできません。
     - ESC[n~ — F12 はパスしますが、F2 はパスできません。
   - Windows で、ホストの再起動直後に非常時管理システム (EMS) コンソールが開かれた場合は、特殊管理コンソール (SAC) ターミナルが破損する可能性があります。SOL セッションを終了し、ターミナルを閉じ、別のターミナルを開いて、同じコマンドを使用して SOL セッションを開始します。

   メモ: Windows OS の設定により、ssh および IPMI ツールを介して接続されている SOL セッションでは、起動後に空白の画面が表示される場合があります。もう一度 SOL セッションを切断して再接続し、SAC プロンプトを表示します。

Linux での OpenSSH からの SOL の使用

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

メモ: 必要に応じて、**iDRAC 設定** > **サービス** で、デフォルトの SSH タイムアウトを変更できます。

1. シェルを起動します。
2. ssh *<iDRAC-ip- アドレス>* -l *<ログイン名>* コマンドを使用して iDRAC に接続します。
3. コマンドプロンプトで次のいずれかのコマンドを入力して、SOL を開始します。
   - `connect`
   - `console com2`

   これは、iDRAC を管理下システムの SOL ポートに接続します。SOL セッションが確立されると、iDRAC コマンド ライン コンソールは使用できなくなります。正しいエスケープ シーケンスに従って、iDRAC コマンド ライン コンソールを開きます。また、SOL セッションが接続されるとすぐに、画面にエスケープ シーケンスも出力されます。管理下システムが無効になっている場合は、SOL セッションの確立に時間がかかります。

   メモ: console com1 または console com2 を使用して、SOL を起動することができます。サーバーを再起動して接続を確立します。

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

履歴バッファーのデフォルト（および最大）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することができます。

```
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。

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ためのコマンドは、ユーティリティーに基づいています。ユーティリティーを終了するには、SOL セッションが完全に終了している必要があります。

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

- SOL リダイレクトを終了するには、<Enter>、<Esc>、<T> キーを押します。
  SOL セッションが閉じます。

ユーティリティーで SOL セッションが完全に終了していない場合は、他の SOL セッションを使用できない可能性があります。この問題を解決するには、Web インターフェイスの **iDRAC 設定** > **接続性** > **シリアル オーバー LAN** 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 ベースのオペレーティングシステムに対して IPv6 アドレスプロトコルもサポートします。

ウェブインタフェースを使用した IPMI over LAN の設定

IPMI Over LAN を設定するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**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。

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

IPMI Over LAN を設定するには、次の手順を実行します。

1. **iDRAC 設定ユーティリティ** で、**ネットワーク** に移動します。
   iDRAC 設定ネットワーク ページが表示されます。
2. **IPMI の設定** に値を指定します。

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

3. **戻る**、**終了** の順にクリックし、**はい** をクリックします。
   IPMI Over LAN が設定されます。

RACADM を使用した IPMI over LAN の設定

1. IPMI over LAN を有効にします。

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

メモ: この設定で、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>
```

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

3. 必要に応じて、IPMI LAN チャネルの暗号化キーを設定します。

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

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

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

リモート RACADM の有効化または無効化

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

メモ: リモート RACADM はデフォルトで有効に設定されています。

ウェブインタフェースを使用したリモート RACADM の有効化または無効化

1. iDRAC ウェブインタフェースで、**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. 115」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、https://www.dell.com/openmanagemanuals から入手可能な『*OpenManage サーバー管理者ユーザーズガイド*』を参照してください。

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

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。

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

2. カーネル行に次の 2 つにオプションを追加します。

```
kernel ............. console=ttyS1,115200n8r console=tty1
```

3. GRUB のグラフィカルインタフェースを無効にし、テキストベースのインタフェースを使用します。テキストベースのインタフェースを使用しないと、GRUB 画面が RAC 仮想コンソールで表示されません。グラフィカルインタフェースを無効にするには、`splashimage` で始まる行をコメントアウトします。

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

```
# grub.conf generated by anaconda
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You do not have a /boot partition. This means that all
# kernel and initrd paths are relative to /, e.g.
# root (hd0,0)
# kernel /boot/vmlinuz-version ro root=/dev/sda1
# initrd /boot/initrd-version.img
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

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

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

```
title Red Hat Linux Advanced Server-up (2.4.9-e.3) root (hd0,00)
kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
initrd /boot/initrd-2.4.9-e.3.im
```

4. RAC シリアル接続を介した仮想コンソールセッションを開始するための複数の GRUB オプションを有効にするには、すべてのオプションに次の行を追加します。

```
console=ttyS1,115200n8r console=tty1
```

この例は、最初のオプションに `console=ttyS1,57600` を追加した例です。

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。

起動後の仮想コンソールへのログインの有効化

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

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

次の例は、新しい行が追加されたサンプルファイルを示しています。

```
#inittab This file describes how the INIT process should set up
#the system in a certain run-level.
#Author:Miquel van Smoorenburg
#Modified for RHS Linux by Marc Ewing and Donnie Barnes
#Default runlevel. The runlevels used by RHS are:
#0 - halt (Do NOT set initdefault to this)
#1 - Single user mode
#2 - Multiuser, without NFS (The same as 3, if you do not have #networking)
#3 - Full multiuser mode
#4 - unused
#5 - X11
#6 - reboot (Do NOT set initdefault to this)
id:3:initdefault:
#System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
#Things to run in every runlevel.
ud::once:/sbin/update
ud::once:/sbin/update
#Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
#When our UPS tells us power has failed, assume we have a few
#minutes of power left. Schedule a shutdown for 2 minutes from now.
#This does, of course, assume you have power installed and your
#UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
#If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
```

```
#Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6
```

```
#Run xdm in runlevel 5
#xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

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

```
ttyS1
```

次の例は、新しい行が追加されたサンプルファイルを示しています。

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

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

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エントリのみに適用し、`GRUB_CMDLINE_LINUX` を使用してすべてのメニューエントリに適用します。

   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、別の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。

```
[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=1152001
```

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

スキームの種類	アルゴリズム
非対称暗号化	
公開キー	ssh-rsa ecdsa-sha2-nistp256

表 19. SSH 暗号化スキーム（続き）

スキームの種類	アルゴリズム
対称暗号	
キー交換	curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha1
暗号化	chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com
MAC	hmac-sha1 hmac-ripemd160 umac-64@openssh.com
Compression（圧縮）	なし

メモ: OpenSSH 7.0 以降を有効にすると、DSA 公開キーのサポートが無効になります。iDRAC のセキュリティ強化のため、デルは DSA 公開キーのサポートを有効にしないことをお勧めします。

SSH の公開キー認証の使用

iDRAC は、SSH 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できます。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、「ユーザーの設定」ユーザー権限に基づいています。この権限により、ユーザーは他のユーザーの SSH キーを設定できます。この権限は慎重に割り当てる必要があります。

Windows 用の公開キーの生成

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

1. アプリケーションを選択し、キーの種類に対する RSA を選択します。

2. キーのビット数を入力します。このビット数は 2048 ~ 4096 ビットにする必要があります。
3. **生成** をクリックし、指示に従ってマウスポインタをウィンドウ内で移動させます。
   キーが生成されます。
4. キーコメントフィールドを変更できます。
5. キーをセキュアにするためにパスフレーズを入力します。
6. 公開キーと秘密キーを保存します。

Linux 用の公開キーの生成

ssh-keygen アプリケーションを使用してベーシックキーを作成するには、ターミナルウィンドウを開き、シェルプロンプトで `ssh-keygen -t rsa -b 2048 -C testing` と入力します。

ここで、

- `-t` は *rsa* です。
- `-b` は 2048 ~ 4096 で、ビット暗号化サイズを指定します。
- `-C` を使用すると、公開キーコメントを変更できます。これはオプションです。

メモ: オプションでは大文字と小文字が区別されます。

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

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

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

SSH キーのアップロード

SSH インタフェース上で使用する公開キーは、*1 人のユーザーあたり*最大 4 つ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。iDRAC は、新しいキーが追加される前に以前のキーが削除されることをチェックしません。新しいキーが追加されると、SSH インタフェースが有効な場合にそのキーが使用可能になります。

ウェブインタフェースを使用した SSH キーのアップロード

SSH キーをアップロードするには、次の手順を実行します。

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

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

RACADM を使用した SSH キーのアップロード

SSH キーをアップロードするには、次のコマンドを実行します。

メモ: キーのアップロードとコピーを同時に行うことはできません。

- ローカル RACADM の場合：`racadm sshpkauth -i <2 to 16> -k <1 to 4> -f <filename>`
- SSH を使用したリモート RACADM の場合：`racadm sshpkauth -i <2 to 16> -k <1 to 4> -t <key-text>`

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

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

メモ: `-f` オプションは、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。
   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 番号をクリックします。
   ユーザーメインメニュー ページが表示されます。
3. **SSH キー設定** で、**SSH キーの表示 / 削除** を選択し、**次へ** をクリックします。
   SSH キーの表示 / 削除 ページが、キーの詳細と共に表示されます。

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。
   Local Groups（ローカルグループ） ページが表示されます。
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。
   Edit User（ユーザーの編集） ページが表示されます。
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`

8

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。管理者によるユーザー 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ー 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。ディレクトリー 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
- ユーザー名およびパスワードで推奨される文字
- 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。

表 20. iDRAC の役割

現在の世代	以前の世代	Privileges
システム管理者	システム管理者	ログイン、設定、ユーザーの設定、ログ、システム制御、仮想コンソールへのアクセス、仮想メディアへのアクセス、システム操作、デバッグ
オペレータ	電力ユーザー	ログイン、設定、システム制御、仮想コンソールへのアクセス、仮想メディアへのアクセス、システム操作、デバッグ
読み取り専用	ゲストユーザー	ログイン
なし	なし	なし

次の表では、ユーザー権限について説明します。

表 21. iDRAC ユーザー権限

現在の世代	以前の世代	説明
ログイン	iDRAC へのログイン	ユーザーによる iDRAC へのログインを可能にします。
設定	iDRAC の設定	ユーザーによる iDRAC の設定を可能にします。この権限を持つユーザーは、電源管理、仮想コンソール、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。
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。		

表 21. iDRAC ユーザー権限（続き）

現在の世代	以前の世代	説明
ユーザーの設定	ユーザーの設定	ユーザーによる特定のユーザーに対するシステムへのアクセスの許可を可能にします。
ログ	ログを消去	ユーザーによるシステムイベントログ（SEL）のクリアのみを可能にします。
システム制御	システムの制御と設定	ホストシステムのパワーサイクルを許可します。
仮想コンソールへのアクセス	仮想コンソールリダイレクションへのアクセス（ブレードサーバーの場合） 仮想コンソールへのアクセス（ラックおよびタワーサーバーの場合）	ユーザーによる仮想コンソールの実行を可能にします。
仮想メディアへのアクセス	仮想メディアへのアクセス	ユーザーによる仮想メディアの実行と使用を可能にします。
システム操作	アラートのテスト	ユーザー開始およびユーザー生成のイベントを許可します。情報は非同期通知として送信され、ログされます。
デバッグ	診断コマンドの実行	ユーザーによる診断コマンドの実行を可能にします。

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：

表 22. ユーザー名に推奨される文字

文字	長さ
0 ~ 9 A ~ Z a ~ z - !# $ % & ( ) *; ?[\ ] ^ _ ` { | } ~ + < = >	1 ~ 16

表 23. パスワードに推奨される文字

文字	長さ
0 ~ 9 A ~ Z a ~ z ' - !" # $ % & ( ) * , ./ : ; ?@ [\ ] ^ _ ` { | } ~ + < = >	1 ~ 40

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、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決定されます。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。

ローカルユーザーの設定

iDRAC では、特定のアクセス許可を持つローカルユーザーを最大 16 人設定できます。iDRAC ユーザーを作成する前に、現在のユーザーが存在するかどうかを確認してください。これらのユーザーには、ユーザー名、パスワード、および権限付きの役割を設定できます。ユーザー名とパスワードは、iDRAC でセキュア化された任意のインタフェース（つまり、ウェブインタフェース、RACADM、または WS-MAN）を使用して変更できます。ユーザーごとに SNMPv3 認証を有効または無効にすることもできます。

iDRAC ウェブインタフェースを使用したローカルユーザーの設定

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

メモ: iDRAC ユーザーを作成するには、ユーザーの設定権限が必要です。

1. iDRAC ウェブインタフェースで、**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 1 は IPMI の匿名ユーザー用に予約されており、この設定は変更できません。

   User Configuration（ユーザー設定） ページが表示されます。
3. **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ー名、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タイプ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。
4. **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

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

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

同じ設定で複数の iDRAC ユーザーを設定するには、次の手順を実行してください。

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

新しい 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 バッ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: サーバー上で SEKM が有効にされている場合は、このコマンドを使用する前に `racadm sekm disable` コマンドを使用して SEKM を無効にします。このコマンドを実行して iDRAC から SEKM 設定が消去された場合、iDRAC によって保護されているストレージ デバイスがロック アウトされるのを防ぐことができます。

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。

```
racadm get iDRAC.Users.<index>.UserName
```

複数のパラメーターとオブジェクト 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: コマンド

```
racadm get -f <myfile.cfg>
```

を使用すると、

```
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、iDRAC のすべての構成パラメーターが含まれます。

ユーザーに対して SNMP v3 認証を有効にするには、**SNMPv3AuthenticationType**、**SNMPv3Enable**、**SNMPv3PrivacyType** オブジェクトを使用します。詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

サーバ設定プロファイルファイルを使用してユーザーを設定する場合は、**AuthenticationProtocol**、**ProtocolEnable**、**PrivacyProtocol** 属性を使用して SNMPv3 認証を有効にします。

RACADM を使用した iDRAC ユーザーの追加

1. インデックスおよびユーザー名を設定します。

   ```
   racadm set idrac.users.<index>.username <user_name>
   ```

パラメータ	説明
<index>	ユーザー固有のインデックス
<user_name>	ユーザー名

2. パスワードを設定します。

   ```
   racadm set idrac.users.<index>.password <password>
   ```

3. ユーザー権限を設定します。

   詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

4. ユーザーを有効にします。

   ```
   racadm set.idrac.users.<index>.enable 1
   ```

確認するには、次のコマンドを使用します。

```
racadm get idrac.users.<index>
```

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

許可を持つ iDRAC ユーザーの有効化

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

1. 使用可能なユーザーインデックスを探します。

   ```
   racadm get iDRAC.Users <index>
   ```

2. 新しいユーザー名とパスワードで次のコマンドを入力します。

```
racadm set iDRAC.Users.<index>.Privilege <user privilege bit mask value>
```

メモ: デフォルトの権限値は 0 で、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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

Active Directory ユーザーの設定

会社で Microsoft Active Directory ソフトウェアを使用している場合、iDRAC にアクセス権を付与するようにソフトウェアを設定できます。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。

メモ: 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（またはその逆に）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、次を確認してください。

- Active Directory インフラストラクチャが展開済み。詳細については、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 へのセキュアな認証を行います。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 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*任意*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。**自動証明書要求セットアップウィザード** が表示されます。
3. **次へ** をクリックして、**ドメインコントローラ** を選択します。
4. **次へ**、**終了** の順にクリックします。SSL 証明書がインストールされます。

ドメインコントローラのルート CA 証明書の iDRAC へのエクスポート

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. **スタンドアロンスナップイン** ウィンドウで **証明書** を選択して **追加** をクリックします。
7. **コンピュータ** を選択して **次へ** をクリックします。
8. **ローカルコンピュータ** を選択し、**終了** をクリックして **OK** をクリックします。
9. **コンソール 1** ウィンドウで、**証明書 個人用 証明書** フォルダと移動します。
10. ルート CA 証明書を見つけて右クリックし、**すべてのタスク** を選択して **エクスポート...** をクリックします。
11. **証明書のエクスポートウィザード** で **次へ** を選択し、**いいえ、秘密キーはエクスポートしません** を選択します。
12. **次へ** をクリックし、フォーマットとして **Base-64 エンコード X.509 (.cer)** を選択します。
13. **次へ** をクリックし、システムのディレクトリに証明書を保存します。
14. 手順 13 で保存した証明書を iDRAC にアップロードします。

iDRAC ファームウェアの SSL 証明書のインポート

iDRAC SSL 証明書は、iDRAC ウェブサーバ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 Windows に自動的に選択させるか、希望する証明書ストアを参照します。
7. **終了**、**OK** の順にクリックします。iDRAC ファームウェアの SSL 証明書が、すべてのドメインコントローラの信頼済み証明書リストにインポートされます。

サポートされている Active Directory 認証メカニズム

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

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

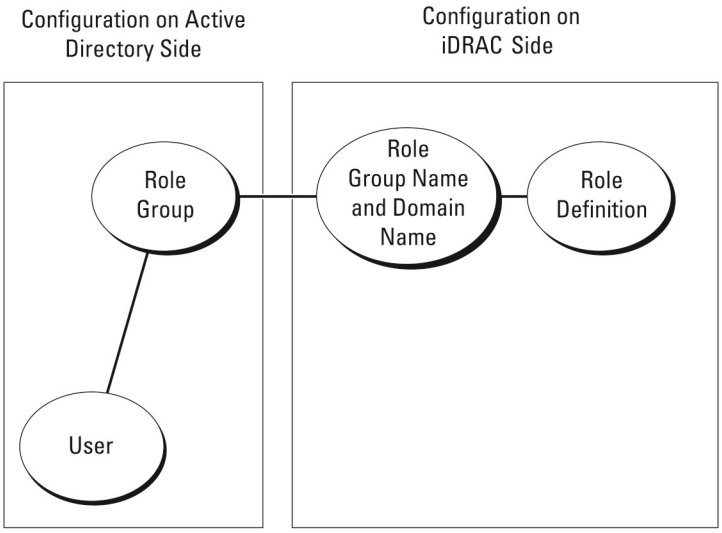


図 1. Active Directory 標準スキーマでの iDRAC の設定

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ーになります。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

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

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

シングルドメインとマルチドメインのシナリオの違い

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

すべてのログインユーザーと役割グループ、またはネストされているグループのいずれかが複数のドメインにある場合、グローバルカタログサーバのアドレスを 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 dat、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 サーバとユーザーアカウントの場所の情報を指定します。また、iDRAC ログイン時に iDRAC が Active Directory からの応答を待機する時間を指定します。

   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用に制御認証ポリシーを設定します。
    Active Directory 設定と管理手順 4 の 4b ページが開きます。
11. 権限を指定して、**適用** をクリックします。

    設定が適用され、**Active Directory 設定と管理手順 4 の 4a** ページが開きます。

12. **終了** をクリックします。標準スキーマ用の Active Directory 設定が行われます。

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

1. 次のコマンドを使用します。

```
racadm set iDRAC.ActiveDirectory.Enable 1
racadm set iDRAC.ActiveDirectory.Schema 2
racadm set iDRAC.ADGroup.Name <common name of the role group>
racadm set iDRAC.ADGroup.Domain <fully qualified domain name>
racadm set iDRAC.ADGroup.Privilege <Bit-mask value for specific RoleGroup permissions>
racadm set iDRAC.ActiveDirectory.DomainController1 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController2 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.DomainController3 <fully qualified domain name or IP
address of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog1 <fully qualified domain name or IP address
of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog2 <fully qualified domain name or IP address
of the domain controller>
racadm set iDRAC.ActiveDirectory.GlobalCatalog3 <fully qualified domain name or IP address
of the domain controller>
```

- ドメインの完全修飾ドメイン名 (FQDN) ではなく、ドメインコントローラの FQDN を入力します。たとえば、`dell.com` ではなく `servername.dell.com` と入力します。
- 特定の役割グループ許可用のビットマスク値については、「デフォルトの役割グループ権限」を参照してください。
- 3 つのドメインコントローラアドレスのうち少なくとも 1 つを入力する必要があります。iDRAC は、正常に接続できるまで、設定された各アドレスに対して 1 つずつ接続を試みます。標準スキーマでは、これらはユーザーアカウントと役割グループが位置するドメインコントローラのアドレスです。
- グローバルカタログサーバは、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にのみ必要です。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、ユーザードメインのリストを設定しておく場合は、次のコマンドを使用します。

```
racadm set iDRAC.UserDomain.<index>.Name <fully qualified domain name or IP Address of the
domain controller>
```

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

拡張スキーマ Active Directory の概要

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

拡張スキーマのためのベストプラクティス

拡張スキーマはデル関連オブジェクトを使用して iDRAC と許可を結びつけます。これにより、与えられたすべての許可に基づいて iDRAC を使用できます。デル関連オブジェクトのデフォルトのアクセスコントロールリスト (ACL) で自己管理者およびドメイン管理者は iDRAC オブジェクトの許可と範囲を管理できます。

デフォルトでは、デル関連オブジェクトは親の Active Directory オブジェクトからすべての許可を継承するわけではありません。デル関連オブジェクトの継承を有効にしている場合は、その関連オブジェクトの継承された許可が選択されたユーザーおよびグループに付与されます。これは意図しない権限が iDRAC に与えられる原因となる場合があります。

拡張スキーマを安全に使用するために、デルは、拡張スキーマの実装においてデル関連オブジェクトの継承を有効にしないことをお勧めします。

Active Directory スキーマ拡張

Active Directory データは、*属性*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 つの例がユーザークラスです。ユーザー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 でスキーマを拡張するために、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、管理者に、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ビネーションについて、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。

認証と許可のために 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 つの iDRAC デバイスオブジェクトを作成します。複数の関連オブジェクトを作成することができ、各関連オブジェクトは、必要な数のユーザー、ユーザーグループ、または iDRAC デバイスオブジェクトにリンクできます。ユーザーおよび iDRAC ユーザーグループは、企業内のどのドメインのメンバーでもかまいません。

ただし、各関連オブジェクト (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、特定の iDRAC デバイス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する際に、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、認証と許可に必要な接続が提供されていることを示しています。

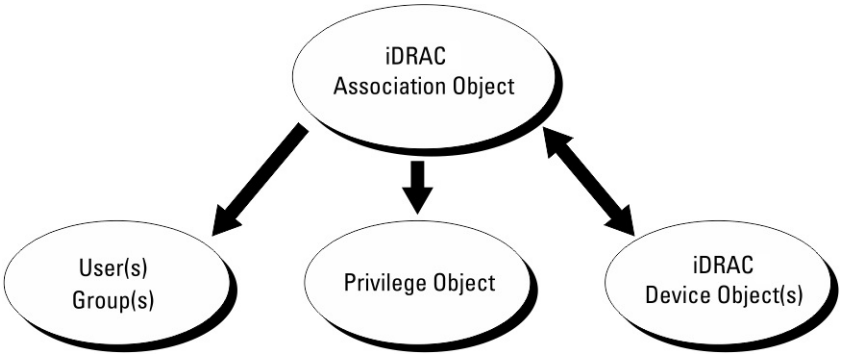


図 2. Active Directory オブジェクトの標準的なセットアップ

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

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

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

別のドメインからユニバーサルグループを追加するときは、ユニバーサルスコープを持つ関連オブジェクトを作成します。Dell Schema Extender ユーティリティによって作成されるデフォルトの関連オブジェクトは、ドメインローカルグループであり、他のドメインのユニバーサルグループとは連動しません。

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

拡張スキーマを使用した権限の蓄積

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

次の図は、拡張スキーマを使用して権限を蓄積する例を示しています。

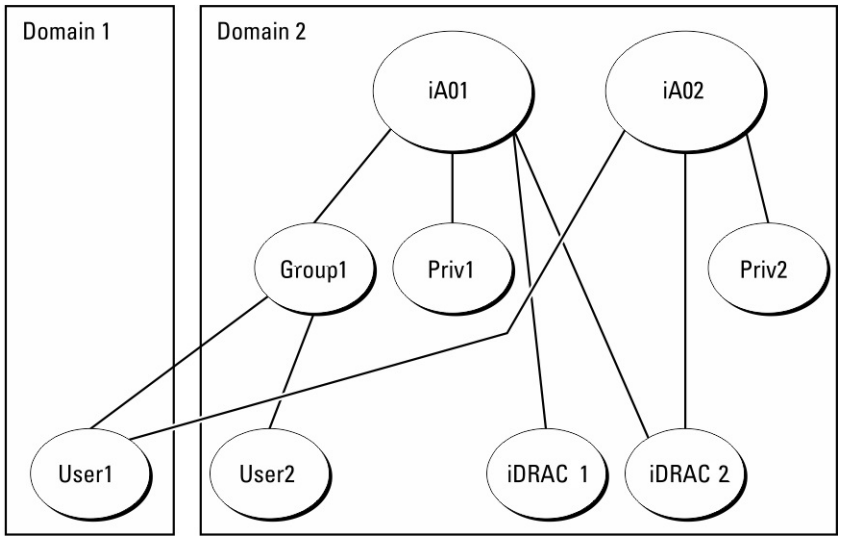


図 3. ユーザーのための権限の蓄積

この図は、A01 と A02 の 2 つの関連オブジェクトを示しています。ユーザー 1 は、両方の関連オブジェクトを介して iDRAC2 に関連付けられています。

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

この例では、ユーザー 1 は iDRAC2 に対する Priv1 権限と Priv2 権限の両方を所有しており、iDRAC1 に対しては Priv1 権限のみを所有しています。ユーザー 2 は iDRAC1 と iDRAC2 の両方に対して Priv1 権限を所有しています。さらに、この図は、ユーザー 1 が異なるドメインに属し、グループのメンバーになることができることを示しています。

拡張スキーマ Active Directory の設定

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

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

Active Directory スキーマの拡張

Active Directory スキーマを拡張すると、Active Directory スキーマに Dell の組織単位、スキーマクラスと属性、および権限例と関連オブジェクトが追加されます。スキーマを拡張する前に、ドメインフォレストのスキーママスター 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用** を選択するか、スキーマ管理者権限でユーザー名とパスワードを入力します。
4. **次へ** をクリックして、Dell Schema Extender を実行します。
5. **終了** をクリックします。

   スキーマが拡張されます。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. 158 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

クラス名	割り当てられたオブジェクト識別番号 (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

表 26. DelliDRACdevice クラス

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

表 27. delliDRACAssociationObject クラス

OID	1.2.840.113556.1.8000.1280.1.7.1.2
説明	Dell 関連オブジェクトを表します。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。
クラスの種類	構造体クラス
SuperClasses	グループ

表 27. delliDRACAssociationObject クラス （続き）

OID	1.2.840.113556.1.8000.1280.1.7.1.2
属性	dellProductMembers dellPrivilegeMember

表 28. dellRAC4Privileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.3
説明	iDRAC の権限（許可権限）を定義します。
クラスの種類	補助クラス
SuperClasses	なし
属性	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsConsoleRedirectUser dellIsVirtualMediaUser dellIsTestAlertUser dellIsDebugCommandAdmin

表 29. dellPrivileges クラス

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

表 30. dellProduct クラス

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

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

属性名 / 説明	割り当てられた OID/ 構文オブジェクト識別子	単一値
dellPrivilegeMember	1.2.840.113556.1.8000.1280.1.1.2.1	FALSE

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

属性名 / 説明	割り当てられた OID/ 構文オブジェクト識別子	単一値
この属性に属する dellPrivilege オブジェクトのリスト。	識別名（LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12）	
dellProductMembers この役割に属する dellRacDevice オブジェクトと DelliDRACDevice オブジェクトのリスト。この属性は、dellAssociationMembers バックワードリンクへのフォワードリンクです。 リンク ID：12070	1.2.840.113556.1.8000.1280.1.1.2.2 識別名（LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12）	FALSE
dellIsLoginUser ユーザーにデバイスへのログイン権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.3 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsCardConfigAdmin ユーザーにデバイスのカード設定権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.4 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsUserConfigAdmin ユーザーにデバイスのユーザー設定権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.5 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsLogClearAdmin ユーザーにデバイスのログクリア権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.6 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsServerResetUser ユーザーにデバイスのサーバーリセット権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.7 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsConsoleRedirectUser ユーザーにデバイスの仮想コンソール権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.8 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsVirtualMediaUser ユーザーにデバイスの仮想メディア権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.9 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsTestAlertUser ユーザーにデバイスのテストアラートユーザー権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.10 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellIsDebugCommandAdmin ユーザーにデバイスのデバッグコマンド管理権限がある場合は TRUE。	1.2.840.113556.1.8000.1280.1.1.2.11 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
dellSchemaVersion スキーマのアップデートに現在のスキーマバージョンが使用されます。	1.2.840.113556.1.8000.1280.1.1.2.12 大文字小文字を区別しない文字列（LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905）	TRUE

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

属性名 / 説明	割り当てられた OID/ 構文オブジェクト識別子	単一値
dellRacType この属性は delliDRACDevice オブジェクトの現在の RAC タイプで dellAssociationObjectMembers フォワードリンク へのバックワードリンクです。	1.2.840.113556.1.8000.1280.1.1.2.13 大文字小文字を区別しない文字列（LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905）	TRUE
dellAssociationMembers この製品に属する dellAssociationObjectMembers のリスト。この属性は、dellProductMembers にリンクされた属性へのバックワードリンクです。 リンク ID：12071	1.2.840.113556.1.8000.1280.1.1.2.14 識別名（LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12）	FALSE

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

Active Directory でスキーマを拡張する場合は、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 ソフトウェアクイックインストールガイド』を参照してください。64 ビットの Windows オペレーティングシステムの場合、スナップインのインストーラは次の場所にあります。

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

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

Active Directory への iDRAC ユーザーと権限の追加

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

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

iDRAC デバイスオブジェクトの作成

iDRAC デバイスオブジェクトを作成するには、次の手順を実行します。

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

権限オブジェクトの作成

権限オブジェクトを作成するには、次の手順を実行します。

メモ: 権限オブジェクトは、関係のある関連オブジェクトと同じドメイン内に作成する必要があります。

1. **コンソールのルート**（MMC）ウィンドウでコンテナを右クリックします。
2. **新規** > **Dell リモート管理オブジェクトの詳細設定** を選択します。
   新規オブジェクト ウィンドウが表示されます。
3. 新しいオブジェクトの名前を入力します。
4. **権限オブジェクト** を選択し、OK をクリックします。
5. 作成した権限オブジェクトを右クリックして **プロパティ** を選択します。
6. **リモート管理権限** タブをクリックして、ユーザーまたはグループに対する権限を設定します。

関連オブジェクトの作成

関連オブジェクトを作成するには、次の手順を実行します。

メモ: iDRAC の関連オブジェクトはグループから派生し、その範囲はドメインローカルに設定されています。

1. **コンソールのルート**（MMC）ウィンドウでコンテナを右クリックします。
2. **新規** > **Dell リモート管理オブジェクトの詳細設定** を選択します。
   この **新規オブジェクト** ウィンドウが表示されます。
3. 新規オブジェクトの名前を入力し、**関連オブジェクト** を選択します。
4. **関連オブジェクト** の範囲を選択し、OK をクリックします。
5. 認証済みユーザーに、作成された関連オブジェクトにアクセスするためのアクセス権限を提供します。

関連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、ユーザーまたはユーザーグループ、権限オブジェクト、iDRAC デバイスまたは iDRAC デバイスグループを関連付けることができます。

ユーザーおよび iDRAC デバイスのグループを追加できます。

ユーザーまたはユーザーグループの追加

ユーザーまたはユーザーグループを追加するには、次の手順を実行します。

1. **関連オブジェクト** を右クリックし、**プロパティ** を選択します。
2. **ユーザー** タブを選択して、**追加** を選択します。
3. ユーザーまたはユーザーグループの名前を入力し、**OK** をクリックします。

権限の追加

権限を追加するには、次の手順を実行します。

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または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または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またはユーザーグループが使用可能なネットワークに接続している iDRAC デバイスを 1 つ追加します。関連オブジェクトには複数の 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。
   Active Directory 設定と管理手順 4 の 1 ページが開きます。
2. 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。
3. **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。
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 からの応答を待機す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)** 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 設定と管理手順 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。

```
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。

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 0
  ```

  この場合、CA 証明書をアップロードする必要はありません。
- SSL ハンドシェイク中に証明書の検証を実施する場合は、次のコマンドを実行します（オプション）。

  ```
  racadm set iDRAC.ActiveDirectory.CertValidationEnable 1
  ```

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

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

  メモ: 証明書の検証が有効になっている場合、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。

  ```
  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 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。

   メモ: 証明書検証を有効化がチェックされた状態で Active Directory 設定をテストする場合、iDRAC では、Active Directory サーバが IP アドレスではなく FQDN で識別されている必要があります。Active Directory サーバが IP アドレスで識別されていると、iDRAC が Active Directory サーバと通信できないため、証明書の検証に失敗します。

RACADM を使用した Active Directory の設定のテスト

Active Directory の設定をテストするには、`testfeature` コマンドを使用します。

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

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。この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、およびユーザーとグループ間のリンクに異なる属性名がある場合があります。これらの処置は、iDRAC で設定できます。

メモ: スマートカードベースの 2 要素認証 (TFA) とシングルサインオン (SSO) ログインは、汎用 LDAP ディレクトリサービスではサポートされません。

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 Settings (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アカウントの場所情報を指定します。

   メモ: 証明書の検証を有効にした場合は、LDAP サーバの FQDN を指定し、**iDRAC Settings(iDRAC 設定)** > **Network (ネットワーク)** で DNS が正しく設定されたことを確認します。

   メモ: 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。ファームウェアは、ユーザー DN に一致するグループのダイレクトメンバーを検索します。また、シングルドメインのみがサポートされています。クロスドメインは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 3a 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 3b ページが表示されます。
7. グループ識別名とそのグループに関連付けられた権限を指定し、**適用** をクリックします。

メモ: Novell eDirectory を使用していて、グループ DN 名に # (ハッシュ)、" (二重引用符)、; (セミコロン)、> (より大きい)、, (カンマ)、または < (より小さい) などの文字を使用した場合は、それらの文字をエスケープする必要があります。

役割グループの設定が保存されます。**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 を繰り替えします。
9. **終了** をクリックします。汎用 LDAP ディレクトリサービスが設定されました。

RACADM を使用した汎用 LDAP ディレクトリサービスの設定

LDAP ディレクトリサービスを設定するには、`iDRAC.LDAP` および `iDRAC.LDAPRole` グループのオブジェクトを使用します。

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

LDAP ディレクトリサービス設定のテスト

LDAP ディレクトリサービス設定をテストして、設定に誤りがないかどうかを確認したり、障害のある LDAP ログインの問題を診断することができます。

iDRAC ウェブインタフェースを使用した LDAP ディレクトリサービスの設定のテスト

LDAP ディレクトリサービスの設定をテストするには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**iDRAC Settings (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 *ユーザーログインの属性* 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ーとしてユーザーのログインを試みます。ログインに失敗した場合、ローカルユーザーの検索が有効になります。

   テスト結果およびテストログが表示されます。

RACADM を使用した LDAP ディレクトリサービス設定のテスト

LDAP ディレクトリサービス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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

9

システム設定ロックダウン モード

システム設定ロックダウン 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。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、ブロックされます。重要なシステム設定を変更しようとすると、エラーメッセージが表示されます。システム ロックダウン モードを有効にすると、ベンダー ツールを使用したサード パーティー I/O カードのファームウェア アップデートがブロックされます。

システム ロックダウン モードは、エンタープライズ ライセンスをお持ちのお客様のみが使用できます。

4.40.00.00 リリースでは、システム ロックダウン機能は NIC にも拡張されています。

メモ: NIC の強化されたロックダウンでは、ファームウェア アップデートを防止するためにファームウェアのロックダウンのみが含まれます。設定 (x-UEFI) ロックダウンはサポートされていません。

メモ: システムロックダウンモードが有効になると、構成設定は変更できなくなります。システム設定フィールドは無効です。

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 Web インターフェイス
- 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
- 工場出荷時の System Erase

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。

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。

メモ: OMSA、SysCfg、USC などのインターフェイスは設定のみを確認できますが、構成を変更することはできません。

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徴、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

無効	機能の維持

• ライセンスの削除
• DUP アップデート
• SCP インポート
• デフォルトにリセット
• OMSA/OMSS
• IPMI
• DRAC/LC
• DTK-Syscfg
• Redfish
• OpenManage Essentials
• BIOS (F2 設定は読み取り専用になります)
• グループ マネージャー
• ネットワーク カードの選択
	• 電源操作 - 電源のオン/オフ、リセット
	• 電力上限設定
	• 電源の優先度
	• 操作の識別 (シャーシまたは PERC)
	• 部品交換、簡易復元、システム ボードの交換
	• 診断プログラムの実行
	• モジュラー操作 (FlexAddress またはリモート割り当てアドレス)
	• Group Manager パスコード
	• デバイスに直接アクセスするすべてのベンダー ツール (一部 NIC を除く)
	• ライセンスのエクスポート
	• PERC
	  ○ PERC CLI
	  ○ DTK-RAIDCFG

表 32. ロックダウンモードの影響を受けるアイテム

無効	機能の維持
	○ F2/Ctrl+R ● デバイスに直接アクセスするすべてのベンダーツール ● NVMe ○ DTK-RAIDCFG ○ F2/Ctrl+R ● BOSS-S1 ○ Marvell CLI ○ F2/Ctrl+R ● ISM/OMSA の設定 (OS BMC の有効、watchdog ping、OS 名、OS バージョン)

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。

10

シングルサインオンまたはスマートカードログインのための iDRAC の設定

本項では、スマートカードログイン（ローカルユーザーおよび Active Directory ユーザー向け）とシングルサインオン（SSO）ログイン（Active Directory ユーザー向け）用に iDRAC を設定するための情報を記載します。SSO とスマートカードログインは、ライセンスが必要な機能です。

iDRAC は、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
- 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 ログインの設定
- スマート カード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 の時刻を 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. 104」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。

  メモ: ホスト名が DNS リバースルックアップに一致しない場合は、ケルベロス認証に失敗します。
- 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. 350」を参照してください。

  メモ: Google Chrome と Safari は SSO ログインのための Active Directory をサポートしません。

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 サーバー**] の IP アドレスを指定します。この値は、ルート ドメインの一部である有効な DNS サーバーの IP アドレスです。
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。
6. 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、*認証済みユーザー*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 キータブ ユーザーを作成します。

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 AES 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 キータブを生成します。

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

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]**、**[プロパティ]**、**[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。

メモ: 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 プリンシパルとして設定する場合と同様の手順を実行します。

ktpass ツール (サーバー インストール CD/DVD の一部としてマイクロソフトから入手可能) を用いて、ユーザー アカウントにバインドするサービス プリンシパル名 (SPN) を作成し、信頼情報を MIT 形式の Kerberos *keytab* ファイルにエクスポートすることで、外部ユーザーやシステムとキー配布センター (KDC) の間の信頼関係が有効になります。keytab ファイルには暗号キーが含まれており、これはサーバーと KDC の間での情報の暗号化に使用されます。Kerberos 認証をサポートする UNIX ベースのサービスは、ktpass ツールを用いることで、Windows Server Kerberos KDC サービスから提供される相互運用性機能を利用できるようになります。**ktpass** ユーティリティーの詳細については、マイクロソフトの Web サイト **technet.microsoft.com/en-us/library/cc779157(WS.10).aspx** を参照してください。

keytab ファイルを生成する場合、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。

ktpass ツールを使用して keytab ファイルを生成するには、次の手順を実行します。

1. ktpass ユーティリティを、Active Directory 内のユーザーアカウントに iDRAC をマップするドメインコントローラ(Active Directory サーバー) 上で実行します。
2. 次の ktpass コマンドを使用して、Kerberos keytab ファイルを作成します。

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

暗号化タイプは、AES256-SHA1 です。プリンシパル タイプは、KRB5_NT_PRINCIPAL です。サービス プリンシパル名がマップされているユーザー アカウントのプロパティは、**このアカウントに AES 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。

メモ: **iDRACname** および**サービス プリンシパル名**には小文字を使用します。例に示されているように、ドメイン名には大文字を使用します。

keytab ファイルが生成されます。

メモ: keytab ファイルを作成した iDRAC ユーザーで問題が生じた場合は、ユーザーおよび keytab ファイルを新規に作成します。最初に作成したのと同じ keytab ファイルが再び実行される場合は、設定が正しくありません。

ウェブインタフェースを使用した Active Directory ユーザーのための iDRAC SSO ログインの設定

Active Directory SSO ログイン用に iDRAC を設定するには、次の手順を実行します。

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

1. iDRAC DNS 名が iDRAC 完全修飾ドメイン名に一致するかどうかを確認します。確認するには、iDRAC Web インターフェイスで、**[iDRAC 設定]** > **[ネットワーク]** > **[共通設定]** の順に移動し、[**DNS iDRAC 名**] プロパティを調べます。
2. 標準スキーマまたは拡張スキーマに基づいてユーザーアカウントをセットアップするために Active Directory を設定する間、次の 2 つの追加手順を実行して SSO を設定します。
   - **Active Directory の設定と管理手順 4 の 1** ページで keytab ファイルをアップロードします。
   - **Active Directory の設定と管理手順 4 の 2** ページで **シングルサインオンの有効化** オプションを選択します。

RACADM を使用した Active Directory ユーザーのための iDRAC SSO ログインの設定

SSO を有効にするには、Active Directory の設定手順を完了し、次のコマンドを実行します。

```
racadm set iDRAC.ActiveDirectory.SSOEnable 1
```

管理ステーションの設定

Active Directory ユーザーの 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、[**イントラ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。
   - Firefox ブラウザーを起動し、URL に「about:config」と入力します。
   - [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、ブラウザーを閉じます。
   - 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にする前に、次を確認してください。

- iDRAC 許可を設定していること。
- 適切な証明書での iDRAC ローカルユーザー設定または Active Directory ユーザー設定が完了していること。

メモ: スマート カード ログインが有効になっている場合は、SSH、IPMI オーバー LAN、シリアル オーバー LAN、リモート RACADM は無効になります。この場合も、スマート カード ログインを無効にすると、インターフェイスは自動的に有効になりません。

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オン機能を有効化または無効化するには、次の手順を実行します。

1. iDRAC 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オンの設定)** 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オンを有効化するか、**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オン試行では、スマートカードログインが要求されます。

RACADM を使用したスマートカードログインの有効化または無効化

スマートカードログインを有効にするには、`iDRAC.SmartCard` グループのオブジェクトで `set` コマンドを使用します。

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

iDRAC 設定ユーティリティを使用したスマートカードログインの有効化または無効化

スマートカードログオン機能を有効化または無効化するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**スマートカード** に移動します。
   iDRAC 設定のスマートカード ページが表示されます。
2. スマートカードログオンを有効にするには、**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オン機能が有効化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 スマート カード設定の場合、iDRAC は標準または拡張スキーマ SSO ログインで設定されている必要があります。

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

Active Directory ユーザー用の iDRAC スマートカードログインを設定する前に、必要な前提条件を満たしていることを確認します。

スマートカードログインのために iDRAC に設定するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、標準スキーマまたは拡張スキーマに基づいたユーザーアカウントをセットアップするために Active Directory を設定している際に、**Active Directory の設定と管理手順 4 の 1** ページ上で、次の作業を実行します。
   - 証明書の検証を有効にします。
   - 信頼済み CA 署名付き証明書をアップロードします。
   - keytab ファイルをアップロードします。
2. スマートカードログインを有効にします。オプションの詳細については、『iDRAC オンラインヘルプ』を参照してください。

ローカルユーザーのための iDRAC スマートカードログインの設定

スマートカードログインできるように iDRAC ローカルユーザーを設定するには、次の手順を実行します。

1. スマートカードユーザー証明書および信頼済み CA 証明書を iDRAC にアップロードします。
2. スマートカードログインを有効にします。

スマートカードユーザー証明書のアップロード

ユーザー証明書をアップロードする前に、スマートカードベンダーからのユーザー証明書が Base64 フォーマットでエクスポートされていることを確認してください。SHA-2 証明書もサポートされています。

ウェブインタフェースを使用したスマートカードユーザー証明書のアップロード

スマートカードユーザー証明書をアップロードするには、次の手順を実行します。

1. iDRAC Web インターフェイスで、**[iDRAC 設定]** > **[ユーザー]** > **[スマート カード]** の順に移動します。

   メモ: 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。

2. **[スマート カード ログオンの設定]** 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 ログオンの 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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

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、必要なドライバー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ーのステータスを確認します。
3. ブ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。
4. [**ユーザー名**] と [**パスワード**] を入力し、[**OK**] をクリックします。
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 カード認証情報を入力します。
10. スマート カード PIN を入力し、[**送信**] をクリックします。

スマートカード用の信頼済み CA 証明書のアップロード

CA 証明書をアップロードする前に、CA 署名付きの証明書があることを確認してください。

ウェブインタフェースを使用したスマートカード用の信頼済み CA 証明書のアップロード

スマートカードログイン用の信頼済み CA 証明書をアップロードするには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**iDRAC Settings (iDRAC 設定)** > **Network (ネットワーク)** > **User Authentication (ユーザー認証)** > **Local Users (ローカルユーザー)** と移動します。
   ユーザー ページが表示されます。
2. **ユーザー ID** 列で、ユーザー ID 番号をクリックします。
   ユーザーメインメニュー ページが表示されます。
3. **スマートカード設定** で、**信頼済み CA 証明書のアップロード** を選択し、**次へ** をクリックします。
   信頼済み CA 証明書のアップロード ページが表示されます。
4. 信頼済み CA 証明書を参照して選択し、**適用** をクリックします。

RACADM を使用したスマートカード用の信頼済み CA 証明書のアップロード

スマートカードログインのために信頼済み CA 証明書をアップロードするには、**usercertupload** オブジェクトを使用します。詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

スマート カードを使用したログイン

メモ: 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 カードを使用してログインするには、次の手順を実行します。

1. 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。
2. `http://IP/`を使用して iDRAC を起動するか、FQDN `http://FQDN/`を使用して起動します。
3. スマート カード プラ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。

11

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 トラップ、IPMI アラート、リモートシステムログ、Redfish イベント、または WS イベント) を生成するように設定されている場合、アラートが 1 つ、または複数の設定済み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、電源の入れ直し、電源のオフなど) 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ように iDRAC を設定するには、次の手順を実行します。

1. アラートを有効化します。
2. オプションで、アラートをカテゴリまたは重要度でフィルタリングできます。
3. 電子メールアラート、IPMI アラート、SNMP トラップ、リモートシステムログ、オペレーティングシステムログ、Redfish イベント、および / または WS イベントを設定します。
4. 次のようなイベントの警告とアクションを有効にします。
   - 電子メールアラート、IPMI アラート、SNMP トラップ、リモートシステムログ、Refish イベント、オペレーティングシステムログ、または WS イベントを設定済みの宛先に送信する。
   - 管理下システムの再起動、電源オフ、またはパワーサイクルを実行する。

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 トラップ、または IPMI トラップ設定の設定
- 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 インターフェイスで、**[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 カテゴリーを選択します。
   - 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、カテゴリー、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.IPMILan.AlertEnable <n>
```

n=0 — 無効

n=1 — 有効

iDRAC 設定ユーティリティを使用したアラートの有効化または無効化

アラートの生成またはイベント処置を有効化または無効化するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**アラート** に進みます。
   iDRAC 設定アラート ページが表示されます。
2. **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: 読み取り専用権限を持つユーザーであっても、アラートのフィルタは可能です。

1. iDRAC ウェブインタフェースで、**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、ユーザーログイン / 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。

メモ: これは、ファームウェアインベントリ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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

イベントアラートの設定

E-メールアラート、IPMI アラート、SNMP トラップ、リモートシステムログ、オペレーティングシステムログ、および WS イベントなどのイベントアラートを、設定された宛先に送信されるように設定できます。

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 イベンティング
   - 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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

アラート反復イベントの設定

システムが吸気口温度のしきい値制限を超過して稼動し続けた場合に、iDRAC が追加のイベントを特定の間隔で生成するよう設定できます。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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

iDRAC ウェブインタフェースを使用した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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

電子メールアラート、SNMP トラップ、または IPMI トラップ設定の設定

管理ステーションは、Simple Network Management Protocol (SNMP) および Intelligent Platform Management Interface (IPMI) トラップを使用して、iDRAC からデータを受信します。多数のノードを含むシステムの管理ステーションにとって、発生し得るすべての状態について各 iDRAC をポーリングするのは効率的ではない場合があります。たとえば、イベントトラップはノード間の負荷分散や、認証が失敗した場合のアラート送信で、管理ステーションを援助します。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 トラップの送信先となる SNMP v3 ユーザーを指定できます。

電子メール、SNMP、または IPMI トラップを設定する前に、次を確認します。

- RAC の設定許可を持っている。
- イベントフィルタを設定した。

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 によるサーバ監視に必要な iDRAC MIB については、https://www.dell.com/openmanagemanuals から入手可能な『*Dell EMC OpenManage SNMP リファレンス ガイド*』を参照してください。

ウェブインタフェースを使用した IP アラート宛先の設定

ウェブインタフェースを使用してアラート送信先設定を行うには、次の手順を実行します。

1. 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 と電子メールの設定）** 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、**IPMI トラップのテスト** と **SNMP トラップのテスト** でそれぞれ **送信** をクリックします。
6. **適用** をクリックします。
   アラート送信先が設定されます。
7. **SNMP トラップフォーマット** セクションで、トラップ宛先でトラップの送信に使用されるプロトコルバージョンである **SNMP v1**、**SNMP v2**、または **SNMP v3** を選択して、**適用** をクリックします。
   メモ: **SNMP 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

トラップアラートを設定するには、次の手順を実行します。

1. トラップを有効にするには、次の手順を実行します。

```
racadm set idrac.SNMP.Alert.<index>.Enable <n>
```

パラメータ	説明
<index>	宛先索引。有効な値は 1~8 です。
<n>=0 **<n>=1**	トラップの無効化 トラップの有効化

2. トラップの送信先アドレスを設定するには、次の手順を実行します。

```
racadm set idrac.SNMP.Alert.<index>.DestAddr <Address>
```

パラメータ	説明
<index>	宛先索引。有効な値は 1~8 です。
<Address>	有効な IPv4、IPv6、または FQDN アドレスです。

3. 次の手順を実行して、SNMP コミュニティ名文字列を設定します。

```
racadm set idrac.ipmilan.communityname <community_name>
```

パラメータ	説明
<community_name>	SNMP コミュニティ名です。

4. SNMP の送信先を設定するには、次の手順を実行します。
   - SNMPv3 の SNMP トラップの送信先を設定します。

     ```
     racadm set idrac.SNMP.Alert.<index>.DestAddr <IP address>
     ```
   - トラップの送信先の SNMPv3 ユーザーを設定します。

     ```
     racadm set idrac.SNMP.Alert.<index>.SNMPv3Username <user_name>
     ```
   - ユーザーの SNMPv3 を有効にします。

     ```
     racadm set idrac.users.<index>.SNMPv3Enable Enabled
     ```
5. 必要に応じてトラップをテストするには、次の手順を実行します。

```
racadm testtrap -i <index>
```

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

iDRAC 設定ユーティリティを使用した IP アラート宛先の設定

iDRAC 設定ユーティリティを使用してアラート送信先 (IPv4、IPv6、または FQDN) を設定できます。この操作を行うには、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名を入力します。
   オプションについては、『iDRAC 設定ユーティリティオンラインヘルプ』を参照してください。
4. **戻る**、**終了** の順にクリックし、**はい** をクリックします。
   アラート送信先が設定されます。

電子メールアラートの設定

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 アラート受信用の E メール ID を入力できます。
   - カスタム 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 メールの**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）
     - **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** - SMTP プロトコルを SSL を介して実行します

     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。
   - 認証
   - ユーザー名

   サーバー設定の場合、使用されるポートは `connectionencryptiontype` によって異なります。これは RACADM を使用した場合にのみ設定できます。
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]
```

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

2. 電子メール設定を行う：

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

パラメータ	説明
index	メールの宛先索引です。有効な値は 1~4 です。
email-address	プラットフォームイベントアラートを受信する送信先の電子メールアドレスです。

3. 送信者の E メール設定を行う：

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

パラメータ	説明
index	送信者の E メールの索引です。
email-address	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。

4. カスタムメッセージを設定する：

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

パラメータ	説明
index	メールの宛先索引です。有効な値は 1~4 です。
custom-message	カスタムメッセージ

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]
```

パラメータ	説明
index	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。

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

SMTP 電子メールサーバーアドレス設定

電子メールアラートを指定の送信先に送信するためには、SMTP サーバーアドレスを設定する必要があります。

iDRAC ウェブインタフェースを使用した SMTP 電子メールサーバーアドレスの設定

SMTP サーバーアドレスを設定するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**Configuaration (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。
   上記のフィールドの詳細については、『iDRAC オンラインヘルプ』を参照してください。
5. **適用** をクリックします。
   SMTP が設定されます。

RACADM を使用した SMTP 電子メールサーバアドレスの設定

SMTP 電子メールサーバを設定するには、次の手順を実行します。

```
racadm set iDRAC.RemoteHosts.SMTPServerIPAddress <SMTP E-mail Server IP Address>
```

WS Eventing の設定

WS Eventing プロトコルは、クライアントサービス (サブスクライバ) が、サーバーイベント (通知またはイベントメッセージ) を含むメッセージの受信用にサーバー (イベントソース) にインタレスト (サブスクリプション) を登録するために使用されます。WS Eventing メッセージの受信に関心を持つクライアントは、iDRAC にサブスクライブして Lifecycle Controller ジョブ関連のイベントを受信することができます。

Lifecycle Controller ジョブに関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 サポートの仕様書に記載されています。この仕様書の他にも、DSP0226 (DMTF WS 管理

仕様) の第 10 項「通知」(Eventing) 文書で、WS Eventing プロトコルについての完全な情報を参照してください。Lifecycle Controller 関連のジョブは、DCIM ジョブ制御プロファイルマニュアルに記載されています。

Redfish Eventing の設定

Redfish Eventing プロトコルは、クライアントサービス (サブスクライバ) が、Redfish イベント (通知またはイベントメッセージ) を含むメッセージの受信用にサーバ (イベントソース) にインタレスト (サブスクリプション) を登録するために使用されます。Redfish Eventing メッセージの受信に関心を持つクライアントは、iDRAC にサブスクライブして Lifecycle Controller ジョブ関連のイベントを受信することができます。

シャーシイベントの監視

PowerEdge FX2/FX2s シャーシでは、iDRAC 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。サーバ上の iDRAC が機能していない場合、CMC は最初の 16 個のイベントをキューに入れ、残りを CMC ログに記録します。これらの 16 個のイベントは、**Chassis monitoring (シャーシの監視)** が有効に設定された時点で iDRAC に送信されます。

iDRAC が必要な CMC 機能がないことを検知した場合、CMC のファームウェアアップグレードなしでは使用できない機能があることを知らせる警告メッセージが表示されます。

iDRAC ウェブインタフェースを使用したシャーシイベントの監視

iDRAC ウェブインタフェースを使用してシャーシイベントを監視するには、次の手順を実行します。

メモ: このセクションは、**サーバーモードでのシャーシ管理** が CMC で **監視** または **管理と監視** に設定されている場合に PowerEdge FX2/FX2s シャーシに対してのみ表示されます。

1. CMC インタフェースで、**Chassis Overview (シャーシ概要)** > **Setup (セットアップ)** > **General (一般)** をクリックします。
2. **サーバーモードでのシャーシ管理** ドロップダウンメニューで **管理と監視** を選択して、**適用** をクリックします。
3. iDRAC ウェブインタフェースを起動し、**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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

アラートメッセージ ID

次の表に、アラートに対して表示されるメッセージ ID の一覧を示します。

表 33. アラートメッセージ ID

メッセージ ID	説明	説明 (MX プラットフォーム用)
AMP	アンペア数	アンペア数
ASR	自動システムリセット	自動システムリセット
BAT	バッテリイベント	バッテリイベント
BIOS	BIOS 管理	BIOS 管理
BOOT	起動制御	起動制御
CBL	ケーブル	ケーブル
CPU	プロセッサ	プロセッサ
CPUA	プロセッサ不在	プロセッサ不在
CTL	ストレージコントローラ	ストレージコントローラ
DH	証明書管理	証明書管理
DIS	自動検出	自動検出
ENC	ストレージエンクロージャ	ストレージエンクロージャ
FAN	ファンイベント	ファンイベント
FSD	デバッグ	デバッグ
HWC	ハードウェア設定	ハードウェア設定
IPA	DRAC IP 変更	DRAC IP 変更
ITR	イントルージョン	イントルージョン
JCP	ジョブ制御	ジョブ制御
LC	Lifecycle Controller	Lifecycle Controller
LIC	ライセンス	ライセンス
LNK	リンクステータス	リンクステータス
LOG	ログイベント	ログイベント
MEM	メモリ	メモリ
NDR	NIC OS ドライバ	NIC OS ドライバ
NIC	NIC 設定	NIC 設定
OSD	OS 導入	OS 導入
OSE	OS イベント	OS イベント

表 33. アラートメッセージ ID（続き）

メッセージ ID	説明	説明（MX プラットフォーム用）
PCI	PCI デバイス	PCI デバイス
PDR	物理ディスク	物理ディスク
PR	部品交換	部品交換
PST	BIOS POST	BIOS POST
PSU	電源装置	電源装置
PSUA	PSU 不在	PSU 不在
PWR	電力消費	電力消費
RAC	RAC イベント	RAC イベント
RDU	冗長性	冗長性
RED	FW ダウンロード	FW ダウンロード
RFL	IDSDM メディア	IDSDM メディア
RFLA	IDSDM 不在	IDSDM 不在
RFM	FlexAddress SD	適用なし
RRDU	IDSDM の冗長性	IDSDM の冗長性
RSI	リモートサービス	リモートサービス
SEC	セキュリティイベント	セキュリティイベント
SEL	システムイベントログ	システムイベントログ
SRD	ソフトウェア RAID	ソフトウェア RAID
SSD	PCIe SSD	PCIe SSD
STOR	保管時	保管時
SUP	FW アップデートジョブ	FW アップデートジョブ
SWC	ソフトウェア設定	ソフトウェア設定
SWU	ソフトウェアの変更	ソフトウェアの変更
SYS	System Info	System Info
TMP	温度	温度
TST	テストアラート	テストアラート
UEFI	UEFI イベント	UEFI イベント
USR	ユーザー追跡	ユーザー追跡
VDR	仮想ディスク	仮想ディスク

表 33. アラートメッセージ ID（続き）

メッセージ ID	説明	説明（MX プラットフォーム用）
VF	vFlash SD カード	vFlash SD カード
VFL	vFlash イベント	vFlash イベント
VFLA	vFlash 不在	vFlash 不在
VLT	電圧	電圧
VME	仮想メディア	仮想メディア
VRM	仮想コンソール	仮想コンソール
WRK	作業メモ	作業メモ

12

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 マネージャー機能は、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 1XMany 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 マネージャー機能にアクセスできるのは、iDRAC 管理ユーザーのみです。

メモ: ユーザー体験を向上できるよう、グループ マネージャーは最大で 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
- iDRAC グループのファームウェア アップデート

グループマネージャ

グループ マネージャー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 マネージャーのようこそ画面で [**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 マネージャーのようこそ画面には、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

オプション	説明
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 間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。グループを作成した特定の 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任意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 を選択すると、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、ユーザーは

表 34. グループ マネージャーのオプション（続き）

オプション	説明
	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。

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れません。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、先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 ユーザーには影響しません。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が 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セク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のホームページ（サマリビュー）は大別して 3 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。

- ローカル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、サー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、この警告ボックスは表示されません。
- グループを制御する iDRAC（プライマリとセカンダリコントローラ）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 のリストがを表示されます。

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、ユーザーは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。

表 35. サーバ属性

サーバ属性	説明
Health（正常性）	特定のサーバの正常性ステータスを示します。
ホスト名	サーバ名を表示します。
iDRAC の IP アドレス	正確な IPV4 および IPV6 アドレスを表示します。
サービスタグ	サービスタグ情報を表示します。
モデル	デルサーバのモデル番号を表示します。
iDRAC	iDRAC のバージョンを表示します。
最新ステータスの更新	サーバの最新更新時のタイムスタンプを表示します。

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、エクスプレスサービスコード、オペレーティングシステム、アセットタグ、ノード 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、サーバに関する詳細情報が表示されます。行を 1 つダブルクリックするか、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クションです。

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 ネットワーキングを使用して iDRAC 間の通信を行います (Web ブラウザー 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 は同じ vLAN 上にある必要があり、トラフィックはルーターを通過することはできません)。

グループ マネージャーが有効な場合、iDRAC の現在のユーザー定義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 ネットワーキングを使用すると、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なくなります。

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)
- C000 -> F000 はグループ内で通信するメンバーごとに 1 つの空きポートを動的に識別

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 トポロジー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見なされ、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 ホストと iDRAC を検出して共通グループにオンボ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、共通グループにオンボ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内に個別のジョブを所有します。Group Manager はメンバー iDRAC での変更を検出したり、メンバーの設定をロックしたりしません。

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。

グループから離脱しても、メンバー iDRAC のローカルユーザーまたは変更設定は変更されません。

新規ユーザーの追加

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プロファイル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にユーザーを追加するために作成されます。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)** ページにあります。

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

オプション	説明
新規ユーザー情報	新しいユーザーの詳細情報を入力できます。
iDRAC 権限	将来使用するために、ユーザーの役割を定義できます。
詳細ユーザー設定	(IPMI) ユーザー特権を設定でき、SNMP を有効にできます。

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。

ユーザーパスワードの変更

このセクションを使用して、ユーザーのパスワード情報を変更します。個々のユーザーの**ユーザー**詳細が、**ユーザー名**、**ロール**および**ドメイン**情報とともに表示されます。グループジョブは、そのグループ内のすべてのサーバのユーザーパスワードを変更するために作成されます。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)** ページにあります。

ユーザーがすでに存在する場合、パスワードを更新できます。システムロックダウンが有効なメンバー iDRAC はすべて (つまりグループの一部)、ユーザーパスワードが更新されなかったことを示すエラーを返します。ユーザーが存在しない場合、ユーザーがシステムに存在しないことを示すエラーが Group Manager に返されます。Group Manager GUI に表示されるユーザーのリストは、プライマリコントローラとして動作している iDRAC の現在のユーザーリストに基づきます。すべての iDRAC のすべてのユーザーが表示されるわけではありません。

ユーザーの削除

このセクションを使用して、すべてのグループサーバからユーザーを削除します。グループジョブは、すべてのグループサーバからユーザーを削除するために作成されます。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)** ページにあります。

ユーザーがすでにメンバー iDRAC に存在する場合、ユーザーを削除できます。システムロックダウンが有効なメンバー iDRAC はすべて (つまりグループの一部)、ユーザーが削除されなかったことを示すエラーを返します。ユーザーは存在していない場合は、その iDRAC に対して正常に削除されたことが示されます。Group Manager GUI に表示されるユーザーのリストは、プライマリコントローラとして動作している iDRAC の現在のユーザーリストに基づきます。すべての iDRAC のすべてのユーザーが表示されるわけではありません。

アラートの設定

このセクションを使用して電子メールアラートを設定します。デフォルトではアラートは無効です。ただし、いつでもアラートを有効にできます。グループジョブは、電子メールアラート設定をすべてのグループサーバに適用するために作成されます。グループジョブのステータスは、**Group Manager (グループマネージャ) の** > **Jobs (ジョブ)** ページで監視できます。グループマネージャの電子メールアラートは、すべてのメンバー上の電子メールアラートを設定します。同じグループ内のすべてのメンバー上の SMTP サーバを設定します。各 iDRAC が個別に構成されます。電子メールの設定は、グローバルで保存されません。現在の値は、プライマリコントローラとして動作している iDRAC に基づきます。グループを残しても電子メールアラートは再設定されません。

アラートの設定の詳細については、「アラートを送信するための iDRAC の設定」を参照してください。

表 37. アラートオプションの設定

オプション	説明
SMTP (電子メール) サーバアドレス設定	サーバの 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、ユーザー名とパスワードを入力する必要があります。
電子メールアドレス	複数の電子メール ID を設定して、システムステータスの変更についての電子メール通知を受信するようにできます。1 通のテ

表 37. アラートオプションの設定（続き）

オプション	説明
	スト用電子メールをシステムから設定済みアカウントに送信できます。
アラートカテゴリ	複数のアラートカテゴリを選択して電子メール通知を受信するようにできます。

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 の接続性
- 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までは、該当するビューの唯一のメンバーとして表示されます。

メモ: グループマネージャコンソールの 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

オプション	説明
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オ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ディング時にそのパスワードを変更する必要があります。 グループオンボーディングにより、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。
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。
無視しない	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。
再スキャン	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。

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。

表 39. Jobs（ジョブ）ビュー

オプション	説明
ステータス	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。
ジョブ	ジョブの名前を表示します。
ID	ジョブの ID を表示します。
開始時刻	開始時刻を表示します。
終了時刻	終了時刻を表示します。
処置	• 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 - ジョブが失敗状態になったときは、ユーザーは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。
エクスポート	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。

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に完了します。ジョブの開始から完了までは 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

オンボーディ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。オンボーディ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 (グループ上方) パネルには、統合さ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 (グループの設定) ボタンをクリックしてアクセスできる、Group Settings (グループの設定) 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

グループ属性	説明
グループ名	グループの名前を表示します。
システムの数	グループ内のシステムの合計数を表示します。
作成日	タイムスタンプの詳細を表示します。
作成者	グループ管理者の詳細を表示します。
制御システム	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。
バックアップシステム	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。

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

処置	説明
名前の変更	**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。
Change Passcode (パスコードの変更)	**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。
システムの削除	グループから複数のシステムを一度に削除できます。
グループの削除	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。

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

オプション	説明
正常なシャットダウン	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。
コールドリブート	電源を切ってからシステムを再起動します。
仮想コンソール	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。 **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。

Group Manager のシングルサインオン

グループ内のすべての iDRAC は、共有シークレット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、ピアメンバーに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、ユーザーが最初にログインした iDRAC のサービスタグです。

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

- プ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、プ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継ぎます。

- プ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、新しいプ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。
- ユーザー設定やユーザーの関与は必要ありません。

iDRAC グループのファームウェア アップデート

iDRAC グループのファームウェアをアップデートするには、ローカル ディレクトリーから DUP ファイルを使用して、次の手順を実行します。

1. グループ マネージャー コンソールの重要なビューにアクセスして、概要ビューの下にある **iDRAC ファームウェアのアップデート** をクリックします。
2. 表示されたファームウェア アップデート ダイアログ ボックスで、インストールするローカル iDRAC DUP ファイルを参照して選択します。**アップロード** をクリックします。
3. ファイルが iDRAC にアップロードされ、整合性の検証が行われます。
4. ファームウェア アップデートを確認します。グループ iDRAC ファームウェア アップデート ジョブは、即時に実行するようにスケジュールされています。グループ マネージャーで他のグループ ジョブが実行されている場合は、前のジョブが完了した後に実行されます。
5. グループ ジョブ ビューから iDRAC 更新ジョブの実行を追跡することができます。

メモ: この機能は iDRAC バージョン 3.50.50.50 以降でのみサポートされています。

13

ログの管理

iDRAC は、システム、ストレージデバイス、ネットワークデバイス、ファームウェアのアップデート、設定変更、ライセンスメッセージなどに関連するイベントが含まれた Lifecycle ログを提供します。ただし、システムイベントは、システムイベントログ (SEL) と呼ばれる別のログとしても使用できます。Lifecycle ログは、iDRAC ウェブインタフェース、RACADM、および WSMan 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 ログにも、同じ SEL エントリーが提供されます。

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`

SEL エントリをクリアする場合：`racadm clrsel`

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

iDRAC 設定ユーティリティを使用したシステムイベントログの表示

iDRAC 設定ユーティリティを使用してシステムイベントログ（SEL）のレコードの総数を確認し、ログをクリアすることができます。この操作を行うには、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。

- SSH
- Web インターフェイス
- RACADM
- Redfish
- 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: パーソナリティモード変更に対する Lifecycle ログは、ホストのウォームブート中にしか生成されません。

RACADM CLI または iDRAC Web インターフェイ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ーフェイス、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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

Lifecycle Controller ログのエクスポート

Lifecycle Controller ログ全体（アクティブ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と並べられます。

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。

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

   フィールドについては、『iDRAC オンラインヘルプ』を参照してください。
3. **エクスポート** をクリックしてログを指定した場所にエクスポートします。

RACADM を使用した Lifecycle Controller ログのエクスポート

Lifecycle Controller ログをエクスポートするには、`lclog export` コマンドを使用します。

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

作業メモの追加

iDRAC にログインする各ユーザーは、作業メモを追加でき、これはイベントとして Lifecycle ログに保存されます。作業メモを追加するには iDRAC ログ権限が必要です。それぞれの新しい作業メモで最大 255 文字がサポートされます。

メモ: 作業メモは削除できません。

作業メモを追加するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**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。

   メモ: 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ギングの設定

リモート Syslog サーバーを設定するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**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にも同時に書き込まれます。

RACADM を使用したリモートシステムロギングの設定

リモートシステムロギングを設定するには、`iDRAC.SysLog` グループのオブジェクトで `set` コマンドを使用します。

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

14

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
- ピーク時のヘッドルーム値および瞬間的ヘッドルーム値 (ラックおよびタワーサーバーの場合)

メモ: システムの電力消費傾向 (時間単位、日単位、週単位) のヒストグラムが維持されるのは iDRAC の実行中のみです。iDRAC が再起動されると、既存の電力消費データが失われ、ヒストグラムも再び開始されます。

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、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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

電力消費量の警告しきい値の設定

ラックおよびタワーシステム内の電力消費センサーに対する警告しきい値を設定することができます。ラックおよびタワーシステムに対する警告 / 重要電力しきい値により、PSU の容量と冗長ポリシーに基づいて、システムの電源サイクルが変更される場合があります。ただし、冗長ポリシーの電源装置容量が変更される場合でも、警告しきい値が重要しきい値を超えることはできません。

ブレード システムの警告電力しきい値は、CMC（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。

メモ: 警告のしきい値は、racreset または iDRAC アップデートを実行した後にデフォルト値にリセットされます。

ウェブインタフェースを使用した電力消費量の警告しきい値の設定

1. iDRAC ウェブインタフェースで、**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。
   Edit Warning Threshold（警告しきい値の編集） ページが表示されます。
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** の値よりも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 https://www.dell.com/idracmanuals から入手可能な『*Lifecycle Controller リモート サービス クイック スタート ガイド*』および『*Dell 電源状態管理*』プロファイルマニュアルを参照してください。

iDRAC によるサーバ電源制御操作は、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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

電力制限

高負荷のシステムがデータセンターに示す AC および DC 電力消費量の範囲を対象とする電力しきい値の限界を表示できます。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 インベントリーに基づいて、ブレード サーバーに電源を入れる前に、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量まで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過する場合があります。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、周辺光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。

電力上限値が推奨される最小しきい値よりも低く設定されると、iDRAC は要求された電力上限を維持できないことがあります。

この値は、ワット、BTU/ 時、または推奨される電力上限に対する割合で指定できます。

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

電力ポリシーを表示し、設定するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**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。

- System.Power.Cap.Enable
- System.Power.Cap.Watts
- System.Power.Cap.Btuhr
- System.Power.Cap.Percent

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

iDRAC 設定ユーティリティを使用した電力上限ポリシーの設定

電力ポリシーを表示し、設定するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**電源設定** に進みます。

   メモ: 電源設定 リンクは、サーバーの電源装置が電源監視をサポートする場合にのみ使用可能です。

   iDRAC 設定の電源設定 ページが表示されます。
2. **電力上限ポリシー** を有効にするには、**有効** を選択します。それ以外の場合は、**無効** を選択します。
3. 推奨設定を使用するか、**ユーザー定義の電源上限ポリシー** で必要な制限値を入力します。
   オプションの詳細については、『iDRAC 設定ユーティリティオンラインヘルプ』を参照してください。
4. **戻る**、**終了** の順にクリックし、**はい** をクリックします。
   電力上限値が設定されます。

電源装置オプションの設定

冗長性ポリシー、ホットスペア、およびパワーファクタ補正などの電源装置オプションを設定できます。

ホットスペアは、冗長電源装置 (PSU) を設定して、サーバーの負荷に応じて電源をオフする PSU の機能です。これにより、残りの PSU はより高い負荷および効率で動作できます。これには、この機能をサポートする PSU が必要で、必要なときに迅速に電源オンできます。

2 台の 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 *アウェイク*状態で、大部分の電流を提供します。もう 1 台の PSU はスリープモードになり、少量の電流を提供します。これは 2 台の PSU による 1+0 と呼ばれることが多く、ホットスペアは有効になっています。すべての PSU-1 が回路 -A にあり、すべての PSU-2 が回路 -B 上にある場合、ホットスペアを有効にする (工場出荷時のデフォルト設定) と、回路 -B への負荷は大幅に低くなり、警告がトリガされます。ホットスペアを無効にしている場合、電源の共有は、2 台の PSU 間で五分五分となり、回路 -A と回路 -B は通常、同一の負荷を分担します。

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ブジェクトを使用します。

- System.Power.RedundancyPolicy
- System.Power.Hotspare.Enable
- System.Power.Hotspare.PrimaryPSU
- System.Power.PFC.Enable

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

iDRAC 設定ユーティリティを使用した電源装置オプションの設定

電源装置オプションを設定するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**電源設定** に進みます。

   メモ: 電源設定 リンクは、サーバーの電源装置が電源監視をサポートする場合にのみ使用可能です。

   iDRAC 設定の電源設定 ページが表示されます。
2. **電源装置オプション** で次の操作を行います。
   - 電源装置の冗長性を有効化または無効化する。
   - ホットスペアを有効化または無効化する。
   - プライマリ電源装置を設定する。
   - 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。
   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の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。これには以下が含まれています（限定はされません）。

- 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正確に把握できるようにする大規模なセンサーのセット（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ー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て、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要件の指定方法に関する業界標準）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 の冷却がどのよう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. カードがサード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小の LFM 値を確認します。

4. サード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でき、カスタムカードの仕様を通じてユーザーの意識が向上します。

- 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）および排気温度のカスタム設定ができます。

1. これらの設定のほとんどは、ベースラインの冷却に温度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。

   メモ: サードパーティ製の PCIe カード用に追加されたファン速度は上記の例外となります。温度アルゴリズムがプロビジョニングするサードパーティ製カードのエアフローは、実際にカードに必要な冷却よりも多かったり少なかったりする場合があります。お客様はサードパーティ製のカードに対応する LFM を入力して、カードに対する応答を微調整する必要がある場合があります。

2. 排気温度のカスタムオプションは、排気温度をお客様の希望する設定に制限します。

   メモ: 特定の設定と負荷によっては、希望する設定以下に排気を物理的に減らすことができない場合がありますのでご注意ください（たとえば、吸気温度が高い｛例：30 ℃｝、高負荷な設定｛高いシステム電力消費、低いエアフロー｝でカスタム排気設定 45 ℃ など）。

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 電力消費量を抑え、ファンの速度と防音を制御します。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があります。

- 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（高出力の実現）、システム構成が高密度になります。これにより、システムの制限が減り、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。

- カスタムファンは、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）。

- カスタムヒートシンクは、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。

15

iDRAC ダイレクト アップデート

iDRAC は、PowerEdge サーバーのさまざまなコンポーネントのファームウェアをアップデートするための帯域外機能を提供します。iDRAC ダイレクト アップデートは、アップデート中にステージング ジョブを排除するために役立ちます。

かつて、iDRAC は、コンポーネントのファームウェア アップデートを開始するために段階的なアップデートを行っていました。このリリースから、PSU およびバックプレーンにダイレクト アップデートが適用されています。ダイレクト アップデートとバックプレーンを使用すると、迅速なアップデートが可能になります。PSU の場合、再起動が 1 回 (アップデートの初期化のための) 回避され、アップデートを 1 回の再起動で行うことができます。

iDRAC のダイレクト アップデート機能を使用すると、アップデートを開始するための最初の再起動を排除できます。2 回目の再起動は、デバイス自体によって制御されます。ジョブのステータスによって個別にリセットする必要がある場合、iDRAC はユーザーに通知します。

16

ネットワークデバイスのインベントリ、監視、および設定

次のネットワークデバイスをインベントリ、監視、および設定できます。

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

CNA デバイスで NPAR または個々のパーティションを無効にする前に、必ずすべての I/O アイデンティティ属性（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リティを無効にすることでパーティションを無効にできます。

インストールされている CNA デバイスのタイプによって、パーティション属性の設定が、パーティションがアクティブだった最後の時点から保持されないことがあります。パーティションを有効にする場合は、すべての I/O アイデンティティ属性とパーティション関連の属性を設定します。VirtualizationMode 属性の設定を NPAR に変更するか、またはパーティションのパーソナリティなど（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ーと監視
- テレメトリー ストリーミング
- シリアル データ キャプチャ
- 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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』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、ネットワークケーブル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]** と移動して、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]** > **[共通設定]** > **[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。

フィールドまたはオプション	説明
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す。
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、ブレード シャーシのサービス 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。
- **ディスカバリー 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によるスイッチ内の iDRAC 接続ポートの検出ができます。ディスカバリー 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もので、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。ディスカバリー LLDP では、IP アドレス、MAC アドレス、サービス タグなどの iDRAC に類似した詳細情報が保持されるため、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: ポート/パーティションの仮想 MAC アドレスがクリアされた場合、仮想 MAC アドレスは 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 サーバーに対しては有効になっており、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 を使用して、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に、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

可能な接続ビューデータ	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 QP PCIe 10 Gb • X710 + I350 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
QLogic	• QL41162 PCIe 10GE 2P

製造元	タイプ
	• 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

メモ: 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みます。**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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』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ーと監視

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、インベントリーを表示できます。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
- IB 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ツ ナンバーです。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
- リビジョン
- シリアル番号
- デバイス識別子/タイプ情報

- ケーブルの長さ（メートル）

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 デバイス情報を確認するには、**[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 デバイス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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』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、分析、アラート サービス」に対してストリーミングします。この機能は、データに関するオンデマンドのデータ コレクションもサポートしています。

テレメトリー データには、メトリック/インベントリーおよびログ/イベントが含まれます。データは、Redfish クライアントおよびリモート Syslog サーバーなどのリモート Consumer に対して、iDRAC からのストリーム（プッシュアウト）または収集（プル）ができます。テレメトリー データの提供は、iDRAC SupportAssist Data Collector に対してオンデマンドでも行われます。データ コレクションとレポートは、定義済みの Redfish テレメトリー メトリック、トリガー、およびレポートの定義に基づいて実施されます。テレメトリー ストリーミングの設定は、RACADM、SCP、Redfish、およびサーバー設定プロファイル（SCP）を介して行えます。

テレメトリーを設定するには、必要なデバイス レポートまたはログを有効化ないし選択して、データ ストリーミングの動作と頻度を定義します。テレメトリーは**設定** > **システム設定**ページで設定します。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。

タイプ	メトリック グループ	インベントリ	センサー	統計情報	設定	メトリクス
I/O デバイス	NIC	いいえ	はい	はい	いいえ	いいえ
	FC HBA	いいえ	はい	はい	いいえ	いいえ
サーバー デバイス	CPU	いいえ	はい	いいえ	いいえ	はい
	メモリ	いいえ	はい	いいえ	いいえ	はい
	ファン	いいえ	はい	いいえ	いいえ	いいえ
	PSU	いいえ	いいえ	いいえ	いいえ	はい
	センサー	いいえ	はい	いいえ	いいえ	いいえ
環境	サーマル	いいえ	はい	いいえ	いいえ	はい
	電源	いいえ	いいえ	はい	いいえ	はい
	パフォーマンス	いいえ	いいえ	はい	いいえ	いいえ
アクセラレーター	GPU	いいえ	いいえ	はい	いいえ	はい

テレメトリー セクションのフィールドの説明については、*iDRAC のオンライン ヘルプ*を参照してください。

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 ドライブ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にないドライブについてのみレポートされます。
- NVMeSMARTData は、SSD (PCIeSSD/NVMe Express) ドライブで 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 メモリー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。
- 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。
- 4.40.00.00 リリースでは、CUPS レポートは SystemUsage に名称変更されており、インテルと AMD の両方のプラットフォームでサポートされています。

テレメトリーのワークフロー:

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 テレメトリー設定として、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 インター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

   メモ: テレメトリー レポートを必要とする特定のハードウェアに対し、iDRAC Alerts および Redfish イベントを有効にします。
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、サブスクライブ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。

機能的な制限:

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 ベースのもの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、すべてのサブスクライブ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受信するのは、サブスクリプションが正常に作成された場合のみです。
- 指標データには、ソースからのデータ収集の時点の、ISO 形式 UTC 時間でのタイムスタンプ (「Z」で終わる) が含まれています。
- 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。配信エラー数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への通知は、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、`racresetcfg` 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 データをキャプキャして保存し、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にすることができます。この属性を有効にすると、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。

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。

メモ:
- 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、バッファーには最新のデータが追加され続けます。ユーザーがシリアル 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。

ユーザーが任意のインターフェイスからシリアル 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 は継続的にデータ キャプチャーを開始し、512KB を上限として共有メモリーに保存します。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化 (つまり、オペレーティングシステムの再起動、ウォームリセット、コールドリセット、または AC サイクル) に基づいて、また、その電源状態に対する永続性ポリシーに基づいて設定を適用できます。これにより、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。

IO アイデンティティ機能を使用すると、次の操作を行うことが出来ます。
- ネットワークおよび Fibre Channel デバイスに対する仮想アドレスの表示と設定 (たとえば、NIC、CNA、FC HBA)。
- イニシエータ (iSCSI および FCoE 用) およびストレージターゲット設定 (iSCSI、FCoE、および FC 用) の設定。
- システム AC 電源の喪失、システムのコールドリセットとウォームリセットに対する設定値の永続性またはクリアランスの指定。

仮想アドレス、イニシエータ、およびストレージターゲットに設定された値は、システムリセット時の主電源の処理方法や、NIC、CNA、または FC HBA デバイスに補助電源があるかどうかに基づいて変更される場合があります。IO アイデンティティ設定の永続性は、iDRAC を使用したポリシー設定に基づいて実現できます。

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。

表 43. I/O アイデンティティ最適化対応のカード

製造元	タイプ
Broadcom	• 5719 Mezz 1 GB • 5720 PCIe 1 GB • 5720 bNDC 1 GB • 5720 rNDC 1 GB • 57414 PCIe 25 GbE
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*) • QL41262HMKR-DE Fab A/B Mezz 25 Gb (*MX プラットフォーム用*) • QL41232HMKR-DE Fab A/B Mezz 25 Gb (*MX プラットフォーム用*)

表 43. I/O アイデンティティ最適化対応のカード（続き）

製造元	タイプ
	• 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 • LPe31002-M6-D DP PCIe FC16 • LPe32000-M2-D SP PCIe FC32 • LPe32002-M2-D DP PCIe FC32 • LPe31002-D Fab C Mezz FC16（*MX プラットフォーム用*） • LPe32002-D Fab C Mezz FC32（*MX プラットフォーム用*） • LPe35002-M2 FC32 2-ポート • LPe35000-M2 FC32 1-ポート

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 ファームウェアバージョンを示しています。

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 / リモート割り当てアドレスと永続性ポリシーの動作

OME Modular でのリモート割り当てアドレス機能の状態	iDRAC で設定されているモード	iDRAC における IO アイデンティティ機能状況	SCP	永続性ポリシー	永続性ポリシーのクリア - 仮想アドレス
リモート割り当てアドレス有効	リモート割り当てアドレスモード	有効	仮想アドレス管理（VAM）設定済み	設定された VAM が持続	リモート割り当てアドレスに設定
リモート割り当てアドレス有効	リモート割り当てアドレスモード	有効	VAM 未設定	リモート割り当てアドレスに設定	永続性なし - リモート割り当てアドレスに設定
リモート割り当てアドレス有効	リモート割り当てアドレスモード	無効	Lifecycle Controller で指定したパスを使って設定済み	当該のサイクルに対してリモート割り当てアドレスに設定	永続性なし - リモート割り当てアドレスに設定
リモート割り当てアドレス有効	リモート割り当てアドレスモード	無効	VAM 未設定	リモート割り当てアドレスに設定	リモート割り当てアドレスに設定
リモート割り当てアドレス無効	リモート割り当てアドレスモード	有効	VAM 設定済み	設定された VAM が持続	永続性のみ - クリアは使用できません。
リモート割り当てアドレス無効	リモート割り当てアドレスモード	有効	VAM 未設定	ハードウェア MAC アドレスに設定	永続性のサポートなし。カードの動作に依存

表 44. 仮想 /リモート割り当てアドレスと永続性ポリシーの動作（続き）

OME Modular でのリモート割り当てアドレス機能の状態	iDRAC で設定されているモード	iDRAC における IO アイデンティティ機能状況	SCP	永続性ポリシー	永続性ポリシーのクリア - 仮想アドレス
リモート割り当てアドレス無効	リモート割り当てアドレスモード	無効	Lifecycle Controller で指定したパスを使って設定済み	当該のサイクルに対して Lifecycle Controller 設定が持続	永続性のサポートなし。カードの動作に依存
リモート割り当てアドレス無効	リモート割り当てアドレスモード	無効	VAM 未設定	ハードウェア MAC アドレスに設定	ハードウェア MAC アドレスに設定
リモート割り当てアドレス有効	コンソールモード	有効	VAM 設定済み	設定された VAM が持続	永続性とクリアの両方が機能することが必要
リモート割り当てアドレス有効	コンソールモード	有効	VAM 未設定	ハードウェア MAC アドレスに設定	ハードウェア MAC アドレスに設定
リモート割り当てアドレス有効	コンソールモード	無効	Lifecycle Controller で指定したパスを使って設定済み	当該のサイクルに対して Lifecycle Controller 設定が持続	永続性のサポートなし。カードの動作に依存
リモート割り当てアドレス無効	コンソールモード	有効	VAM 設定済み	設定された VAM が持続	永続性とクリアの両方が機能することが必要
リモート割り当てアドレス無効	コンソールモード	有効	VAM 未設定	ハードウェア MAC アドレスに設定	ハードウェア MAC アドレスに設定
リモート割り当てアドレス無効	コンソールモード	無効	Lifecycle Controller で指定したパスを使って設定済み	当該のサイクルに対して Lifecycle Controller 設定が持続	永続性のサポートなし。カードの動作に依存
リモート割り当てアドレス有効	コンソールモード	無効	VAM 未設定	ハードウェア MAC アドレスに設定	ハードウェア MAC アドレスに設定

FlexAddress および IO アイデンティティに対するシステム動作

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

タイプ	CMC における FlexAddress 機能状況	iDRAC における IO アイデンティティ機能状況	再起動サイクルに対するリモートエージェント VA の可用性	VA プログラミングソース	再起動サイクル VA 持続動作
FA と同等の永続性を持つサーバー	有効	無効		CMC からの FlexAddress	FlexAddress 仕様による
	N/A、有効、または無効	有効	はい - 新規または永続的	リモートエージェント仮想アドレス	FlexAddress 仕様による
			無	仮想アドレスがクリア済み	
	無効	無効			
VAM 永続性ポリシー機能を備えたサーバー	有効	無効		CMC からの FlexAddress	FlexAddress 仕様による
	有効	有効	はい - 新規または永続的	リモートエージェント仮想アドレス	リモートエージェントポリシー設定による

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（続き）

タイプ	CMC における FlexAddress 機能状況	iDRAC における IO アイデンティティ機能状況	再起動サイクルに対するリモートエージェント VA の可用性	VA プログラミングソース	再起動サイクル VA 持続動作
			無	CMC からの FlexAddress	FlexAddress 仕様による
	無効	有効	はい - 新規または永続的	リモートエージェント仮想アドレス	リモートエージェントポリシー設定による
			無	仮想アドレスがクリア済み	
	無効	無効			

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が、I/O アイデンティティー最適化機能を有効にすると、起動最適化を行うことができます。この機能が有効である場合、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、イニシエータ、およびストレージターゲットの属性が設定されるため、2 回目の BIOS 再起動が必要なくなります。デバイス設定と起動操作は一回のシステム起動で実行され、起動時間パフォーマンスのために最適化されます。

I/O アイデンティティ最適化を有効にする前に、次を確認してください。

- ログイン、設定、およびシステム管理の権限がある。
- BIOS、iDRAC、およびネットワークカードが最新のファームウェアにアップデートされています。

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

I/O アイデンティティ最適化を有効化または無効化するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**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。
   I/O Identity Optimization（I/O アイデンティティ最適化） ページが表示されます。
2. **II/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 IO アイデンティティ最適化の有効化または無効化

I/O アイデンティティ最適化を有効化するには、次のコマンドを使用します。

```
racadm set idrac.ioidopt.IOIDOptEnable Enabled
```

この機能を有効にした後、設定を有効にするには、システムを再起動してください。

I/O アイデンティティ最適化を無効化するには、次のコマンドを使用します。

```
racadm set idrac.ioidopt.IOIDOptEnable Disabled
```

I/O アイデンティティ最適化設定を表示するには、次のコマンドを使用します。

```
racadm get iDRAC.IOIDOpt
```

SSD 摩耗しきい値

iDRAC では、すべての SSD の残留定格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 トラップ、IPMI アラート、リモート Syslog への記録、WS イベンティング、OS ログも実行します。

iDRAC は、SSD の残留定格書き込み耐久性がしきい値の設定値を下回った段階でユーザーにアラートを出すことで、システム管理者による SSD のバックアップまたは交換を行えるようにします。

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、およびストレージターゲット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属性はそれぞれ、システム内の適用可能なすべてのデバイスのすべてのポートおよびパーティションに適用されます。デバイスの動作は、補助電源駆動デバイスと非補助電源駆動デバイスで異なります。

メモ: **永続性ポリシー**機能はデフォルトに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 プラットフォームでない場合) または **RemoteAssignedAddress** (MX プラ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 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
- ストレージターゲット

永続性ポリシーを適用する前に、次の操作を行ってください。

- ネットワークハードウェアのインベントリを少なくとも 1 回実行します。つまり、Collect System Inventory On Restart を有効にします。
- I/O アイデンティティ最適化を有効にします。

次の場合に、イベントは Lifecycle Controller ログに記録されます。

- I/O アイデンティティ最適化が有効または無効になっている。
- 持続性ポリシーが変更された。
- 仮想アドレス、イニシエータ、およびターゲットの値が、ポリシーに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

永続性ポリシー	AC 電源喪失	コールドブート	ウォームブート
仮想アドレス：補助電源駆動デバイス	選択されていません	選択済み	選択済み
仮想アドレス：非補助電源駆動デバイス	選択されていません	選択されていません	選択済み
イニシエータ	選択済み	選択済み	選択済み
ストレージターゲット	選択済み	選択済み	選択済み

メモ: 永続的ポリシーが無効になっているとき、および仮想アドレスを削除するための操作を実行するときは、永続的ポリシーを再度有効にしても仮想アドレスは取得されません。永続的ポリシーを有効にした後で再度仮想アドレスを設定する必要があります。

メモ: 永続性ポリシーが有効で、CNA デバイスのパーティションで仮想アドレス、イニシエータ、またはストレージターゲットが設定されている場合は、VirtualizationMode またはパーティションのパーソナリティを変更する前に、仮想アドレス、イニシエータ、およびストレージターゲットに設定された値をリセットまたはクリアしないでください。永続性ポリシーを無効にすると、アクションは自動的に実行されます。設定ジョブを使用して、仮想アドレスの属性を 0 に、イニシエータとストレージターゲットの値を iSCSI イニシエータとストレージターゲットのデフォルト値 、p. 220 に定義されたとおりに明示的に設定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 アイデンティティー最適化]** と移動します。
2. **I/O アイデンティティ最適化** タブをクリックします。
3. **永続性ポリシー** セクションで、それぞれの永続性ポリシーに対して次の 1 つまたは複数選択します。
   - **[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 オブジェクトと **set** サブコマンドを使用します。

- 仮想アドレスには、**iDRAC.IOIDOpt.VirtualAddressPersistencePolicyAuxPwrd** および **iDRAC.IOIDOpt.VirtualAddressPersistencePolicyNonAuxPwrd** オブジェクトを使用
- イニシエータには、**iDRAC.IOIDOPT.InitiatorPersistencePolicy** オブジェクトを使用
- ストレージターゲットには、**iDRAC.IOIDOpt.StorageTargetPersistencePolicy** オブジェクトを使用

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

iSCSI イニシエータとストレージターゲットのデフォルト値

次の表は、永続性ポリシーがクリアされたときの iSCSI イニシエータおよびストレージターゲットのデフォルト値の一覧です。

表 47. iSCSI イニシエータ - デフォルト値

iSCSI イニシエータ	IPv4 モードでのデフォルト値	IPv6 モードでのデフォルト値
IscsiInitiatorIpAddr	0.0.0.0	::
IscsiInitiatorIpv4Addr	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Addr	::	::
IscsiInitiatorSubnet	0.0.0.0	0.0.0.0
IscsiInitiatorSubnetPrefix	0	0
IscsiInitiatorGateway	0.0.0.0	::
IscsiInitiatorIpv4Gateway	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6Gateway	::	::
IscsiInitiatorPrimDns	0.0.0.0	::
IscsiInitiatorIpv4PrimDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6PrimDns	::	::
IscsiInitiatorSecDns	0.0.0.0	::
IscsiInitiatorIpv4SecDns	0.0.0.0	0.0.0.0
IscsiInitiatorIpv6SecDns	::	::
IscsiInitiatorName	値がクリア	値がクリア
IscsiInitiatorChapId	値がクリア	値がクリア
IscsiInitiatorChapPwd	値がクリア	値がクリア
IPVer	Ipv4	Ipv6

表 48. iSCSI ストレージ ターゲットの属性 — デフォルト値

iSCSI ストレージターゲットの属性	IPv4 モードでのデフォルト値	IPv6 モードでのデフォルト値
ConnectFirstTgt	無効	無効
FirstTgtIpAddress	0.0.0.0	::

表 48. iSCSI ストレージ ターゲットの属性 — デフォルト値（続き）

iSCSI ストレージターゲットの属性	IPv4 モードでのデフォルト値	IPv6 モードでのデフォルト値
FirstTgtTcpPort	3260	3260
FirstTgtBootLun	0	0
FirstTgtIscsiName	値がクリア	値がクリア
FirstTgtChapId	値がクリア	値がクリア
FirstTgtChapPwd	値がクリア	値がクリア
FirstTgtIpVer	Ipv4	
ConnectSecondTgt	無効	無効
SecondTgtIpAddress	0.0.0.0	::
SecondTgtTcpPort	3260	3260
SecondTgtBootLun	0	0
SecondTgtIscsiName	値がクリア	値がクリア
SecondTgtChapId	値がクリア	値がクリア
SecondTgtChapPwd	値がクリア	値がクリア
SecondTgtIpVer	Ipv4	

17

ストレージデバイスの管理

iDRAC 3.15.15.15 リリース以降、iDRAC は第 14 世代 PowerEdge サーバで Boot Optimized Storage Solution (BOSS) コントローラをサポートします。BOSS コントローラは、サーバのオペレーティングシステムの起動専用に設計されています。これらのコントローラは限定的な RAID 機能をサポートし、構成はステージングされます。

iDRAC 4.30.30.30 リリース以降、iDRAC は、AMD システム用の PERC 11、HBA 11、および BOOS 1.5 をサポートします。

メモ: BOSS コントローラは RAID レベル 1 のみをサポートします。

メモ: BOSS コントローラーの場合、両方の PD がプラグアウトされてから再びプラグインされると、完全な VD 情報が使用できない場合があります。

メモ: PERC 11 以降のコントローラーは、ハードウェア Root of Trust (RoT) をサポートします。

iDRAC のエージェントフリー管理は拡張され、PERC コントローラの直接設定も含まれます。それによって、システムに接続されたストレージコンポーネントをランタイムにリモートで設定できます。これらのコンポーネントには、接続されている RAID および非 RAID コントローラ、チャネル、ポート、エンクロージャ、およびディスクが含まれます。PowerEdge Rx4xx/Cx4xx サーバーでは、PERC 9 および PERC 10 コントローラーがサポートされています。PowerEdge Rx5xx/Cx5xx AMD プラットフォーム サーバーでは、PERC 11 がサポートされています。

Comprehensive Embedded Management (CEM) フレームワークでのストレージサブシステムの完全な検出、トポロジ、正常性の監視と設定は、I2C インタフェース経由の MCTP プロトコルを使用した内部および外部 PERC コントローラとのインタフェースによって実現します。リアルタイム設定の場合、CEM では PERC9 コントローラがサポートされます。PERC9 コントローラ の ファームウェアバージョンは、9.1 以降である必要があります。

メモ: ソフトウェア RAID (SWRAID) は CEM でサポートされないため、iDRAC GUI でもサポートされません。SWRAID は RACADM、WSMAN、Redfish のいずれかを使用して管理することができます。

iDRAC を使用すると、OpenManage Storage Management で使用可能な、リアルタイム (再起動以外) の設定コマンドなど、ほとんどの機能を実行できます (仮想ディスクの作成など)。オペレーティングシステムをインストールする前に、RAID を完全に設定できます。

BIOS にアクセスせずにコントローラ機能を設定および管理することができます。これらの機能には、仮想ディスクの設定と、RAID レベルおよびデータ保護用のホットスペアの適用が含まれます。再構築とトラブルシューティングなど、その他多くのコントローラ機能を開始できます。データ冗長性の設定またはホットスペアの割り当てによって、データを保護できます。

ストレージデバイスには、次のものがあります。

- コントローラ - ほとんどのオペレーティングシステムでは、ディスクから直接データの読み取りと書き込みを行わず、読み取りと書き込みの指示をコントローラに送信します。コントローラは、システム内のハードウェアで、データの書き込みと取り出しを行うためにディスクと直接やり取りします。コントローラには、1 つまたは複数の物理ディスクに接続されたコネクタ (チャネルまたはポート)、または物理ディスクを収容するエンクロージャが搭載されています。RAID コントローラーは、ディスクの境界をまたがり、複数のディスクの容量を使用して拡張されたストレージ スペース、すなわち仮想ディスクを作成できます。また、コントローラは、再構築の開始やディスクの初期化など、その他のタスクも実行します。これらのタスクを完了するため、コントローラではファームウェアおよびドライバと呼ばれる特別なソフトウェアが必要となります。コントローラが正常に機能するには、必要最低限のバージョンのファームウェアとドライバがインストールされていることが必要です。コントローラによって、データの読み取りおよび書き込み方法や、タスクの実行方法の特徴が異なります。これらの機能を理解しておくと、ストレージを最も効率的に管理するのに役立ちます。
- 物理ディスクまたは物理デバイスは、エンクロージャ内に存在するか、コントローラに接続されています。RAID コントローラ上では、物理ディスクまたはデバイスを使用して仮想ディスクが作成されます。
- 仮想ディスク - RAID コントローラによって 1 つまたは複数の物理ディスクから作成されたストレージです。仮想ディスクは複数の物理ディスクで作成される場合もありますが、オペレーティングシステムはこれを 1 つのディスクとして認識します。使用する RAID レベルによって、仮想ディスクはディスク障害時に冗長データを保持する場合や、特定の性能属性を備える場合があります。仮想ディスクは RAID コントローラでのみ作成できます。
- エンクロージャ - これはシステムに外部接続されますが、バックプレーンとその物理ディスクはシステム内蔵です。
- バックプレーン - エンクロージャに似ています。バックプレーンで、コントローラのコネクタと物理ディスクがエンクロージャに接続されますが、外付けのエンクロージャに関する管理機能 (温度プローブ、アラームなど) は搭載されません。物理ディスクは、エンクロージャに収容するか、またはシステムのバックプレーンに接続することができます。

メモ: ストレージ スレッドとコンピュート スレッドを含むすべての MX シャーシでは、そのシャーシ内のいずれかのコンピュート スレッドに関連する iDRAC がすべてのストレージ スレッド（割り当て済みおよび割り当て解除の両方）をレポートします。割り当て済みまたは割り当て解除のブレードのいずれかが警告または重要の正常性状態にある場合、ブレード コントローラーも同じステータスをレポートします。

エンクロージャに収容された物理ディスクの管理に加え、エンクロージャのファン、電源装置、温度プローブの状態も監視できます。エンクロージャはホットプラグに対応しています。ホットプラグとは、オペレーティングシステムの実行中に、コンポーネントをシステムに追加することを意味します。

コントローラに接続された物理デバイスには、最新のファームウェアが必要です。最新の対応ファームウェアについては、サービスプロバイダにお問い合わせください。

PERC からのストレージ イベントは、適用可能として SNMP トラップおよび WSMan イベントにマップされます。ストレージ構成に対する変更はすべて、Lifecycle ログに記録されます。

表 49. PERC 機能

PERC 機能	CEM 設定応コントローラ（PERC 9.1 以降）	CEM 設定非対応のコントローラ（PERC 9.0 およびそれ以前）
リアルタイム	**メモ:** PowerEdge Rx5xx/Cx5xx サーバーでは、PERC 9、PERC 10 および PERC 11 コントローラーがサポートされています。 コントローラに対して保留中の既存のジョブもスケジュールされたジョブも存在しない場合、設定が適用されます。 そのコントローラに対して保留中またはスケジュール済みのジョブがある場合は、ジョブをクリアするか、ジョブが完了するまで待ってからランタイムに設定を適用する必要があります。ランタイムまたはリアルタイムは、再起動を必要としないことを意味します。	設定が適用されます。エラーメッセージが表示されます。ジョブの作成が正常に完了せず、Web インターフェイスを使用してリアルタイム ジョブを作成できません。
ステージング	設定オペレーションがすべてステージングされている場合、設定は再起動後にステージングされ、適用されるか、リアルタイムで適用されます。	設定は再起動後に適用されます。

トピック：

- 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
- ストレージデバイスの対応機能のサマリ
- 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にあるデータの保存を管理するためのテクノロジです。RAID の重要な要素は、複数の物理ディスクの容量の組み合わせを単一の拡張ディスク容量として扱うことができるように、物理ディスクをスパンする機能です。RAID のその他の重要な要素には、ディスク障害が発生した場合にデータを復元するために使用できる冗長データを維持する機能があります。RAID では、ストライピング、ミラーリング、パリティなどの異なる方法を使用してデータの保存と再構築を行います。RAID レベルには、データの保存と再構築のために異なる方法を使う異なるレベルがあります。RAID レベルには、読み書きパフォーマンス、データ保護、ストレージ容量という観点では異なる特徴があります。冗長データはすべての RAID レベルで維持されるものではなく、一部の RAID レベルでは失われたデータを復元できません。選択する RAID レベルは、優先事項がパフォーマンスか、保護か、ストレージ容量かによって変わります。

メモ: RAB（RAID Advisory Board）は、RAID の実装に使用される仕様を定義しています。RAB は RAID レベルを定義しますが、異なるベンダーによる RAID レベルの商用実装は、実際の RAID 仕様が異なる場合があります。特定のベンダーの実装は、読み取りおよび書き込みパフォーマンスとデータの冗長性の度合いに影響することがあります。

ハードウェアとソフトウェア RAID

RAID は、ハードウェアまたはソフトウェアのどちらでも実装できます。ハードウェア RAID を使用するシステムには、RAID レベルを実装し、物理ディスクに対するデータの読み書きを処理する RAID コントローラがあります。オペレーティングシステム提供のソフトウェア RAID を使用するときは、オペレーティングシステムが RAID レベルを実装します。このため、ソフトウェア RAID のみを使用するとシステムパフォーマンスを低下させることがあります。ただし、ハードウェア RAID ボリュームとソフトウェア RAID を合わせて使用することによって、パフォーマンスと RAID ボリュームの設定の多様性を向上させることができます。たとえば、2 つの RAID コントローラ間でハードウェア RAID 5 ボリュームのペアをミラーリングすることによって、RAID コントローラの冗長性を提供することができます。

RAID の概念

RAID では特定の方法を使用してデータをディスクに書き込みます。これらの方法を使うと、RAID でデータの冗長性またはパフォーマンスの向上を実現できます。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。ミラーのディスクのうち 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行できます。ミラーリングしたディスクの両方に常に同じデータが入っています。ミラーのいずれも動作側として機能します。ミラーリングされた RAID ディスクグループは、読み取り操作では RAID 5 ディスクグループのパフォーマンスと同等ですが、書き込み速度はより高速です。
- ストライピング - 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、仮想ディスク内の各物理ディスクにシーケンシャルパターンを使用して固定サイズの単位でマッピングされた、連続する仮想ディスクデータアドレスで構成されます。たとえば、仮想ディスクに 5 つの物理ディスクがある場合、ストライピングによって、1 から 5 までの物理ディスクに、どの物理ディスクも重複することなく、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。物理ディスク上に存在するストライプ部分が、ストライプエレメントです。ストライピング自体には、データの冗長性がありません。パリティと組み合わせることで、ストライピングによるデータの冗長性を実現します。
- ストライプサイズ - パリティディスクを含まない、ストライプによって消費される総ディスク容量。たとえば、64KB のディスク容量で、ストライプの各ディスクには 16KB のデータが存在するようなストライプを考えます。この場合、ストライプサイズは 64KB、ストライプエレメントサイズは 16KB となります。
- ストライプエレメント — 単一の物理ディスク上にあるストライプの一部分です。
- ストライプエレメントサイズ - ストライプエレメントによって消費されるディスク容量。たとえば、64KB のディスク容量で、ストライプの各ディスクには 16KB のデータが存在するようなストライプを考えます。この場合、ストライプエレメントサイズは 16KB、ストライプサイズは 64KB となります。
- パリティ - ストライピングとアルゴリズムを組み合わせて使用することによって維持される冗長データ。ストライピングを行っているディスクの 1 つが失敗した場合、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。
- スパン — 物理ディスクグループのストレージ容量を RAID 10、50 または 60 の仮想ディスクとして組み合わせるために使用する RAID 技術。

RAID レベル

各 RAID レベルではミラーリング、ストライピング、パリティを併用することでデータ冗長性や読み書きパフォーマンスの向上を実現します。各 RAID レベルの詳細については、「RAID レベルの選択」を参照してください。

可用性とパフォーマンスを高めるためのデータストレージの編成

RAID は、ディスクストレージをまとめるための異なる方法または RAID レベルを提供します。一部の RAID レベルでは、ディスクの障害発生後にデータを復元できるように冗長データが維持されます。RAID レベルが異なると、システムの I/O（読み書き）パフォーマンスが影響を受けることがあります。

冗長データを維持するには、追加の物理ディスクを使用する必要があります。ディスク数が増えると、ディスク障害の可能性も増加します。I/O パフォーマンスと冗長性に違いがあるため、オペレーティング環境のアプリケーションと保存するデータの性質によっては、ある RAID レベルが他の RAID レベルより適している場合があります。

RAID レベルを選択する場合は、パフォーマンスとコストに関する次の注意事項が適用されます。

- 可用性または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 ボリュームでは、可用性またはフォールトトレランスは冗長データを維持することによって達成できます。冗長データにはミラー（複製データ）とパリティ情報（アルゴリズムを使用したデータの再構成）が含まれています。
- パフォーマンス - 選択する RAID レベルによって、読み取りおよび書き込みパフォーマンスが向上したり低下したりします。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 ボリュームに関連付けられている冗長データまたはパリティ情報を維持するには、追加のディスク容量が必要です。データが一時的なものである、簡単に複製できる、不可欠ではない、といった場合は、データ冗長性のためのコスト増は妥当とは言えません。
- 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られませんが、社内のシステムサポートスタッフの仕事量に影響します。
- ボリューム - ボリュームは、単一ディスクによる非 RAID 仮想ディスクを指します。O-ROM<Ctrl> <r> などの外部ユーティリティを使ってボリュームを作成できます。Storage Management はボリュームの作成をサポートしません。ただし、十分な空き容量がある場合は、ボリュームを表示し、これらのボリュームからドライブを使って新しいボリュームディスクや既存の仮想ディスクの Online Capacity Expansion（OCE）を作成できます。

RAID レベルの選択

RAID を使用して、複数のディスクのデータストレージをコントロールできます。各 RAID レベルまたは連結には、異なるパフォーマンスとデータ保護の特徴があります。

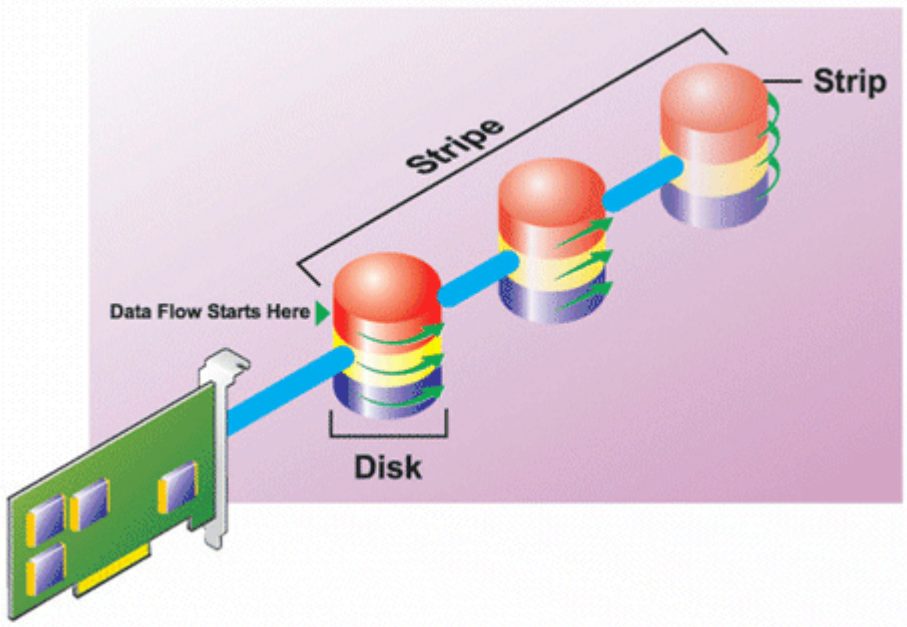
メモ: H3xx PERC コントローラは RAID レベル 6 および 60 をサポートしません。

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（ミラーリング）
- RAID レベル 5（分散パリティを用いたストライピング）
- RAID レベル 6（追加された分散パリティを用いたストライピング）
- RAID レベル 50（RAID 5 セット全体へのストライピング）
- RAID レベル 60（RAID 6 セット全体へのストライピング）
- RAID レベル 10（ミラーセット全体へのストライピング）

RAID レベル 0 - ストライピング

RAID 0 はデータのストライピングを使用します。つまり複数の物理ディスクにわたり同じサイズのセグメントにデータを書き込みます。RAID 0 はデータの冗長性を提供しません。

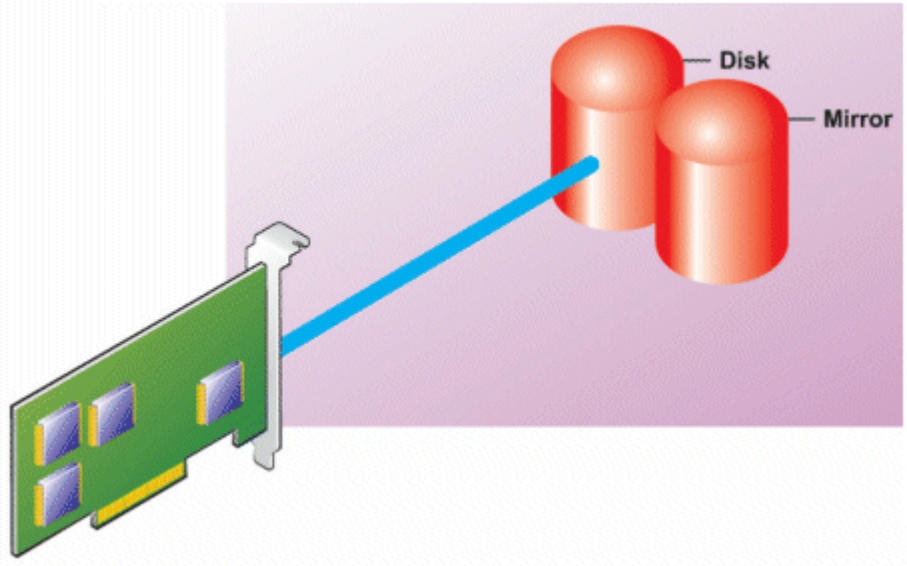


RAID 0 の特徴

- *n* 個のディスクを、(最小ディスクサイズ) * *n* 個分のディスク容量を備えた 1 つの大容量仮想ディスクとしてまとめます。
- データは各ディスクに交互に保存されます。
- 冗長データは保存されません。1 つのディスクに障害が発生すると大容量仮想ディスクにもエラーが発生し、データを再構築する方法はありません。
- 読み書きのパフォーマンスが向上します。

RAID レベル 1 (ミラーリング)

RAID 1 は冗長データを維持する最もシンプルな方式です。RAID 1 では、データは 1 台または複数台の物理ディスクにミラー化 (複製) されます。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。



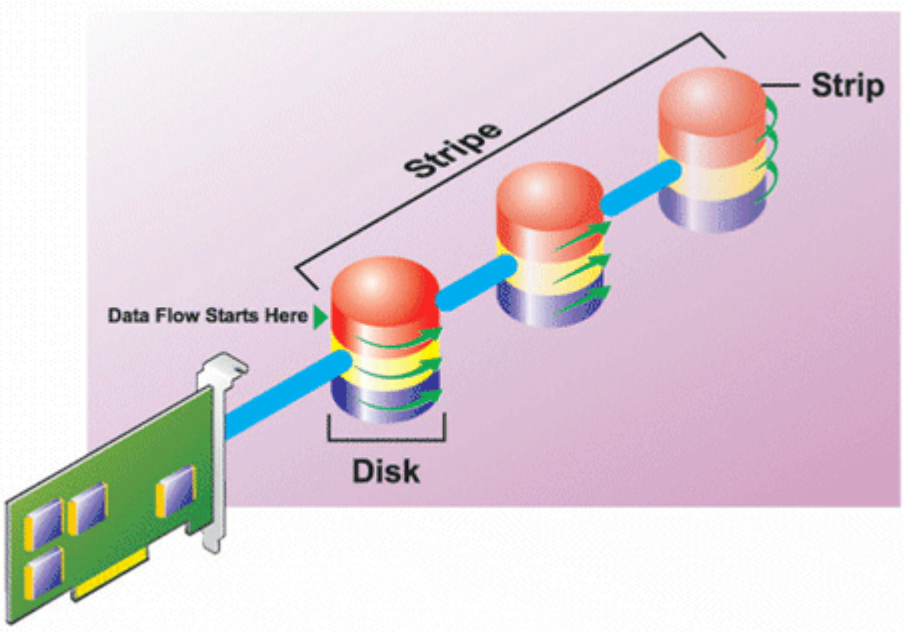
RAID 1 の特徴

- *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化されるため、ストレージの総容量はディスク 1 つ分に等しくなります。
- データは両方のディスクに複製されます。
- いずれかのディスクで障害が起きても、仮想ディスクの動作は中断されません。データは、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のではなく、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。

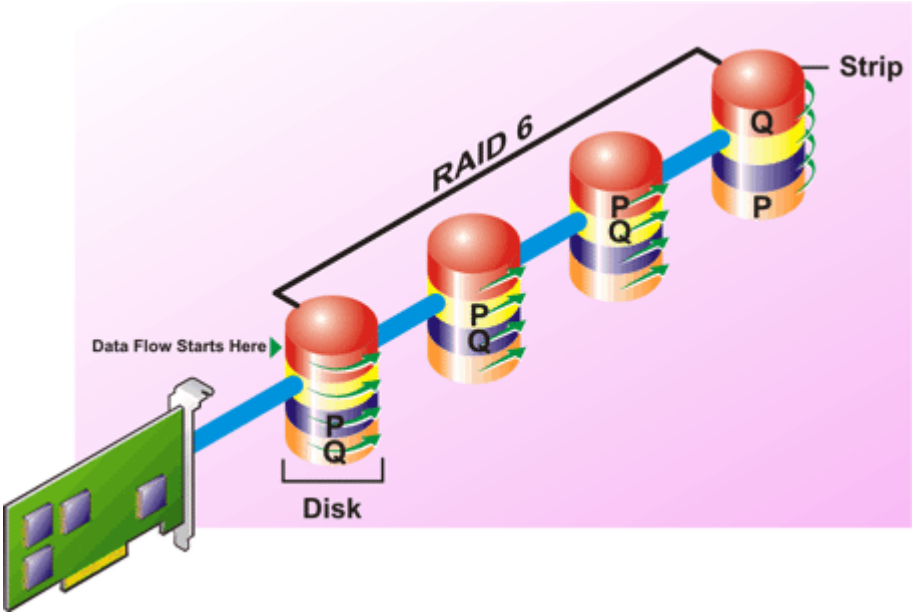


RAID 5 の特徴

- *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。



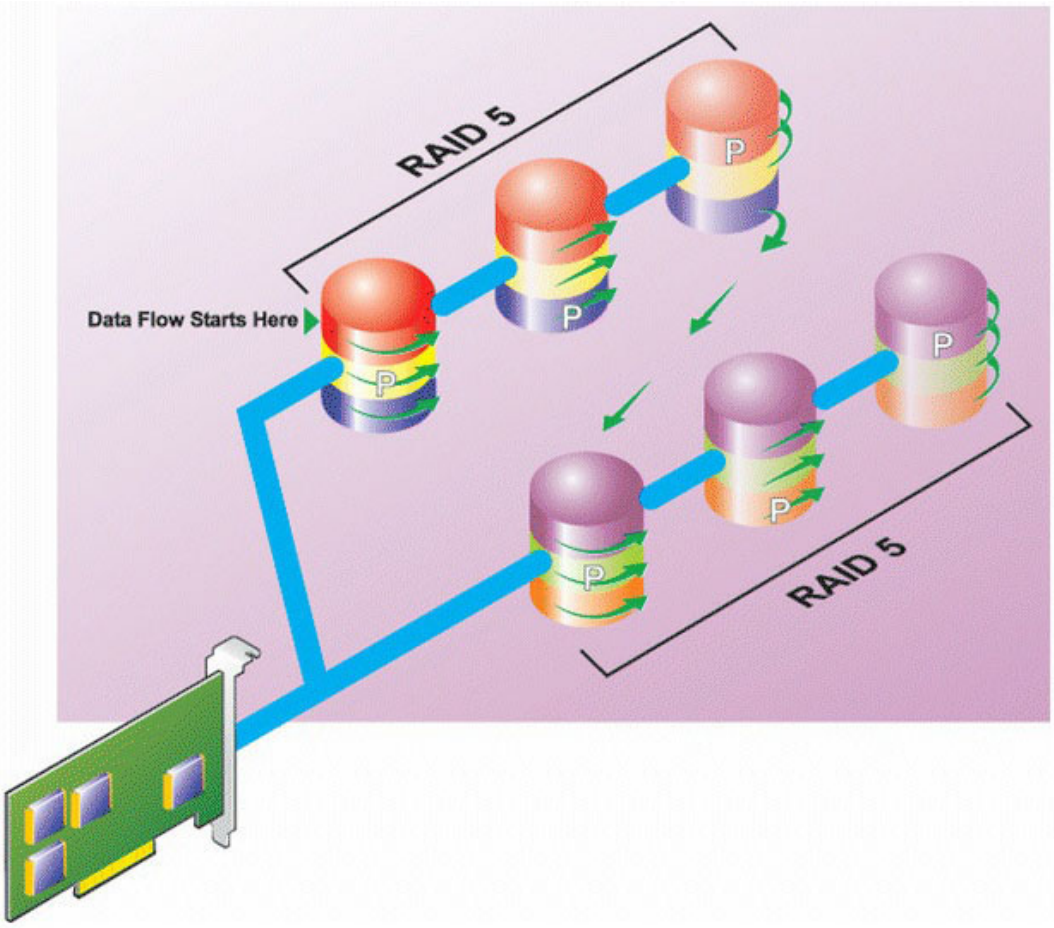
RAID 6 の特徴

- *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。

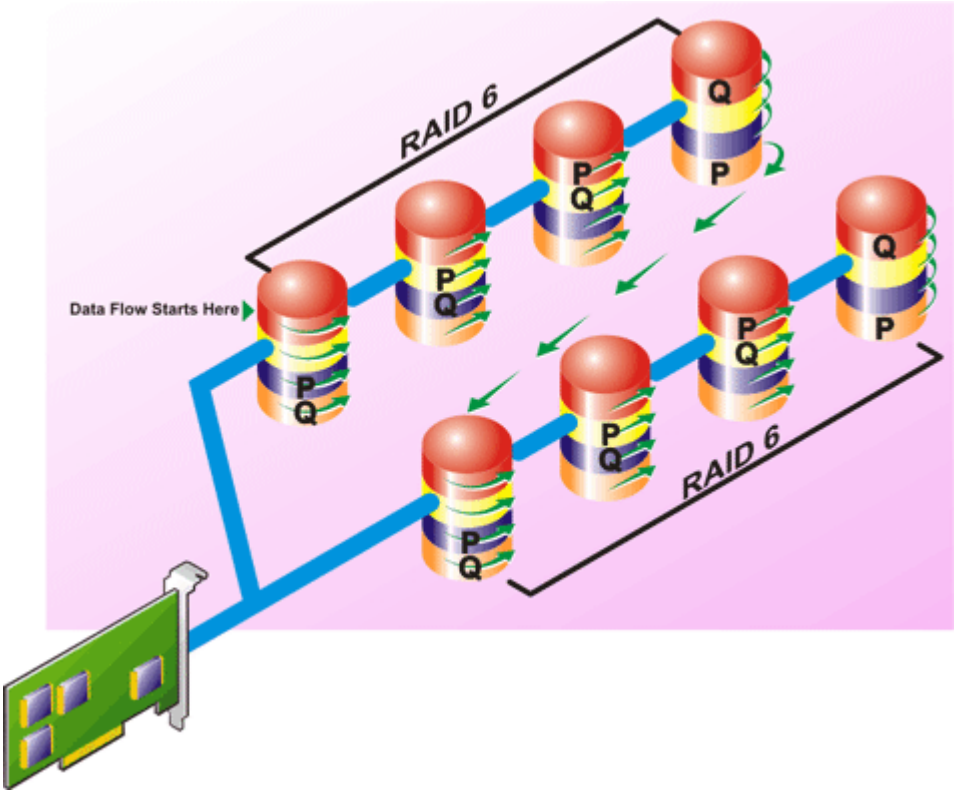


RAID 50 の特徴

- *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が必要です。
- データはすべてのスパンにストライプされます。RAID 50 はディスク容量の点でより高価です。

RAID レベル 60 (RAID 6 セット全体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。

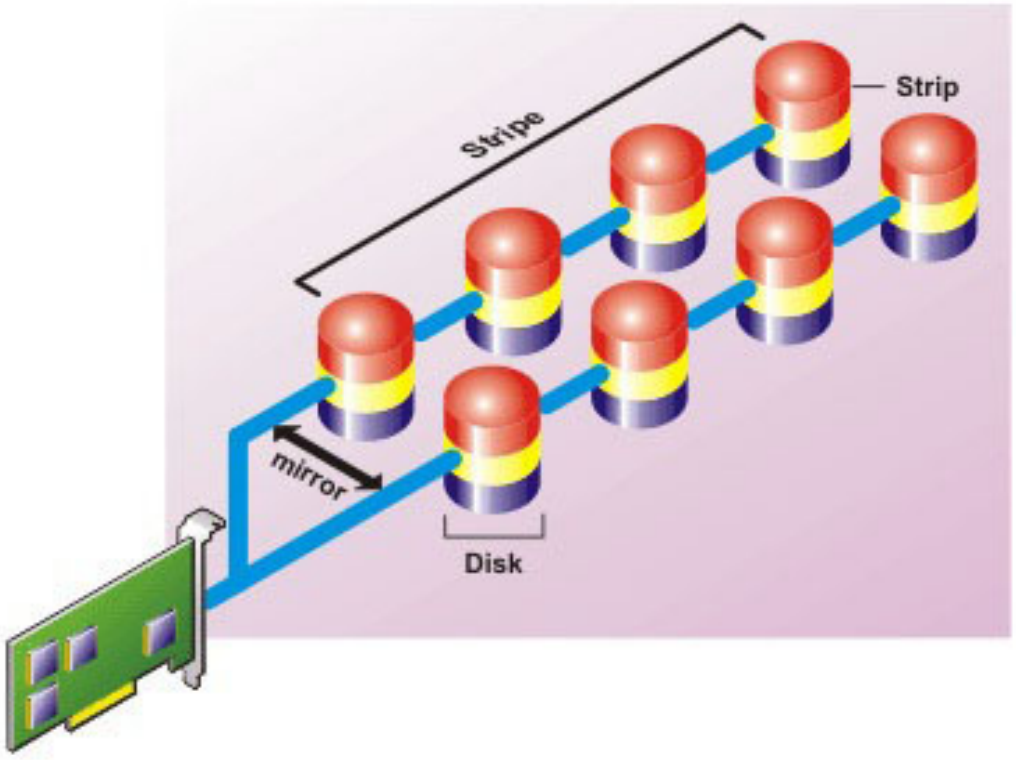


RAID 60 の特徴

- *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 50 よりも優れたデータ保護を提供します。
- RAID 6 と同量に比例するパリティ情報が必要です。
- パリティには、1 スパンあたり 2 つのディスクが必要です。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)

RAB は RAID レベル 10 を RAID レベル 1 の実装とみなします。RAID 10 は物理ディスクのミラーリング (RAID 1) とデータストライピング (RAID 0) の組み合わせです。RAID 10 では、データは複数の物理ディスクに分かれてストライプ化されます。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断されません。データはミラーリングされた障害の発生していないディスク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

RAID レベル	データ冗長性	読み取りパフォーマンス	書き込みパフォーマンス	再構築パフォーマンス	必要な最小ディスク数	使用例
RAID 0	なし	大変良好	大変良好	該当なし	無	非重要データ。
RAID 1	優秀	大変良好	正常	正常	2N (N = 1)	小規模のデータベース、データベースログ、および重要情報。
RAID 5	正常	連続読み取り：良。トランザクション読み取り：大変良好	ライトバックキャッシュを使用しない限り普通	普通	N + 1(N = ディスクが最低限 2 台)	データベース、および読み取り量の多いトランザクションに使用。

表 50. RAID レベルパフォーマンスの比較（続き）

RAID レベル	データ冗長性	読み取りパフォーマンス	書き込みパフォーマンス	再構築パフォーマンス	必要な最小ディスク数	使用例
RAID 10	優秀	大変良好	普通	正常	2N x X	データの多い環境（大きいレコードなど）。
RAID 50	正常	大変良好	普通	普通	N + 2（N = 最低限 4 台）	中規模のトランザクションまたはデータ量が多い場合に使用。
RAID 6	優秀	連続読み取り：良。トランザクション読み取り：大変良好	ライトバックキャッシュを使用しない限り普通	不良	N + 2（N = ディスクが最低限 2 台）	重要な情報。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。
RAID 60	優秀	大変良好	普通	不良	X x (N + 2)（N = 最低限 2 台）	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。
N = 物理ディスク数 X = RAID セットの数						

対応コントローラ

対応 RAID コントローラ

iDRAC インタフェースは次の 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（ブレードサーバ用）
- BOSS-S2 アダプター

iDRAC インターフェイスは次の 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

iDRAC インタフェースは次の 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 インタフェースは次の PERC 9 コントローラをサポートしています。

- PERC 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。

iDRAC は、AMD プラットフォーム用の HBA355i 前面および HBA355i アダプターをサポートしています。

対応エンクロージャ

iDRAC は、MD1400 および MD1420 エンクロージャをサポートしています。

メモ: HBA コントローラに接続されている Redundant Array of Inexpensive Disks (RBODS) はサポートされません。

メモ: PERC H480 (バージョン 10.1 以降) のファームウェアは、ポートあたり最大 4 台のエンクロージャをサポートしています。

ストレージデバイスの対応機能のサマリ

次の表に、iDRAC 経由でストレージデバイスによってサポートされる機能を示します。

表 51. ストレージコントローラによってサポートされる機能

特長	PERC 11			PERC 10			PERC 9				
	H755 前面	H755N 前面	H755 アダプター	H740P ミニ	H740P アダプタ	H840 アダプタ	H330 ミニ	H330 アダプタ	H730P ミニ	H730P アダプタ	FD33xS
グローバルホットスペアとしての物理ディスクの割り当てまたは割り当て解除	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
RAID への変換	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし
RAID / 非 RAID に変換します。	リアルタイム (ドライブを非 RAID ePD-PT ボリュームに変換)	リアルタイム (ドライブを非 RAID ePD-PT ボリュームに変換)	リアルタイム (ドライブを非 RAID ePD-PT ボリュームに変換)	リアルタイム (eHBA コントローラー モードでのみサポートされ、ドライブを非 RAID ePD-PT ボリュームに変換)	リアルタイム (eHBA コントローラー モードでのみサポートされ、ドライブを非 RAID ePD-PT ボリュームに変換)	リアルタイム (eHBA コントローラー モードでのみサポートされ、ドライブを非 RAID ePD-PT ボリュームに変換)	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
再構築	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
再構築のキャンセル	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
仮想ディスクの作成	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム

表 51. ストレージコントローラによってサポートされる機能（続き）

特長	PERC 11			PERC 10			PERC 9				
	H755 前面	H755N 前面	H755 アダプター	H740P ミニ	H740P アダプタ	H840 アダプタ	H330 ミニ	H330 アダプタ	H730P ミニ	H730P アダプタ	FD33xS
仮想ディスクの名前の変更	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
仮想ディスクキャッシュポリシーの編集	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
仮想ディスク整合性チェック	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
整合性チェックのキャンセル	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
仮想ディスクの初期化	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
初期化のキャンセル	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
仮想ディスクの暗号化	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	適用なし	適用なし	リアルタイム	リアルタイム	リアルタイム
専用ホットスペアの割り当てと割り当て解除	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
仮想ディスクの削除	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
バックグラウンドの初期化のキャンセル	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
オンライン容量拡張	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
RAID レベルの移行	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
保存キャッシュの破棄	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	適用なし	適用なし	リアルタイム	リアルタイム	リアルタイム
巡回読み取りモードの設定	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム

表 51. ストレージコントローラによってサポートされる機能（続き）

特長	PERC 11			PERC 10			PERC 9				
	H755 前面	H755N 前面	H755 アダプター	H740P ミニ	H740P アダプタ	H840 アダプタ	H330 ミニ	H330 アダプタ	H730P ミニ	H730P アダプタ	FD33xS
手動巡回読み取りモード	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
未設定領域の巡回読み取り	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム（Web インターフェイスのみ）	リアルタイム（Web インターフェイスのみ）	リアルタイム（Web インターフェイスのみ）	リアルタイム（Web インターフェイスのみ）	リアルタイム（Web インターフェイスのみ）
整合性チェックモード	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
コピーバックモード	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
ロードバランスモード	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
整合性チェック率	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
再構築率	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
BGI 率	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
再構成率	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
外部設定のインポート	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
外部設定の自動インポート	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
外部設定のクリア	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
コントローラ設定のリセット	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
セキュリティキーの作成または変更	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	適用なし	適用なし	リアルタイム	リアルタイム	リアルタイム
Secure Enterprise Key Manager	ステージング	ステージング	ステージング	ステージング	ステージング	ステージング	適用なし	適用なし	適用なし	適用なし	適用なし
PCIe SSD デバイスの	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし

表 51. ストレージコントローラによってサポートされる機能（続き）

特長	PERC 11			PERC 10			PERC 9				
	H755 前面	H755N 前面	H755 アダプター	H740P ミニ	H740P アダプタ	H840 アダプタ	H330 ミニ	H330 アダプタ	H730P ミニ	H730P アダプタ	FD33xS
インベントリとリモートでの正常性の監視											
PCIe SSD を取り外す準備。	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし
PCIe SSD のデータを安全に消去	適用なし	リアルタイム	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし
バックプレーンモードの設定（分割／統合）。	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
コンポーネント LED の点滅または点滅解除	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム	リアルタイム
コントローラモードの切り替え	適用なし	適用なし	適用なし	ステージング	ステージング	ステージング	ステージング	ステージング	ステージング	ステージング	ステージング
仮想ディスクの T10PI サポート	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし	適用なし

メモ: 次のサポートを追加

- 非 RAID ディスクへの変換をサポートする PERC 10.2 以降のファームウェア用の eHBA モード
- コントローラーの HBA モードへの切り替え
- RAID 10 不均等スパン

表 52. MX プラットフォーム向けストレージ コントローラーの対応機能

機能	PERC 11	PERC 10	PERC 9
	H755 MX	H745P MX	H730P MX
仮想ディスクの初期化	リアルタイム	リアルタイム	リアルタイム
初期化のキャンセル	リアルタイム	リアルタイム	リアルタイム
仮想ディスクの暗号化	リアルタイム	リアルタイム	リアルタイム
専用ホットスペアの割り当てと割り当て解除	リアルタイム	リアルタイム	リアルタイム
仮想ディスクの削除	リアルタイム	リアルタイム	リアルタイム

表 52. MX プラットフォーム向けストレージ コントローラーの対応機能 (続き)

機能	PERC 11	PERC 10	PERC 9
	H755 MX	H745P MX	H730P MX
バックグラウンドの初期化のキャンセル	リアルタイム	リアルタイム	リアルタイム
オンライン容量拡張	リアルタイム	リアルタイム	リアルタイム
RAID レベルの移行	リアルタイム	リアルタイム	リアルタイム
保存キャッシュの破棄	リアルタイム	リアルタイム	リアルタイム
巡回読み取りモードの設定	リアルタイム	リアルタイム	リアルタイム
手動巡回読み取りモード	リアルタイム	リアルタイム	リアルタイム
未設定領域の巡回読み取り	リアルタイム	リアルタイム	リアルタイム(Web インターフェイスのみ)
整合性チェックモード	リアルタイム	リアルタイム	リアルタイム
コピーバックモード	リアルタイム	リアルタイム	リアルタイム
ロードバランスモード	リアルタイム	リアルタイム	リアルタイム
整合性チェック率	リアルタイム	リアルタイム	リアルタイム
再構築率	リアルタイム	リアルタイム	リアルタイム
BGI 率	リアルタイム	リアルタイム	リアルタイム
再構成率	リアルタイム	リアルタイム	リアルタイム
外部設定のインポート	リアルタイム	リアルタイム	リアルタイム
外部設定の自動インポート	リアルタイム	リアルタイム	リアルタイム
外部設定のクリア	リアルタイム	リアルタイム	リアルタイム
コントローラー設定のリセット	リアルタイム	リアルタイム	リアルタイム
セキュリティキーの作成または変更	リアルタイム	リアルタイム	リアルタイム
PCIe SSD デバイスのインベントリとリモートでの正常性の監視	リアルタイム	適用なし	適用なし
PCIe SSD を取り外す準備。	適用なし	適用なし	適用なし
PCIe SSD のデータを安全に消去	リアルタイム	適用なし	適用なし
バックプレーン モードの設定 (分割/統合)	リアルタイム	適用なし	適用なし
コンポーネント LED の点滅または点滅解除	リアルタイム	リアルタイム	リアルタイム
コントローラー モードの切り替え	適用なし	適用なし	ステージング
仮想ディスクの T10PI サポート	適用なし	適用なし	適用なし

メモ: H745P MX は、PERC 10.2 以降の eHBA モードをサポートします。

表 53. ストレージデバイスによってサポートされる機能

特長	PCIe SSD	BOSS S1	BOSS S2
仮想ディスクの作成	適用なし	ステージング	ステージング

表 53. ストレージデバイスによってサポートされる機能（続き）

特長	PCIe SSD	BOSS S1	BOSS S2
コントローラー設定のリセット	適用なし	ステージング	ステージング
高速初期化	適用なし	ステージング	ステージング
仮想ディスクの削除	適用なし	ステージング	ステージング
完全初期化	適用なし	適用なし	適用なし
PCIe SSD デバイスのインベントリとリモートでの正常性の監視	リアルタイム	適用なし	適用なし
PCIe SSD を取り外す準備。	リアルタイム	適用なし	適用なし
PCIe SSD のデータを安全に消去	ステージング	適用なし	適用なし
コンポーネント LED の点滅または点滅解除	リアルタイム	適用なし	リアルタイム
ドライブのホット プラグ	適用なし	適用なし	リアルタイム

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 トラップは、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間にシステムにエンクロージャビューの WSMan コマンドを列挙すると、エンクロージャビューのプライマリステータスは、**警告** ではなく **正常** として表示されます。

メモ: ストレージ正常性ロールアップは、Dell EMC OpenManage 製品と同じ規則に従います。詳細については、https://www.dell.com/openmanagemanuals から入手可能な『*OpenManage サーバー管理者ユーザーズガイド*』を参照してください。

メモ: バックプレーンが複数あるシステムでは、物理ディスクが別のバックプレーンに表示されることがあります。点滅機能を使用して、ディスクを識別してください。

Web インターフェイスを使用したストレージ デバイスの監視

Web インターフェイ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**の順に移動して、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** > **概要** > **コントローラー**の順に移動して、RAID コントローラー情報を表示します。**コントローラー**ページが表示されます。
- **ストレージ** > **概要** > **物理ディスク**の順に移動して、物理ディスク情報を表示します。**物理ディスク**ページが表示されます。
- **ストレージ** > **概要** > **仮想ディスク**の順に移動して、仮想ディスク情報を表示します。**仮想ディスク**ページが表示されます。
- **ストレージ** > **概要** > **エンクロージャ**の順に移動して、エンクロージャ情報を表示します。**エンクロージャ**ページが表示されます。

フィルタを使用して、特定のデバイス情報を表示することもできます。

メモ: システムに CEM サポート付きストレージデバイスがない場合、ストレージハードウェアのリストは表示されません。

メモ: SWRAID コントローラーの背後にある NVMe SSD が RAID モードの場合、Web インターフェイスでは、エンクロージャ ページに NVMe SSD のスロット情報が表示されません。詳細については、物理ディスクのページを参照してください。

メモ: Dell 認定されていない、またはサード パーティー製の NVMe デバイスの動作は、iDRAC で一貫していない可能性があります。

メモ: バックプレーンスロットの NVMe SSD が NVMe-MI コマンドをサポートし、バックプレーンスロットへの I2C 接続が正常な場合は、iDRAC は NVMe SSD を検出し、対応するバックプレーンスロットへの PCI 接続に関係なくインタフェースに表示します。

表示されたプロパティの詳細と、フィルタオプションの使用法については、『iDRAC オンラインヘルプ』を参照してください。

RACADM を使用したストレージデバイスの監視

ストレージデバイス情報を表示するには、`storage` コマンドを使用します。

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

iDRAC 設定ユーティリティを使用したバックプレーンの監視

iDRAC 設定 ユーティリティで、**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の表示

主要ストレージコンポーネントの階層型物理コンテインメントビューを表示できます。つまり、コントローラ、コントローラに接続されているエンクロージャ、および各エンクロージャに収容されている物理ディスクへのリンクが一覧表示されます。コントローラに直接接続されている物理ディスクも表示されます。

ストレージデバイスのトポロジを表示するには、**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、次のことを実行できます。

- 物理ディスクプロパティの表示
- グローバルホットスペアとしての物理ディスクの割り当てまたは割り当て解除
- RAID 対応ディスクへの変換
- 非 RAID ディスクへの変換
- LED の点滅または点滅解除
- 物理ディスクの再構成
- 物理ディスクの再構成のキャンセル
- 暗号的消去

グローバルホットスペアとしての物理ディスクの割り当てまたは割り当て解除

グローバルホットスペアは、ディスクグループの一部になっている未使用のバックアップディスクです。ホットスペアはスタンバイモードになります。仮想ディスクで使用されている物理ディスクに障害が発生すると、割り当てられたホットスペアが有効になり、システムに割り込みされたり介入要求されることなく、故障した物理ディスクと置換されます。ホットスペアが有効になると、故障した物理ディスクを使用していたすべての冗長仮想ディスクのデータが再構築されます。

メモ: iDRAC v3.00.00.00 以降からは、仮想ディスクが作成されていないときにグローバル ホット スペアを追加することができます。

ホットスペアの割り当ては、ディスクの割り当てを解除し、必要に応じて別のディスクを割り当てることで変更できます。複数の物理ディスクをグローバルホットスペアとして割り当てることができます。

グローバルホットスペアの割り当てと割り当て解除は手動で行う必要があります。グローバルホットスペアは特定の仮想ディスクには割り当てられません。仮想ディスクにホットスペアを割り当てる（仮想ディスクでエラーが発生する物理ディスクの代替）場合は、「専用ホットスペアの割り当てまたは割り当て解除」を参照してください。

仮想ディスクを削除する場合、コントローラに関連する最後の仮想ディスクが削除されると、割り当てられたグローバルホットスペアがすべて自動的に割り当て解除される可能性があります。

設定をリセットすると、仮想ディスクが削除され、すべてのホットスペアの割り当てが解除されます。

ホットスペアに関連したサイズ要件とその他の考慮事項を把握しておいてください。

物理ディスクをグローバルホットスペアとして割り当てる前に、次のことを行います。

- Lifecycle Controller が有効になっていることを確認します。
- 準備完了状態のディスクドライブがない場合は、追加ディスクドライブを挿入し、そのドライブが準備完了状態であることを確認してください。
- 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。

  メモ: POST 中に、F2 キーを押して、セットアップユーティリティまたはデバイスセットアップを起動します。PERC 10 では、Ctrl+R オプションはサポートされなくなりました。Ctrl+R は、起動モードが BIOS に設定されている場合にのみ、PERC 9 で動作します。

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、保留操作は作成されますが、ジョブは作成されません。その後、同じディスク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。

保留操作への追加モードで物理ディスクのグローバルホットスペアとしての割り当てを解除した場合は、保留操作は作成されますが、ジョブは作成されません。その後、同じディスクをグローバルホットスペアとして割り当てると、グローバルホットスペアの割り当て解除保留操作はクリアされます。

最後の VD が削除されると、グローバルホットスペアも準備完了状態に戻ります。

PD がすでにグローバルホットスペアになっている場合、ユーザーは、グローバルホットスペアとして再度割り当てることができます。

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。
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。

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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』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で使用されます。

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サポートされています。

物理ディスクドライブは、次の手順を実行することによって RAID または非 RAID モードに変換することができます。

- iDRAC Web インターフェイス、RACADM、Redfish、WSMan などの iDRAC インターフェイスを使用する。
- サーバの再起動中に <Ctrl+R> キーを押し、必要なコントローラを選択する。

メモ: PERC コントローラに接続されている物理ドライブが非 RAID モードの場合、iDRAC GUI、RACADM、Redfish、WSMan などの iDRAC インタフェースに表示されるディスクのサイズは、実際のディスクサイズよりわずかに小さい場合があります。ただし、ディスクの全容量を使用してオペレーティングシステムを導入できます。

メモ:

- PERC H330 のホット プラグ ディスクは、常に非 RAID モードになっています。他の RAID コントローラでは、これらは常に RAID モードになります。
- PERC 11 のホット プラグ対応ディスクは、現在の自動設定動作の設定によって、準備完了または EPD PT のいずれかです。

iDRAC Web インターフェイスを使用した物理ディスクの RAID 対応または非 RAID モードへの変換

物理ディスクを RAID モードまたは非 RAID モードに変換するには、次の手順を実行します。

1. iDRAC Web インターフェイスで、**ストレージ** > **概要** > **物理ディスク** の順にクリックします。
2. **フィルター オプション** をクリックします。**すべてのフィルターのクリア** と **詳細フィルター** の 2 つのオプションが表示されます。**詳細フィルター** オプションをクリックします。
   さまざまなパラメーターを構成できる詳細なリストが表示されます。
3. **グループ化** ドロップダウン メニューから、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に関連付けられたパラメーターが表示されます。
4. 目的のパラメーターをすべて選択したら、**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

RAID モードに変換するか、または非 RAID モードに変更するかに応じて、次の RACADM コマンドを使用します。

- RAID モードに変換するには、`racadm storage converttoraid` コマンドを使用します。
- 非 RAID モードに変換するには、`racadm storage converttononraid` コマンドを使用します。

メモ: S140 コントローラでは、RACADM インタフェースのみを使用して、ドライブを非 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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』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。

メモ: システム消去は、サーバー内のドライブにのみ適用されます。iDRAC では、JBOD などの外部エンクロージャ内のドライブを消去することはできません。

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、これは 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。

```
# racadm storage get pdisks -o -p SystemEraseCapability
```

メモ: サーバー上で SEKM が有効にされている場合は、このコマンドを使用する前に `racadm sekm disable` コマンドを使用して SEKM を無効にします。このコマンドを実行して iDRAC から SEKM 設定が消去された場合、iDRAC によって保護されているストレージ デバイスがロック アウトされるのを防ぐことができます。

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。

```
# 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。

```
# 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、https://www.dell.com/idracmanuals から入手可能な『*Lifecycle Controller ユーザーズ ガイド*』を参照してください。

SED/ISE デバイス データの消去

メモ: サポートされているデバイスが仮想ディスクの一部である場合、この操作はサポートされません。デバイスを消去する前に、ターゲットのサポート対象デバイスが仮想ディスクから取り外されている必要があります。

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/ISE 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、サポートされているデバイス上の全データが完全に失われます。暗号消去の実行中、ホストはサポートされているデバイスにアクセスできません。SED/ISE デバイスの消去は、リアル タイムで実行するか、システムの再起動後に適用することができます。

暗号消去を実行中にシステムを再起動したり停電になったりすると、暗号消去はキャンセルされます。システムを再起動し、処理を再起動する必要があります。

SED/ISE デバイス データを消去する前に、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。
- 選択中のサポート対象ドライブは仮想ディスクの一部ではありません。

メモ:

- SED/ISE 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。

- ドライブが消去された後も、データ キャッシュにより OS 内にアクティブとして表示される場合があります。この場合は、OS を再起動すると、消去されたドライブは表示されなくなり、データも報告されなくなります。
- 暗号消去機能は、PowerEdge サーバー向けの SED/ISE でサポートされています。

Web インターフェイスを使用した SED/ISE デバイス データの消去

対応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 Web インターフェイスで、**[概要]** > **[ストレージ]** > **[物理ディスク]** の順に移動します。
   [物理ディスク] 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、コントローラーを選択して関連するデバイスを表示します。
3. ドロップダウン メニューから、1 つまたは複数の SED/ISE に対する **[暗号消去]** を選択します。
   [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、**[処置]** を選択してドロップダウン メニューをクリックし、その他のオプションを表示します。
4. **操作モードの適用** ドロップダウンメニューから、次のいずれかのオプションを選択します。
   - **[今すぐ適用]** - このオプションを選択すると、アクションを直ちに適用します。システムの再起動は必要がありません。
   - **次回の再起動時** - このオプションを選択して、次回のシステム再起動時に処置を適用します。
   - **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ると、選択されたコントローラーにジョブ ID が作成されたことを示すメッセージが表示されます。**ジョブキュー** をクリックすると、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かった場合は、エラー メッセージが表示されます。保留中の操作が正常に実行され、ジョブの作成に失敗した場合は、エラー メッセージが表示されます。

RACADM を使用した 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。

```
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。

```
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。

```
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。

```
racadm jobqueue view -i <job ID>
```

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

物理ディスクの再構成

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。

Cancel Rebuild (再構築のキャンセル) を使用すると、進行中の再構成をキャンセルできます。再構築をキャンセルすると、仮想ディスクが劣化した状態のままになります。追加の物理ディスクが故障すると、仮想ディスクで障害が発生し、データが失われる可能性があります。故障した物理ディスクの再構築は、極力早めに実行するよう推奨します。

ホットスペアとして割り当てられた物理ディスクの再構築をキャンセルする場合は、データを復元するため、同じ物理ディスクで再構築を再開します。物理ディスクの再構築をキャンセルしてから別の物理ディスクをホットスペアとして割り当てても、ホットスペアにデータの再構築が新しく割り当てられることにはなりません。

仮想ディスクの管理

仮想ディスクに対して次の操作を実行できます。

- 作成
- 削除
- ポリシーの編集
- 初期化
- 整合性チェック
- 整合性チェックのキャンセル
- 仮想ディスクの暗号化
- 専用ホットスペアの割り当てまたは割り当て解除
- 仮想ディスクの点滅および点滅解除
- バックグラウンドの初期化のキャンセル
- オンライン容量拡張
- 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。

メモ: PERC 10 は、デイジーチェーン配置をサポートしていないため、カウントがより少なくなっています。

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 つまたは複数の物理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。
- ジョブが現在実行している場合、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。このジョブが完了するまで待つか、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 Web インターフェイス、RACADM、Redfish、WSMan などの iDRAC インターフェイスを使用するか、<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: 保留中の操作に追加 モードで仮想ディスクを作成し、ジョブが作成されない場合、またその後に仮想ディスクを削除した場合は、仮想ディスクに対する保留中の作成操作がクリアされます。

メモ: PERC H330 では RAID 6 および RAID 60 はサポートされません。

メモ: BOSS コントローラでは、M.2 物理ストレージメディアのフルサイズと同じサイズの仮想ディスクのみを作成できます。サーバ設定プロファイルを使用して BOSS 仮想ディスクを作成する場合は、仮想ディスクのサイズをゼロに設定してください。RACADM や WSMan、Redfish などの他のインターフェイスでは、仮想ディスクのサイズは指定できません。

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、次を考慮します。

- コントローラー上に保存されない仮想ディスク名 — 作成する仮想ディスクの名前は、コントローラー上に保存されません。このため、別のオペレーティング システムを使って再起動した場合、新しいオペレーティング システムが独自の命名規則を使って仮想ディスク名を変更することがあります。
- ディスク グループとは、1 つまたは複数の仮想ディスクが作成される RAID コントローラーに接続されたディスクを論理的にグループ化したものです。その際、ディスク グループのすべての仮想ディスクは、ディスク グループのすべての物理ディスクを使用します。現在の実装では、論理デバイス作成の際に、混在したディスクグループのブロックがサポートされています。
- 物理ディスクはディスク グループにまとめられています。したがって、1 つのディスク グループに 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ーによって異なります。仮想ディスクの作成で、コントローラーは一定数のストライプとスパン (物理ディスク上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には制限があるため、使用可能な物理ディスクの数も制限されます。ストライプとスパンの制限により、RAID レベルは次のような影響を受けます。
  - 最大スパン数は、RAID 10 、RAID 50、および RAID 60 に影響します。
  - 最大ストライプ数は、RAID 0、RAID 5、RAID 50、RAID 6 および RAID 60 に影響します。
  - 1 つのミラー内の物理ディスク数は常に 2 です。これは RAID 1 および RAID 10 に影響します。

  メモ:
  - RAID 1 は、BOSS コントローラーでのみサポートされています。
  - SWRAID コントローラーは、RAID 0、1、5、10 のみをサポートします。
- PCIe SSD 上で仮想ディスクを作成できません。ただし、PERC 11 以降のコントローラーでは、PCIe SSD を使用した仮想ディスクの作成がサポートされています。

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** フィールドに、仮想ディスクのサイズを入力します。
      ディスクを選択すると、最大サイズが表示され、更新されます。
   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できません。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、RAID 10、RAID 50、および RAID 60 に適用されます。RAID 10 選択時にコントローラーが不均等 RAID 10 をサポートしている場合、スパン数の値は表示されません。コントローラーによって、適切な値が自動的に設定されます。RAID 50 および RAID 60 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。より多数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。

メモ: ディスク名には、英数字、スペース、ダッシュ、アンダースコアを使用できます。

その他の特殊文字を入力しても、仮想ディスクの作成時に、それらはすべて削除され、スペースに置き換えられます。

RACADM を使用した仮想ディスクの作成

`racadm storage createvd` コマンドを使用します。

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

メモ: S140 コントローラで管理しているドライブでは、ディスクのスライスやパーシャル VD の設定に RACADM を使用することができません。

仮想ディスクキャッシュポリシーの編集

仮想ディスクの読み取り、書き込み、またはディスクキャッシュポリシーを変更することができます。

メモ: コントローラによって、サポートされない読み取りまたは書き込みポリシーがあります。そのため、ポリシーを適用すると、エラーメッセージが表示されます。

読み取りポリシーは、コントローラがデータを探すときに、仮想ディスクの連続セクタを読み取るかどうかを指定します。

- **適応先読み** — 2 件の最新読み取り要求がディスクの連続セクタにアクセスした場合にのみ、コントローラは先読みを開始します。後続の読み取り要求がディスクのランダムセクタにアクセスする場合、コントローラは先読みなしのポリシーに戻ります。コントローラは読み取り要求がディスクの連続セクタにアクセスしているかを引き続き評価し、必要に応じて先読みを開始します。
- **先読み** — コントローラはデータシーク時に仮想ディスクの連続セクタを読み取ります。データが仮想ディスクの連続セクタに書かれている場合、先読みポリシーによってシステムパフォーマンスが向上します。
- **先読みなし** — 先読みなしポリシーを選択すると、コントローラは先読みポリシーを使用しません。

書き込みポリシーは、コントローラが書き込み要求完了信号を、データがキャッシュに保存された後、またはディスクに書き込まれた後のどちらの時点で送信するかを指定します。

- **ライトスルー** — コントローラはデータがディスクに書き込まれた後でのみ書き込み要求完了信号を送信します。ライトスルーキャッシュは、ディスクドライブにデータが無事に書き込まれた後にのみデータが利用可能になるとシステムが判断することから、ライトバックキャッシュよりも優れたデータセキュリティを提供します。
- **ライトバック** — コントローラは、データがコントローラのキャッシュに保存されたがディスクには書き込まれていない時点で、書き込み要求完了信号を送信します。ライトバックキャッシュは、後続の読み取り要求が、ディスクと比べてキャッシュからより素早くデータを取得できるため、パフォーマンスが向上します。ただし、ディスクへのデータ書き込みを阻むシステム障害の発生時に、データ損失が生じる可能性があります。他のアプリケーションでも、データがディスクにあると、処置により想定されたときに、問題が発生する可能性があります。
- **ライトバックの強制** — コントローラにバッテリが搭載されているかどうかに関係なく、書き込みキャッシュが有効になります。コントローラにバッテリが搭載されていない場合、強制ライトバックキャッシングが使用されると、電源障害時にデータの損失が発生する可能性があります。

ディスクキャッシュポリシーは、特定の仮想ディスクでの読み取りに適用されます。この設定は先読みポリシーには影響しません。

メモ:

- コントローラキャッシュのコントローラ不揮発性キャッシュおよびバッテリバックアップは、コントローラがサポートできる読み取りポリシーまたは書き込みポリシーに影響します。すべての PERC にバッテリとキャッシュが搭載されているとは限りません。
- 先読みおよびライトバックにはキャッシュが必要になります。つまり、コントローラにキャッシュがない場合は、ポリシーの値を設定することはできません。

  同様に、PERC にキャッシュがあってもバッテリがなく、ポリシーがキャッシュへのアクセスを必要とする設定になっている場合、ベースの電源がオフになるとデータロスが生じる恐れがあります。そのため、一部の PERC ではこのポリシーは許可されません。

  したがって、PERC に応じてポリシーの値が設定されます。

仮想ディスクの削除

仮想ディスクを削除すると、仮想ディスクに常駐するファイルシステムおよびボリュームなどの情報がすべて破壊され、コントローラの設定からその仮想ディスクが削除されます。仮想ディスクを削除する場合、コントローラに関連する最後の仮想ディスクが削除されると、割り当てられたグローバルホットスペアがすべて自動的に割り当て解除される可能性があります。ディスクグループの最後の仮想ディスクを削除すると、割り当てられている専用ホットスペアすべてが自動的にグローバルホットスペアになります。

グローバルホットスペアの仮想ディスクをすべて削除すると、そのグローバルホットスペアは自動的に削除されます。

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。

この操作が許可されている場合、起動用仮想ドライブを削除できます。この操作はサイドバンドから実行されるため、オペレーティングシステムには依存しません。そのため、仮想ドライブを削除する前に警告メッセージが表示されます。

仮想ディスクを削除した直後に、削除したディスクと特性がすべて同じ新規仮想ディスクを作成した場合、コントローラは最初の仮想ディスクが全く削除されなかったかのようにデータを認識します。この状況では、新しい仮想ディスクを再作成した後に古いデータが必要ない場合は、仮想ディスクを再初期化します。

仮想ディスク整合性のチェック

この操作は、冗長 (パリティ) 情報の正確性を検証します。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 インターフェイスまたは 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。

仮想ディスクの整合性をチェックするには、ログインおよびサーバー制御の権限を持っている必要があります。

メモ: 整合性チェックは、RAID0 モードでドライバをセットアップしている場合はサポートされません。

メモ: 整合性チェック操作が進行中でないときに、整合性のキャンセル操作を実行すると、整合性チェックのキャンセルではなく、GUI の保留操作が BGI のキャンセルとして表示されます。

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。

メモ: 既存の構成を再作成している時に仮想ディスクの初期化を行わないでください。

高速初期化または完全初期化を実行することも、初期化操作をキャンセルすることもできます。

メモ: 初期化のキャンセルは、リアルタイムの操作です。RACADM は使用せず、iDRAC ウェブインタフェースのみを使用して、初期化をキャンセルできます。

高速初期化

高速初期化操作で、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にのみ実行してください。高速初期化は完了までにあまり時間がかかりません (通常は 30 ~ 60 秒)。

注意: 高速初期化の実行中は既存のデータにアクセスできなくなります。

高速初期化タスクは物理ディスク上のディスクブロックにゼロを書き込みません。これは、高速初期化タスクが書き込み操作を実行しないためであり、これでディスクの劣化が少なくなります。

仮想ディスクの高速初期化では、仮想ディスクの最初と最後の 8 MB が上書きされ、ブートレコードすべてまたはパーティション情報がクリアされます。操作完了にかかるのは 2~3 秒で、仮想ディスク再作成時に推奨されます。

バックグラウンド初期化は高速初期化の完了 5 分後に開始されます。

完全または低速初期化

完全初期化（低速初期化）で、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。完全初期化は仮想ディスクの作成後に実行することができます。高速初期化操作と比較して、物理ディスクに問題がある場合、または不良ディスクブロックがあると思われる場合は完全初期化の使用が必要になることがあります。完全初期化操作は、不良ブロックを再マップし、すべてのディスクブロックにゼロを書き込みます。

仮想ディスクの完全初期化を実行した場合、バックグラウンド初期化は必要ありません。完全初期化中、ホストは仮想ディスクにアクセスできません。完全初期化中にシステムを再起動すると、操作は中止され、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。

以前にデータが保存されていたドライブには、完全初期化を実行することが常に推奨されます。完全初期化には、1GB あたり 1 ~ 2 分かかる場合があります。初期化の速度は、コントローラのモデル、ハードドライブの速度、およびファームウェアのバージョンによって異なります。

完全初期化タスクは 1 度に 1 台ずつ物理ディスクを初期化します。

メモ: 完全初期化は、リアルタイムでのみサポートされます。完全初期化をサポートするコントローラはごく一部です。

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を SED ドライブ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す。VD が OMSA から作成された場合にのみ、自動的に暗号化されます。

専用ホットスペアの割り当てまたは割り当て解除

専用ホットスペアは、仮想ディスクに割り当てられた未使用のバックアップディスクです。仮想ディスク内の物理ディスクが故障すると、ホットスペアがアクティブ化されて故障した物理ディスクと交換されるため、システムが中断したり、ユーザー介入が必要になることもありません。

この操作を実行するには、ログインおよびサーバー制御の権限を持っている必要があります。

4K ドライブのみを 4K 仮想ディスクにホットスペアとして割り当てることができます。

Add to Pending Operation（保留中の操作に追加）モードで物理ディスクを専用ホットスペアとして割り当てた場合、保留中操作が作成されますが、ジョブは作成されません。その後で専用ホットスペアの割り当てを解除しようとすると、専用ホットスペアを割り当てる保留中操作がクリアされます。

Add to Pending Operation（保留中の操作に追加）モードで物理ディスクを専用ホットスペアとしての割り当てから解除した場合、保留中操作が作成されますが、ジョブは作成されません。その後で専用ホットスペアの割り当てを行おうとすると、専用ホットスペアの割り当てを解除する保留中操作がクリアされます。

メモ: ログエクスポート操作の進行中は、**Manage Virtual Disks（仮想ディスクの管理）**ページで専用ホットスペアに関する情報を表示することができません。ログエクスポート操作の完了後、**Manage Virtual Disks（仮想ディスクの管理）**ページを再ロードまたは更新して情報を表示します。

VD の名前変更

仮想ディスクの名前の変更には、システム制御権限が必要です。仮想ディスクの名前には英数字、スペース、ダッシュ、およびアンダースコアのみを使用できます。最大文字数はコントローラによって異なります。多くの場合、最大文字数は 15 文字です。仮想ディスク名の始めと終わりにスペースを使用することはできません。仮想ディスクの名前を変更するたびに、LC ログが作成されます。

ディスク容量の編集

Online Capacity Expansion (オンライン容量拡張)(OCE) 機能によって、システムをオンラインにしたままで、選択した RAID レベルのストレージ容量を増やすことができます。コントローラは、各 RAID アレイの末端に使用可能な新たな容量を設け、アレイ上にデータを再配布します (再構成と呼ばれます)。

Online Capacity Expansion (オンライン容量拡張)(OCE) は、次の 2 通りの方法で行うことができます。

- 仮想ディスクの LBA を開始後に、仮想ディスクグループの最小の物理ドライブ上の空き容量が使用可能な場合は、仮想ディスクの容量はその空き容量の範囲内で拡張可能です。このオプションにより、新たに増加した仮想ディスクのサイズを入力できるようになります。LBA の開始前にのみ使用可能な空き容量が、仮想ディスク内のディスクグループにある場合は、物理ドライブに使用可能な容量があっても、同一のディスクグループ内での Edit Disk Capacity (ディスク容量の編集) は許可されません。
- 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ループ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 にパーセンテージで伝達されます (このパーセンテージは、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)。このパーセンテージロジックのため、再設定完了後の最終 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は、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 (パーセンテージは 100% 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 サイズに違いは見られません。

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

ソース VD レイアウト	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	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
R0 (単一ディスク)	R1	該当なし
R0	R5/R6	該当なし
R1	R0/R5/R6	R0
R5	R0/R6	R0
R6	R0/R5	R0/R5

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

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)	VD 側から (OCE/RLM 経由で機能)	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	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
設定のリセット	削除	点滅	削除
ログのエクスポート	点滅	点滅解除	点滅

表 55. 許可される操作（続き）

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）	VD 側から（OCE/RLM 経由で機能）	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	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
巡回読み取りモードの設定	点滅解除	グローバル ホット スペアの割り当て	点滅解除
巡回読み取りの開始		非 RAID ディスクへの変換	名前の変更
コントローラプロパティの変更			ポリシーの変更
物理ディスク電源の管理			低速初期化
RAID 対応ディスクへの変換			高速初期化
非 RAID ディスクへの変換			メンバー ディスクの交換
コントローラー モードの変更			

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 つのみのシナリオ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 が完了するまでは、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。
- 対応する仮想ディスク / 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。
- OCE/RLM 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を手動で取り消すことができます。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。

メモ: 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 インターフェイスで、**[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**] ウィ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** — 所定のボリュームについて、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、コントローラは先読みなしモードに戻ります。
    - **先読みなし** — 所定のボリュームについて、先読みポリシーが使用されないことを示します。
    - **先読み** — 所定のボリュームについて、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せん。
  - **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** — 所定のボリュームについて、ディスクサブシステム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。
    - **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ングを使用した場合、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ングが使用されると、電源障害時にデータの損失が発生する可能性があります。
  - **ディスクキャッシュポリシー**：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** — ディ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** — ディ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** — ディ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。
- [**ディスク容量の編集**] - このウィンドウで、選択した仮想ディスクに物理ディスクを追加できます。このウィンドウには、物理ディスクを追加する仮想ディスクの現在の容量と追加した後の新しい容量も表示されます。
- [**RAID レベルの移行**] - ディスク名、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。

4. [**今すぐ適用**] をクリックすると変更がすぐに適用され、[**次の再起動時**] をクリックすると変更が次の起動後に適用され、[**スケジュールされた時刻**] をクリックすると特定の時刻に変更が適用され、[**すべての保留を破棄**] をクリックすると変更が破棄されます。

   選択した操作モードに基づいて、設定が適用されます。

RACADM を使用した仮想ディスクの管理

仮想ディスクの管理には、次のコマンドを使用します。

- 仮想ディスクを削除するには：

```
racadm storage deletevd:<VD FQDD>
```

- 仮想ディスクを初期化するには：

```
racadm storage init:<VD FQDD> -speed {fast|full}
```

- 仮想ディスクの整合性をチェックするには (RAID0 ではサポートされません) ：

```
racadm storage ccheck:<vdisk fqdd>
```

整合性チェックをキャンセルするには：

```
racadm storage cancelcheck: <vdisks fqdd>
```

- 仮想ディスクを暗号化するには：

```
racadm storage encryptvd:<VD FQDD>
```

- 専用ホットスペアを割り当て、または割り当て解除するには：

```
racadm storage hotspare:<Physical Disk FQDD> -assign <option> -type dhs -vdkey: <FQDD of VD>
```

<option>=yes
ホットスペアの割り当て

<Option>=no
ホットスペアの割り当て解除

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: 物理ディスクを強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

機能	RACADM コマンド	説明
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、コントローラーはドライブをオンライン状態に戻し、仮想ディスク内のメンバーシップを復元します。これは、コントローラーがドライブから読み取り、そのメ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。
メモ: データのリカバリーは、ディスクの一部が損傷している場合にのみ可能です。オンライン強制機能は、すでに障害が発生したディスクを修復することはできません。		
オフライン強制	`racadm storage forceoffline:<PD FQDD>`	この機能は、仮想ディスク設定からドライブを削除してオフラインにするため、VD 設定が劣化します。ドライブ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が、まだ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ブを使用する場合にも使用できます。
物理ディスクの交換	`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。

表 56. RAID 設定機能（続き）

機能	RACADM コマンド	説明
起動デバイスとしての仮想ディスク	`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	`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ブを認証するために使用されます。ロック解除されると、ドライブを 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
- BGI 率
- 再構成率
- 拡張自動インポート外部設定
- セキュリティキーの作成または変更
- 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、またはホットスペアとして割り当てられていない。
- 物理ディスクは、次のタスクのうち 1 つを実行している仮想ディスクに含まれます。
  - 再構築
  - 再構成または再構築
  - バックグラウンド初期化
  - 整合性チェック

さらに、巡回読み取り操作は高負荷の I/O 動作中は一時停止され、その I/O が終了すると再開されます。

メモ: 自動モードにおいて巡回読み取りタスクが実行される頻度に関する詳細については、お使いのコントローラのマニュアルを参照してください。

メモ: コントローラ内に仮想ディスクがない場合、**開始**や**停止**などの巡回読み取りモード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 コントローラでのみ使用可能です。

BGI 率

メモ: H330 と H345 のどちらにも、バックグラウンド初期化操作を実行するためにドライバーをロードする必要があります。

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が仮想ディスクの作成 0 ~ 5 分後に自動的に開始されます。冗長仮想ディスクのバックグラウンド初期化によって、仮想ディスクは冗長データの維持と書き込みパフォーマンスの向上に備えます。たとえば、RAID 5 仮想ディスクのバックグラウンド初期化完了後、パリティ情報が初期化されます。RAID 1 仮想ディスクのバックグラウンド初期化完了後は、物理ディスクがミラーリングされます。

バックグラウンド初期化プロセスは、コントローラが、後に冗長データに発生するおそれのある問題を識別し、修正するのに役立ちます。この点では、バックグラウンド初期化プロセスは整合性チェックに似ています。バックグラウンド初期化は、完了するまで実行する必要があります。キャンセルすると、0 ~ 5 分以内に自動的に再開されます。バックグラウンド初期化の実行中は、読み取りや書き込みなどの一部のプロセスは操作可能です。仮想ディスクの作成のような他の処理は、バックグラウンド初期化と同時に実行できません。これらの処理は、バックグラウンド初期化がキャンセルされる原因となります。

0 ~ 100 % の範囲で設定可能なバックグラウンド初期化率は、バックグラウンド初期化タスクの実行専用のシステムリソースの割合を表します。0 % では、コントローラに対するバックグラウンド初期化の優先順は最下位となり、完了までに最も長い時間がかかりますが、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率が 0% でも、バックグラウンド初期化が停止または一時停止されることはありません。100 % では、コントローラに対してバックグラウンド初期化は最優先になります。バックグラウンド初期化の時間が最短になりますが、システムパフォーマンスに与える影響は最大となります。

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にのみ適用されます。必要に応じて、整合性チェックタスクで冗長データが再構築されます。仮想ディスクが冗長性失敗状況にあるときは、整合性チェックの実行により仮想ディスクが準備完了状況に戻る場合があります。

0 ~ 100 % の範囲で設定可能な整合性チェック率は、整合性チェックタスクの実行専用のシステムリソースの割合を表します。0% では、コントローラに対する整合性チェックの優先順は最下位となり、完了までに最も長い時間がかかりますが、システムパフォーマンスに与える影響は最小になります。整合性チェック率が 0% でも、処理が停止または一時停止されることはありません。100% では、コントローラに対して整合性チェックは最優先になります。整合性チェックの時間が最短になりますが、システムパフォーマンスに与える影響は最大となります。

セキュリティキーの作成または変更

コントローラのプロパティを設定するときは、セキュリティキーを作成したり、変更したりできます。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作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 関連の設定も行う必要があります。

メモ:
- 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。

メモ:
- 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 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 モードになっていない同一システムで、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 モードになっていない 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ーで 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。

メモ: ホット プラグ接続されたロック済みのボ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。
   コントローラのセットアップ ページが表示されます。
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にあるデータです。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劣化状態の仮想ディスク、あるいはインポート可能かすでに存在している仮想ディスク専用のホットスペアが含まれている場合にのみインポートできます。

すべての仮想ディスクデータが存在する必要がありますが、仮想ディスクが冗長 RAID レベルを使用している場合、追加の冗長データは不要です。

たとえば、外部設定に RAID 1 仮想ディスクのミラーリングの片方のみが含まれる場合、仮想ディスクは劣化状態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 RAID 5 として設定された物理ディスク 1 台のみが外部設定に含まれる場合、RAID 5 仮想ディスクは失敗状態にあり、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 (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。

メモ: 外部設定のインポートタスクは、コントローラに追加された物理ディスクにあるすべての仮想ディスクをインポートします。複数の外部仮想ディスクが存在する場合は、全設定がインポートされます。

PERC9 コントローラでは、ユーザーの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、検出された外部設定を自動インポートできます。無効にすると、PERC は外部設定を自動インポートしません。

外部設定をインポートするには、ログインおよびサーバー制御の権限を持っている必要があります。

このタスクは、HBA モードで実行されている PERC ハードウェアコントローラではサポートされません。

メモ: システムでオペレーティングシステムを実行している最中に外部エンクロージャのケーブルを抜くことは推奨されません。ケーブルを抜くと、接続の再確立時に外部設定が生じる原因となる可能性があります。

次の場合に外部構成を管理できます。

- 構成内のすべての物理ディスクが取り外され、再度挿入されている。
- 構成内の一部の物理ディスクが取り外され、再度挿入されている。

- 仮想ディスク内のすべての物理ディスクが取り外され（ただし、取り外しは同時には行われなかった）、再度挿入されている。
- 非冗長仮想ディスク内の物理ディスクが取り外されている。

インポートを検討している物理ディスクには以下の制約が適用されます。
- 物理ディスクの状態は、実際にインポートされる際に、外部構成がスキャンされたときから変わっている場合があります。外部インポートでは、未構成良好状態のディスクのみがインポートされます。
- 故障状態またはオフライン状態のドライブはインポートできません。
- ファームウェアの制約により、8 つを超える外部構成をインポートすることはできません。

ウェブインタフェースを使用した外部設定のインポート

メモ: 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。

メモ: 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。物理ディスク状態をチェックすることで、以前に使用されていた物理ディスクに外部設定（仮想ディスク）が含まれているかを識別できます。物理ディスクの状態が外部の場合、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、コントローラに接続される物理ディスク上のすべてのデータが永続的に消去されます。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。
   コントローラ設定 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、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、コントローラ上のホットスペアがすべて割り当て解除されます。設定からディスクが削除される以外に、データは消去されません。また、設定をリセットしても、外部設定は削除されません。この機能のリアルタイムサポートは PERC 9.1 ファームウェアでのみ使用できます。設定をリセットしても、データは消去されません。初期化せずにまったく同じ設定を再作成できるので、データが修復される可能性があります。サーバ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

コントローラの設定をリセットするには、次の手順を実行します。

```
racadm storage resetconfig:<Controller FQDD>
```

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

コントローラモードの切り替え

PERC 9.1 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 コントローラーと同様に動作します。コントローラモードの変更はステージングされた操作であり、リアルタイムでは行われません。

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。

メモ:

- 拡張 HBA は、非 RAID の PD およびすべての RAID レベルの VD をサポートします。
- RAID0、RAID1、RAID10 の VD の作成のみをサポートします。
- 拡張 HBA は、PERC 11 ではサポートされていません。

拡張 HBA モードには、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。
- 非 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
- 未設定ディスクがホット挿入されている場合

メモ: RAID 5、6、50、または 60 の仮想ディスクの作成またはインポートはサポートされていません。また、拡張 HBA モードでは、非 RAID ディスクが最初に昇順で列挙され、RAID ボリュームは降順で列挙されます。

コントローラモードを RAID から HBA に変更する前に、次を確認してください。

- RAID コントローラがコントローラモードの変更をサポートしている。コントローラモードを変更するオプションは、RAID パーソナリティがライセンスを必要とするコントローラでは使用できません。
- すべての仮想ディスクが削除されている。
- ホットスペアが削除されている。
- 外部設定がクリアまたは削除されている。
- 障害の発生した状態のすべての物理ディスクが削除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 キーを削除する必要があります。
- コントローラに保存キャッシュが存在していない (必須)。
- コントローラモードを切り替えるためのサーバー制御権限がある。

メモ: モードを切り替えるとデータが削除されるため、外部設定、セキュリティキー、仮想ディスク、およびホットスペアをバックアップしてからモードを切り替えるようにしてください。

メモ: コントローラー モードを変更する前に、PERC FD33xS および FD33xD ストレージ スレッドに対して CMC ライセンス(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 にある『*PowerEdge FX2/FX2s* 対応 *Dell Chassis Management Controller バージョン 1.2 ユーザーズ ガイド*』を参照してください。

コントローラモードの切り替え時の例外

次のリストに、ウェブインタフェース、RACADM、および 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 モードに設定されている場合は、HBA モードに変更する前に、仮想ディスク、ホットスペア、外部設定、コントローラキー、または保存キャッシュをクリアする必要があります。
- コントローラモードの設定中にその他の RAID 操作を設定することはできません。たとえば、PERC が RAID モードであるときに PERC の保留中の値を HBA モードに設定して、BGI 属性を設定しようとすると、保留中の値が開始されません。
- PERC コントローラを HBA から RAID モードに切り替えると、ドライブは 非 RAID 状態のままとなり、準備完了 状態に自動的に設定されません。また、**RAIDEnhancedAutoImportForeignConfig** 属性は自動的に **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、ドライブを準備完了に変換して仮想ディスクを作成するようにエクスポート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 pseudo** 属性がアップデート (デフォルトの動作) に設定されます。属性が実行され、仮想ディスクが作成されますが、これは失敗します。コントローラモードは変更されますが、ジョブはエラーで終了します。この問題を回避するには、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 スタック操作の検証をサポートしていません。

iDRAC Web インターフェイスを使用したコントローラー モードの切り替え

コントローラモードを切り替えるには、次の手順を実行します。

1. iDRAC Web インターフェイスで、**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**ページで、**アクション** > **編集**をクリックします。
   現在の値 列にコントローラの現在の設定が表示されます。
3. ドロップダウン メニューから目的のコントローラー モードを選択し、**次の再起動時**をクリックします。
   変更を有効にするためにシステムを再起動します。

RACADM を使用したコントローラモードの切り替え

RACADM を使用してコントローラモードを切り替えるには、以下のコマンドを実行します。

- コントローラの現在のモードを表示するには：

```
$ racadm get Storage.Controller.1.RequestedControllerMode[key=<Controller_FQDD>]
```

次の出力が表示されます。

```
RequestedControllerMode = NONE
```

- HBA としてコントローラモードを設定するには：

```
$ racadm set Storage.Controller.1.RequestedControllerMode  HBA [Key=<Controller_FQDD>]
```

- 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。

```
$ 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 ドライバーがロードされている必要があります。POST 後、HBA ポートは無効になります。HBA デバイス ドライバーは、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、ドライバーはロードされず、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。

第 14 世代の iDRAC インターフェイスは、12 Gbps SAS HBA コントローラー、HBA330（内蔵またはアダプター）コントローラー、HBA330 MMZ および HBA330 MX アダプターをサポートしています。

AMD プラットフォームは、HBA355i 前面および HBA355i 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、電源供給ユニット、温度プローブのプロパティを表示します。プロパティは、コントローラーのタイプに基づいて表示されます。
- ソフトウェアとハードウェアのインベントリ情報の表示。
- 12 Gbps SAS HBA コントローラの裏側にあるエンクロージャのファームウェアのアップデート（ステージング）。
- 変更が検出された場合の物理ディスクの SMART トリップステータスに対するポーリングまたはポーリング頻度の監視。
- 物理ディスクのホットプラグまたはホット取り外しステータスの監視。
- LED の点滅または点滅解除。

メモ:

- 非 RAID コントローラーをイン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 インベントリーの収集（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送信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、複数のジョブを後で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。仮想ディスクがオフラインになったり、何らかの理由で削除されたりした場合は、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ダーティー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 秒当たりの入出力速度（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 は、高速 PCIe 2.0、PCIe 3.0、または PCIe 4.0 準拠のインターフェイスを備えた Single Level Cell

(SLC) および Multi-Level Cell (MLC) NAND フラッシュ テクノロジーに基づいて設計されています。第 14 世代の PowerEdge サーバーでは、SSD を接続する方法は 3 つあります。エクステンダーを使用してバックプレーンで SSD を接続する方法、エクステンダーなしのスリムライン ケーブルを使用して、バックプレーンからマザーボードに SSD を直接接続する方法、マザーボード上にある HHHL (アドイン) カードを使用する方法が使用できます。

メモ:
- 第 14 世代の PowerEdge サーバーは、業界標準の NVMe-MI 仕様ベースの NVMe SSD をサポートしています。
- PERC 11 は、PERC 背後の PCIe SSD/NVMe デバイスのインベントリーの監視および構成をサポートしています。

iDRAC インタフェースを使用して、NVMe PCIe SSD の表示および設定が行えます。

PCIe SSD には、次の主な機能があります。
- ホットプラグ対応
- 高性能デバイス

第 14 世代の PowerEdge サーバーの一部では、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
- デバイスの LED の点滅または点滅解除 (デバイスの識別)

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 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 LED 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 デバイスを S140 で制御している場合、取り外し準備と暗号消去操作はサポートされていませんが、点滅および点滅解除がサポートされています。

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。
- ソフトウェアインベントリには、PCIe SSD のファームウェアのバージョンだけが含まれます。

ウェブインタフェースを使用した PCIe SSD のインベントリと監視

PCIe SSD デバイスをインベントリおよび監視するには、iDRAC ウェブインタフェースで、**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。**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 のインベントリおよび監視

`racadm storage get controllers:<PcieSSD controller FQDD>` コマンドを使用して、PCIe SSD のインベントリと監視を行います。

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: 次の場合、この操作はサポートされません。

- PCIe SSD が S140 コントローラーを使用して設定されている場合。
- NVMe デバイスが PERC 11 の背後にある場合。

PCIe SSD は手順を踏んだホットスワップに対応しており、デバイスを搭載しているシステムの一時停止や再起動なしで、デバイスを追加および削除できます。データ ロスを避けるため、デバイスを物理的に取り外す前には、取り外しの準備操作を行う必要があります。

所定のホット 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にのみサポートされます。PCIe SSD に対する設定が正しい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。

メモ: 取り外しの準備操作は、iDRAC サービス モジュール バージョン 2.1 以降を使用する ESXi 6.0 搭載システムでサポートされています。

取り外しの準備 操作は iDRAC サービスモジュールを使用してリアルタイムで実行できます。

取り外しの準備操作を行うと、デバイスを安全に取り外すことができるように、バックグラウンド処理および進行中のあらゆる I/O 処理が停止します。この操作を行うと、デバイスのステータス LED が点滅します。次の条件下で取り外しの準備操作を実行すると、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 パターンで点滅している場合 (橙色に点滅)。
- PCIe SSD にシステムからアクセスできない。

PCIe SSD の取り外しを準備する前に、以下を確認してください。

- iDRAC サービスモジュールが取り付けられている。
- Lifecycle Controller が有効化されている。
- サーバ制御およびログインの権限がある。

ウェブインタフェースを使用した PCIe SSD の取り外しの準備

PCIe SSD の取り外しを準備するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**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** ドロップダウンメニューから、エクステンダを選択して関連する PCIe SSD を表示します。
3. ドロップダウンメニューから、1 つまたは複数の PCIe SSD に対する **取り外しの準備** を選択します。
   取り外しの準備 を選択した場合に、ドロップダウンメニューのその他のオプションを表示するには、**処置** を選択し、ドロップダウンメニューをクリックしてその他のオプションを表示します。
   メモ: `preparetoremove` 操作を実行するには、iSM がインストールおよび実行されていることを確認します。

4. **操作モードの適用** ドロップダウンメニューから、**今すぐ適用** を選択してただちに処置を適用します。
   完了予定のジョブがある場合、このオプションはグレー表示になります。
   メモ: PCIe SSD デバイスの場合、**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。
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 の取り外しの準備

PCIeSSD ドライブの取り外しを準備するには、次の手順を実行します。

```
racadm storage preparetoremove:<PCIeSSD FQDD>
```

`preparetoremove` コマンドを実行した後にターゲットジョブを作成するには、次の手順を実行します。

```
racadm jobqueue create <PCIe SSD FQDD> -s TIME_NOW --realtime
```

返されたジョブ ID を問い合わせるには、次の手順を実行します。

```
racadm jobqueue view -i <job ID>
```

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』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 SWRAID コントローラーを使用して設定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 で暗号消去を実行するとすべてのブロックが上書きされ、PCIe SSD 上のすべてのデータが恒久的に消失します。暗号消去の実行中、ホストは PCIe SSD にアクセスできません。変更内容は、システムの再起動後に適用されます。

暗号消去を実行中にシステムを再起動または停電になると、暗号消去はキャンセルされます。システムを再起動し、処理を再起動する必要があります。

PCIe SSD デバイスのデータを消去する前に、次を確認してください。

- Lifecycle Controller が有効化されている。
- サーバ制御およびログインの権限がある。

メモ:

- PCIe SSD の消去は、ステージング操作としてのみ実行できます。
- ドライブは消去された後、オンラインとしてオペレーティングシステムに表示されますが、初期化されていません。再使用する前に、ドライブを初期化してフォーマットする必要があります。
- PCIe SSD のホットプラグを実行した後、Web インターフェイスで表示されるまでに数秒かかる場合があります。

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。
   Physical Disk (物理ディスク) ページが表示されます。
2. **コントローラ** ドロップダウンメニューから、コントローラを選択して関連付けられている PCIe SSD を表示します。

3. ドロップダウンメニューから、1 つまたは複数の PCIe SSD に対する **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** 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。
     - 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
- ユニバーサルモードまたはスプリットモードの設定
- スロット情報の表示（ユニバーサルまたは共有）
- SGPIO モードの設定
- Set Asset Tag
- アセット名

バックプレーンモードの設定

第 14 世代 Dell PowerEdge サーバーは、新しい内蔵ストレージ トポロジーをサポートします。このトポロジーでは、1 つのエキスパンダーを通して 2 台のストレージ コントローラー（PERC）を 1 組の内蔵ドライブに接続することができます。この構成ではフェールオーバーや高可用性（HA）機能のない高パフォーマンスモードに使用されます。エキスパンダは、2 台のストレージコントローラ間

で内蔵ドライブアレイを分割します。このモードでは、仮想ディスクの作成で特定のコントローラに接続されたドライブのみが表示されます。この機能のライセンス要件はありません。この機能は、一部のシステムでのみサポートされています。

バックプレーンは次のモードをサポートします。

- 統合モード — デフォルトのモードです。2 台目の PERC コントローラーが取り付けられている場合でも、プライマリー PERC コントローラーは、バックプレーンに接続されたすべてのドライブにアクセスできます。
- 分割モード — 1 台のコントローラーは最初の 12 台のドライブにアクセスでき、2 台目のコントローラーは、残りの 12 台のドライブにアクセスできます。1 台目のコントローラー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ーに接続されているドライブには 12 ~ 23 の番号が付けられます。
- 分割モード 4:20 — 1 台のコントローラーは最初の 4 台のドライブにアクセスでき、2 台目のコントローラーは残りの 20 台のドライブにアクセスできます。1 台目のコントローラー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ーに接続されているドライブには 4 ~ 23 の番号が付けられます。
- 分割モード 8:16 — 1 台のコントローラーに最初の 8 台のドライブへのアクセス権があり、2 台目のコントローラーに残りの 16 台のドライブへのアクセス権があります。1 台目のコントローラー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ーに接続されているドライブには 8 ~ 23 の番号が付けられます。
- 分割モード 16:8 — 1 台のコントローラーに最初の 16 台のドライブにアクセスでき、2 台目のコントローラーは残りの 8 台のドライブにアクセスできます。1 台目のコントローラー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ーに接続されているドライブには 16 ~ 23 の番号が付けられます。
- 分割モード 20:4 — 1 台のコントローラーに最初の 20 台のドライブへのアクセス権があり、2 台目のコントローラーに残りの 4 台のドライブへのアクセス権があります。1 台目のコントローラー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ー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。
- 分割モード 6:6:6:6 — 1 つのシャーシに 4 枚のブレードが取り付けられており、各ブレードには 6 台のドライブが割り当てられています。このモードは PowerEdge C シリーズブレードでのみサポートされています。
- 情報が利用不可 — コントローラ情報は利用できません。

iDRAC では、エキスパンダーに構成をサポートする機能がある場合、分割モードを設定できます。2 台目のコントローラーを取り付ける前に、このモードが有効になっていることを確認してください。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しますが、2 台目の PERC コントローラーが存在するかどうかはチェックしません。

メモ: PERC を 1 台のみ接続した状態でバックプレーンを分割モードにするか、PERC を 2 台接続した状態でバックプレーンを統合モードにすると、ケーブル エラー (またはその他のエラー) が表示されることがあります。

設定を変更するには、サーバー制御権限を持っている必要があります。

他の RAID 操作が保留中であるか、または何らかの RAID ジョブがスケジュール設定されている場合は、バックプレーン モードを変更することはできません。同様に、この設定が保留中の場合は、他の RAID ジョブをスケジュールすることはできません。

メモ:

- 設定が変更されるときは、データロスのおそれがあることを示す警告メッセージが表示されます。
- LC ワイプまたは iDRAC のリセット操作では、このモードに対するエキスパンダ設定は変更されません。
- この操作は、リアルタイムでのみサポートされており、ステージされません。
- バックプレーン設定は複数回変更することができます。
- バックプレーンの分割処理は、ドライブの関連付けが一つのコントローラから別のコントローラに変更された場合、データ損失または外部設定を引き起こす可能性があります。
- バックプレーンの分割処理中は、ドライブの関連付けに応じて RAID 設定が影響を受ける場合があります。

この設定の変更は、システムの電源リセット後にのみ有効になります。分割モードから統合モードに変更すると、次回起動時に 2 台目のコントローラがドライブを認識しないことを示すエラーメッセージが表示されます。また、1 台目のコントローラは外部設定を認識します。エラーを無視すると、既存の仮想ディスクが失われます。

ウェブインタフェースを使用したバックプレーンモードの設定

iDRAC ウェブインタフェースを使用してバックプレーンモードを設定するには、次の手順を実行します。

1. iDRAC 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

メモ: 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。

```
racadm get storage.enclosure.1.backplanecurrentmode
```

   出力は次のとおりです。

```
BackplaneCurrentMode=UnifiedMode
```

2. 要求されたモードを表示するには、次のコマンドを実行します。

```
racadm get storage.enclosure.1.backplanerequestedmode
```

   出力は次のとおりです。

```
BackplaneRequestedMode=None
```

3. 要求されたバックプレーンモードをスプリットモードに設定するには、次のコマンドを実行します。

```
racadm set storage.enclosure.1.backplanerequestedmode "splitmode"
```

   コマンドが成功したことを示すメッセージが表示されます。
4. 次のコマンドを実行して、**backplanerequestedmode** 属性がスプリットモードに設定されていることを確認します。

```
racadm get storage.enclosure.1.backplanerequestedmode
```

   出力は次のとおりです。

```
BackplaneRequestedMode=None (Pending=SplitMode)
```

5. `storage get controllers` コマンドを実行して、コントローラのインスタンス ID を書き留めます。
6. ジョブを作成するには、次のコマンドを実行します。

```
racadm jobqueue create <controller instance ID> -s TIME_NOW --realtime
```

   ジョブ ID が返されます。
7. ジョブステータスのクエリを実行するには、次のコマンドを実行します。

```
racadm jobqueue view -i JID_xxxxxxxx
```

ここで、JID_xxxxxxxx は手順 6 のジョブ ID です。

ステータスが保留中として表示されます。

完了ステータスが表示されるまで、ジョブ ID のクエリを続行します (このプロセスには最大で 3 分かかります)。

8. backplanerequestedmode 属性値を表示するには、次のコマンドを実行します。

```
racadm get storage.enclosure.1.backplanerequestedmode
```

出力は次のとおりです。

```
BackplaneRequestedMode=SplitMode
```

9. サーバをコールドリブートするには、次のコマンドを実行します。

```
racadm serveraction powercycle
```

10. システムが POST と CSIOR を完了した後、次のコマンドを入力して backplanerequestedmode を確認します。

```
racadm get storage.enclosure.1.backplanerequestedmode
```

出力は次のとおりです。

```
BackplaneRequestedMode=None
```

11. バックプレーンモードがスプリットモードに設定されていることを確認するには、次のコマンドを実行します。

```
racadm get storage.enclosure.1.backplanecurrentmode
```

出力は次のとおりです。

```
BackplaneCurrentMode=SplitMode
```

12. 次のコマンドを実行して、ドライブ 0 ~ 11 のみが表示されていることを確認します。

```
racadm storage get pdisks
```

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

ユニバーサルスロットの表示

一部の第 14 世代 PowerEdge サーバー バックプレーンは、同じスロット内の 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、同じスロットで SAS/SATA と PCIe SSD ドライブの両方をサポートする CPU バックプレーンによって、プライマリー ストレージ コントローラー (PERC) と PCIe 拡張カードまたは直接接続マネージャーのいずれかが有線で繋がっています。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について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、数の大きいほうから 4 個のスロットはユニバーサルです。例えば、24 個のスロットをサポートするユニバーサル バックプレーンでは、スロット 0 ~ 19 は SAS/SATA ディスクのみをサポートし、スロット 20 ~ 23 は SAS/SATA または PCIe SSD のいずれ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の正常性状態を結合したものです。**トポロジー**ページのエンクロージャ リンクには、関連づけられているコントローラーに関係なく、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 コントローラー (PERC と PCIe エクステンダー) は同じバックプレーンに接続できるため、PERC コントローラーに関連付けられているバックプレーンのみが、**システム インベントリー**ページに表示されます。

ストレージ > **エンクロージャ** > **プロパティ** ページの **物理ディスクの概要** セクションに、次の情報が表示されます。

- **空きスロット** — スロットが空の場合に表示されます。
- **PCIe 対応** — PCIe 対応スロットがない場合、この列は表示されません。
- **バス プロトコル** — ユニバーサル バックプレーンのスロットの 1 つに PCIe SSD が取り付けられている場合、この列に **PCIe** が表示されます。
- **ホットスペア** — この列は PCIe SSD には適用されません。

メモ: ユニバーサル スロットではホット スワップがサポートされています。PCIe SSD ドライブを取り外して SAS/SATA ドライブとスワップする場合は、まず、PCIe SSD ドライブの PrepareToRemove タスクを完了してください。このタスクを実行しないと、ホスト オペレーティング システムにブルー スクリーン、カーネル パニックなどの問題が発生する可能性があります。

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、パッシブ バックプレーンのみでサポートされます。このモードは、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 モードのパッシブ バックプレーンではサポートされません。バックプレーンのファームウェアは、機能、現在の状態、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。

設定の変更を有効にするには、サーバーの電源を入れ直す必要があります。

この設定を変更するには、サーバー制御の特権権限を持っている必要があります。

メモ: iDRAC 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かチェックされ、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では、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かチェックされ、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: 資産名の上限は 32 文字です (NULL 文字を含む)。

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。

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）** - ただちに設定を適用するには、このオプションを選択します。このオプションは PERC 9 コントローラでのみ使用できます。完了予定のジョブがある場合、このオプションはグレー表示になります。このジョブの完了には、2 分以上かかります。
   - **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。
     - 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）
   - **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。

   メモ:
   - **Add to Pending Operations（保留中の操作に追加）** オプションは **Pending Operations（保留中の操作）** ページ、および **Physical Disks（物理ディスク）** > **Setup（セットアップ）** ページの PCIe SSD には適用されません。
   - **今すぐ適用** オプションは、**エンクロージャのセットアップ** ページのみで使用できます。
3. **適用** をクリックします。
   選択したオペレーションモードに基づいて、設定が適用されます。

RACADM を使用した操作モードの選択

操作モードを選択するには、`jobqueue` コマンドを使用します。

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

保留中の操作の表示と適用

ストレージコントローラに対する保留中の操作すべてを表示および確定できます。すべての設定は、選択したオプションに基づいて、直ちに、次回の再起動中に、またはスケジュールされた時刻に適用されます。コントローラのすべての保留中の操作を削除することができますが、個々の保留中の操作を削除することはできません。

保留中の操作は、選択したコンポーネント（コントローラ、エンクロージャ、物理ディスク、および仮想ディスク）に対して作成されます。

設定ジョブはコントローラに対してのみ作成されます。PCIe SSD の場合、ジョブは PCIe エクステンダではなく PCIe SSD ディスクに対して作成されます。

ウェブインタフェースを使用した保留中の操作の表示、適用、または削除

1. iDRAC ウェブインタフェースで、**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（コールドブート）
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、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。

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

ストレージデバイス — 操作適用のシナリオ

ケース 1：動作モードの適用（今すぐ適用、次の再起動時、または スケジュールされた時刻）を選択し、既存の保留中の操作がない場合

今すぐ適用、**次の再起動時**、または **スケジュールされた時刻** を選択して **適用** をクリックした場合、まず選択したストレージ設定操作のための保留中の操作が作成されます。

- 保留中の操作が正常に完了し、それ以前に他に既存の保留中の操作がなければ、ジョブが作成されます。ジョブが正常に作成された場合、選択したデバイスにそのジョブ ID が作成されたことを示すメッセージが表示されます。**ジョブキュー** をクリックすると、**ジョブキュー** ページでジョブの進行状況が表示されます。ジョブが作成されなかった場合、ジョブの作成が正常に終了しなかったことを示すメッセージが表示されます。また、メッセージ ID、および推奨される対応処置が表示されます。
- 保留中の操作の作成が正常に行われず、それ以前に既存の保留中の操作がない場合、ID およびエラーメッセージと、推奨される対応処置が表示されます。

ケース 2：動作モードの適用（今すぐ適用、次の再起動時、または スケジュールされた時刻）を選択し、既存の保留中の操作がある場合

今すぐ適用、**次の再起動時**、または **スケジュールされた時刻** を選択して **適用** をクリックした場合、まず選択したストレージ設定操作のための保留中の操作が作成されます。

- 保留中の操作が正常に作成され、既存の保留中の操作がある場合、メッセージが表示されます。
  - そのデバイスの保留中の操作を表示するには、**保留中の操作の表示** リンクをクリックします。
  - 選択したデバイスにジョブを作成するには、**Create Job（ジョブの作成）** をクリックします。ジョブが正常に作成された場合、選択したデバイスにそのジョブ ID が作成されたことを示すメッセージが表示されます。**ジョブキュー** をクリックすると、**ジョブキュー** ページでジョブの進行状況が表示されます。ジョブが作成されなかった場合、ジョブの作成が正常に終了しなかったことを示すメッセージが表示されます。また、メッセージ ID、および推奨される対応処置が表示されます。
  - ジョブを作成しない場合は、**キャンセル** をクリックします。その場合、続いてストレージ設定操作を行うため、そのページに止まります。
- 保留中の操作が正常に作成されず、既存の保留中の操作がある場合、エラーメッセージが表示されます。
  - そのデバイスの保留中の操作を表示するには、**保留中の操作** をクリックします。
  - 既存の保留中の操作にジョブを作成するには、**Create Job For Successful Operations**（正常な操作のためのジョブの作成）をクリックします。ジョブが正常に作成された場合、選択したデバイスにそのジョブ ID が作成されたことを示すメッセージが表示されます。**ジョブキュー** をクリックすると、**ジョブキュー** ページでジョブの進行状況が表示されます。ジョブが作成されなかった場合、ジョブの作成が正常に終了しなかったことを示すメッセージが表示されます。また、メッセージ ID、および推奨される対応処置が表示されます。
  - ジョブを作成しない場合は、**キャンセル** をクリックします。その場合、続いてストレージ設定操作を行うため、そのページに止まります。

ケース 3：保留中の操作に追加 を選択し、既存の保留中の操作がない場合

保留中の操作に追加 を選択し **適用** をクリックした場合、まず選択されたストレージ設定操作の保留中の操作が作成されます。

- 保留中の操作が正常に作成され、既存の保留中の操作がない場合、次の参考メッセージが表示されます。
  - **OK** をクリックすると、続けてストレージ設定操作を行うため、このページに止まります。
  - 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。
- 保留中の操作が正常に作成されず、既存の保留中の操作がない場合、エラーメッセージが表示されます。

ケース 4：保留中の操作に追加 を選択し、それ以前に既存の保留中の操作がある場合

保留中の操作に追加 を選択し **適用** をクリックした場合、まず選択されたストレージ設定操作の保留中の操作が作成されます。

- 保留中の操作が正常に作成され、既存の保留中の操作がある場合、次の参考メッセージが表示されます。
  - **OK** をクリックすると、続けてストレージ設定操作を行うため、このページに止まります。
  - そのデバイスの保留中の操作を表示するには、**保留中の操作** をクリックします。
- 保留中の操作が正常に作成されず、既存の保留中の操作がある場合、エラーメッセージが表示されます。
  - **OK** をクリックすると、続けてストレージ設定操作を行うため、このページに止まります。
  - そのデバイスの保留中の操作を表示するには、**保留中の操作** をクリックします。

メモ:

- いかなる時にも、ストレージ設定ページにジョブを作成するオプションがない場合は、既存の保留中の操作を表示し、必要なコントローラでジョブを作成するには、**ストレージの概要** > **保留中の操作** ページにアクセスします。
- PCIe SSD には、ケース 1 および 2 のみが適用されます。PCIe SSD の保留中の操作を表示することはできないため、**Add to Pending Operations（保留中の操作に追加）** オプションは使用できません。PCIe SSD の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。

コンポーネント LED の点滅または点滅解除

ディスク上の発光ダイオード (LED) のいずれかを点滅させることによって、エンクロージャ内の物理ディスク、仮想ディスクドライブ、および PCIe SSD を見つけることができます。

LED を点滅または点滅解除するには、ログイン権限を持っている必要があります。

コントローラは、リアルタイム設定対応であることが必要です。この機能のリアルタイムサポートは、PERC 9.1 以降のファームウェアでのみ使用できます。

メモ: バックプレーンを装備していないサーバーの点滅または点滅解除はサポートされません。

ウェブインタフェースを使用したコンポーネントの LED の点滅または点滅解除

コンポーネント LED を点滅または点滅解除するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、必要に応じて次のいずれかのページに移動します。
   - **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。

```
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。

18

BIOS 設定

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ーを変更できます。1 つ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ーが表示されます。別の属性を変更する前に、属性の複数のパラメーター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。

メモ:

- 属性レベルのヘルプコンテンツは動的に生成されます。
- iDRAC Direct USB ポートは、すべての USB ポートが無効になっている場合でも、ホストの再起動なしで使用できます。

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、https://www.dell.com/idracmanuals から入手可能な『*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、直近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

属性またはブート シーケンス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。どちらの適用オプションを選択しても、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。

適用して再起動 をクリックすると、すぐにサーバが再始動され、必要な変更がすべて設定されます。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、EEMI メッセージが生成され、表示されます。

次回の再起動時に適用

属性またはブート シーケンス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。どちらの適用オプションを選択しても、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 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。次の再起動セッションが正常に完了するまで、直近の設定変更は操作環境に反映されません。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、EEMI メッセージが生成され、表示されます。

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、直近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 プライマリー 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 iDRAC Datacenter 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 ブート時
- 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 のリカバリーとハードウェア 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 プライマリー 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 iDRAC Datacenter 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 ブート時
- 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 のリカバリーとハードウェア 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損した 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/リカバリー BIOS は、(プライマリー BIOS SPI 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 タスクの主要なオーケストレーターになります。

1. **BIOS プライマリー イメージ/リカバリー イメージの自動リカバリー**: Intelboot 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ーされます。
2. **BIOS プライマリー/リカバリー イメージの強制リカバリー**: 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、ユーザーが 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。ユーザーがインターフェイスを使用して 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 のセキュア ブートが保証され、ホスト ブート プロセスのセキュリティが強化されます。

メモ: ハードウェア RoT の詳細については、次のリンクを参照してください。 https://downloads.dell.com/Manuals/Common/dell-emc-idrac9-security-root-of-trust-bios-live-scanning.pdf

19

仮想コンソールの設定と使用

iDRAC の vConsole には強化された HTML5 オプションが追加されており、標準 VNC クライアントを介して vKVM (仮想キーボード、ビデオ、マウス) を使用できます。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。仮想コンソール上のすべての設定にアクセスするには、iDRAC 設定権限が必要です。

仮想コンソールで設定可能な属性のリストは次のとおりです。

- vConsole 有効化 - 有効/無効
- 最大セッション数 - 1~6
- アクティブ セッション数 - 0~6
- リモートプレゼンスポート
- ビデオ暗号化 - 有効/無効
- ローカル サーバー ビデオ - 有効/無効
- プラグイン タイプ - eHTML5 (デフォルト)、ActiveX、Java、HTML5
- リクエスト タイムアウト共有時の動的アクション - フル アクセス、読み取り専用アクセス、アクセス拒否
- 自動システム ロック - 有効/無効
- キーボード/マウスの連結状態 - 自動連結、連結、分離

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、eHTML5 プラグインを使って、対応 Web ブラウザー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 eHTML5 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 つのコンソールセッションを開くことはできません。
- 2 人目のユーザーが仮想コンソールセッションを要求すると、最初のユーザーが通知を受け、アクセスを拒否する、読み取り専用アクセスを許可する、または完全な共有アクセスを許可するオプションが与えられます。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付与されます。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。
- 起動ログとクラッシュ ログは MPEG1 形式のビデオ ログとして収集されます。
- クラッシュ画面は JPEG ファイルとして収集されます。
- 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。
- 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

Mac クライアント	Win クライアント	Linux クライアント
Ctrl-Al-Del	Ctrl-Alt-Del	Ctrl-Alt-Del
Alt-SysRq-B	Alt-SysRq-B	Alt-SysRq-B
-	Win-P	-
-	-	Ctrl-Alt-F<1-12>
Alt-SysRq	-	-

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（続き）

Mac クライアント	Win クライアント	Linux クライアント
SysRq	-	-
PrtScrn	-	-
Alt-PrtScrn	-	-
一時停止	-	-

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: Web インターフェイ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 Web インターフェイス セッションのみです。この数には、SSH、RACADM などの他のインターフェイスからのセッションは含まれません。

メモ: お使いのブラウザを仮想コンソールにアクセスするように設定する場合は、「仮想コンソールを使用するためのウェブブラウザの設定 、p. 75」を参照してください。

メモ: KVM アクセスを無効にするには、OME Modular Web インターフェイスで、シャーシの設定にある**無効**オプションを使用します。

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

画面解像度	リフレッシュレート (Hz)
720x400	70
640x480	60、72、75、85
800x600	60、70、72、75、85
1024x768	60、70、72、75、85
1280x1024	60
1920x1200	60

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 1920 x 1200 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が低下します。

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 コントローラー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。

モニターのアスペクト比に基づく仮想コンソールの最大解像度：

- 16:10 モニター：最大解像度 1920 x 1200
- 16:9 モニター：最大解像度 1920 x 1080

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: 物理 KVM やモニターがない仮想コンソールでより高い解像度が必要な場合は、VGA ディスプレイ エミュレーター ドングルを活用して外部モニター接続を疑似的に再現し、最大 1920 x 1080 の解像度を実現できます。

メモ: 仮想コンソール セッションがアクティブで、低解像度モニターが仮想コンソールに接続されている場合、ローカル コンソールでサーバーが選択されると、サーバー コンソールの解像度がリセットされることがあります。システムで Linux オペレーティング システムを実行している場合は、ローカル モニターに X11 コンソールが表示されないことがあります。iDRAC 仮想コンソールで<Ctrl><Alt><F1>を押し、Linux をテキスト コンソールに切り替えます。

仮想コンソールの設定

仮想コンソールを設定する前に、管理ステーションが設定されていることを確認します。

仮想コンソールは、iDRAC ウェブインタフェースまたは RACADM コマンドラインインタフェースを使用して設定できます。

Web インターフェイスを使用した仮想コンソールの設定

iDRAC Web インターフェイ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. **設定** > **仮想コンソール**の順に移動します。**仮想コンソールの起動**リンクをクリックすると、仮想コンソール ページが表示されます。
2. 仮想コンソールを有効化し、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。

   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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

仮想コンソールのプレビュー

仮想コンソールを起動する前に、**System（システム）** > **Properties（プロパティ）** > **System Summary（システムサマリ）** ページで仮想コンソールの状態をプレビューできます。**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にのみ表示できます。

仮想コンソールの起動

仮想コンソールは、iDRAC Web インターフェイスまたは URL を使用して起動できます。

メモ: 管理下システムの Web ブラウザー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。
- Web ブラウザーは、HTML5、eHTML5、Java、ActiveX のいずれかのプラグインを使用するように設定されている。
- 最低限のネットワーク帯域幅 (1 MB/ 秒) が利用可能。

メモ: 内蔵ビデオコントローラが BIOS で無効化されているときに仮想コンソールを起動した場合、仮想コンソールビューアには何も表示されません。

32 ビット版または 64 ビット版 IE ブラウザーを使用して仮想コンソールを起動する場合は、HTML5/eHTML5 を使用するか、または該当するブラウザー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、すべてのブラウザーで共通です。

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低速で、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 プラグインのダウンロード時間は、この時間を超える場合があります。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/eHTML5 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。

仮想メディアにアクセスするには、仮想コンソールで使用可能な**仮想メディアへの接続**オプションをクリックします。

仮想コンソールには、次のコンソール制御機能があります。

1. **一般** - キーボード マクロ、アスペクト比、タッチ モードを設定することができます。
2. **KVM** - フレーム率、帯域幅、圧縮、パケット率を設定することができます。
3. **パフォーマンス** - このオプションを使用して、ビデオの画質とビデオのスピードを変更することができます。
4. **ユーザー リスト** - コンソールに接続されているユーザーのリストを表示することができます。

Web インターフェイ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。

- **設定** > **仮想コンソール**の順に移動します。**仮想コンソールの起動**リンクをクリックします。仮想コンソール ページが表示されます。

仮想コンソール ビューアーにリモート システムのデスクトップが表示されます。このビューアーを使用して、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。

ビューアー ウィンドウには 2 つのマウス ポインターが表示されることがあります。1 つは管理下サーバー用で、もう 1 つは管理ステーション用です。

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て、ローカル、Active Directory、LDAP、またはスマートカードログインが有効になっている場合は、対応する **ログイン** ページが表示されます。
   - シングルサインオンが有効になっている場合は、**仮想コンソール ビューア** が起動し、**仮想コンソール** ページがバックグラウンドに表示されます。

   メモ: Internet Explorer は、ローカル、Active Directory、LDAP、スマートカード (SC)、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。

メモ: 仮想コンソールへのアクセス権限はないが仮想メディアへのアクセス権限があるという場合は、この URL を使用すると仮想コンソールの代わりに仮想メディアが起動します。

Java または ActiveX プラグインを使用した仮想コンソールまたは仮想メディアの起動中における警告メッセージの無効化

Java プラグインを使用して、仮想コンソールまたは仮想メディアの起動中における警告メッセージを無効化することができます。

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

1. Java プラグインを使用して仮想コンソールまたは仮想メディアを起動した当初、発行元を確認するプロンプトが表示されます。**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. 証明書警告メッセージで、**この証明書を常に信頼** オプションを選択して **続行** をクリックします。
7. ビューアを終了します。
8. 仮想コンソールを再起動すると、警告メッセージは表示されません。

仮想コンソールビューアの使用

仮想コンソールビューアでは、マウスの同期、仮想コンソールスケーリング、チャットオプション、キーボードマクロ、電源操作、次の起動デバイス、および仮想メディアへのアクセスなどのさまざまな制御を実行できます。これらの機能の使用方法については、『*iDRAC オンラインヘルプ*』を参照してください。

メモ: リモートサーバーの電源がオフになっている場合は、「信号なし」のメッセージが表示されます。

仮想コンソールビューアのタイトルバーには、管理ステーションから接続する先の iDRAC の DNS 名または IP アドレスが表示されます。iDRAC に DNS 名がない場合は、IP アドレスが表示されます。フォーマットは次のとおりです。

- ラックおよびタワーサーバーの場合：

  `<DNS name / IPv6 address / IPv4 address>, <Model>, User: <username>, <fps>`

- ブレードサーバーの場合：

  `<DNS name / IPv6 address / IPv4 address>, <Model>, <Slot number>, User: <username>, <fps>`

場合によっては、仮想コンソールビューアに表示されるビデオの品質が低くなることがあります。これは、ネットワーク接続が低速になっていること原因で、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 ~ 2 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 **仮想コンソールプレビュー** セクションで、**更新** をクリックします。
- **仮想コンソールビューア** の **パフォーマンス** タブで、スライダを **最高ビデオ品質** に設定します。

eHTML5 ベースの仮想コンソール

メモ: eHTML5 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、およびブラウザーで同じ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。

eHTML5 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、**プラグイン タイプ** オプションを eHTML5 に設定する必要があります。

メモ: デフォルトでは、仮想コンソールのタイプは eHTML5 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 プレビュー セッションで使用可能な**仮想コンソールの起動**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**リンクをクリックします。
- 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ます。

eHTML5 仮想コンソールでは、次のメニュー オプションを使用できます。

- 電源
- 起動
- 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

すべてのキーストロークをサーバーに渡すオプションは、eHTML5 仮想コンソールではサポートされません。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。

- **全般** -
  - **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 マクロ - これは eHTML5 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
      - Alt+F5
      - Alt+F6
      - Alt+F7
      - Alt+F8
      - Alt+F9
      - Alt+F10
      - Alt+F11
      - Alt+F12

- PrntScrn
- Alt+PrntScrn
- F1
- 一時停止
- タブ
- Ctrl+Enter
- SysRq
- Alt+SysRq
- Win-P

■ アスペクト比 - eHTML5 仮想コンソールのビデオ イメージは、画像を可視化するためにサイズが自動的に調整されます。次の設定オプションがドロップダウンリストに表示されます。
- 保守
- 維持しない

適用 をクリックしてサーバーに選択された設定を適用します。

■ タッチ モード - eHTML5 仮想コンソールはタッチ モード機能をサポートします。次の設定オプションがドロップダウンリストに表示されます。
- ダイレクト
- 相対座標

適用 をクリックしてサーバーに選択された設定を適用します。

- **仮想クリップボード** - テキスト バッファーの切り取り/コピー/貼り付けが、仮想コンソールから iDRAC ホスト サーバーに対して行えます。ここでのホスト サーバーとなれるものには、BIOS、UEFI、OS プロンプトがあります。この操作は、クライアント コンピューターから 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。
  - ホスト サーバーのデスクトップの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。
  - vConsole で [**コンソール制御**] を選択します。
  - OS クリップボード バッファーからのコピーを、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。
  - [**クリップボードをホストに送信**] をクリックします。
  - 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 Datacenter ライセンスでのみ使用可能です。
  - 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 バ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ーが貼り付けられた場合、iDRAC GUI の編集ボックスでは、最大バッファー サイズへの切り捨てが行われます。
- **KVM** - このメニューには、次の読み取り専用コンポーネントがリストされています。
  - フレーム率
  - 帯域幅
  - Compression (圧縮)
  - パケット率
- **パフォーマンス** - スライダー ボタンを使用して、**ビデオの最大画質**と**最大ビデオ スピード**を調整することができます。
- **ユーザー リスト** - 仮想コンソールにログインしているユーザーのリストを表示することができます。
- **キーボード** - 物理キーボードと仮想キーボードの違いは、仮想キーボードはブラウザーの言語に従ってレイアウトを変更することです。
- **仮想メディア** - **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。
  - **仮想メディアの接続** - このメニューには、CD/DVD のマップ、リムーバブル ディスクのマップ、外部デバイスのマップ、USB リセットの各オプションが含まれています。
  - **仮想メディア統計情報** - このメニューには、転送速度 (読み取り専用) が表示されます。また、マップの詳細、ステータス (読み取り専用であるかどうか)、経過時間、読み取り/書き込みバイト数など、CD/DVD およびリムーバブル ディスクの詳細情報が表示されます。
  - **イメージの作成** - このメニューを使用して、ローカル フォルダーを選択し、ローカル フォルダーのコンテンツを含む FolderName.img ファイルを生成することができます。

メモ: セキュリティ上の理由から、eHTML5 による仮想コンソールへのアクセス時は読み取り/書き込みアクセスが無効になります。Java または ActiveX プラグインを使用すると、プラグインに読み取り / 書き込み権限が付与される前にセキュリティメッセージを受信することができます。

対応ブラウザ

eHTML5 仮想コンソールは次のブラウザーでサポートされています。

- Internet Explorer 11
- Chrome 78/79
- Firefox 70/71
- Safari 13.1

メモ: 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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC リリース ノート*』を参照してください。

HTML5 ベースの仮想コンソール

メモ: 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、およびブラウザで同じ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、**プラグイン タイプ** オプションを HTML5 に設定する必要があります。

仮想コンソールは、次のいずれかの方法を使用することによって、ポップアップウィンドウとして起動することができます。

- iDRAC ホーム ページから、コンソール プレビュー セッションで使用可能な**仮想コンソールの起動**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**リンクをクリックします。
- 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ます。

HTML5 の仮想コンソールでは、次のメニューオプションを使用できます。

- 電源
- 起動
- 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ークをサーバに渡す) オプションは、HTML5 仮想コンソールではサポートされません。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。
  - 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
- Alt+F5
- Alt+F6
- Alt+F7
- Alt+F8
- Alt+F9
- Alt+F10
- Alt+F11
- Alt+F12
- PrntScrn
- Alt+PrntScrn
- F1
- 一時停止
- タブ
- Ctrl+Enter
- SysRq
- Alt+SysRq
- Win-P

○ 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。
- 保守
- 維持しない

適用 をクリックしてサーバーに選択された設定を適用します。

○ 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に選択された設定を適用します。

- **仮想クリップボード** - テキスト バッファーの切り取り/コピー/貼り付けが、仮想コンソールから iDRAC ホスト サーバーに対して行えます。ここでのホスト サーバーとなれるものには、BIOS、UEFI、OS プロンプトがあります。この操作は、クライアント コンピューターから 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。
  ○ ホスト サーバーのデスクトップの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。
  ○ vConsole で [**コンソール制御**] を選択します。
  ○ OS クリップボード バッファーからのコピーを、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。
  ○ [**クリップボードをホストに送信**] をクリックします。
  ○ 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 Datacenter ライセンスでのみ使用可能です。
- 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 バ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ーが貼り付けられた場合、iDRAC GUI の編集ボックスでは、最大バッファー サイズへの切り捨てが行われます。

- **キーボード** - 物理キーボードと仮想キーボードの違いは、仮想キーボードはブラウザーの言語に従ってレイアウトを変更することです。
- 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に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。
  - 絶対座標（Windows、Linux の最新バージョン、Mac OS-X）
  - 相対座標、アクセラレーションなし
  - 相対座標（RHEL、または Linux の旧バージョン）
  - Linux RHEL 6.x および SUSE Linux Enterprise Server 11 以降

  適用 をクリックしてサーバーに選択された設定を適用します。
- **仮想メディア** - **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。仮想メディアが接続されている場合は、CD/DVD のマップ、リムーバブル ディスクのマップ、および USB のリセットなどのオプションを確認できます。

メモ: セキュリティ上の理由から、HTML5 による仮想コンソールへのアクセス時は読み取り / 書き込みアクセスが無効になります。Java または ActiveX プラグインを使用すると、プラグインに読み取り / 書き込み権限が付与される前にセキュリティメッセージを受信することができます。

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 78/79
- Firefox 70/71
- Safari 13.1

メモ: 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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC リリース ノート*』を参照してください。

マウスポインタの同期

仮想コンソールを介して管理下システムに接続すると、管理下ステムのマウスの加速度が管理ステーションのマウスポインタと同期されず、ビューアのウィンドウに 2 つのマウスポインタが表示される場合があります。

Red Hat Enterprise Linux または Novell SUSE Linux を使用する場合、仮想コンソールビューアを起動する前に、Linux のマウスモードを設定します。オペレーティングシステムのデフォルトマウス設定が、仮想コンソールビューアにおけるマウス矢印の制御に使用されます。

クライアント仮想コンソールビューアに 2 つのマウスカーソルが表示される場合、サーバ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を示します。これは、Linux オペレーティングシステムまたは Lifecycle Controller でよく起こる現象で、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設定と異なる場合に 2 つのマウスカーソルが表示されます。この問題を解決するには、シングルカーソルに切り替えるか、管理下システムと管理ステーション上でマウスの加速を一致させます。

- シングルカーソルに切り替えるには、**ツール** メニューから **シングルカーソル** を選択します。
- マウス加速を設定するには、**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。

シングルカーソルモードを終了するには、<F9>、または設定した終了キーを押します。

メモ: Windows オペレーティングシステムを実行している管理下システムは絶対位置をサポートしているため、これは適用されません。

仮想コンソールを使用して、最新の Linux 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。iDRAC 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/peripherals/mouse/%gconf.xml** ファイルで、さらに次の変更を行います。

`motion_threshold` および `motion_acceleration` の値を `-1` に変更します。

GNOME デスクトップでマウス加速をオフにした場合、仮想コンソールビューアで、**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排他的アクセスについては、ローカルコンソールを無効化し、**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 のプラグイ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アを介して管理ステーションから管理下システムに送信できます。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アで、**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プラグインタイプ (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 (単一カーソル) モードを動作させるには、ネイティブライブラリをロードする必要があります。ネイティブライブラリが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 (シングルカーソル)** オプションは選択解除されています。いずれかのオプションを選択しようとすると、選択したオプションはサポートされていないことを示すエラーメッセージが表示されます。

  ActiveX クライアントの場合、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ライブラリをロードする必要があります。ネイティブライブラリが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)** オプションは選択解除されています。このオプションを選択しようとすると、この機能がサポートされていないことを示すエラーメッセージが表示されます。

  MAC オペレーティングシステムの場合、すべてのキーストロークをサーバーに渡す機能を動作させるためには、**ユニバーサルアクセス** 内の **補助装置にアクセスできるようにする** オプションを有効にします。

- 管理ステーションおよび管理下システムで実行されているオペレーティングシステム。管理ステーションのオペレーティングシステムにとって意味のあるキーの組み合わせは、管理下システムに渡されません。
- 仮想コンソールビューアモード — ウィンドウ表示または全画面表示。

  全画面モードでは、**すべてのキーストロークをサーバーに渡す** がデフォルトで有効になっています。

  ウィンドウモードでは、仮想コンソールビューアが表示されてアクティブになっている場合にのみ、キーが渡されます。

  全画面モードからウィンドウモードに変更すると、すべてのキーを渡す機能の以前の状態が再開されます。

Windows オペレーティングシステム上で動作する Java ベースの仮想コンソールセッション

- Ctrl+Alt+Del キーは、管理対象システムに送信されませんが、常に管理ステーションによって解釈されます。
- すべてのキーストロークをサーバーに渡す機能が有効な場合、次のキーは管理下システムに送信されません。
  - ブラウザの戻るキー

- ブラウザの進むキー
- ブラウザの更新キー
- ブラウザの停止キー
- ブラウザの検索キー
- ブラウザのお気に入りキー
- ブラウザの開始およびホームキー
- 音量をミュートするキー
- 音量を下げるキー
- 音量を上げるキー
- 次のトラックキー
- 前のトラックキー
- メディアの停止キー
- メディアの再生 / 一時停止キー
- メールの起動キー
- メディアの選択キー
- アプリケーション 1 の起動キー
- アプリケーション 2 の起動キー

- 個々のキー (異なるキーの組み合わせではなく、単一のキーストローク) はすべて、常に管理下システムに送信されます。これには、すべてのファンクションキー、Shift、Alt、Ctrl、および Menu キーが含まれます。これらのキーの一部は、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を有効にすると、<Ctrl+Alt+Del> が管理下システムのオペレーティングシステムに渡されます。
- マジック SysRq キーは、Linux カーネルによって認識されるキーの組み合わせです。管理ステーションまたは管理下システムのオペレーティングシステムがフリーズし、システムを回復する必要がある場合に便利です。次のいずれかの方法を使用して、Linux オペレーティングシステムのマジック SysRq キーを有効にできます。
  - **/etc/sysctl.conf** にエントリを追加する
  - echo "1" > /proc/sys/kernel/sysrq
- すべてのキーストロークをサーバに渡す機能を有効にすると、マジック SysRq キーが管理下システムのオペレーティングシステムに送信されます。オペレーティングシステムをリセット (つまり、アンマウントまたは同期なしで再起動) するキーシーケンスの動作は、管理ステーションでマジック SysRq が有効になっているか無効になっているかによって異なります。
  - 管理ステーションで SysRq が有効になっている場合は、システムの状態に関わらず、<Ctrl+Alt+SysRq+b> または <Alt+SysRq+b> によって管理ステーションがリセットされます。
  - 管理ステーションで SysRq が無効になっている場合は、<Ctrl+Alt+SysRq+b> または <Alt+SysRq+b> キーによって管理下システムのオペレーティングシステムがリセットされます。
  - その他の SysRq キーの組み合わせ (<Alt+SysRq+k>、<Ctrl+Alt+SysRq+m> など) は、管理ステーションで SysRq キーが有効になっているかどうかに関わらず、管理下システムに渡されます。

リモートコンソール経由での SysRq マジックキーの使用

SysRq マジックキー は、次のいずれかを使用してリモートコンソール経由で有効化することができます。

- Opensoure IPMI ツール
- SSH または外部シリアル コネクターの使用

オープンソース IPMI ツールの使用

BIOS/iDRAC 設定が SOL を使用したコンソールリダイレクトをサポートしていることを確認します。

1. コマンドプロンプトで、SOL をアクティブ化するコマンドを入力します。

```
Ipmitool –I lanplus –H <ipaddr> -U <username> -P <passwd> sol activate
```

   SOL セッションがアクティブ化されます。
2. サーバ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/kernel/sysrq を使用して有効にします。
4. ブレークシーケンス ~B を実行します。
5. SysRq マジックキーを使用して SysRq 機能を有効にします。たとえば、次のコマンドはコンソールにメモリ情報を表示します。

```
echo m > /proc/sysrq-trigger displays
```

SSH または外部シリアル コネクターの使用 (シリアル ケーブル経由で直接接続)

1. SSH セッションの場合は、iDRAC のユーザー名とパスワードを使用してログインした後、/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部シリアル コネクターを使用するコンソールのリダイレクトでは、サーバーがオペレーティング システムから起動した後、localhost.localdomain ログイン プロンプトが表示されます。
3. オペレーティングシステムのユーザー名とパスワードを使用してログインします。
4. SysRq が有効になっていない場合は、echo 1 >/proc/sys/kernel/sysrq を使用して有効にします。
5. SysRq 関数を有効にするには、マジック キーを使用します。例えば、次のコマンドを実行すると、サーバーが再起動します。

```
echo b > /proc/sysrq-trigger
```

   メモ: マジック SysRq キーを使用する前に、ブレークシーケンスを実行する必要はありません。

Windows オペレーティングシステム上で動作する ActiveX ベースの仮想コンソールセッション

Windows オペレーティングシステムで動作する ActiveX ベースの仮想コンソールセッションの すべてのキーストロークをサーバーに渡す機能の動作は、Windows 管理ステーションで実行されている Java ベースの仮想コンソールセッションで説明された動作に似ていますが、次の例外があります。

- すべてのキーを渡すが無効な場合、F1 を押すと、管理ステーションと管理下システムの両方でアプリケーションのヘルプが起動し、次のメッセージが表示されます。

  ```
  Click Help on the Virtual Console page to view the online Help
  ```

- メディアキーを明示的にブロックすることはできません。
- <Alt + Space>、<Ctrl + Alt + +>、<Ctrl + Alt + -> は管理下システムに送信されず、管理ステーション上のオペレーティングシステムによって解釈されます。

20

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 インターフェイス、Redfish、RACADM、WSMan など、iDRAC インターフェイスで使用可能な追加データを提供することによって、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ー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 とメモリーを制御できます。ホスト OS のコマンド ライン インターフェイスが導入されたことで、PSU を除くすべてのシステム コンポーネントについて、フル パワー サイクルのステータスの有効化と無効化が行えるようになりました。

メモ: iDRAC9 では iSM バージョン 3.01 以降を使用します。

メモ: iDRAC サービスモジュールは、iDRAC Express または iDRAC Enterprise ライセンスがインストールされている場合にのみ、有効にすることができます。

iDRAC サービスモジュールを使用する前に、以下を確認します。

- iDRAC サービスモジュールの各機能を有効または無効にするための、iDRAC におけるログイン、設定、およびサーバー制御権限を持っている。
- **ローカル RACADM を使った iDRAC 設定** オプションは無効にしないでください。
- OS から iDRAC へのパススルーチャネルが iDRAC 内の内部 USB バスによって有効化されている。

メモ: LC ワイプを実行しても、 `idrac.Servicemodule` で示される値が古い値のままであることがあります。

メモ:

- iDRAC サービスモジュールの初回実行時、デフォルトでは、モジュールは iDRAC で OS から iDRAC へのパススルーチャネルを有効にします。iDRAC サービスモジュールをインストールした後に、この機能を無効にする場合は、後で iDRAC で手動で有効にする必要があります。
- OS から iDRAC へのパススルーチャネルが iDRAC の LOM から有効にされている場合は、iDRAC サービスモジュールを使用できません。

トピック：

- iDRAC サービスモジュールのインストール
- iDRAC サービスモジュール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 Web インターフェイスからの 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

iDRAC サービスモジュールのインストール

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。

メモ: この機能は Dell Precision PR7910 システムには適用されません。

iDRAC Express および Basic からの iDRAC サービスモジュールのインストール

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。

1. サービスモジュールインストーラは、ホストオペレーティングシステムで利用でき、ジョブが iDRAC 内に作成されます。

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: インストーラ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 インストーラ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: インストーラ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/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。

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
- インバンド 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、https://www.dell.com/support/article/en-us/sln310557/dell-emc-idrac%E3%82%B5%E3%83%BC%E3%83%93%E3%82%B9-%E3%83%A2%E3%82%B8%E3%83%A5%E3%83%BC%E3%83%AB%E3%81%AE%E3%82%B5%E3%83%9D%E3%83%BC%E3%83%88?lang=ja を参照してください。

- リモートサーバのパワーサイクル

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 Web インターフェイス、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**オプションがターゲットとして選択されているすべてのイベント (**警告** ページ内、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 ログに含められるデフォルトのログのセットは、SNMP の警告またはトラップに設定されたものと同じです。

iDRAC サービスモジュールは、オペレーティングシステムが動作していない時に発生したイベントもログに記録します。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 syslog 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ラを使用して、Windows OS ログ内での Lifecycle Controller ログのレプリケーション場所を設定できます。場所の設定は、iDRAC サービスモジュールのインストール時、または iDRAC サービスモジュールインストーラの変更時に行うことができます。

OpenManage Server Administrator がインストールされている場合は、この監視機能は、OS のログ内の SEL エントリの重複を避けるために無効に設定されます。

メモ: Microsoft Windows では、アプリケーションログではなくシステムログに iSM イベントが記録される場合、Windows イベントログサービスを再起動するか、またはホスト OS を再起動します。

システムの自動リカバリオプション

自動システムリカバリ機能は、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が、電源スイッチがアクティブ化されたかのようにサーバがリセットされます。ASR は、継続的に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。この機能を有効にできるのは、オペレーティングシステムのウォッチドッグタイマーが無効になっている場合のみです。OpenManage Server Administrator がインストールされていると、この監視機能は、ウォッチドッグタイマーと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、サーバハードウェア、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) に基づいて 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 プロバイダーは、Microsoft System Center などのシステム管理コンソールとの統合に役立ち、Microsoft Windows サーバーを管理するためのスクリプト作成を可能にします。

iDRAC で WMI オプションを有効または無効にすることができます。iDRAC は、iDRAC サービスモジュールを通じて 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。クラスは、`root/cimv2/dcim` ネームスペースで公開されています。

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。

このコンテンツは、**DCIM_iDRACCardString** および **DCIM_iDRACCardInteger** クラスを使用して WMI 情報機能が iDRAC サービス モジュールに提供する機能を示しています。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。

以下にリストされた属性は、必要な権限を持つ**ユーザー アカウント**の設定に使用されます。

属性名	WSMAN-Class	権限	ライセンス	説明	サポートされる操作
ユーザー名	DCIM_iDRACCardString	**書き込み権限：**ユーザー構成、ログイン **読み取り権限：**Login	基本	16 ユーザー： Users.1#UserName ~ Users.16#UserName	Enum、Get、Invoke
パスワード	DCIM_iDRACCardString	**書き込み権限：**ユーザー構成、ログイン **読み取り権限：**ログイン	基本	Users.1#Password ~ Users.16#Password	Enum、Get、Invoke
権限	DCIM_iDRACCardInteger	**書き込み権限：**ユーザー構成、ログイン **読み取り権限：**ログイン	基本	Users.1#Password ~ Users.16#Password	Enum、Get、Invoke

- `Enumerate` または前述のクラスでの `Get` 操作によって、属性に関連するデータが提供されます。
- 属性を設定するには、 `ApplyAttribute` または `SetAttribute` コマンドを **DCIM_iDRACCardService** クラスから呼び出します。

メモ: DCIM_Account クラスが WSMAN から削除され、この機能は属性モデルを介して提供されます。**DCIM_iDRACCardString** および **DCIM_iDRACCardInteger** クラスには、iDRAC ユーザー アカウントを構成する同様のサポートが備わっています。

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 のリモートリセット操作を実行できます。iDRAC をリモートからリセットするには、ホスト OS の管理者権限が付与されているようにしてください。iDRAC のリモートハードリセット機能はデフォルトで有効になっています。iDRAC Web インターフェイス、RACADM、WSMan を使用して、iDRAC のリモート ハード リセットを実行することができます。

コマンドの使用方法

本項では、iDRAC のハードリセットを実行するための Windows、Linux、および ESXi のオペレーティングシステムに対するコマンドの使用方法を説明します。

- **Windows**
  - ローカル Windows Management Instrumentation (WMI) を使用する：

```
winrm  i  iDRACHardReset wmi/root/cimv2/dcim/DCIM_iSMService?InstanceID=”
iSMExportedFunctions”
```

- リモート WMI インタフェースを使用する：

```
winrm i iDRACHardReset wmi/root/cimv2/dcim/dcim_ismservice -u:<admin-username> -p:<admin-passwd> -r: http://<remote-hostname OR IP>/wsman -a:Basic -encoding:utf-8 -skipCACheck -skipCNCheck
```

- 強制的および非強制的に Windows PowerShell スクリプトを使用する：

```
Invoke-iDRACHardReset -force
```

```
Invoke-iDRACHardReset
```

- **プログラムメニュー** のショートカットを使用する：

  簡素化のために、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。

メモ: 次の警告メッセージが [**アプリケーション ログ**] カテゴリー下の [**イベント ビューア**] に表示されます。この警告に対し、これ以上の操作は必要はありません。

```
A provider, ismserviceprovider, has been registered in the Windows Management Instrumentation namespace Root\CIMV2\DCIM to use the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests.
```

- **Linux**

  iSM はすべての iSM 対応 Linux オペレーティングシステムで実行可能なコマンドを提供します。このコマンドは、SSH または同等のプロトコルを使用してオペレーティングシステムにログインすることによって実行できます。

```
Invoke-iDRACHardReset
```

```
Invoke-iDRACHardReset -f
```

- **ESXi**

  すべての iSM 対応 ESXi オペレーティングシステムにおいて、iSM v2.3 は、WinRM リモートコマンドを使用した iDRAC のリモートリセットを実行するための Common Management Programming Interface (CMPI) メソッドプロバイダをサポートします。

```
winrm i iDRACHardReset http://schemas.dell.com/wbem/wscim/1/cim-schema/2/root/cimv2/dcim/DCIM_iSMService?__cimnamespace=root/cimv2/dcim+InstanceID=iSMExportedFunctions -u:<root-username> -p:<passwd> -r:https://<Host-IP>:443/WSMan -a:basic -encoding:utf-8 -skipCNCheck -skipCACheck -skipRevocationcheck
```

メモ: VMware ESXi オペレーティングシステムは、iDRAC をリセットする前に確認のプロンプトを表示しません。

メモ: VMware ESXi 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。

表 59. エラー処理

結果	説明
0	成功
1	iDRAC リセット対応ではない BIOS バージョン
2	非対応プラットフォーム
3	アクセス拒否
4	iDRAC リセット失敗

iDRAC SNMP アラートのインバンド 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 マルチプレクシング (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。インバンド 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。

  iSM 2.4.0 からは、次のコマンドを使用して Agent-x をインバンド iDRAC SNMP アラートのデフォルト プロトコルとして設定できます。

  ```
  ./Enable-iDRACSNMPTrap.sh 1/agentx –force
  ```

  `–force` が指定されていない場合は、net-SNMP が設定され、snmpd サービスを再起動していることを確認します。

  - この機能を有効にするには、次の手順を実行します。

    ```
    Enable-iDRACSNMPTrap.sh 1
    ```

    ```
    Enable-iDRACSNMPTrap.sh enable
    ```

  - この機能を無効にするには、次の手順を実行します。

    ```
    Enable-iDRACSNMPTrap.sh 0
    ```

    ```
    Enable-iDRACSNMPTrap.sh disable
    ```

  メモ: **--force** オプションは、トラップを転送するように Net-SNMP を設定します。ただし、トラップ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。

```
winrm i EnableInBandSNMPTraps http://schemas.dell.com/wbem/wscim/1/cim-schema/2/root/cimv2/dcim/DCIM_iSMService?__cimnamespace=root/cimv2/dcim+InstanceID=iSMExportedFunctions -u:<user-name> -p:<passwd> -r:https://<remote-host-name
```

```
ip-address>:443/WSMan -a:basic -encoding:utf-8 -skipCNCheck -skipCACheck -skipRevocationcheck @{state="[0/1]"}
```

メモ: トラップに対する VMware ESXi システム全体の SNMP 設定を見直し、設定する必要があります。

メモ: 詳細については、https://www.dell.com/support にあるテクニカル ホワイト ペーパー『**インバンド 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 Web インターフェイス、WSMan、RedFish インターフェイスを介して、ハードウェア パラメーターを設定およびモニタリングできます。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。

- webpack を使用して iDRAC アクセス機能をインストールする。
- iSM PowerShell スクリプトを使用して設定する。

MSI を使ったインストール

この機能は、webpack 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 はインバウンドファイアウォールルールの OS2iDRAC を作成します。リスニングポート番号が、ホストオペレーティングシステムの OS2iDRAC ファイアウォールルールに追加され、受信接続を可能にします。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ート設定を回復できます。

```
Enable-iDRACAccessHostRoute -status get
```

このコマンドの出力は、この機能が有効か無効かを示します。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: この機能を機能させるには、お使いのシステムで Microsoft IP ヘルパーサービスが実行されてることを確認してください。

iDRAC Web インターフェイスにアクセスするには、ブラウザーで `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 Web インターフェイス、WSMan、RACADM インターフェイスから、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。

メモ: この機能は IPv4 アドレスのみをサポートします。

Linux オペレーティングシステム経由の iDRAC アクセス

この機能は、webpack で利用可能な `setup.sh` ファイルを使用してインストールできます。この機能は、デフォルトまたは通常の iSM インストール済み環境では無効になっています。この機能のステータスを取得するには、次のコマンドを使用します。

```
Enable-iDRACAccessHostRoute get-status
```

この機能をインストール、有効化、設定するには、次のコマンドを使用します。

```
./Enable-iDRACAccessHostRoute <Enable-Flag> [ <source-port> <source-IP-range/source-ip-range-mask>]
```

<Enable-Flag>=0

無効

<source-port>および<source-IP-range/source-ip-range-mask>は必須ではありません。

<Enable-Flag>=1

有効化

<source-port>は必須、<source-ip-range-mask>はオプションです。

<source-IP-range>

IP 範囲は *<IP-Address/subnet-mask>* 形式です。例：10.95.146.98/24

OpenManage Server Administrator と iDRAC サービスモジュールの共存

システムで、OpenManage Server Administrator と iDRAC サービスモジュールの両方を共存させて、正常かつ個別に機能させることができます。

iDRAC サービスモジュールのインストール中に監視機能を有効にした場合、インストールが完了した後に iDRAC サービスモジュールが OpenManage Server Administrator の存在を検出すると、iDRAC サービスモジュールは重複している監視機能一式を無効にします。OpenManage Server Administrator が実行されている場合、iDRAC サービスモジュールは、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 Web インターフェイスからの iDRAC サービス モジュールの使用

iDRAC Web インターフェイスから iDRAC サービス モジュールを使用するには、次の手順を実行します。

1. **iDRAC 設定** > **概要** > **iDRAC サービス モジュール** > **サービス モジュールの設定**の順に移動します。
   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、すべてエラーが表示され

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 システムのログに含めるようにします。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ー動作を実行します。
     - **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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

21

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 インターフェイスを使用してシステムに接続し、iDRAC Web インターフェイスや RACADM などのシステム管理ツールにアクセスします。
- USB ドライブに保存されている 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 ドライブ上のサーバ設定ファイル（SCP）のインポートによるサーバの設定を行うには、システム制御権限が必要です。

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 ドライブ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。

  メモ: USB ドライブに有効な SCP ファイルが含まれていることを確認します。

  メモ: タイプ A から Micro-B USB に変換するには、OTG アダプタを使用します。USB ハブからの接続はサポートされていません。
- **iDRAC 管理対象：USB SCP**— USB ドライブに保存されている 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 Web インターフェイス
  - **圧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。

    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。
  - **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 デバイスのサーバー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。

サポート対象ブ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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC リリース ノート*』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. 300」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. ウェブインタフェース、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。
たとえば、iDRAC ウェブインタフェースにアクセスするには、サポートされているブラウザを開いて、アドレス *169.254.0.3* を入力し、Enter キーを押します。
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。
LED が消灯します。

USB デバイスのサーバー設定プロファイルを使用した iDRAC の設定

新しい iDRAC USB 管理ポートを使用すると、iDRAC をサーバ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。

メモ: サーバーに DRAC デバイスが接続されていない場合にのみ、DRAC インタフェースを使用して USB 管理ポートを設定できます。

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に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 **オン** 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は、**システムインベントリ** ページの ハードウェアインベントリ セクションの下に、その USB デバイスの情報が表示されます。

以下の場合は、イベントが Lifecycle Controller ログに記録されます。
- USB デバイスが自動または iDRAC モードのときに、デバイスが挿入されたか取り外された。
- USB 管理ポートのモードが変更された。
- デバイスが iDRAC から OS に自動的に切り替えられます。
- デバイスは iDRAC または OS から除外されました

デバイスが USB 仕様で許可されている電源要件を超えると、デバイスは切り離され、次のプロパティを含む過電流イベントが生成されます。
- カテゴリ：システム正常性
- タイプ：USB デバイス
- 重大度：警告
- 通知許可：電子メール、SNMP トラップ、リモート syslog および WS-Eventing
- アクション：なし

エラーメッセージが表示され、次のような場合には Lifecycle Controller ログに記録されます。
- サーバー制御ユーザの権限なしで、USB 管理ポートを設定しようとした場合。
- USB デバイスが iDRAC で使用されており、USB 管理ポートのモードを変更しようとした場合。
- USB デバイスが iDRAC で使用されているときにデバイスを取り外した。

ウェブインタフェースを使用した USB 管理ポートの設定

USB ポートを設定するには、次の手順を実行します。
1. iDRAC ウェブインタフェースで、**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 ドライブ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**
   - **サーバーにデフォルト資格情報があるときにのみ有効**
   - **圧縮された設定ファイルにのみ有効**
   - **有効**

フィールドについては、『iDRAC オンラインヘルプ』を参照してください。

メモ: 圧縮された設定ファイルをインポートする前に圧縮するため、iDRAC9 では、有効 を選択した場合にのみ、圧縮されたファイルをパスワードで保護できます。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。

4. 設定を適用するには、**適用** をクリックします。

RACADM を使用した USB 管理ポートの設定

USB 管理ポートを設定するには、次の RACADM サブコマンドおよびオブジェクトを使用します。

- USB ポートのステータスを表示するには、次のコマンドを使用します。

```
racadm get iDRAC.USB.PortStatus
```

- USB ポートの設定を表示するには、次のコマンドを使用します。

```
racadm get iDRAC.USB.ManagementPortMode
```

- USB デバイスのインベントリを表示するには、次のコマンドを使用します。

```
racadm hwinventory
```

- 過電流アラート設定をセットアップするには、次のコマンドを使用します。

```
racadm eventfilters
```

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

iDRAC 設定ユーティリティを使用した USB 管理ポートの設定

USB ポートを設定するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**メディアおよび USB ポートの設定** に移動します。
   iDRAC 設定：メディアおよび USB ポートの設定 ページが表示されます。
2. **iDRAC ダイレクト：USB 設定 XML** ドロップダウンメニューからオプションを選択し、USB ドライブ上に保存されているサーバー設定プロファイルをインポートしてサーバーを設定します。
   - **無効**
   - **サーバーにデフォルト資格情報があるときにのみ有効**
   - **圧縮された設定ファイルにのみ有効**
   - **有効**

   各フィールドについては、『iDRAC 設定ユーティリティオンラインヘルプ』を参照してください。
3. **戻る**、**終了** の順にクリックし、**はい** をクリックして設定を適用します。

USB デバイスからのサーバー設定プロファイルのインポート

必ず USB デバイスのルートに `System_Configuration_XML` というディレクトリーを作成し、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 ディレクトリーの下の `System_Configuration_XML` サブディレクトリーにあります。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、サーバー上の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`、`<modelnumber>-config.json`、`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

control.xml ファイルの例を次に示します。

```
<InstructionTable>
  <InstructionRow>
     <InstructionType>Configuration XML import Host control Instruction
     </InstructionType>
     <Instruction>ShutdownType</Instruction>
     <Value>NoReboot</Value>
     <ValuePossibilities>Graceful,Forced,NoReboot</ValuePossibilities>
  </InstructionRow>
  <InstructionRow>
     <InstructionType>Configuration XML import Host control Instruction
     </InstructionType>
     <Instruction>TimeToWait</Instruction>
     <Value>300</Value>
     <ValuePossibilities>Minimum value is 300 -Maximum value is
      3600 seconds.</ValuePossibilities>
  </InstructionRow>
  <InstructionRow>
     <InstructionType>Configuration XML import Host control Instruction
     </InstructionType>
     <Instruction>EndHostPowerState</Instruction>
     <Value>On</Value>
     <ValuePossibilities>On,Off</ValuePossibilities>
  </InstructionRow>
</InstructionTable>
```

この操作を実行するには、サーバー制御の権限を持っている必要があります。

メモ: 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 ディレクトリーの下にある System_Configuration_XML サブディレクトリーにあります。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なっている場合にのみ、[**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。

22

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に簡単にアクセスできます。これにより、サーバ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、修復アクションの実行を必要に応じて行えます。また、サーバ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、これはハードウェア アップセルであり、機能は iDRAC ソフトウェア ライセンスとは関係ありません。

メモ: MX プラットフォーム システムで Quick Sync 2 を設定する方法の詳細については、**dell.com/support/manuals** で入手できる『*OpenManage Enterprise Modular ユーザーズ ガイド*』および『*OpenManage Mobile ユーザーズ ガイド*』を参照してください。

iDRAC Quick Sync 2 の設定手順：

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、https://www.dell.com/openmanagemanuals から入手可能な『*Dell EMC OpenManage Mobile ユーザーズ ガイド*』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 秒です。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。オンにするには、アクティブ化ボタンを再度押します。
  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を許可しません。

- [**読み取り認証**] — 有効に設定されています。これはデフォルト オプションです。
- [**WiFi**] — 有効に設定されています。これはデフォルト オプションです。

これらの設定を構成するには、サーバー制御権限が必要です。設定を有効にするためにサーバーを再起動する必要はありません。設定が完了したら、左コントロール パネルにある Quick Sync 2 ボタンをアクティブにすることができます。Quick Sync のライトが点灯していることを確認します。次に、モバイル デバイスから Quick Sync 情報にアクセスします。

設定が変更された場合は、Lifecycle Controller ログにエントリが記録されます。

ウェブインタフェースを使用した iDRAC Quick Sync 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 (設定)** > **System Settings (システム設定)** > **Hardware Settings (ハードウェア設定)** > **iDRAC Quick Sync (iDRAC Quick Sync)** の順に移動します。
2. **iDRAC Quick Sync (iDRAC Quick Sync)** セクションで、**Access (アクセス)** メニューから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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

iDRAC 設定ユーティリティを使用した iDRAC Quick Sync 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 (設定)** > **Systems Settings (システム設定)** > **Hardware Settings (ハードウェア設定)** > **iDRAC Quick Sync** 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、https://www.dell.com/openmanagemanuals から入手可能な『*Dell EMC OpenManage Mobile ユーザーズ ガイド*』を参照してください。

23

仮想メディアの管理

iDRAC では、HTML5 ベースのクライアントで仮想メディアを提供し、ローカルの ISO および IMG ファイル、リモートの ISO および IMG ファイルをサポートしています。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。設定を変更するには、「iDRAC 構成」権限が必要です。

構成可能な属性は次のとおりです。

- 連結メディアの有効化 - 有効/無効
- 連結モード - 自動連結、連結、分離
- 最大セッション数 - 1
- アクティブ セッション数 - 1
- 仮想メディアの暗号化 - 有効 (デフォルト)
- フロッピーのエミュレーション - 無効 (デフォルト)
- 一回のみの起動 - 有効/無効
- 接続ステータス - 接続/切断

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、仮想光学ドライブ (CD/DVD) および USB フラッシュ ドライブをサポートします。
- 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。

- 接続された仮想メディアは、管理下システム上の物理デバイスをエミュレートします。
- Windows ベースの管理下システムでは、仮想メディア ドライブを接続してドライブ レターを設定した場合、自動マウントされます。
- 複数の設定からなる Linux ベースの管理システムでは、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。
- 管理下システムからのすべての仮想ドライブアクセス要求は、ネットワークを介して管理ステーションに送信されます。
- 仮想デバイスは、管理下システムで 2 つのドライブとして表示されます (ドライブにはメディアが取り付けられません)。
- 2 つの管理下システム間で管理ステーションの CD/DVD ドライブ (読み取り専用) を共有できますが、USB メディアを共有することはできません。
- 仮想メディア は 128 Kbps 以上のネットワーク帯域幅を必要とします。
- LOM または NIC フェールオーバーが発生した場合は、仮想メディア セッションを切断できません。

仮想コンソールを用いた仮想メディア イメージの接続後、ドライブが 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、ドライバーをアップデートするかまたはドライバー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。

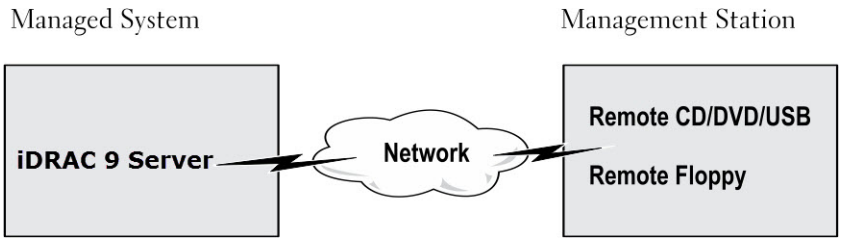


図 4. 仮想メディアセットアップ

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。

表 60. 対応ドライブとデバイス

ドライブ	対応ストレージメディア
仮想光学ドライブ	• CD-ROM • DVD • CD-RW • コンビネーションドライブ (CD-ROM メディア)
USB フラッシュドライブ	• CD-ROM メディアのある USB CD-ROM ドライブ • ISO9660 フォーマットの USB キーイメージ

仮想メディアの設定

仮想メディアを設定する前に、ウェブブラウザが Java または ActiveX プラグインを使用するように設定されていることを確認してください。

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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

iDRAC 設定ユーティリティを使用した仮想メディアの設定

iDRAC 設定ユーティリティを使用すると、仮想メディアの連結、連結解除、自動連結を行うことがきます。この操作を行うには、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 61. 連結されたメディアの状態とシステムの応答

連結されたメディアの状態	システム応答
分離	イメージをシステムにマップできません。
連結	メディアは、**クライアントビュー** が閉じられている場合であってもマップされます。
自動連結	メディアは、**クライアントビュー** が開いている場合にはマップされ、**クライアントビュー** が閉じている場合にはマップ解除されます。

仮想メディアで仮想デバイスを表示するためのサーバー設定

空のドライブを認識できるようにするには、管理ステーションで次の設定項目を設定する必要があります。これを行うには、Windows 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 **Hile 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、しないに関わりなくアクセスすることができます。仮想メディアにアクセスする前に、ウェブブラウザを設定するようにしてください。

仮想メディアと RFS は相互排他的です。RFS 接続がアクティブであるときに仮想メディアのクライアントの起動を試みると、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

仮想コンソールを介して仮想メディアを起動する前に、次を確認してください。

- 仮想コンソールが有効になっている。
- システムが、空のドライブを表示するように設定されている - Windows エクスプローラで、**フォルダオプション** に移動し、**空のドライブはコンピューターフォルダに表示しない** オプションをクリアして、**OK** をクリックします。

仮想コンソールを使用して仮想メディアにアクセスするには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**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。
   仮想コンソールビューア が起動します。

メモ: Linux では、Java が仮想コンソールへのアクセスのためのデフォルトのプラグインタイプです。Windows では、.jnlp ファイルを開いて Java を使用して、仮想コンソールを起動します。

3. **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。
   仮想メディアセッションが確立され、**仮想メディア** メニューにマッピングに利用可能なデバイスのリストが表示されます。

   メモ: 仮想メディアにアクセスしている間は、**仮想コンソールビューア** ウィンドウがアクティブな状態である必要があります。

仮想コンソールを使用しない仮想メディアの起動

仮想コンソールが無効になっているときに仮想メディアを起動する前に、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とを確認します。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。

または、次の手順に従って仮想メディアを起動することもできます。

1. **設定** > **仮想コンソール**の順に移動します。
2. **仮想コンソールの起動** をクリックします。次のメッセージが表示されます。

```
Virtual Console has been disabled. Do you want to continue using Virtual Media redirection?
```

3. **OK** をクリックします。**仮想メディア** ウィンドウが表示されます。
4. **仮想メディア** メニューから **CD/DVD のマップ** または、**リムーバブルディスクのマップ** をクリックします。詳細については、「仮想ドライブのマッピング」を参照してください。
5. **仮想メディア統計情報**には、ターゲットドライブ、それらのマッピング、ステータス（読み取り専用であるかないか）、接続時間、読み取り/書き込みバイト数、転送速度のリストが表示されます。

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

メモ: Internet Explorer セキュリティ強化が設定された 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応するエントリは動作しません。このため、*image（イメージ）*の使用中に **.img** ファイルを移動したり、削除したりすることは推奨されません。ただし、**.img** ファイルは、最初に関連するエントリが選択解除され、エントリを削除する **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。

ドライバーへのアクセス

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 ドライバーがすべて搭載されています。iDRAC を使用すると、ドライバー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。

ドライバー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ー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. 仮想コンソールビューアで、**ツール** > **統計** をクリックします。
   統計 ウィンドウが表示されます。
2. **仮想メディア** 下で、**USB のリセット** をクリックします。
   USB 接続をリセットすると、仮想メディア、キーボード、マウスを含むターゲットデバイスへのすべての入力に影響を与える可能性があることを警告するメッセージが表示されます。
3. **Yes**（はい）をクリックします。
   USB がリセットされます。

   メモ: iDRAC ウェブインタフェースセッションからログアウトしても、iDRAC 仮想メディアは終了しません。

仮想ドライブのマッピング

仮想ドライブをマップするには、次の手順を実行します。

メモ: ActiveX 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）をマップするには、管理者権限が必要です。ドライブをマップするには、IE を管理者として起動するか、iDRAC の IP アドレスを信頼済みサイトのリストに追加します。

1. 仮想メディアセッションを確立するには、**仮想メディア** メニューから **仮想メディアの接続** をクリックします。
   ホストサーバーからのマップに使用できる各デバイスのために、**仮想メディア** メニュー下にメニューアイテムが表示されます。メニューアイテムは、次にあるようにデバイスタイプに従って命名されています。
   - CD/DVD をマップ
   - リムーバブルディスクのマップ

   CD/DVD のマップ オプションは ISO ファイル用に使用することができ、**リムーバブルディスクのマップ** オプションをイメージに使用することができます。

メモ:
- HTML5 ベースの仮想コンソールを使用して USB ベースのドライブ、CD または DVD などの物理メディアをマップすることはできません。
- 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。
- eHTML リムーバブル メディアに NTFS 形式の物理メディアをマップすることはできません。FAT または exFAT デバイスを使用してください。

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 Web インターフェイス セッション、別の Web インターフェイス セッションからアクティブであるかどうかを表示します。

3. **ドライブ / イメージファイル** フィールドで、ドロップダウンリストからデバイスを選択します。

リストには、マッピングが可能な (マップされていない) デバイス (CD/DVD とリムーバブル 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 ディスクでは IMG です。

イメージをデフォルトのパス (デスクトップ) に作成した場合、**リムーバブルディスクをマップ** を選択すると、作成したイメージをドロップダウンメニューから選択できるようになります。

別の場所にイメージを作成した場合、**リムーバブル ディスクをマップ**を選択しても、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ません。**参照**をクリックして、イメージを指定してください。

メモ:
- **読み取り専用**オプションは、eHTML5 ベースの JAVA リムーバブル メディアではグレー表示になります。
- フロッピーのエミュレーションは eHTML5 プラグインではサポートされていません。

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/ファイルのマップ後、デバイス名を示すためにその**仮想メディア**メニュー アイテムの名前が変わります。たとえば、CD/DVD デバイスが `foo.iso` という名前のイメージ ファイルにマップされた場合、[仮想メディア] メニューの CD/DVD メニュー アイテムは、**CD/DVD にマップされた foo.iso** という名前になります。そのメニューアイテムのチェックマークは、それがマップされていることを示します。

マッピング用の正しい仮想ドライブの表示

Linux ベースの管理ステーションでは、仮想メディアの**クライアント**ウィンドウに管理ステーションの一部ではないリムーバブル ディスクが表示されることがあります。正しい仮想ドライブをマップ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. 管理ステーションでオペレーティング システムを再起動します。POST 中に < F2 > を押して、**システム セットアップ**を起動します。
2. **SATA 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**クライアント**ウィンドウにアクセスします。マップできる適切な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。
そのメニューア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 に連結されている 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、次を確認してください。

- *ユーザーの設定* 権限がある。
- 仮想メディアのオプションを使用して、ローカルまたは仮想ドライブ（CD/DVD、フロッピー、または USB フラッシュデバイス）をブータブルメディアまたはイメージにマップする。
- 起動順序に仮想ドライブが表示されるように、仮想メディアが *連結* 状態になっている。

一回限りの起動オプションを有効にし、仮想メディアから管理下システムを起動するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**概要** > **サーバー** > **連結されたメディア** と移動します。
2. **仮想メディア** で **一回限りの起動の有効化** を選択し、**適用** をクリックします。
3. 管理下システムの電源を入れて、起動中に **<F2>** を押します。
4. リモート仮想メディアデバイスから起動するように、起動順序を変更します。
5. サーバーを再起動します。
管理下システムが 1 回だけ仮想メディアから起動します。

24

vFlash SD カードの管理

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: SD カードのサイズ制限はなく、工場出荷時に取り付けられた SD カードを交換して、より大容量の SD カードにすることができます。vFlash は FAT32 ファイル システムを使用しているため、ファイル サイズは 4 GB までに制限されます。

システムの vFlash SD カード スロットにカードがない場合は、**概要** > **サーバー** > **vFlash** の iDRAC Web インターフェイスに次のエラー メッセージが表示されます。

```
SD card not detected. Please insert an SD card of size 256MB or greater.
```

メモ: iDRAC vFlash カード スロットには、vFlash 互換の SD カードのみを挿入するようにしてください。互換性のない SD カードを挿入すると、カードの初期化の際に「*SD カードの初期化中にエラーが発生しました*」というエラー メッセージが表示されます。

主な機能は次のとおりです。

- ストレージ容量を提供し、USB デバイスをエミュレートします。
- 最大 16 のパーティションを作成します。連結されると、これらのパーティションは、選択したエミュレーション モードに応じて、フロッピー ドライブ、ハード ディスク ドライブ、または CD/DVD ドライブとしてシステムに表示されます。
- パーティションの作成を、サポートされるファイル システムのタイプで行います。フロッピー用に **.img** フォーマット、CD/DVD 用に **.iso** フォーマット、およびハード ディスク エミュレーション タイプ用に **.iso** および **.img** フォーマットの両方がサポートされています。
- 起動可能な USB デバイスを作成します。
- エミュレートされた USB デバイスから一度だけ起動します。

  メモ: vFlash の利用中に、vFlash ライセンスが期限切れになる可能性もあります。そうした場合でも、進行中の vFlash オペレーションは正常に完了されます。

メモ: FIPS モードが有効の場合は、vFlash 操作を実行できません。

トピック：

- vFlash SD カードの設定
- vFlash パーティションの管理

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、https://www.dell.com/poweredgemanuals から入手可能な『*設置およびサービス マニュアル*』を参照してください。

メモ: vFlash 機能を有効または無効にしたり、カードを初期化したりするには、仮想メディアへのアクセス権限を持っている必要があります。

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、次のオブジェクトで `get` コマンドを使用します。

- iDRAC.vflashsd.AvailableSize
- iDRAC.vflashsd.Health
- iDRAC.vflashsd.Licensed
- iDRAC.vflashsd.Size
- iDRAC.vflashsd.WriteProtect

これらのオブジェクトの詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

iDRAC 設定ユーティリティを使用した vFlash SD カードプロパティの表示

vFlash SD カードのプロパティを表示するには、**iDRAC 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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

iDRAC 設定ユーティリティを使用した vFlash SD カードの初期化

iDRAC 設定ユーティリティを使用して vFlash SD カードを初期化するには、次の手順を実行します。

1. iDRAC 設定ユーティリティで、**メディアおよび USB ポートの設定** に移動します。
   iDRAC 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 SSH またはシリアル コンソールを開き、ログインします。
2. `racadm vFlashsd status` コマンドを入力します。
   SD カードに送信されたコマンドのステータスが表示されます。

3. すべての vflash パーティションの最後のステータスを取得するには、`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後のステータスを取得するには、`racadm vflashpartition status -i (index)` コマンドを使用します。

   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）** 権限が必要です。

- 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*または*ハードディスク*タイプのパーティションを作成できます。パーティションタイプ CD は、イメージを使ったパーティションの作成中にのみサポートされます。

空のパーティションを作成する前に、次を確認してください。

- **仮想メディアへのアクセス** 権限を持っている。
- カードが初期化されている。
- カードが書き込み禁止になっていない。
- カード上で初期化が実行中ではない。

ウェブインタフェースを使用した空のパーティションの作成

空の vFlash パーティションを作成するには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**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。

- パーティションサイズとして非整数値が入力された、入力値がカード上で利用可能な容量を超えている、または 4 GB を超えている。
- カード上で初期化が実行中。

RACADM を使用した空のパーティションの作成

空のパーティションを作成するには、次の手順を実行します。

1. 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ー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 (**.img**)、ハードディスク (**.img**)、または CD (**.iso**) のエミュレーションタイプです。作成され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と問題になります。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。フロッピーまたはハードディスクエミュレーションタイプには、読み取り / 書き込みパーティションが作成されます。次の場合には、エラーメッセージが表示されます。
   - カードが書き込み禁止になっている。
   - ラベル名が既存のパーティションのラベルに一致する。

- イメージファイルのサイズが 4 GB を超えるか、カード上の空き容量を超えている。
- イメージファイルが存在しないか、拡張子が .img または .iso ではない。
- カード上で初期化がすでに実行中である。

RACADM を使用したイメージファイルからのパーティションの作成

RACADM を使用してイメージファイルからパーティションを作成するには、次の手順を実行します。

1. SSH またはシリアル コンソールを使用してシステムにログインします。
2. コマンドを入力します。

```
racadm vflashpartition create -i 1 -o drive1 -e HDD -t image -l //myserver/sharedfolder/
foo.iso -u root -p mypassword
```

デフォルトでは、作成され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。

```
-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)** の順に移動します。**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 SSH またはシリアル コンソールを開き、ログインします。
2. 次のコマンドを入力します。
   - すべての既存パーティションおよびそのプロパティを一覧表示する場合

     ```
     racadm vflashpartition list
     ```

   - パーティション 1 上での動作ステータスを取得する場合

     ```
     racadm vflashpartition status -i 1
     ```

   - すべての既存パーティションのステータスを取得する場合

     ```
     racadm vflashpartition status -a
     ```

   メモ: -a オプションは、ステータス処置と併用する場合に限り有効です。

パーティションの変更

読み取り専用パーティションを読み取り / 書き込みパーティションに変更したり、その逆を行うことができます。パーティションを変更する前に、次を確認してください。

- vFlash 機能が有効になっている。
- **仮想メディアへのアクセス** 権限がある。

メモ: デフォルトでは、読み取り専用パーティションが作成されます。

ウェブインタフェースを使用したパーティションの変更

パーティションを変更するには、次の手順を実行します。

1. 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。
   パーティションの管理 ページが表示されます。
2. **読み取り専用** 列で、次の操作を行います。
   - パーティションのチェックボックスを選択し、**適用** をクリックして読み取り専用に変更します。
   - パーティションのチェックボックスのチェックを外し、**適用** をクリックして読み取り / 書き込みに変更します。

     選択内容に応じて、パーティションは読み取り専用または読み取り / 書き込みに変更されます。

     メモ: パーティションが CD タイプの場合、状態は読み取り専用です。この状態を読み取り / 書き込みに変更することはできません。パーティションが連結されている場合、チェックボックスはグレー表示になっています。

RACADM を使用したパーティションの変更

カード上の使用可能なパーティションとそれらのプロパティを表示するには、次の手順を実行します。

1. SSH またはシリアル コンソールを使用してシステムにログインします。
2. 次の方法のいずれかを使用します。
   - `set` コマンドを使って、パーティションの読み取り/書き込み状態を変更します。

- 読み取り専用パーティションを読み取り / 書き込みに変更：

```
racadm set iDRAC.vflashpartition.<index>.AccessType 1
```

- 読み取り / 書き込みパーティションを読み取り専用に変更：

```
racadm set iDRAC.vflashpartition.<index>.AccessType 0
```

- set コマンドを使用して、エミュレーション タイプを指定します。

```
racadm set iDRAC.vflashpartition.<index>.EmulationType <HDD, Floppy, or CD-DVD>
```

パーティションの連結または分離

1 つ、または複数のパーティションを連結すると、これらのパーティションはオペレーティングシステムおよび BIOS によって USB 大容量ストレージデバイスとして表示されます。複数のパーティションを割り当てられたインデックスに基づいて連結すると、オペレーティングシステムおよび BIOS の起動順序メニューに昇順で一覧表示されます。

パーティションを分離すると、オペレーティングシステムおよび BIOS の起動順序メニューには表示されません。

パーティションを連結または分離すると、管理下システムの USB バスがリセットされます。これは vFlash を使用するアプリケーションに影響を及ぼし、iDRAC 仮想メディアセッションを切断します。

パーティションを連結または分離する前に、次を確認してください。

- vFlash 機能が有効になっている。
- カード上で初期化がすでに実行開始されていない。
- **仮想メディアへのアクセス** 権限を持っている。

ウェブインタフェースを使用したパーティションの連結または分離

パーティションを連結または分離するには、次の手順を実行します。

1. 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。
   パーティションの管理 ページが表示されます。
2. **連結** 列で、次の操作を行います。
   - パーティションのチェックボックスを選択し、**適用** をクリックしてパーティションを連結します。
   - パーティションのチェックボックスのチェックを外し、**適用** をクリックしてパーティションを分離します。

   パーティションは選択に基づいて連結または分離されます。

RACADM を使用したパーティションの連結または分離

パーティションを連結または分離するには、次の手順を実行します。

1. SSH またはシリアル コンソールを使用してシステムにログインします。
2. 次のコマンドを使用します。
   - パーティションを連結：

```
racadm set iDRAC.vflashpartition.<index>.AttachState 1
```

   - パーティションを分離：

```
racadm set iDRAC.vflashpartition.<index>.AttachState 0
```

連結されたパーティションに対するオペレーティングシステムの動作

Windows および Linux オペレーティングシステムの場合は、次のように動作します。

- オペレーティングシステムは連結されたパーティションを制御し、ドライブ文字を割り当てます。
- 読み取り専用パーティションは、オペレーティングシステムでは読み取り専用ドライブとなります。

- オペレーティングシステムは連結されたパーティションのファイルシステムをサポートしている必要があります。サポートしていない場合、オペレーティングシステムからパーティションの内容の読み取りや変更を行うことはできません。たとえば、Windows 環境では、Linux 固有のパーティションタイプ EXT2 を読み取ることはできません。また、Linux 環境では、Windows 固有のパーティションタイプ NTFS を読み取ることはできません。
- vFlash パーティションのラベルは、エミュレートされた USB デバイス上のファイルシステムのボリューム名とは異なります。エミュレートされた USB デバイスのボリューム名はオペレーティングシステムから変更できますただし、iDRAC で保存されているパーティションラベル名は変更されません。

既存のパーティションの削除

既存のパーティションを削除する前に、次を確認してください。
- vFlash 機能が有効になっている。
- カードが書き込み禁止になっていない。
- パーティションが連結されていない。
- カード上で初期化が実行中ではない。

ウェブインタフェースを使用した既存のパーティションの削除

既存のパーティションを削除するには、次の手順を実行します。
1. 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。
パーティションの管理 ページが表示されます。
2. **削除** 行で、削除するパーティションの削除アイコンをクリックします。
この処置を実行すると、パーティションが恒久的に削除されることを示すメッセージが表示されます。
3. **OK** をクリックします。
パーティションが削除されます。

RACADM を使用した既存のパーティションの削除

パーティションを削除するには、次の手順を実行します。
1. システムに対する 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。
パーティションのダウンロード ページが表示されます。
2. **ラベル** ドロップダウンメニューでダウンロードするパーティションを選択し、**ダウンロード** をクリックします。

メモ: すべての既存のパーティション（連結されたパーティションは除く）がリストに表示されます。最初のパーティションがデフォルトで選択されています。

3. ファイルの保存場所を指定します。
   選択したパーティションの内容が指定した場所にダウンロードされます。
   メモ: フォルダの場所が指定された場合に限り、パーティションラベルがファイル名として使用されます。また、CD およびハードディスクタイプのパーティションには **.iso** 拡張子、フロッピーおよびハードディスクタイプのパーティションんには **.img** 拡張子が使用されます。

パーティションからの起動

連結された vFlash パーティションを次回起動時の起動デバイスとして設定できます。

パーティションを起動する前に、次を確認してください。

- vFlash パーティションに、デバイスから起動するための起動可能なイメージ（**.img** 形式または **.iso** 形式）が含まれている。
- vFlash 機能が有効になっている。
- 仮想メディアへのアクセス 権限を持っている。

ウェブインタフェースを使用したパーティションからの起動

vFlash パーティションを最初の起動デバイスとして設定するには、「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. 322」を参照してください。

メモ: 連結された vFlash パーティションが **最初の起動デバイス** ドロップダウンメニューのリストに表示されていない場合は、BIOS が最新バージョンにアップデートされていることを確認します。

RACADM を使用したパーティションからの起動

最初の起動デバイスとして vFlash パーティションを設定するには、`iDRAC.ServerBoot` オブジェクトを使用します。

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

メモ: このコマンドを実行すると、vFlash パーティションラベルが 1 回限りの起動に自動的に設定されます（`iDRAC.ServerBoot.BootOnce` が `1` に設定されます）。1 回限りの起動では、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ありません。

25

SMCLP の使用

メモ: SMCLP は、4.00.00.00 より前のバージョンの iDRAC でのみサポートされています。

Server Management Command Line Protocol (SMCLP) 仕様は、CLI ベースのシステム管理を可能にします。SMCLP は標準文字単位のストリームを介して管理コマンドを送信するためのプロトコルを定義します。このプロトコルでは、人間指向型コマンドセットを使用して Common Information Model Object Manager (CIMOM) にアクセスします。SMCLP は、複数のプラットフォームにわたるシステム管理を合理化するための Distributed Management Task Force (DMTF) SMASH イニシアチブのサブコンポーネントです。SMCLP 仕様には、管理下エレメントアドレス指定仕様や、SMCLP マッピング仕様に対する多数のプロファイルとともに、さまざまな管理タスク実行のための標準動詞とターゲットについて記述されています。

メモ: ここでは、ユーザーに Systems Management Architecture for Server Hardware (SMASH) イニシアチブおよび Server Management Working Group (SMWG) SMCLP 仕様についての知識があることを前提としています。

SM-CLP は、複数のプラットフォームにわたるサーバ管理を合理化するための Distributed Management Task Force (DMTF) SMASH イニシアチブのサブコンポーネントです。SM-CLP 仕様は、管理下エレメントアドレス指定仕様や、SM-CLP マッピング仕様に対する多数のプロファイルとともに、さまざまな管理タスク実行のための標準バーブとターゲットについて説明しています。

SMCLP は iDRAC コントローラーのファームウェアからホストされ、SSH、およびシリアルベースのインターフェイスをサポートしています。iDRAC SMCLP インタフェースは、DMTF が提供する SMCLP 仕様バージョン 1.0 に基づいています。

メモ: プロファイル、拡張、MOF に関する情報は https://www.dell.com/support から、DMTF に関する全情報は **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

SSH インターフェイスを使用して SMCLP コマンドを実行することができます。SSH を開いて、管理者として iDRAC にログインします。SMCLP プロンプト (admin->) が表示されます。

SMCLP プロンプト：

- yx1x ブレード サーバーは-$を使用します。
- yx1x ラックおよびタワー サーバーは admin->を使用します。
- yx2x ブレード、ラック、およびタワー サーバーは admin->を使用します。

y は、M (ブレード サーバーの場合)、R (ラック サーバーの場合)、T (タワー サーバーの場合) などの英数字です。x は数字で、Dell PowerEdge サーバーの世代を示します。

メモ: -$を使用したスクリプトでは、これらを yx1x システムに使用できますが、yx2x システム以降は、ブレード、ラック、タワー サーバーに 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 62. SMCLP 動詞

動詞	定義
cd	シェルを使用して MAP を移動します
set	プロパティを特定の値に設定します
ヘルプ	特定のターゲットのヘルプを表示します
reset	ターゲットをリセットします
show	ターゲットのプロパティ、動詞、サブターゲットを表示します
start	ターゲットをオンにします
stop	ターゲットをシャットダウンします
exit	SMCLP シェルセッションを終了します
バージョン	ターゲットのバージョン属性を表示します
load	バイナリイメージを URL から指定されたターゲットアドレスに移動します

次の表は、ターゲットのリストが示されています。

表 63. SMCLP ターゲット

ターゲット	定義
admin1	管理ドメイン
admin1/profiles1	iDRAC 内の登録済みプロファイル
admin1/hdwr1	ハードウェア
admin1/system1	管理下システムターゲット
admin1/system1/capabilities1	管理下システム SMASH 収集機能

表 63. SMCLP ターゲット（続き）

ターゲット	定義
admin1/system1/capabilities1/elecap1	管理下システムターゲット機能
admin1/system1/logs1	レコードログ収集ターゲット
admin1/system1/logs1/log1	システムイベントログ（SEL）のレコードエントリ
admin1/system1/logs1/log1/record*	管理下システムの SEL レコードの個々のインスタンス
admin1/system1/settings1	管理下システム SMASH 収集機能
admin1/system1/capacities1	管理下システム機能 SMASH 収集
admin1/system1/consoles1	管理下システムコンソール SMASH 収集
admin1/system1/sp1	サービスプロセッサ
admin1/system1/sp1/timesvc1	サービスプロセッサ時間サービス
admin1/system1/sp1/capabilities1	サービスプロセッサ機能 SMASH 収集
admin1/system1/sp1/capabilities1/clpcap1	CLP サービス機能
admin1/system1/sp1/capabilities1/pwrmgtcap1	システムの電源状態管理サービス機能
admin1/system1/sp1/capabilities1/acctmgtcap*	アカウント管理サービス機能
admin1/system1/sp1/capabilities1/rolemgtcap*	ローカル役割ベースの管理機能
admin1/system1/sp1/capabilities1/elecap1	認証機能
admin1/system1/sp1/settings1	サービスプロセッサ設定収集
admin1/system1/sp1/settings1/clpsetting1	CLP サービス設定データ
admin1/system1/sp1/clpsvc1	CLP サービスプロトコルサービス
admin1/system1/sp1/clpsvc1/clpendpt*	CLP サービスプロトコルエンドポイント

表 63. SMCLP ターゲット（続き）

ターゲット	定義
admin1/system1/sp1/clpsvc1/tcpendpt*	CLP サービスプロトコル TCP　エンドポイント
admin1/system1/sp1/jobq1	CLP サービスプロトコルジョブキュー
admin1/system1/sp1/jobq1/job*	CLP サービスプロトコルジョブ
admin1/system1/sp1/pwrmgtsvc1	電源状態管理サービス
admin1/system1/sp1/account1-16	ローカルユーザーアカウント
admin1/sysetm1/sp1/account1-16/identity1	ローカルユーザー識別アカウント
admin1/sysetm1/sp1/account1-16/identity2	IPMI 識別（LAN）アカウント
admin1/sysetm1/sp1/account1-16/identity3	IPMI 識別（シリアル）アカウント
admin1/sysetm1/sp1/account1-16/identity4	CLP 識別アカウント
admin1/system1/sp1/acctsvc2	IPMI アカウント管理サービス
admin1/system1/sp1/acctsvc3	CLP アカウント管理サービス
admin1/system1/sp1/rolesvc1	ローカル役割ベース認証（RBA）サービス
admin1/system1/sp1/rolesvc1/Role1-16	ローカル役割
admin1/system1/sp1/rolesvc1/Role1-16/privilege1	ローカル役割権限
admin1/system1/sp1/rolesvc2	IPMI RBA サービス
admin1/system1/sp1/rolesvc2/Role1-3	IPMI 役割
admin1/system1/sp1/rolesvc2/Role4	IPMI シリアルオーバー LAN（SOL）役割
admin1/system1/sp1/rolesvc3	CLP RBA サービス
admin1/system1/sp1/rolesvc3/Role1-3	CLP 役割

表 63. SMCLP ターゲット（続き）

ターゲット	定義
admin1/system1/sp1/rolesvc3/Role1-3/privilege1	CLP 役割権限

MAP アドレス領域のナビゲーション

SM-CLP で管理できるオブジェクトは、Manageability Access Point（MAP）アドレス領域と呼ばれる階層領域に分類されたターゲットで表されます。アドレスパスは、アドレス領域のルートからアドレス領域のオブジェクトへのパスを指定します。

ルートターゲットは、スラッシュ（/）またはバックスラッシュ（\）で表されます。これは、iDRAC にログインするときのデフォルトの開始ポイントです。cd 動詞を使用してルートから移動します。

メモ: スラッシュ（/）およびバックスラッシュ（\）は、SM-CLP アドレスパスで互換性があります。ただし、コマンドラインの末尾にバックスラッシュを置くと、コマンドが次のラインまで続くことになり、コマンドの解析時に無視されます。

たとえば、システムイベントログ（SEL）で 3 番目のレコードに移動するには、次のコマンドを入力します。

```
->cd /admin1/system1/logs1/log1/record3
```

ターゲットなしで cd 動詞を入力し、アドレス領域内の現在の場所を検索します。省略形 .. と . の機能は Windows および Linux の場合と同様であり、.. は親レベルを示し、. は現在のレベルを示します。

show 動詞の使用

ターゲットの詳細を確認するには、show 動詞を使用します。この動詞は、ターゲットのプロパティ、サブターゲット、関連性、およびその場所で許可されている SM-CLP 動詞のリストを表示します。

-display オプションの使用

show -display オプションでは、コマンドの出力を 1 つ、または複数のプロパティ、ターゲット、アソシエーション、バーブに制限できます。たとえば、現在の場所のプロパティおよびターゲットのみを表示するには、次のコマンドを使用します。

```
show -display properties,targets
```

特定のプロパティのみを表示するには、次のコマンドのように修飾します。

```
show -d properties=(userid,name) /admin1/system1/sp1/account1
```

1 つのプロパティのみを表示する場合は、括弧を省略できます。

-level オプションの使用

show -level オプションは、指定されたターゲットよりも下の追加レベルで show を実行します。アドレス領域内のすべてのターゲットとプロパティを参照するには、-l all オプションを使用します。

-output オプションの使用

-output オプションは、4 つの SM-CLP 動詞出力フォーマット（**テキスト**、**clpcsv**、**キーワード**、**clpxml**）のうち、1 つを指定します。

デフォルトのフォーマットは **テキスト** であり、最も読みやすい出力です。**clpcsv** フォーマットは、スプレッドシートプログラムへのロードに適した、コンマ区切り値フォーマットです。**キーワード** 1 行につき 1 つのキーワード = 値のペアとして情報を出力します。**Clpxml** フォーマットは、**response** XML 要素を含む XML ドキュメントです。DMTF は、**clpcsbv** フォーマットと **clpxml** フォーマットを指定しています。これらの仕様は、DMTF ウェブサイト（**dmtf.org**）で確認できます。

次の例は、SEL の内容を XML で出力する方法を示しています。

```
show -l all -output format=clpxml /admin1/system1/logs1/log1
```

使用例

本項では、SMCLP の使用事例のシナリオについて説明します。

- サーバー電源管理 、p. 328
- SEL 管理 、p. 328
- MAP ターゲットナビゲーション 、p. 329

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
help
exit
version
```

- SEL レコードを表示する場合

  `show/system1/logs1/log1`

  次の出力が表示されます：

```
/system1/logs1/log1/record4
Properties:
LogCreationClassName= CIM_RecordLog
CreationClassName= CIM_LogRecord
LogName= IPMI SEL
RecordID= 1
MessageTimeStamp= 20050620100512.000000-000
Description= FAN 7 RPM: fan sensor, detected a failure
ElementName= IPMI SEL Record
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`

26

オペレーティングシステムの導入

管理下システムへのオペレーティングシステムの導入には、次のいずれかのユーティリティを使用できます。

- リモートファイル共有
- 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、次を確認してください。

- iDRAC に対する **設定ユーザー** および **仮想メディアへのアクセス** 権限が、そのユーザーに対して有効である。
- ネットワーク共有に、ドライバおよびオペレーティングシステムの起動可能イメージファイルが **.img** または **.iso** などの業界標準フォーマットで含まれている。

  メモ: イメージファイルの作成中、標準のネットワークベースのインストール手順に従います。展開イメージを読み取り専用としてマークして、各ターゲットシステムが確実に同じ展開手順から起動し、実行するようにします。

RFS を使用してオペレーティングシステムを導入するには、次の手順を実行します。

1. リモートファイル共有（RFS）を使用し、NFS、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、基本、またはダイジェストの各認証を使用する RFS はサポートされていません。認証は必要ありません。HTTPS では、基本認証はサポートされていません。ダイジェスト認証または認証なしが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** オプションを選択して、次のインスタンスについてのみ、管理下システムがイメージファイルを使って再起動するようにします。
5. **適用** をクリックします。
6. 管理下システムを再起動し、画面の指示に従って展開を完了します。

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 HTTP を使ってそれを CD または DVD としてマウントすることにより、管理下サーバのオペレーティングシステムから仮想ドライブとして使用できるようにすることができます。RFS はライセンスが必要な機能です。

メモ: HTTP または HTTPs 経由の RFS はサポートされていません。

リモートファイル共有では **.img** と **.iso** イメージファイル形式のみがサポートされます。**.img** ファイルは仮想フロッピーとしてリダイレクトされ、**.iso** ファイルは仮想 CDROM としてリダイレクトされます。

RFS のマウントを行うには、仮想メディアの権限が必要です。

RFS と仮想メディアの機能は相互排他的です。

- 仮想メディアクライアントがアクティブではない場合に、RFS 接続の確立を試行すると、接続が確立され、リモートイメージがホストのオペレーティングシステムで使用可能になります。
- 仮想メディアクライアントがアクティブである場合に RFS 接続の確立を試行すると、次のエラーメッセージが表示されます。

  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。接続されると、RFS マウントされた仮想ドライブは、iDRAC からログアウトしても切断されません。iDRAC がリセットされた場合、またはネットワーク接続が切断された場合は、RFS 接続が終了します。RFS 接続を終了させるには、CMC 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 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。iDRAC インタフェースは非ルートモードで実行するため、これらの許可が必要になります。
  - 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 **読み取りと実行** 特権に追加します。
- 管理下システムで ESXi が実行されていて、RFS を使用してフロッピーイメージ（**.img**）をマウントした場合、ESXi オペレーティングシステムでは連結されたフロッピーイメージを使用できません。
- 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。
- 仮想メディアが RFS を使用して接続されている場合、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 ウェブインタフェースで、**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。
   連結されたメディア ページが表示されます。
2. **連結されたメディア** の下で、**連結** または **自動連結** を選択します。
3. **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。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。

   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>`

   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。
   - 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

   メモ: ファイルパスには、「/」と「\」のどちらの文字も使用できます。

   CIFS は IPv4 と IPv6 の両方のアドレスをサポートしていますが、NFS は IPv4 アドレスのみをサポートします。

NFS 共有を使用する場合、大文字と小文字が区別されるため、<ファイルパス> と <イメージ名> を正確に入力するようにしてください。

メモ: ユーザー名およびパスワードの推奨文字に関する詳細は、「ユーザー名およびパスワードで推奨される文字 、p. 147」を参照してください。

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決定されます。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。

4. **適用** をクリックして、**接続** をクリックします。
   接続が確立された後、**接続ステータス** に **接続済み** と表示されます。

メモ: リモートファイル共有を設定した場合でも、セキュリティ上の理由から、ウェブインタフェースはユーザー資格情報を表示しません。

メモ: 画像パスにユーザー資格情報が含まれる場合は、HTTPS を使用して、GUI と RACADM に資格情報が表示されないようにします。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 での実行時における手動での mount コマンドの入力が必要な場合があります。コマンドの構文は、次のとおりです。

```
mount /dev/OS_specific_device / user_defined_mount_point
```

`user_defined_mount_point` は、他の mount コマンドの場合と同様に、マウント用に選択したディレクトリです。

RHEL の場合、CD デバイス (**.iso** 仮想デバイス) は `/dev/scd0` で、フロッピーデバイス (**.img** 仮想デバイス) は `/dev/sdc` です。

SLES の場合、CD デバイスは `/dev/sr0` で、フロッピーデバイスは /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、'(一重引用符)、"(二重引用符)、, (コンマ)、< (小なり記号)、> (大なり記号) は使用できません。

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。

- 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

仮想メディアを使用したオペレーティングシステムの導入

仮想メディアを使用してオペレーティングシステムを導入する前に、次を確認してください。

- 起動順序に仮想ドライブが表示されるように、仮想メディアが *連結* 状態になっている。
- 仮想メディアが *自動連結* モードの場合、システムを起動する前に仮想メディアアプリケーションを起動する必要がある。
- ネットワーク共有に、ドライバおよびオペレーティングシステムの起動可能イメージファイルが **.img** または **.iso** などの業界標準フォーマットで含まれている。

仮想メディアを使用してオペレーティングシステムを導入するには、次の手順を実行します。

1. 次のうちのいずれか 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連結します。
2. マップするために必要なイメージが保存されている管理ステーションのドライブを選択します。
3. 次のいずれか 1 つの方法を使用して、必要なデバイスから起動します。
   - iDRAC ウェブインタフェースを使用して、**仮想フロッピー** または **仮想 CD/DVD/ISO** から 1 回限りの起動を行うように起動順序を設定します。
   - 起動時に <F2> を押して、**セットアップユーティリティ** > **システム BIOS 設定** から起動順序を設定します
4. 管理下システムを再起動し、画面の指示に従って展開を完了します。

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の CD/DVD を挿入します。
3. CD/DVD ドライブを再マップします。

SD カードの内蔵オペレーティングシステムの導入

SD カード上の内蔵ハイパーバイザをインストールするには、次の手順を実行します。

1. システムの内蔵デュアル SD モジュール (IDSDM) スロットに 2 枚の SD カードを挿入します。
2. BIOS で SD モジュールと冗長性 (必要な場合) を有効にします。
3. 起動中に <F11> を押して、ドライブの 1 つで SD カードが使用可能かどうかを検証します。
4. 内蔵されたオペレーティングシステムを導入し、オペレーティングシステムのインストール手順に従います。

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 カードのどちらでもマスターにすることができます。たとえば、2 枚の新しい SD カードが IDSDM に装着されている場合、SD1 はアクティブ（マスター）カードであり、SD2 はスタンバイカードです。データは両方のカードに書き込まれますが、データの読み取りは SD1 から行われます。SD1 に障害が発生するか、取り外された場合は常に、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。

27

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
- サーバーステータス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 Web インターフェイスで、**メンテナンス** > **診断**の順に選択します。
   次のオプションがあります。
   - iDRAC をリセットするには、[**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 に再接続してログインします。
   - [**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。[**iDRAC をデフォルト設定にリセット**] をクリックすると、[**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. ユーザーおよびネットワーク設定を保持する。
b. すべての設定を破棄して、ユーザーを出荷時の値 (root/工場出荷時の値) にリセットします。
c. すべての設定を破棄してユーザー名とパスワードをリセットする。

2. 警告メッセージが表示されます。**OK** をクリックして続行します。

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、すぐに再起動するか、次回の再起動またはメンテナンス期間までステージングできます (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 コマンドを使用して、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クされます。TIME NA を指定すると、待機時間は適用されません。

診断テストの種類は次のとおりです。

- 拡張テスト
- エクスプレステスト
- 両方のテストを順に実行

再起動の種類は次のとおりです。

- 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に電源オフの信号を送り 10 分待機。オペレーティングシステムの電源が切れない場合、iDRAC が電源サイクルを実行)

スケジュール可能な診断ジョブ、または一度に実行可能なジョブは 1 つのみです。診断ジョブを実行すると、正常に完了、エラーで終了、または不成功、のいずれかになります。結果を含む診断イベントは Lifecycle Controller ログに記録されます。リモート RACADM、または WSMan を使用して最近実行した診断の結果を取得できます。

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は、ジョブをキャンセルするにはシステムを再起動します。

リモート診断を実行する前に次を確認します。

- Lifecycle Controller が有効化されている。
- ログインおよびサーバー制御権限がある。

RACADM を使用した自動リモート診断のスケジュール

- リモート診断を実行して、結果をローカルシステムに保存するには、次のコマンドを使用します。

```
racadm diagnostics run -m <Mode> -r <reboot type> -s <Start Time> -e <Expiration Time>
```

- 最後に実行されたリモート診断結果をエクスポートするには、次のコマンドを使用します。

```
racadm diagnostics export -f <file name> -l <NFS / CIFS / HTTP / HTTPs share> -u
<username> -p <password>
```

オプションの詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

Post コードの表示

Post コードは、システム BIOS からの進行状況インジケータであり、パワーオンリセットからの起動シーケンスのさまざまな段階を示します。また、システムの起動に関するすべてのエラーを診断することも可能になります。**Post 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直前の Post コードが表示されます。

Post コードを表示するには、**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。

メモ:

- 起動キャプチャおよびクラッシュキャプチャのビデオを再生するには、仮想コンソールへのアクセス権限または管理者権限が必要です。
- iDRAC GUI ビデオ プレ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ることがあります。iDRAC GUI ビデオ プレイヤーには iDRAC タイム ゾーンの時刻が表示され、その他のビデオ 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。

メモ: DVC ブート キャプチャ ファイルはビデオではありません。これらは、サーバー起動中に取得される（特定の解像度の）一連の画面です。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じ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、キャプチャ時と同程度の解像度でエクスポートする必要があります。

メモ: ブート 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、ホストの起動後はブート キャプチャ バ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。

メモ: 内蔵ビデオ コントローラーが無効になっていて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
- 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およびタワーサーバの LCD 前面パネルステータスを表示するには、iDRAC ウェブインタフェースで、**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 (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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』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ェイルセーフモードです。
- 橙色の点滅 — 管理下システムでエラーが発生しています。

システムが正常に動作していると（LED 前面パネルの青色の正常性アイコンで示されます）、**エラーを非表示にする** および **エラーを再表示する** の両方がグレー表示されます。ラックサーバおよびタワーサーバ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、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』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には次のものがあります。

- 電源が入らない
- ファンのノイズ
- ネットワーク接続の喪失
- ハードディスクドライブの不具合
- USB メディアエラー
- 物理的損傷

問題に基づいて、次の方法で問題を修正します。

- モジュールまたはコンポーネントを装着し直して、システムを再起動
- ブレードサーバーの場合は、モジュールをシャーシ内の異なるベイに挿入
- ハードディスクドライブまたは USB フラッシュドライブを交換
- 電源およびネットワークケーブルを再接続 / 交換

問題が解決しない場合は、https://www.dell.com/poweredgemanuals から入手可能な『*設置およびサービス マニュアル*』でハードウェアデバイスに関する特定のトラブルシューティングを参照してください。

注意: 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 インターフェイ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 行目にエラーおよび警告メッセージが表示されます。LCD パネルに表示されるエラーメッセージのリストについては、サーバ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、https://www.dell.com/cmcmanuals から入手可能な『*Chassis Management Controller RACADM CLI ガイド*』を参照してください。詳細については、https://www.dell.com/openmanagemanuals から入手可能な『*PowerEdge MX7000 シャーシ向け OME - Modular RACADM CLI ガイド*』を参照してください。

システムおよびユーザーデータの消去

メモ: 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
- デフォルトへの BIOS リセット
- デフォルトへの iDRAC リセット

システム消去を実行する前に、以下を確認します。

- iDRAC サーバー制御権限がある。
- Lifecycle Controller が有効化されている。

Lifecycle Controller のデータ オプションでは、LC ログ、設定データベース、ロールバックのファームウェア、工場出荷時のログ、FP SPI (または管理ライザ) からの設定情報などのコンテンツが削除されます。

メモ: Lifecycle Controller ログには、システム消去の要求に関する情報と、iDRAC の再起動時に生成された情報が含まれます。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

メモ: サーバー上で SEKM が有効にされている場合は、このコマンドを使用する前に `racadm sekm disable` コマンドを使用して SEKM を無効にします。このコマンドを実行して iDRAC から SEKM 設定が消去された場合、iDRAC によって保護されているストレージ デバイスがロック アウトされるのを防ぐことができます。

詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』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

iDRAC ウェブインタフェースを使用して iDRAC を工場出荷時のデフォルト設定にリセットするには、次の手順を実行します。

1. **Maintenance (メンテナンス)** > **Diagnostics (診断)** と移動します。
   診断コンソール ページが表示されます。
2. **iDRAC をデフォルト設定にリセット** をクリックします。
   完了状態はパーセントで表示されます。iDRAC が再起動し、工場出荷時のデフォルト設定に復元されます。iDRAC IP はリセットされ、アクセスできなくなります。IP は前面パネルまたは BIOS を使用して設定できます。

iDRAC 設定ユーティリティを使用した iDRAC の工場出荷時デフォルト設定へのリセット

iDRAC 設定ユーティリティを使用して iDRAC を工場出荷時のデフォルト値にリセットするには、次の手順を実行します。

1. **iDRAC 設定のデフォルトへのリセット** に移動します。
   iDRAC 設定のデフォルトへのリセット ページが表示されます。
2. **Yes** (はい) をクリックします。
   iDRAC のリセットが開始されます。
3. **戻る** をクリックして、同じ **iDRAC 設定のデフォルトへのリセット** ページに移動し、リセットの成功を示すメッセージを確認します。

28

iDRAC への SupportAssist の統合

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ン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*、姓*、電話番号*、代替番号、および E メール 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。

セカンダリ連絡先情報

名、姓、電話番号、代替番号、電子メールアドレスを入力し、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 ワークフローを有効にするには、SupportAssist 登録プロセス中に**ディスパッチ情報**を入力する必要があります。ディスパッチ パーツ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 サポート付きパーツ ディスパッチ**] を選択します。

メモ: 自動ディスパッチは、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パ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**、**送信ステータス**、**および**、および **送信の日付と時刻** 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。

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す。

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、またはサーバオペレーティングシステムや 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。
- コレクションには、詳細なシステム情報がユーザーにとってわかりやすい形式で大量に記録されています。この情報は、コレクションをテクニカルサポートサイトにアップロードしなくても表示できます。

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。

データ収集が実行されるたびに、イベントが Lifecycle Controller ログに記録されます。イベントには、レポートを開始したユーザー、使用されたインタフェース、エクスポートの日時などの情報が含まれます。

Windows の場合、WMI が無効になると、OS Collector は収集を停止し、エラーメッセージが表示されます。

適切な権限レベルを確認し、レジストリやソフトウェアのデータの収集を妨げているファイアウォールまたはセキュリティ設定がないようにします。

正常性レポートを生成する前に、次を確認します。

- Lifecycle Controller が有効化されている。
- Collect System Inventory On Reboot （ CSIOR ）が有効になっている。
- ログインおよびサーバー制御権限がある。

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. コレクションに含め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ー定義の CIFS または NFS 共有場所に保存されます。

      メモ: *Save to Network (ネットワークを保存する)* 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)（エンドユーザレベル契約 (EULA)）**に同意して続行します。
   以下の場合、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。登録されている場合は、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、ユーザー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。

登録すると、デルにデータを送信するときに、Collection Settings（コレクションの設定）に識別情報を含めることができます。

手動操作を避け、システムの定期的なチェックを維持するために、**Automatic Collection（自動収集）**オプションを有効にしてスケジュールできます。SupportAssist はデフォルトで、イベントがトリガされ、サポートケースが開始されると、自動的にアラートを生成したデバイスからシステムログを収集し、それをデルにアップロードするように設定されています。イベントに基づいて自動収集を有効または無効にできます。自動収集は、ユーザーの要件に基づいてスケジュールできます。使用可能なオプションには、週次、月次、四半期、またはしないがあります。スケジュールされた定期的なイベントの日付と時刻を設定することもできます。自動収集を設定するときに、**ProSupport Plus Recommendation Report（ProSupport Plus の推奨事項のレポート）**を有効または無効にできます。

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。

29

よくあるお問い合わせ（FAQ）

本項では、次に関するよくあるお問い合わせをリストします。

- システムイベントログ
- ネットワークセキュリティ
- Active Directory
- シングルサインオン
- スマートカードログイン
- 仮想コンソール
- 仮想メディア
- vFlash SD カード
- SNMP 認証
- ストレージデバイス
- iDRAC サービスモジュール
- RACADM
- その他

トピック：

- システムイベントログ
- 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
- 仮想メディア
- vFlash SD カード
- SNMP 認証
- ストレージデバイス
- GPU（アクセラレーター）
- 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トラネット上にある場合は、**ローカルイントラネット** を選択し、**レベルのカスタマイズ...** をクリックします。

2. **セキュリティ設定** ウィンドウの **ダウンロード** で、次のオプションが有効になっていることを確認します。
   - ファイルのダウンロード時に自動的にダイアログを表示（このオプションを使用できる場合）
   - ファイルのダウンロード

   注意: iDRAC へのアクセスに使用されるコンピュータの安全性を確実にするため、その他 で アプリケーションと安全でないファイルの起動 オプションは有効にしないでください。

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。

iDRAC には、Web ベースのインターフェイスおよびリモート RACADM を介してアクセスする際にネットワーク セキュリティを確保するためのデフォルトの iDRAC サーバー証明書が含まれています。この証明書は、信頼できる CA によって発行されません。これを解決するには、信頼できる CA によって発行された iDRAC サーバー証明書 (Microsoft 認証局、Thawte、Verisign など) をアップロードします。

DNS サーバーが iDRAC を登録しないのはどうしてですか?

一部の DNS サーバーは、最大 31 文字の iDRAC 名しか登録しません。

iDRAC Web ベース インターフェイスにアクセスすると、SSL 証明書のホスト名が iDRAC ホスト名と一致しないことを示すセキュリティ警告が表示されます。

iDRAC には、Web ベースのインターフェイスおよびリモート RACADM を介してアクセスする際にネットワーク セキュリティを確保するためのデフォルトの iDRAC サーバー証明書が含まれています。この証明書を使用すると、iDRAC に発行されたデフォルト証明書が iDRAC ホスト名 (たとえば、IP アドレス) と一致しないため、Web ブラウザーにセキュリティ警告が表示されます。

これを解決するには、IP アドレスまたは iDRAC ホスト名に発行された iDRAC サーバー証明書をアップロードします。CSR (証明書の発行に使用) を生成する場合、証明書の発行に使用された CSR のコモン ネーム (CN) と iDRAC IP アドレス (証明書が IP に対して発行された場合) または登録済み DNS iDRAC 名 (証明書が iDRAC 登録名に対して発行された場合) を一致させます。

CSR が DNS iDRAC の登録名と一致することを確実にするには、次の手順を実行します。

1. iDRAC Web インターフェイスで、**[概要]** > **[iDRAC 設定]** > **[ネットワーク]** と移動します。**ネットワーク** ページが表示されます。
2. **共通設定** セクションで次の手順を実行します。
   - **iDRAC の DNS への登録** オプションを選択します
   - **DNS iDRAC 名** フィールドに iDRAC 名を入力します。
3. **適用** をクリックします。

Web ブラウザーから iDRAC にアクセスできないのはなぜですか ?

この問題は、HTTP Strict Transport Security (HSTS) が有効になっていると発生することがあります。HSTS は、HTTP ではなく、セキュアな HTTPS プロトコルのみを使用して Web ブラウザー間でのやり取りを可能にする Web セキュリティ機構です。

ブラウザーで HTTPS を有効にし、iDRAC にログインして問題を解決します。

リモート CIFS 共有を含む操作を完了できないのはなぜですか ?

CIFS 共有を使用しているその他のリモート ファイル共有のインポート/エクスポート操作は、SMBv1 のみを使用している場合に失敗します。SMB/CIFS 共有を提供するサーバーで SMBv2 プロトコルが有効になっていることを確認します。SMBv2 プロトコルを有効にする方法については、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。

テレメトリー ストリーミング

Rsyslog サーバーのテレメトリー レポートのストリーミングで一部のレポート データが欠落しています。

古いバージョンの rsyslog サーバーでは、一部のレポートにおいて、断続的にレポート データの若干の欠落が生じる場合があります。新バージョンへのアップグレードをすることでこの問題を回避できます。

Active Directory

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、適切なユーザードメイン名を使用します。ローカル iDRAC ユーザーアカウントが設定されている場合は、ローカル資格情報を使用して iDRAC にログインします。ログイン後は、次を確認します。
  - **Active Directory 設定と管理** ページで **Active Directory 有効** オプションが選択されている。
  - **iDRAC ネットワーク設定** ページで DNS が正しく設定されている。
  - 証明書の検証が有効の場合、正しい Active Directory のルート CA 証明書が iDRAC にアップロードされている。
  - 拡張スキーマを使用している場合、iDRAC 名および iDRAC ドメイン名が Active Directory の環境設定に一致する。
  - 標準スキーマを使用している場合、グループ名とグループドメイン名が Active Directory 設定に一致する。
  - ユーザーと iDRAC オブジェクトが別のドメイン内にある場合は、**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な場合、iDRAC はディレクトリサーバとの 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、次の質問をご覧ください。FQDN を使用している場合は、ドメインではなく、ドメインコントローラの FQDN を使用していることを確認します。たとえば、**example.com** ではなく、**servername.example.com** を使用します。

IP アドレスをドメインコントローラアドレスとして使用しても証明書の検証に失敗します。どのように解決すればよいですか?

ドメインコントローラ証明書の サブジェクト名 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実行します。

- サーバー証明書のサブジェクトまたはサブジェクト代替名と一致するように、iDRAC でドメインコントローラのホスト名 (FQDN) をドメインコントローラアドレスとして設定します。
- iDRAC で設定された IP アドレスと一致する IP アドレスをサブジェクトフィールドまたはサブジェクト代替名フィールドで使用するようにサーバー証明書を再発行します。
- SSL ハンドシェイク中の証明書の検証なしでドメインコントローラを信頼することを選択した場合は、証明書の検証を無効にします。

複数ドメイン環境で拡張スキーマを使用している場合は、ドメインコントローラアドレスをどのように設定しますか?

このアドレスは、iDRAC オブジェクトが属するドメイン用のドメインコントローラのホスト名 (FQDN) または IP アドレスである必要があります。

グローバルカタログアドレスを設定するのはいつですか?

標準スキーマを使用しており、ユーザーおよび役割グループが異なるドメインに属する場合は、グローバルカタログアドレスが必要です。この場合、ユニバーサルグループのみを使用できます。

標準スキーマを使用し、すべてのユーザーおよび役割グループが同じドメインに属する場合は、グローバルカタログアドレスは必要はありません。

拡張スキーマを使用している場合、グローバルカタログアドレスは使用されません。

標準スキーマクエリの仕組みを教えてください。

iDRAC は、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に LDAP 接続を行います。安全ではない接続で LDAP バインドを実行することはありません。

iDRAC で、証明書の検証がデフォルトで有効になっているのはなぜですか?

iDRAC は、iDRAC が接続するドメインコントローラの ID を保護するために強力なセキュリティを施行します。証明書の検証なしでは、ハッカーがドメインコントローラを偽造し、SSL 接続を乗っ取ることが可能になります。証明書の検証を行わずにセキュリティ境界内のすべてのドメインコントローラを信頼することを選択する場合、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のログインにかかる時間は 10 秒未満ですが、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 にログインしようとすると、Active Directory のシングルサインオンログインが失敗します。

これは、誤ったグループタイプが原因です。Active Directory サーバには 2 種類のグループタイプがあります。

- セキュリティ — セキュリティグループでは、ユーザーとコンピュータによる共有リソースへのアクセスの管理や、グループポリシー設定のフィルタが可能です。
- 配布 — 配布グループは、電子メール配布リストとして使用することだけを目的としたものです。

グループタイプは、常にセキュリティにするようにしてください。配布グループはグループポリシー設定のフィルタに使用しますが、オブジェクトへの許可の割り当てに使用することはできません。

シングルサインオン

Windows Server 2008 R2 x64 で SSO ログインが失敗します。これを解決するには、どのような設定が必要ですか?

1. ドメインコントローラとドメインポリシーに対して **technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** を実行します。
2. DES-CBC-MD5 暗号スイートを使用するようにコンピュータを設定します。

   これらの設定は、クライアントコンピュータ、またはお使いの環境内のサービスとアプリケーションとの互換性に影響を与える場合があります。Kerberos ポリシー設定に許可される暗号化タイプは、**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、古いキータブを `klist purge` コマンドで削除します。
5. GPO を更新したら、新しいキータブを作成します。
6. キータブを iDRAC にアップロードします。

これで、SSO を使用して iDRAC にログインできます。

Windows 7 と Windows Server 2008 R2 の Active Directory ユーザーで SSO ログインが失敗するのはなぜですか?

Windows 7 と Windows Server 2008 R2 の暗号化タイプを有効にする必要があります。暗号化タイプの有効化には、次の手順を実行します。

1. システム管理者としてログインするか、管理者権限を持つユーザーとしてログインします。
2. **Start (スタート)** から **ggpedit.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。

3. **Local Computer Settings（ローカルコンピュータ設定）** > **Windows Settings（Windows 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）** と移動します。
4. **ネットワークセキュリティ：kerberos に許可される暗号化方式の設定** を右クリックして、**プロパティ** を選択します。
5. すべてのオプションを有効にします。
6. **OK** をクリックします。これで、SSO を使用して iDRAC にログインできます。

拡張スキーマでは、次の追加設定を行います。

1. **Local Group Policy Editor（ローカルグループポリシーエディタ）** ウィンドウで、**Local Computer Settings（ローカルコンピュータ設定）** > **Windows Settings（Windows 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）** と移動します。
2. **ネットワークセキュリティ：NTLM の制限：リモートサーバーへの発信 NTLM トラフィック** を右クリックして **プロパティ** を選択します。
3. **すべて許可** を選択し、**OK** をクリックしてから、**ローカルグループポリシーエディタ** ウィンドウを閉じます。
4. **Start（スタート）** から cmd を実行します。コマンドプロンプトウィンドウが表示されます。
5. `gpupdate /force` コマンドを実行します。グループポリシーがアップデートされます。コマンドプロンプトウィンドウを閉じます。
6. **Start（スタート）** から regedit を実行します。**レジストリエディタ** ウィンドウが表示されます。
7. **HKEY_LOCAL_MACHINE** > **System（システム）** > **CurrentControlSet** > **Control（制御）** > **LSA** と移動します。
8. 右ペインで、**New（新規）** > **DWORD (32-bit) Value（DWORD（32 ビット）値）** を右クリックして選択します。
9. 新しいキーを **SuppressExtendedProtection** と名付けます。
10. **SuppressExtendedProtection** を右クリックして、**変更** をクリックします。
11. **値データ** フィールドに **1** を入力して **OK** をクリックします。
12. **Registry Editor（レジストリ エディタ）** ウィンドウを閉じます。これで、SSO を使用して iDRAC にログインできます。

iDRAC 用に SSO を有効にし、Internet Explorer を使って iDRAC にログインすると、SSO が失敗し、ユーザー名とパスワードの入力を求められます。どのように解決すればよいですか?

iDRAC の IP アドレスが **Tools（ツール）** > **Internet Options（インターネットオプション）** > **Security（セキュリティ）** > **Trusted sites（信頼済みサイト）** のリストに表示されていることを確認してください。リストに表示されていない場合は、SSO が失敗し、ユーザー名とパスワードの入力を求められます。**キャンセル** をクリックして、先に進んでください。

スマートカードログイン

Active Directory スマートカードログインを使用して iDRAC にログインするには最大 4 分かかります。

通常の Active Directory スマートカードの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）** ページで優先 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 サーバがダウンしている場合は、DNS タイムアウトが発生します。iDRAC は、代替 DNS を使用してユーザーをログインします。

ActiveX プラグインがスマートカードリーダーを検出しません。

スマートカードが Microsoft Windows オペレーティングシステムでサポートされていることを確認します。Windows は、限られた数のスマートカード暗号化サービスプロバイダ（CSP）しかサポートしません。

一般的に、スマートカード CSP が特定のクライアントに存在するかどうかを確認するには、Windows のログオン（Ctrl-Alt-Del）画面でスマートカードをリーダーに挿入して、Windows がスマートカードを検出し、PIN ダイアログボックスを表示するかどうかをチェックします。

間違ったスマートカード PIN です。

間違った PIN での試行回数が多すぎたためにスマートカードがロックされていないかをチェックします。このような場合は、組織のスマートカード発行者に問い合わせて、新しいスマートカードを取得してください。

仮想コンソール

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 Web インターフェイスからログアウトしても、仮想コンソール セッションがアクティブです。これは正常な動作ですか?

はい。仮想コンソールビューアウィンドウを閉じて、対応するセッションからログアウトしてください。

サーバー上のローカルビデオがオフになっている場合に、新しいリモートコンソールビデオセッションを開始できますか?

はい。

ローカルビデオをオフにするように要求してからサーバー上のローカルビデオがオフになるまで 15 秒もかかるのはなぜですか?

ビデオがオフに切り替わる前に、ローカルユーザーが必要に応じて別の操作を実行できるように配慮されています。

ローカルビデオをオンにする場合に、遅延時間は発生しますか?

いいえ。ローカルビデオをオンにする要求を iDRAC が受信すると、ビデオはすぐにオンになります。

ローカルユーザーもビデオをオフにしたり、オンしたりできますか?

ローカルコンソールを無効にすると、ローカルユーザーがビデオをオフにしたり、オンにしたりすることはできません。

ローカルビデオをオフに切り替えると、ローカルキーボードとマウスもオフになりますか?

番号

ローカルコンソールをオフにすると、リモートコンソールセッションのビデオはオフになりますか?

いいえ。ローカルビデオのオン / オフを切り替えても、リモートコンソールセッションには影響しません。

iDRAC ユーザーがローカルサーバービデオをオン / オフにするために必要な権限は何ですか?

iDRAC 設定権限を持っているすべてのユーザーが、ローカルコンソールをオンにしたり、オフにしたりできます。

ローカルサーバービデオの現在のステータスは、どのように取得しますか?

ステータスは、仮想コンソールページに表示されます。

`iDRAC.VirtualConsole.AttachState` オブジェクトのステータスを表示するには、次のコマンドを使用します。

```
racadm get idrac.virtualconsole.attachstate
```

または、SSH またはリモート 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。無効の場合には、黄色の丸が表示され、iDRAC によってローカルコンソールがロックされていることが示されます。

システム画面の一番下が仮想コンソールウィンドウに表示されないのはなぜですか?

管理ステーションのモニターの解像度が 1280 x 1024 に設定されていることを確認してください。

Linux オペレーティングシステムで仮想コンソールビューアウィンドウが文字化けするのはなぜですか?

Linux でコンソールビューアを使用するには、UTF-8 文字セットが必要です。お使いのロケールを確認し、必要に応じて文字セットを再設定します。

Lifecycle Controller の Linux テキスト コンソールでマウスが同期しないのはなぜですか ?

仮想コンソールでは USB マウスドライバが必要ですが、USB マウスドライバは X-Window オペレーティングシステムでのみ使用できます。仮想コンソールビューアで、次のいずれかの手順を実行します。

- **ツール** > **セッションオプション** > **マウス** タブに移動します。**マウス アクセラレーション**で **Linux** を選択します。
- **ツール**メニューで**シングル カーソル**オプションを選択します。

仮想コンソールビューアウィンドウでマウスポインタを同期させるには、どうすればよいですか?

仮想コンソールセッションを開始する前に、オペレーティングシステムに対して正しいマウスが選択されていることを確認します。

iDRAC 仮想コンソール クライアントで、iDRAC 仮想コンソール メニューの**ツール**にある**シングル カーソル**オプションが選択されていることを確認します。デフォルトは、2 カーソルモードです。

仮想コンソールから Microsoft オペレーティングシステムをリモートでインストールしている間に、キーボードまたはマウスを使用できますか?

番号 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必ず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 インジケータがリモートサーバーの Num Lock インジケータのステータスを反映しないのはなぜですか?

iDRAC からアクセスした場合、管理ステーションの Num Lock インジケータが、リモートサーバの Num Lock の状態と一致しないことがあります。Num Lock の状態は、管理ステーションの Num Lock の状態に関わらず、リモートセッション接続時のリモートサーバの設定に依存します。

ローカルホストから仮想コンソールセッションを確立すると、複数のセッションビューアウィンドウが表示されるのはなぜですか?

ローカルシステムから仮想コンソールセッションを設定しています。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?

番号ローカルユーザーがシステムにアクセスすると、双方がシステムを制御することになります。

仮想コンソールセッションの実行に必要な帯域幅はどのくらいですか?

良好なパフォーマンスを得るために、5 MBPS の接続をお勧めします。最低限のパフォーマンスのためには、1 MBPS の接続が必要です。

管理ステーションで仮想コンソールを実行するために最低限必要なシステム要件は何ですか?

管理ステーションには、Intel Pentium III 500 MHz プロセッサと最低限 256 MB の RAM が必要です。

仮想コンソールビューアウィンドウに信号無しメッセージが表示されることがあるのはなぜですか?

このメッセージが表示される理由としては、iDRAC 仮想コンソールプラグインがリモートサーバ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の電源がオフになっている場合に発生します。場合によっては、リモートサーバのデスクトップビデオ受信の誤作動が原因でこのメッセージが表示されることもあります。

仮想コンソールビューアウィンドウに範囲外メッセージが表示されることがあるのはなぜですか?

このメッセージが表示される理由として、ビデオのキャプチャに必要なパラメータが、iDRAC によるビデオキャプチャ可能な範囲を超えていることが考えられます。画面解像度とリフレッシュレートなどのパラメータの値が高すぎると、範囲外の状態になります。通常は、ビデオメモリの容量や帯域幅などの物理的制限によってパラメータの最大範囲が設定されます。

iDRAC Web インターフェイスから仮想コンソール セッションを開始すると、ActiveX セキュリティ ポップアップが表示されるのはなぜですか ?

iDRAC が信頼済みサイトリストに含まれていない可能性があります。仮想コンソールセッションを開始するたびにセキュリティポップアップが表示されないようにするには、クライアントブラウザで iDRAC を信頼済みサイトリストに追加します。

1. **ツール** > **インターネット オプション** > **セキュリティ** > **信頼済みサイト**の順にクリックします。
2. **サイト** をクリックして iDRAC の IP アドレスまたは DNS 名を入力します。
3. **追加**をクリックします。
4. **レベルのカスタマイズ**をクリックします。
5. **セキュリティ設定** ウィンドウの **署名なしの ActiveX Controls のダウンロード** で **プロンプト** を選択します。

仮想コンソールビューアウィンドウに何も表示されないのはなぜですか?

仮想コンソール権限ではなく、仮想メディア権限を持っている場合、ビューアを起動して仮想メディア機能にアクセスすることはできますが、管理下サーバーのコンソールは表示されません。

仮想コンソールを使用しているときに DOS でマウスが同期しないのはなぜですか?

Dell BIOS は、マウスドライバを PS/2 マウスとしてエミュレートします。設計上、PS/2 マウスはマウスポインタに相対位置を使用するので、同期に遅れが生じます。iDRAC には USB マウスドライバが装備されているので、絶対位置とマウスポインタの緻密な追跡が可能です。iDRAC が USB マウスの絶対位置を Dell BIOS に渡したとしても、BIOS エミュレーションによって絶対位置が相対位置に変換されるため、この遅れが残ってしまいます。この問題を解決するには、設定画面でマウスモードを USC/Diags に設定します。

仮想コンソールを起動すると、仮想コンソールではマウスカーソルがアクティブになりますが、ローカルシステムではアクティブになりません。この原因と解決方法を教えてください。

この問題は、**マウス モード**が **USC/Diags** に設定されていると発生します。ローカルシステムでは、**Alt + M** ホットキーを押してマウスを使用します。仮想コンソールでは、**Alt + M** ホットキーを再度押してマウスを使用します。

CMC から起動された iDRAC インターフェイスから仮想コンソールを起動した後、GUI セッションがタイムアウトするのはなぜですか ?

CMC Web インターフェイスから iDRAC への仮想コンソールを起動すると、仮想コンソールを起動するためのポップアップが開きます。このポップアップは、仮想コンソールが開いてしばらくすると閉じます。

管理ステーション上で GUI と仮想コンソールの両方を同じ iDRAC システムに起動した場合、ポップアップが閉じる前に GUI が起動されると、iDRAC GUI のセッションタイムアウトが発生します。仮想コンソールのポップアップが閉じた後で、CMC Web インターフェイスから iDRAC GUI を起動すると、この問題は発生しません。

メモ: MX プラットフォームには該当しません。

Linux SysRq キーが Internet Explorer で機能しないのはなぜですか?

Internet Explorer から仮想コンソールを使用する際には、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 端末でこの機能を有効にできます。

```
echo 1 > /proc/sys/kernel/sysrq
```

2. Active X ビューアのキーボードパススルーモードを有効にします。
3. **Ctrl + Alt + Print Screen** を押します。
4. **Print Screen** のみを放します。
5. **Print Screen+Ctrl+Alt** を押します。

メモ: Internet Explorer および Java では、SysRq 機能は現在サポートされていません。

仮想コンソールの下部に「リンクが切断されました」メッセージが表示されるのはなぜですか?

サーバの再起動中に共有ネットワークポートを使用すると、BIOS がネットワークカードをリセットしている間に 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。

iDRAC ファームウェアをアップデートした後に、Java プラグインを用いた仮想コンソールの起動が失敗します。

Java のキャッシュを削除してから、仮想コンソールを起動します。

Web サーバー ポート (443) を使用してコンソール リダイレクトを有効にする方法

```
racadm>>set iDRAC.VirtualConsole.WebRedirect Enabled
```

外部仮想コンソール ポート (5900) を閉じるには、次の iDRAC プロパティを設定します。

外部仮想コンソールポート (5900) を閉じるには、 `iDRAC.VirtualConsole.WebRedirect` と `iDRAC.VirtualConsole.CloseUnusedPort` の両方を有効にする必要があります。

```
racadm>>set iDRAC.VirtualConsole.CloseUnusedPort Enabled
```

メモ:

- 仮想メディアポートが無効になっている場合、スタンドアロン仮想メディアにアクセスできなくなりますが、仮想コンソールを使用すると仮想メディアを使用できます。
- CloseUnusedPort ポートが有効になっている場合、Java、ActiveX ベースの仮想コンソールおよび仮想メディアは専用の外部ポートが必要となるため、機能しません。HTML5 プラグインを使用した仮想コンソールおよび仮想メディアは、iDRAC Web サーバー ポート (443) 上で機能します。

仮想メディア

仮想メディアクライアントの接続が切断することがあるのはなぜですか?

ネットワークのタイムアウトが発生すると、iDRAC ファームウェアはサーバーと仮想ドライブ間の接続をドロップし、接続を中断します。

クライアントシステムで CD を変更すると、新しい CD には自動起動の機能が付いている場合があります。その場合、クライアントシステムが CD を読み取るのに時間がかかりすぎると、ファームウェアがタイムアウトして接続が失われる可能性があります。接続が失われた場合は、GUI から再接続して、その前の操作を続行します。

仮想メディアの設定を iDRAC Web インターフェイスまたはローカル RACADM コマンドを使用して変更した場合、設定変更の適用時に接続しているすべてのメディアが切断されます。

仮想ドライブを再接続するには、仮想メディアの **クライアントビュー** ウィンドウを使用します。

仮想メディアからの Windows オペレーティングシステムのインストールに長時間かかるのはなぜですか?

『*Dell Systems Management Tools and Documentation*』DVD を使用して Windows オペレーティング システムをインストールする場合、ネットワーク接続の速度が遅いと、ネットワーク遅延が原因で iDRAC Web インターフェイスへのアクセスに通常以上に時間がかかることがあります。インストール ウィンドウにインストールの進行状況は表示されません。

仮想デバイスを起動可能なデバイスとして設定するにはどうすればよいですか?

管理対象システムで BIOS セットアップにアクセスして、起動メニューに移動します。仮想 CD、仮想フロッピー、または vFlash 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、仮想デバイスを起動可能にするには、CMOS セットアップのブート シーケンスで「スペースバー」キーを押します。たとえば、CD ドライブから起動する場合、起動順序の最初のデバイスとして CD ドライブを設定します。

起動可能なデバイスとして設定できるメディアのタイプは?

iDRAC では、次の起動可能なメディアから起動できます。

- CDROM/DVD データメディア
- ISO 9660 イメージ
- 1.44 フロッピーディスクまたはフロッピーイメージ
- オペレーティングシステムがリムーバブルディスクとして認識する USB キー
- USB キーイメージ

USB キーを起動可能なデバイスにするにはどうすればよいですか?

Windows 98 の起動ディスクを使用して起動し、起動ディスクから USB キーにシステム ファイルをコピーすることもできます。たとえば、DOS プロンプトで次のコマンドを入力します。

```
sys a: x: /s
```

ここで x: は起動可能なデバイスとして設定する必要のある USB キーです。

仮想メディアを連結し、リモート フロッピーに接続済みです。しかし、Red Hat Enterprise Linux または SUSE Linux オペレーティング システムを実行しているシステムでは、仮想フロッピー/仮想 CD デバイスを検出できません。この問題を解決するにはどうすればよいですか?

Linux のバージョンによっては、同じ方法を用いても仮想フロッピー ドライブや仮想 CD ドライブが自動マウントされない場合があります。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。次の手順に従って、仮想フロッピー ドライブをマウントします。

1. Linux コマンドプロンプトを開き、次のコマンドを実行します。

   ```
   grep "Virtual Floppy" /var/log/messages
   ```

2. そのメッセージの最後のエントリを確認し、その時刻を書きとめます。
3. Linux のプロンプトで次のコマンドを実行します。

   ```
   grep "hh:mm:ss" /var/log/messages
   ```

   ここで hh:mm:ss は、手順 1 で grep から返されたメッセージのタイムスタンプです。
4. 手順 3 で、grep コマンドの結果を読み、仮想フロッピーに与えられたデバイス名を確認します。
5. 仮想フロッピードライブに連結済みであり、接続されていることを確認します。
6. Linux のプロンプトで次のコマンドを実行します。

   ```
   mount /dev/sdx /mnt/floppy
   ```

   ここで/dev/sdx は手順 4 で確認したデバイス名、/mnt/floppy はマウント ポイントです。

仮想 CD ドライブをマウントするには、Linux が仮想 CD ドライブに割り当てるデバイス ノードを確認します。次の手順に従って、仮想 CD ドライブをマウントします。

1. Linux コマンドプロンプトを開き、次のコマンドを実行します。

   ```
   grep "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
```

ここで/dev/sdx は手順 4 で確認したデバイス名、/mnt/floppy はマウント ポイントです。

iDRAC Web インターフェイスを使用してリモート ファームウェア アップデートを実行した後に、サーバーに連結されていた仮想ドライブが削除されるのはなぜですか？

ファームウェアをアップデートすると、iDRAC がリセットされ、リモート接続は切断され、仮想ドライブはアンマウントされます。iDRAC のリセットが完了すると、再度ドライブが表示さるようになります。

USB デバイスの接続後にすべての USB デバイスの接続が解除されるのはなぜですか?

仮想メディア デバイスと vFlash デバイスは、複合 USB デバイスとしてホスト USB バスに接続され、共通の USB ポートを共有します。仮想メディアまたは vFlash USB デバイスのどれか 1 つでもホスト USB バスに接続されるか、または接続を切断されると、すべての仮想メディアおよび vFlash デバイスがホスト USB バスから一瞬切断され、再度接続されます。ホストのオペレーティング システムが仮想メディア デバイスを使用している場合は、1 つ以上の仮想メディアまたは vFlash デバイスの連結や切り離しを行わないでください。使用する前に、必要な USB デバイスをすべて接続しておく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 Event Collector 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**の順に移動します。**Windows Event Collector** を右クリックして、**停止**をクリックします。

フロッピードライブまたは USB の内容の表示中、仮想メディアを介して同じドライブが連結されると、接続エラーメッセージが表示されます。

仮想フロッピー ドライブに同時にアクセスすることはできません。ドライブの内容を表示しているアプリケーションを閉じてから、ドライブを仮想化してください。

仮想フロッピードライブでサポートされているファイルシステムのタイプは?

仮想フロッピードライブは、FAT16 または FAT32 ファイルシステムをサポートしています。

現在仮想メディアを使用していなくても、仮想メディアを介して DVD/USB に接続しようとするとエラーメッセージが表示されるのはなぜですか?

リモート ファイル共有 (RFS) 機能も使用している場合は、エラー メッセージが表示されます。一度に使用できるのは RFS と仮想メディアのどちらかです。両方は同時に使用できません。

***接続ステータス*が iDRAC に *接続*と表示されていても、仮想メディアにアクセスできません。**

iDRAC で**連結モード**が**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とすると、接続ステータスが**接続**として表示されることがあります。仮想メディアにアクセスするには、**連結モード**を**自動連結**または**連結**のいずれかに変更します。

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 コミュニティの要求のみを受け入れるからです。

SNMP 認証エラーが生成されないようにするには、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 検出セットアップに同じ get コミュニティ名と set コミュニティ名を使用する必要があります。

ストレージデバイス

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 の背後にある外部の JBOD/洞察については、SAS コネクター/IOM の削除のための EEMI メッセージは EEMI メッセージ ID ENC42 で生成されます。ただし、SAS コネクター/IOM の復元のための EEMI メッセージ ENC41 は生成されません。

iDRAC Web インターフェイスで 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。
3. **詳細なプロパティ** で、**冗長パス**の値が**存在**に設定されていることを確認し、IOM 復元が確認されます。

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 をチーミングに追加すると、その構成は無効になります。その結果、iSM は iDRAC と正しく通信できなくなります。

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 Service Module をインストールまたは実行する前に、iDRAC Service Module の Server Administrator の機能を停止してください。

ホストオペレーティングシステムに iDRAC サービスモジュールがインストールされていることを確認する方法を教えてください。

iDRAC サービスモジュールがインストールされているかどうかを確認するには、次の手順を実行します。

- Windows を実行しているシステムの場合：

  コントロール パネル を開いて、表示されるインストール済みプログラムのリストに、iDRAC サービスモジュールがあるかどうかを確認します。

- Linux を実行しているシステムの場合

  コマンド `rpm –qi dcism` を実行します。iDRAC Service Module がインストールされている場合は、ステータスが [**インストール済み**] となります。

- ESXi を実行しているシステムの場合、ホストでコマンド `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。

システムにインストールされている iDRAC サービスモジュールのバージョン番号を確認する方法を教えてください。

iDRAC サービスモジュールのバージョンを確認するには、次の手順のいずれかを実行します。

- **[スタート]** > **[コントロール パネル]** > **[プログラムと機能]** の順にクリックします。インストールされている iDRAC 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。
- に移動します **マイコンピュータ** > **プログラムのアンインストールと変更**.

iDRAC サービス モジュールをインストールするために必要な最低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 Service Module のバージョン 2.0 以前のバージョンでは、iDRAC Service Module のインストール中に、サポートされているサーバではないことを示すエラーメッセージが表示されます。対応サーバーの詳細については、ユーザー ガイドを参照してください。このエラーの解決方法を教えてください。

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ても、OS のログに次のメッセージが表示されます。なぜですか?

iDRAC サービスモジュールは、OS to iDRAC パススルーチャネルを使用して、iDRAC と通信できません

iDRAC Service Module は、OS to iDRAC パススルー機能を使用して、USB NIC 経由で iDRAC との通信を確立します。正しい IP エンドポイントを使用して USB NIC インタフェースが設定されていても、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 64. ルーティング順序の例

送信先	ゲートウェイ	Genmask	フラグ	メトリック	参照	使用インタフェース
デフォルト	10.94.148.1	0.0.0.0	UG	1024	0	0 em1
10.94.148.0	0.0.0.0	255.255.255.0	U	0	0	0 em1
link-local	0.0.0.0	255.255.255.0	U	0	0	0 em1
link-local	0.0.0.0	255.255.255.0	U	0	0	0 enp0s20u12u3

この例では、**enp0s20u12u3** が USB NIC インタフェースであり、リンクローカル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。

- 一意の宛先マスクで iDRAC USBNIC アドレスを変更します。
- ルーティングテーブルから不要なエントリを削除して、ホストが iDRAC USB NIC IPv4 アドレスと通信する際には USB NIC が経路で選択されるようにします。

iDRAC Service Module のバージョン 2.0 またはそれ以前のバージョンでは、VMware ESXi サーバから iDRAC Service Module をアンインストールするときに、vSphere クライアントで仮想スイッチが vSwitchiDRACvusb、ポートグループが iDRAC ネットワークと命名されます。これらを削除する方法を教えてください。

VMware ESXi サーバに iDRAC Service Module VIB をインストールすると、iDRAC Service Module は仮想スイッチとポートグループを作成し、OS to iDRAC パススルーを介して USB NIC モードで iDRAC と通信できるようにします。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：`esxcfg-vmknic -d -p "iDRAC Network"`
  - vSwitch を削除する場合：`esxcfg-vswitch -d vSwitchiDRACvusb`

  メモ: サーバーの機能に問題があるわけではないので、VMware ESXi サーバーに iDRAC サービスモジュールを再インストールすることができます。

複製された Lifecycle ログはオペレーティングシステムのどこにありますか?

複製された Lifecycle ログを表示するには、次の手順を実行します。

表 65. Lifecycle ログの場所

オペレーティングシステム	場所
Microsoft Windows	**イベントビューア** > **Windows ログ** > **システム**.iDRAC サービスモジュールのすべての Lifecycle ログは、**iDRAC Service Module** というソース名の下で複製されます。 **メモ:** iSM バージョン 2.1 以降では、Lifecycle Controller ログのソース名の下に Lifecycle ログが複製されます。iSM バージョン 2.0 およびそれ以前のバージョンでは、ログは iDRAC Service Module のソース名の下に複製されます。 **メモ:** Lifecycle ログの場所は、iDRAC Service Module インストーラを使用して設定できます。iDRAC Service Module のインストール中またはインストーラの変更中に場所を設定できます。
Red Hat Enterprise Linux、SUSE Linux、CentOS、および Citrix XenServer	`/var/log/messages`
VMware ESXi	`/var/log/syslog.log`

Linux のインストール中に、インストールに使用できる Linux 依存パッケージまたは実行可能プログラムとは何ですか?

Linux 依存パッケージのリストを表示するには、https://www.dell.com/idracmanuals から入手可能な『*iDRAC サービス モジュール ユーザーズ ガイド*』で「*Linux 依存性*」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

[プロセッサーの設定] 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

RACADM

iDRAC をリセット (racadm racreset コマンドを使用) した後にコマンドを発行すると、次のメッセージが表示されます。これは何を示していますか?

```
ERROR: Unable to connect to RAC at specified IP address
```

このメッセージは、別のコマンドを発行する前に、iDRAC のリセットの完了を待つ必要があることを示しています。

RACADM コマンドおよびサブコマンドを使用する場合、明瞭ではないエラーがいくつかあります。

RACADM コマンドを使用するとき、次のようなエラーが 1 つ、または複数発生することがあります。

- ローカル RACADM エラーメッセージ — 構文、入力ミス、名前の誤りなどの問題。
- リモート RACADM エラーメッセージ — IP アドレスの誤り、ユーザー名の誤り、パスワードの誤りなどの問題。

iDRAC に対する Ping テスト中、ネットワークモードが専用モードと共有モードの間で切り替えられた場合、Ping に対する応答がありません。

システムの ARP テーブルをクリアしてください。

リモート RACADM が SUSE Linux Enterprise Server (SLES) 11 SP1 から iDRAC への接続に失敗します。

openssl および libopenssl の公式バージョンがインストールされていることを確認します。次のコマンドを実行して、RPM パッケージをインストールします。

```
rpm -ivh --force < filename >
```

`filename` は openssl または libopenssl rpm パッケージファイルです。

例えば次のようになります。

```
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。
- `racresetcfg` コマンドが使用された。
- iDRAC がリセットされた。
- 新しい SSL サーバー証明書がアップロードされた。

ローカル RACADM を使用してパーティションを作成した後にこのパーティションを削除しようとするとエラーメッセージが表示されるのはなぜですか?

これは、パーティションの作成操作が進行中であるために発生します。ただし、しばらくするとパーティションが削除され、パーティションが削除されたことを示すメッセージが表示されます。それ以外の場合は、パーティションの作成操作が完了するのを待ってから、パーティションを削除します。

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すことはできません。

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。

iDRAC のリセット後に、一部の値が iDRAC GUI に表示されないことがあります。

メモ: iDRAC を何らかの理由でリセットした場合、iDRAC のリセットから 2 分以上経過したことを確認してから、iDRAC の設定へのアクセスや設定変更を行ってください。

OS をインストールすると、ホスト名が自動的に表示 / 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、ホスト名を反映される必要があります。
- 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。

ブレードサーバの iDRAC IP アドレスを検索するには、どうすればよいですか?

メモ: Chassis Management Controller（CMC）オプションは、ブ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、https://www.dell.com/cmcmanuals から入手可能な『*Chassis Management Controller RACADM CLI ガイド*』を参照してください。

  iDRAC RACADM コマンドの詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』を参照してください。

- **ローカル RACADM を使用する場合**

  `racadm getsysinfo` コマンドを使用します。次に例を示します。

```
$ racadm getniccfg -m server-1
DHCP Enabled = 1
IP Address    = 192.168.0.1
Subnet Mask   = 255.255.255.0
Gateway       = 192.168.0.1
```

- **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。コンピュータスレッドを選択すると、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**：https://www.dell.com/openmanagemanuals から入手可能な『*Dell EMC OpenManage Mobile ユーザーズ ガイド*』を参照してください。
- **シリアル接続を使用する**
- **LCD を使用する**：メイン メニューでサーバーをハイライト表示してチェック ボタンを押し、必要なサーバーを選択してチェック ボタンを押します。

ブレードサーバーに関連する CMC IP アドレスはどのように検索すればよいですか?

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。

```
$ racadm getniccfg -m chassis
NIC Enabled         = 1
DHCP Enabled        = 1
Static IP Address   = 192.168.0.120
Static Subnet Mask  = 255.255.255.0
Static Gateway      = 192.168.0.1
Current IP Address  = 10.35.155.151
Current Subnet Mask = 255.255.255.0
Current Gateway     = 10.35.155.1
Speed               = Autonegotiate
Duplex              = Autonegotiate
```

  メモ: リモート RACADM を使用してこの操作を実行することもできます。

  CMC RACADM コマンドの詳細については、https://www.dell.com/cmcmanuals から入手可能な『*Chassis Management Controller RACADM CLI ガイド*』を参照してください。

  iDRAC RACADM コマンドの詳細については、https://www.dell.com/idracmanuals から入手可能な『*iDRAC RACADM CLI ガイド*』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、**モジュラーエンクロージャ** > **システム/サーバモジュール** > **メインシステムシャーシ/メインシステム** > **リモートアクセス** 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 を有効にする前に、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、プリブート状態では iDRAC の共有 LOM IP にアクセスできません。

ブレードサーバーをシャーシに挿入して電源スイッチを押しましたが、電源がオンになりません。

- iDRAC では、サーバーの電源がオンになる前の初期化に最大 2 分かかります。
- CMC 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過した可能性があります。

iDRAC の管理者ユーザー名とパスワードを取得するには、どうすればよいですか?

iDRAC をデフォルト設定に復元する必要があります。詳細については、次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. 342

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 インターフェイスにログインし、**[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。

ブレードサーバーの起動中に iDRAC が応答しません。

サーバーを取り外し、挿入し直してください。

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 インターフェイスを確認して、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. 85 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 ブラウザーを使用して 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 ブラウザー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

メモ: SLES では、iDRAC インターフェイスを DHCP に設定します。

Ubuntu では、Netplan ユーティリティーを使用して 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。

図 5. Ubuntu での iDRAC インターフェイスの DHCP モードへの設定

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。

30

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
- 正常な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
- ラック密度の管理
- 新しい電子ライセンスのインストール
- 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

アクセスできない管理下システムのトラブルシューティング

OpenManage Essentials、デルの管理コンソール、またはローカルのトラップコレクタからアラートを受け取った後、データセンター内の 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ります。原因を識別してトラブルシューティングを行い、iDRAC を使用してサーバを再稼働します。

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次を確認し、システムへの接続を再確立します。

メモ: iDRAC ウェブインタフェースにアクセスできない場合は、サーバーに移動して LCD パネルにアクセスし、IP アドレスまたはホスト名を記録してから、管理ステーションの iDRAC ウェブインタフェースを使用して次の操作を実行します。

- サーバーの LED ステータス — 橙色に点滅または点灯。
- 前面パネル LCD ステータスまたはエラーメッセージ — 橙色の LCD またはエラーメッセージ。
- 仮想コンソールにオペレーティングシステムイメージが表示されます。イメージが表示されていれば、システムをリセット（ウォームブート）して、再度ログインします。ログインできる場合、問題は解決されています。
- 前回のクラッシュ画面。
- 起動キャプチャのビデオ。
- クラッシュキャプチャのビデオ。
- サーバー正常性ステータス — 問題のあるシステム部品の赤い x アイコン。
- ストレージアレイステータス — オフラインまたは故障の可能性のあるアレイ
- システムハードウェアおよびファームウェアに関連する重要なイベントの Lifecycle ログ、およびシステムクラッシュ時に記録されたログエントリ。
- テクニカルサポートレポートの生成および収集したデータの表示。
- iDRAC サービスモジュールによって提供される監視機能の使用

システム情報の取得とシステム正常性の評価

システム情報を取得し、システムの正常性を評価するには次の手順を実行します。

- iDRAC ウェブインタフェースで、**Overview（概要）** > **Summary（サマリ）** と移動してシステム情報を表示し、ページのさまざまなリンクにアクセスしてシステムの正常性を評価します。たとえば、シャーシファンの正常性を確認できます。
- シャーシロケータ LED を設定して、色に基づいてシステムの正常性を評価することも可能です。
- iDRAC サービスモジュールが取り付けられている場合は、オペレーティングシステムのホスト情報が表示されます。

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 ログログおよびシステムイベントログ（SEL）を表示およびエクスポートするには、次の手順を実行します。

1. iDRAC ウェブインタフェースで、**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。

   メモ: SEL は Lifecycle ログにも記録されます。フィルタオプションを使用して SEL を表示します。

2. SEL または Lifecycle ログは、XML フォーマットで外部の場所（管理ステーション、USB、ネットワーク共有など）にエクスポートします。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_）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 プラットフォームにのみ該当）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 ユーザーの設定
- 汎用 LDAP ユーザーの設定

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ア 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、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。